**SKILL**

**"IT NETWORK SYSTEM ADMINISTRATION"**

**TEST PROJECT**

**MODULE C:**

**CONFIGURING NETWORKING EQUIPMENT**

**Developed by WSR experts:**

**Dobrynin S.I.**

**Date: 29.06.18**

**Version: 8.3**

## **INTRODUCTION**

Network technologies knowledge is became 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 serve network infrastructure for any multi-branch enterprise.

## **DESCRIPTION OF PROJECT AND TASKS**

This test project was developed using different networking technologies, that are included in the corresponding tracks of CCNA R&S, CCNA Security and CCNP R&S certifications. Tasks are broken down into following configuration sections:

* Basic сonfiguration
* Switching configuration
* WAN configuration
* ROUTING CONFIGURATION
* Services configuration
* Security configuration
* Monitoring and backup configuration
* VPN configuration
* VoIP configuration

All sections are independent but all together they build very complex network infrastructure. Some tasks are pretty simple and straight, some 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 or L2TP, and so on. It is important to understand that if you are cannot come up with any 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 on top as long as functional testing is successful.

## **INSTRUCTIONS TO THE COMPETITOR**

**First and foremost, you should read the entire test project and develop a work plan.** You will have to reconfigure a working network infrastructure of a company, that consists of a main office HQ and two remote offices BR1 and BR2. Offices are connected through two providers named ISP1 and ISP2. You do not have acccess to the providers' equipment, it is fully configured and does not require any additional configuration. You will need to configure the company equipment, namely: SW1, SW2, HQSW1, HQSW2, HQ1, ASA, BR1 and BR2. **You do not have console access to the devices, so be very careful when performing the tasks!** If you loose connection to the equipment, it will be your own fault. You are allowed to reboot your devices, for example: if you have applied an incorrect ACL, that has disabled your telnet connection, but you didn't yet save the configuration.

Remember the saying: **Measure thrice, and cut once.** To perform your tasks you are provided with one physical host, that you may use as either PC1, PC2, PC3 or PC4 by connecting it to the respective devices according to the L1 topology.

Bring your attention that not all tasks are written in chronological order. Some sections may require configuration from other sections below them. For example, task 3 in “Services configuration” section asks you to configure dynamic host configuration protocol which is obviously will not work before you apply all necessary configuration from the “Switching configuration” section that comes right after. This is your responsibility to divide your time and choose what have to be done first and what’s next.

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 so may go back afterwards and fix things that are not working properly if you still have time. In addition, we recommend you to check all your previous work when you complete following modules.

Make sure that all your configurations are still working after equipment reboot.

## **CONNECTING TO DEVICES**

For the first time connection use Telnet protocol. To connect to Cisco ASA use the login: cisco and password: cisco, to enter privileged mode use password cisco To connect to all other devices use password: cisco and the privileged mode password: cisco.

In order to connect to the devices in the HQ, connect your workstation to the port f0/10 of swtich SW2 and configure the address according to the L3 topology diagram. The devices will be available at following addresses:

SW1 – 172.16.10.10

SW2 – 172.16.10.20

HQSW1 – 172.16.10.1

HQSW2 – 172.16.10.2

HQ1 – 172.16.10.100

ASA – 172.16.10.200

In order to connect to the devices in the remote office BR1, connect your workstation to the port GigabitEthernet0 on router BR1. BR1 is available at 192.168.1.1.

In order to connect to the devices in the remote office BR2, connect your workstation to the port GigabitEthernet0 on router BR2. BR2 is available at 192.168.2.1.

## **ASSESSMENT**

The assessment of the test project will be performed automatically. The assessment module will be connected to the port F0/11 of switch SW2, so ensure that the port is configured correctly.

**Important!** Ensure the remote console connection is working from port F0/11 to ALL of the company networking devices, including BR1 and BR2, because if there is no remote access to any of the devices, those devices will not be assessed.

**Basic сonfiguration**

1. Configure hostnames for all devices as you see on the topology
2. Configure domain name wsr2018.com for all network devices on the topology
3. Create user wsr2018 with password cisco on all devices
   1. Only hash of the password should be stored in configuration.
   2. User should have maximum privileges.
4. Configure new AAA model for all devices.
   1. Remote console (vty) authentication should use local username database.
   2. After successful authentication on vty line users should automatically land in privileged mode (except for the ASA firewall).
   3. Enable login authentication on local console.
   4. After successful authentication on local console the user should automatically land in privileged mode with maximal privileges.
   5. After successful authentication on local console of BR2 router the user should automatically land in mode with minimal privileges.
5. Configure RADIUS authentication for all remote consoles (vty) on HQ1 router.
6. Authentication sequence:
   * 1. RADIUS server
     2. Local username database
7. Use “cisco” as the shared key.
8. Use 1812 and 1813 as port numbers for authentication and accounting respectively.
9. IP address of the RADIUS server is 172.16.0.10
10. Configure automatic authorization after successful authentication.
11. Test RADIUS authentication on router HQ1 using radius/cisco credentials.
12. Configure wsr as a privileged mode password for all devices.
    1. Password should be stored in configuration in plain text.
    2. Configure privileged mode authorization on the ASA firewall using user password (without username prompt).
    3. Set the mode where all the passwords in the configuration are stored as a cipher text.
13. ALL devices should be accessible using SSH protocol version 2.

**Switching configuration**

1. Add port f0/0/21 of switch HQSW1 to VLAN 300.
2. Move ports f0/10 and f0/11 of switch SW2 from VLAN100 to VLAN300.
3. To use centralized VLAN configuration in the company switching network use VTP protocol version 3.
   1. Configure HQSW1 as the VTP server.
   2. Use wsr2018.ru as the domain name.
   3. All other swiches must be in client mode.
   4. The VLAN table must be as follows:
4. VLAN100 named MGT.
5. VLAN200 named DATA.
6. VLAN300 named OFFICE.
7. VLAN400 named VOIP.
8. Use IEEE 802.1q trunking protocol mode between all the switches.
9. Trunks between switches HQSW1 and HQSW2 and also between SW1 and SW2 should be configured without negotiation. Disable trunking negotiation explicitly.
10. Trunks between HQSW1 and SW1, SW2, and also between HQSW2 and SW1, SW2 should use dynamic trunking negotiation, where HQSW1 and HQSW2 should initiate trunk creation, while SW1 and SW2 should wait for trunk negotiation, but do not initiate it themselves.
11. Configure link aggregation between switches.
12. Use following port-channel numbers:

1 – between switches HQSW1 (f0/0/6-7) and SW1 (f0/6-7);

2 – between switches HQSW2 (f0/0/6-7) and SW2 (f0/6-7);

3 – between switches HQSW1 (f0/0/1-2) and HQSW2 (f0/0/1-2);

1. The aggregated channel between HQSW1 and SW1 must be organized using LACP as the negotiation protocol. HQSW1 must be configured as active, SW1 must be configured as passive.
2. The aggregated channel between HQSW2 and SW2 must be organized using PAgP as the negotiation protocol. HQSW2 must be configured as desirable, SW2 must be configured as auto.
3. The aggregated channel between HQSW1 and HQSW2 must be configured without any negotiation protocols.
4. Configure spanning tree protocol:
5. HQSW1 switch must be the root of the spanning tree in all VLANs, and if HQSW1 fails, HQSW2 must become the root.
6. Configure all used ports on HQSW1 and HQSW2, so that in all VLANs only HQSW1 and HQSW2 could become root bridges, and if a BPDU with a higher root priority is received on a port, that port should change its state to root-inconsistent.
7. You must have no more than two instances of spanning tree for the whole switching network to use as few resources as possible.
8. Configure port f0/0/21 on the HQSW1 switch, so when it is plugged in, it immediately transitions to forwarding state without waiting for the spanning tree to recalculate. Upon receiving a BPDU, this port must transition to the error-disabled state.
9. Configure IEEE 802.1AB protocol, so that the reception of service messages would be possible on all ports of HQSW1 and HQSW2, but sending is only allowed between these two devices.

**WAN configuration**

1. Configure a PPPoE connection between ISP1 and HQ1 router.
   * 1. Configure the PPPoE client on HQ1.
     2. Use username cisco and password cisco.
     3. The authentication is one-way using CHAP protocol and PPPoE password, only ISP1 checks the username and password.
     4. HQ1 should automatically receive an address from ISP1.
2. The ISP1 provider is using L2TP protocol to connect BR1 office.
3. Configure BR1 as L2TP client.
   * 1. Use 10.1.1.1 as the L2TP server address.
     2. Configure VirtualPPP with number 100.
     3. BR1 should automatically receive an address from ISP1.
     4. MTU 1450
4. Configure Frame Relay connection from HQ1 to ISP2.
   * 1. Use Cisco proprietary incapsulation for Frame Relay.
     2. Use DLCI 102.
5. Configure the connection from BR2 to ISP2 provider using PPP protocol.
   * 1. Configure Multilink PPP.
     2. Use the authentication protocol, that does not send the password in clear text. Username PPPASA and password PPP.
     3. BR2 should automatically receive an address from ISP2.
6. Configure a GRE tunnel to connect from BR2 to ISP1. Use tunnel interface number 10. Use transport addresses according to the L3 diagram.
7. ASA is connected to ISP1 and ISP2 providers using IPoE and has static addresses.

**ROUTING CONFIGURATION**

1. In HQ office, configure OSPF dynamic routing on HQSW1, HQSW2, HQ1 and ASA.
   1. Enable routing updates authentication according to the Routing diagram.
   2. Use area 0
   3. HQSW1 and HQSW2 should establish adjacency only on 172.16.0.0/30 network.
   4. In the DMVPN network HQ must be the DR.
   5. Disable sending routing updates on all interfaces that should not form neighbor relationships.
2. Configure OSPF routing between BR1 and BR2 offices and HQ main office.
   1. Enable routing updates authentication according to the Routing diagram.
   2. Adjacency between the offices (HQ, BR1 and BR2) should be established through secure DMVPN network.
   3. Use area 1 in BR1 office.
   4. Use area 2 in BR2 office.
   5. On HQ1 configure routing, so that BR1 and BR2 offices receive only routes to networks 172.16.0.8/30 and 192.168.3.0/24.
   6. Disable sending routing updates on all interfaces that should not form neighbor relationships.
3. ISP1 is providing a PA (Provider Aggregatable) subnet (11.11.11.11/32) to office BR1. On BR1 router configure EIGRP routing protocol using autonomous system number 2018.
   1. Enable routing updates authentication according to the Routing diagram.
   2. Use key-chain algorithm with WSR key.
   3. Disable sending routing updates on all interfaces that should not form neighbor relationships.
   4. ISP1 service provider is performing route redistribution of the route 11.11.11.11/32 into BGP, so make sure you are correctly announcing this route to the service provider.
4. HQ and BR2 offices have PI (Provider Independent) subnets and autonomous systems 65000 and 65020 respectively. Configure BGP routing protocol on the routers according to the table

|  |  |
| --- | --- |
| Device | AS |
| HQ1 | 65000 |
| ASA | 65000 |
| ISP1 | 65001 |
| ISP2 | 65002 |
| BR2 | 65020 |

* 1. Configure autonomous systems according to the Routing diagram.
  2. HQ1 router and ASA should have iBGP neighbor relationship.
  3. Enable routing updates authentication according to the Routing diagram.
  4. On HQ1 and ASA configure route redistribution for networks 10.10.10.10/32, 20.20.20.20/32 and 30.30.30.0/27 from OSPF to BGP, and also redistribute the default route from BGP to OSPF.
  5. BR2 should not receive all BGP routes, but only the default routes from ISP1 and ISP2.
  6. Configure outbound traffic balancing on BR2, so that the channel through ISP1 is preferred.
  7. Configure inbound traffic balancing on BR2, so that the channel through ISP1 is preferred.

1. Configure OSPFv3 routing protocol over DMVPN network. On HQ1, BR2, BR3 routers and HQSW1, HQSW2 switches configure OSPFv3 routing using process number 1.
   1. Enable routing updates authentication according to the Routing diagram.
   2. HQ1 router must become DR in the DMVPN network.
   3. Use area 0.

**Services configuration**

1. SRV1 is the source server for time synchronization in the network. Configure HQ1 router as NTP client. All other networking devices should use HQ1 as the time server.
   1. Configure YEKT time zone, with UTC difference +5 hours.
   2. Configure network synchronization server. Use stratum 2.
   3. Use MD5 authentication with WSR key.
2. On HQ1 router configure dynamic port address translation (PAT) for OFFICE subnet to the loopback address 1.1.1.1.
3. Configure first-hop redundancy protocol on HQSW1 and HQSW2 switches
4. Configure VRRP group for OFFICE subnet
5. Group number 20
6. Use 192.168.3.254 as the virtual IP address
7. Configure priority 100 for HQSW1 switch and 110 for HQSW2 switch.
8. Configure authentication using password vrrp
9. Configure DHCP using following parameters:
10. On HQ1 router for OFFICE subnet:
11. network address — 192.168.3.0/24
12. default gateway — virtual IP address of VRRP group
13. IP address of the TFTP server is 172.16.0.10
14. Configure DHCP-relay on HQSW1 and HQSW2.
15. Configure certification authority on HQ1 router:
16. Include FQDN of HQ1 router into issued certificates.
17. Use automatic enrollment
18. On routers HQ1, BR1, BR2 and ASA firewall make a request for a certificate to router HQ1. Do not use revocation check.

**Security configuration**

1. Create users with restricted permissions on BR2 router.
   1. Create user user1 and user2 with password cisco.
   2. User1 should be able to execute all user-mode commands and also be able to reboot the router and delete the startup config.
   3. Create a view-context "sh\_view" and assign it to user.
2. Show version command
3. Include all commands show ip \*
4. Include who command
   1. Create view-context ping\_view. Include in it
5. Ping command
6. Include traceroute command
   1. Create superview-context that combines these 2 contexts. User2 should land in this context after successful authentication on local or remote console.
   2. Make sure that users cannot issue any other commands within privileges and contexts that are assigned to them.
7. On port Fa0/10 of SW1 switch enable and configure port-security using following parameters:
8. Maximum MAC addresses — 2
9. MAC addresses should be automatically saved in running configuration.
10. In case of policy violation, security message should be displayed on the console; port should not go to err-disabled state.
11. Turn on DHCP snooping on SW1 switch for OFFICE subnet. Use internal flash to keep DHCP-snooping database.
12. Turn on dynamic ARP inspection on SW1 for OFFICE subnet. Create access control list that permits static IP address 192.168.3.10.
13. Configure Zone-based policy firewall (ZBF) on router BR2.
    1. Configure following zones:
       1. Zone named ISP1 for interface G0/0/0.
       2. Zone named ISP2 for interface Multilink 1.
       3. Zone named LOCAL for interface G0.
       4. Zone named DMVPN for interface Tunnel1.
    2. Use subnet 192.168.2.0/24 for the LOCAL zone.
    3. Deny traffic between ISP1 and ISP2 zones.
    4. Allow only following services from zone LOCAL to zones ISP1 and ISP2: HTTPS, SSH, DNS. Allow SSH in reverse direction.
    5. Allow only following services from zone LOCAL to zone DMVPN: HTTPS, FTP, TELNET, SSH, DNS, ICMP. Allow SSH and ICMP in reverse direction.
    6. Using ZBF allow the following services on BR2: NTP, SNMP, BGP, DMVPN, OSPF, OSPFv3. All other traffic should be blocked.

**Monitoring and backup configuration**

1. Configure logging of system messages on HQ1 router and ASA firewall to SRV1 server, including the informational messages.
2. Configure remote monitoring using SNMP v3 on HQ1 router and ASA firewall.
   1. Set location as YEKT, Russia
   2. Configure system contact [admin@wsr.ru](mailto:admin@hitech.ru)
   3. Use WSR as the group name.
   4. Create a read-only profile named RO.
   5. Use the mode that will provide most security.
   6. Use username: snmpuser and password: snmppass
3. Configure configuration backup on HQ1 router:
   1. Backup copy of running configuration should be automatically saved on SRV1 server using TFTP each time configuration is saved (copied to startup);
   2. Use following naming convention for backup files: <hostname>-<time>.cfg

**VPN configuration**

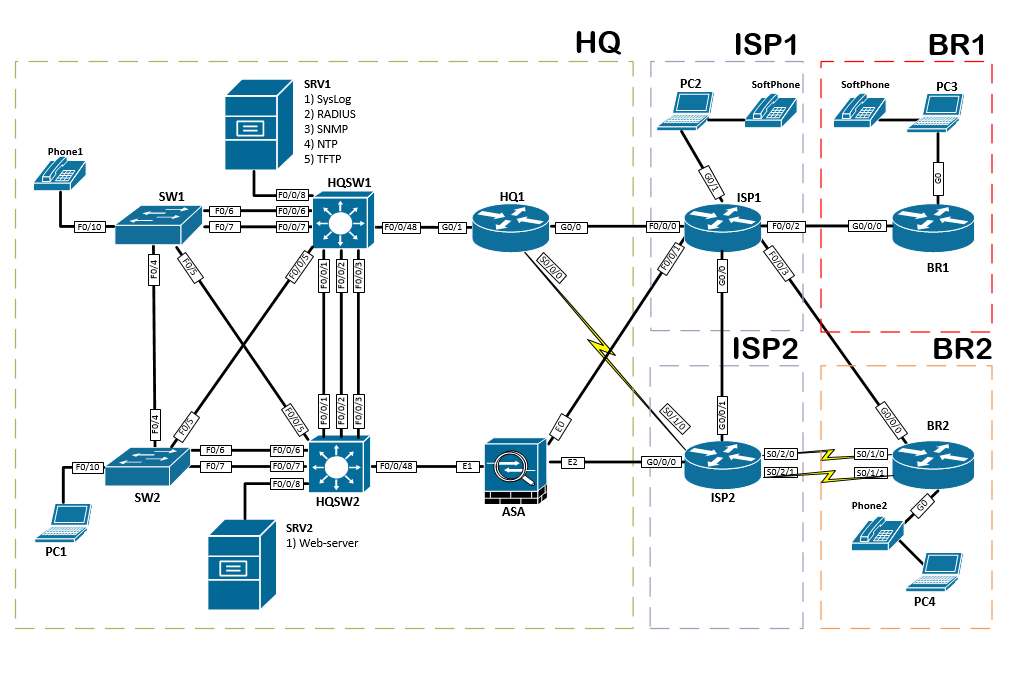
1. Configure DMVPN on HQ1, BR1 and BR2 routers:
2. Use Tunnel1 as VTI;
3. Configure MTU 1400 on all VTIs;
4. Configure IP addressing according to the VPN-diagram;
5. Use GRE Multipoint mode;
6. Use Loopback interface as tunnel source interface on each router according to the VPN-diagram;
7. NHRP configuration:
8. Tunnel ID — 100
9. NHRP authentication password - WSR2018
10. Use HQ1 router as DMVPN hub NHS server;
11. The DMVPN tunnels should be protected by IPsec.
12. Phase 1 parameters:
13. Hash – SHA
14. Encryption – AES-192
15. DH group – 5
16. Use certificates for authentication.
17. Use certificates issued by HQ1 certificate authority.
18. Configure IKEv2
19. Phase 2 parameters:
20. Protocol – ESP
21. Encryption - AES
22. Hash – MD5
23. Configure SSL VPN server on ASA firewall:
24. Create local user vpnuser with cisco password on the ASA.
25. Users should be able to connect using AnyConnect client, which is located on the flash disk of ASA.
26. The connection should be performed to address 40.15.5.2.
27. Check the connection from PC2.

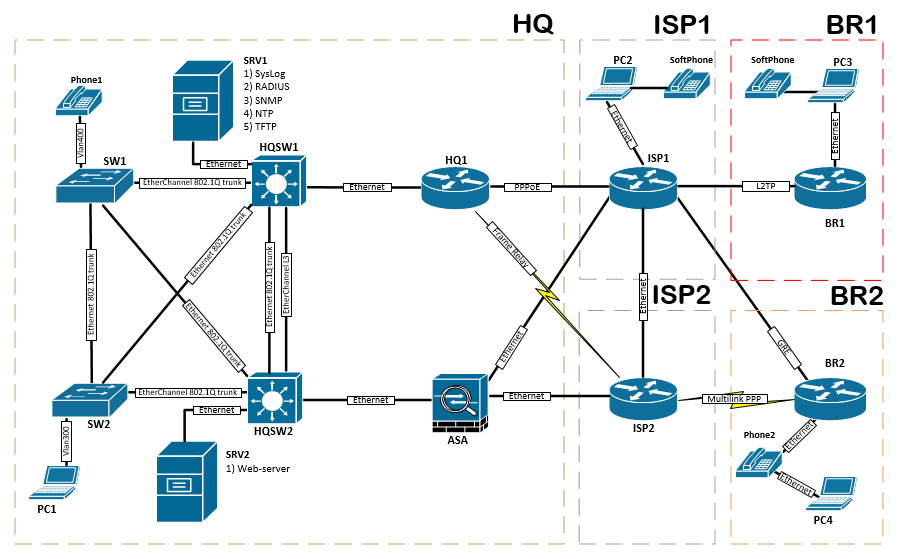
**VoIP configuration**

On HQ1 and BR2 routers configure Call Manager Express using SIP protocol with following parameters:

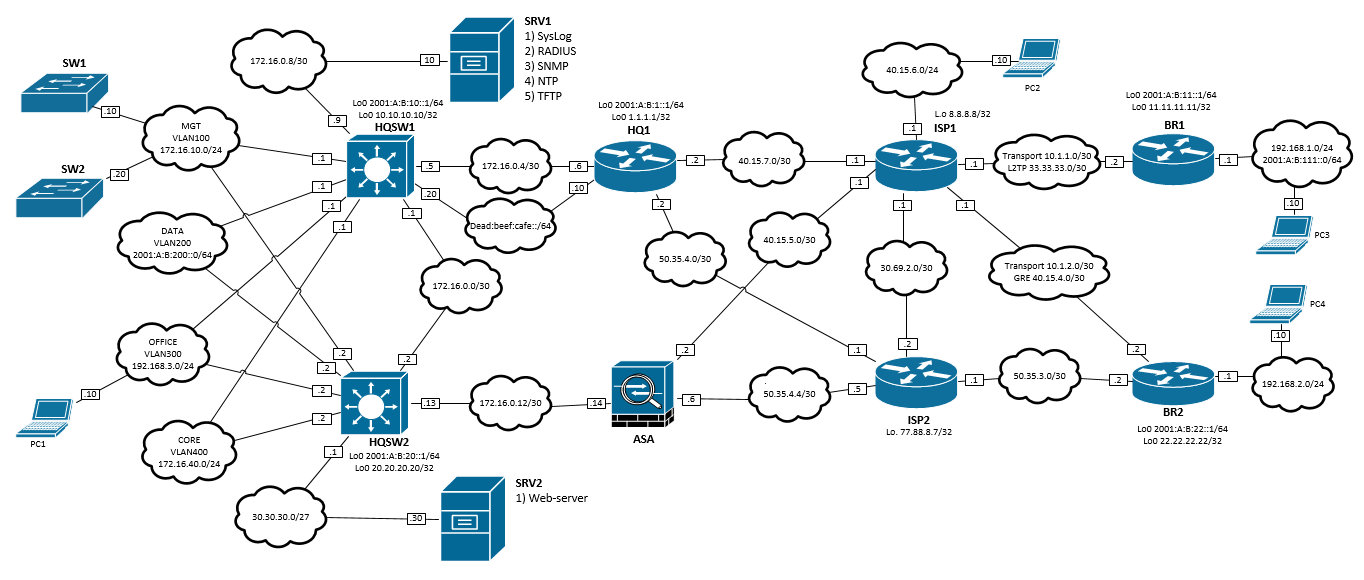
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| User | Line | Extension | Device | СМЕ |
| DugurovD | 1 | 101 | Softphone1 | CME HQ |
| DobryninS | 1 | 102 | Phone1 | CME HQ |
| SilaevN | 1 | 103 | Phone2 | CME HQ |
| ShmakovL | 1 | 104 | Softphone2 | CME BR2 |

1. Customize IP phones so that user name is shown in the upper right corner instead of extension number. Make sure that when calling another extension, user name is displayed instead of extension number.
2. Configure Music-on-Hold on HQ. Use MOH.wav file on HQ1 router.
3. Configure conferencing services to support at least three parties in a conference call.
4. On the phone Dobrynin the second button (second line) should activate intercom to number SilayevN. When calling this number, the phone should pick up automatically with speakerphone and microphone disabled.
5. Configure call parking using Park button. Any user should be able to pick up a parked call by calling number 100
6. Configure a translation rule, so that when you call number 88005555555, the phone with number 104 rings.
7. Configure speed-dial to DobryninS on the button 2 of ShmakovL telephone.

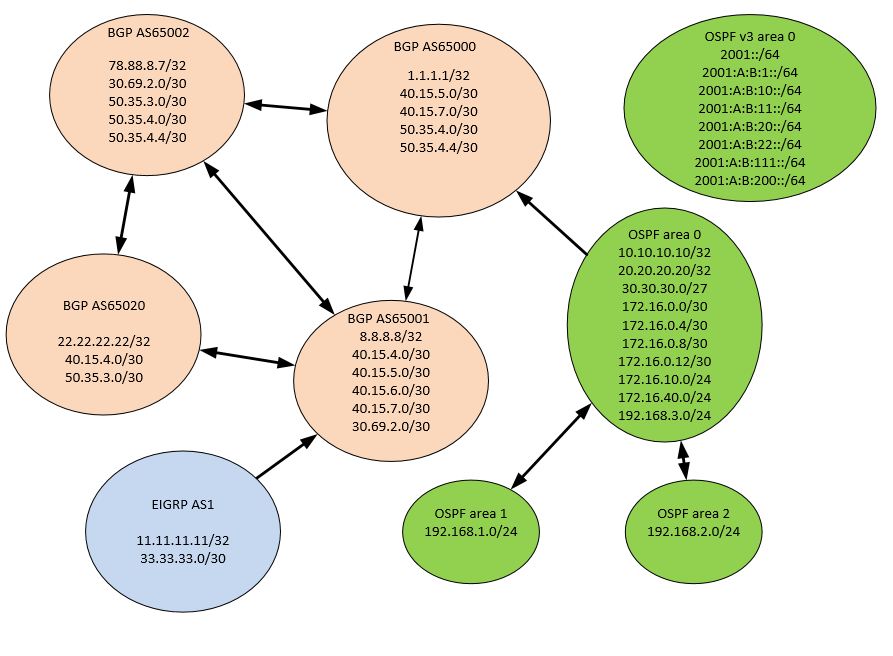
L1 Topology

L2 Topology

L3 Topology



Routing diagram



VPN diagram



IP Telephony diagram

