**Skill**

**"IT Network System Administration"**

**Test project**

**module B:**

**Configuring   
Microsoft Windows OS**

**Developed by**

**Certified WSR expert**

**Dugurov D.V.**

**Date09.04.18**

**Version: 1**

**Introduction.** The time to complete the task is limited - think about how to use it with most efficiency. Develop a working plan. It is quite possible, that in order to configure a fully working system you should complete the tasks in an order that is different from the order given in this test project.

According to the test project legend You are a system administrator of a newly created Moscow-based company. You need to configure services in the local area network of the main office.

Please also note, that the company has recently acquired a small business in Izhevsk. The network in the Izhevsk office was functional, but the system administrator (due to being fired with a scandal) did not provide access credentials for the working local domain controller. You will have to restore access to the Izhevsk domain.

You will also have to configure a secure channel between the offices, trust between domains and remote connection for clients after modeling an Internet service provider.

Please read the entire test project carefully - it represents an integral and holistic system. When accessing the operating systems for the first time either follow the steps of the wizard or, if necessary, use the following credentials: *Administrator/P@ssw0rd*.

If the provided virtual machines would start to spontaneously shutdown during the course of work, try using the *slmgr /rearm* command or ask the workshop supervisor.

**Test project contents**

1. Text files:

* this file with the test project itself;
* a file with additions, containing: the description of pre-configurations, types of operating systems used, recommendations regarding resource allocation for the virtual machines, recommendation regarding possible changes for the 30% changes requirement.

1. Components of the test project provided to the competitors:

* file for importing the users to the Moscow domain (.xlsx);
* start page for the managers.moscow.ru site (.htm);
* start page for the www.moscow.ru site (.htm);
* start page for the www.izhevsk.ru site (.htm);

1. Software:

* Windows server 2016;
* Microsoft Office;
* RSAT tools for Windows 10;
* Windows10.ADMX.

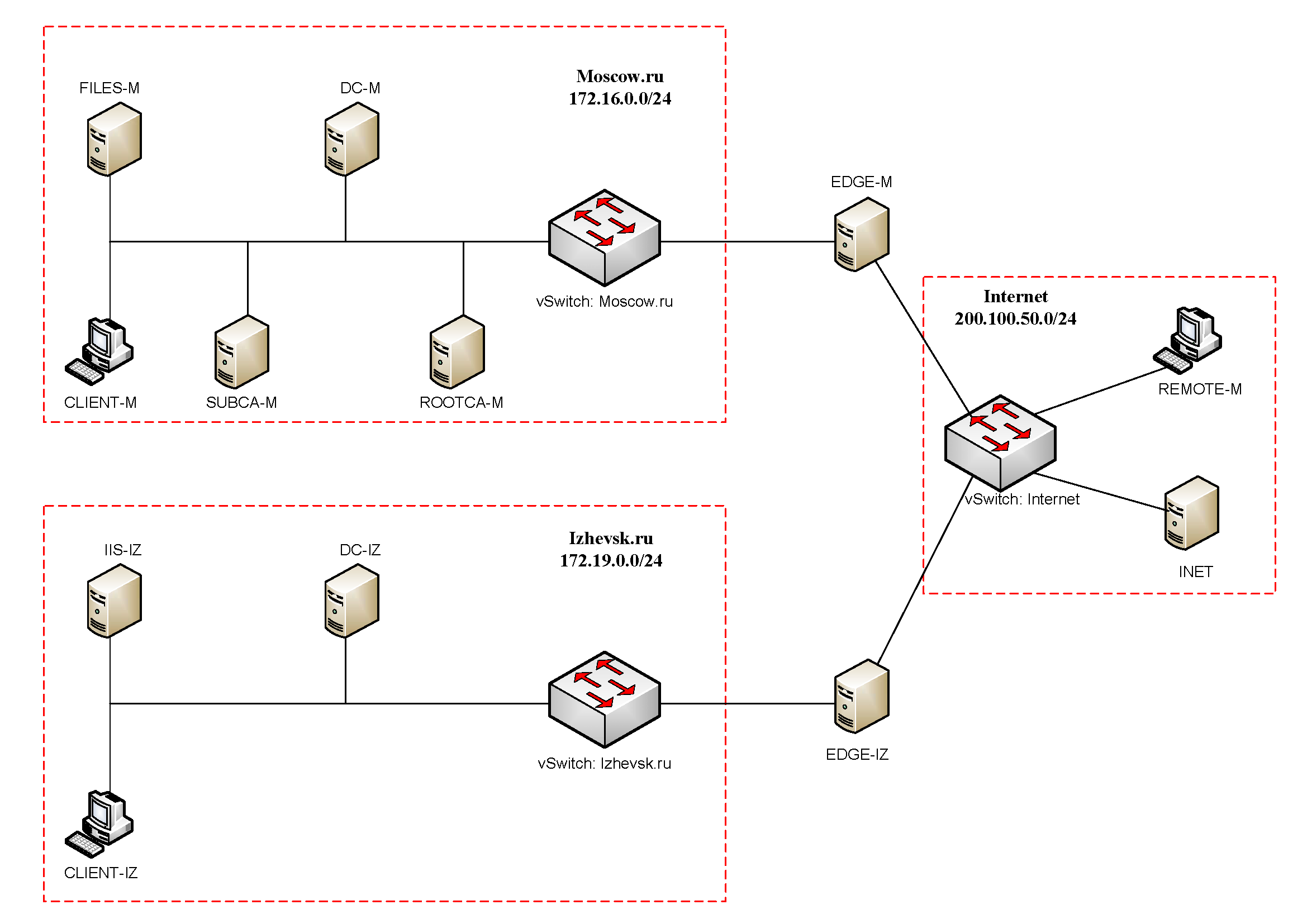
**Attention! All listed components are provided to the competitors in the form of   
 ISO-files located at a local or remote storage.**

**Competitors are not allowed to use any devices except for those present on the working places provided by the organizers.**

**Competitors are not allowed to bring any pre-existing documents and materials to the workplace.**

**As a result of their work, competitors must ensure that the listed virutal machines have the roles and services available and working according to the test project. However competitors are free to choose the way of configuring any particular component and use the resources provided as they see fit.**

**Network diagram**



**DC-M Configuration**

**Basic сonfiguration**

* rename the computer to DC-M
* configure the network according to table 1;
* ensure that ICMP protocol is working (to use ping)

**Active Directory**

* configure the server to be the primary domain controller for Moscow.ru domain;
* configure one-way non-transitional trust with the Izhevsk.ru domain - users of the Moscow.ru domain should have access to the resources of the Izhevsk.ru domain, but not vice-versa.

**DHCP**

* configure the DHCP protocol to automatically configure hosts;
* configure failover: mode – Load balancer, partner server – FILES-M, state switchover – 10 min;
* allocated address pool: 172.16.0.100-200/24;
* configure additional scope options (addresses of both DNS servers and the gateway address)

**DNS**

* configure the required forward and reverse lookup zones and ensure they are working in conjunction with the DNS service on FILES-M;
* manually create all necessary records of the A type and PTR type for the domain servers and required web-services;
* make all configuration necessary for working trust with the Izhevsk.ru domain (if new DNS servers are introduced, they must get the settings required for working trust automatically).

**GPO**

* disable the first-time login user welcome animation on all client computers of the domain.
* members of the IT group must also be members of the local administrators group on all client computers of the domain;
* in IE Explorer and Microsoft Edge browsers (install and use windows10.admx) www.moscow.ru must be configured as the start page.
* disable changing the screensaver and *Recycle bin* on the desktop of all domain users, except the members of the local administrators group of the client computers;
* configure folder redirection of *My Documents* and *Desktop* folders to FILES-M→d:\shared\redirected for the members of the Experts group

**Domain infrastructure elements**

* create organizational units: Experts, Competitors, Managers, Visitors, IT and Project;
* in corresponding organizational units create domain groups: Experts, Competitors, Managers, Visitors, IT, Project\_Budget-R, Project\_Budget-W, Project\_Intranet-R, Project\_Intranet-W, Project\_Logistics-R, Project\_Logistics-W;
* and also create a domain group DAClients;

**Attention! The organizational units and groups listed above must be present in the domain. If you think, that in order to complete the test project you may need additional elements of the domain infrastructure, you may create them.**

* create users, using the excel file provided to you (all user information in the file must be added to the Active Directory); put users in the corresponding organizational units and groups; all the accounts must be enabled and available;
* for each user create a home folder, that would automatically mount as a disk U:\, located at FILES-M→d:\shares\users.

**FILES-M configuration**

**Basic сonfiguration**

* rename the computer to FILES-M;
* configure the network according to table 1;
* ensure that ICMP protocol is working (to use ping)
* add the computer to Moscow.ru domain;
* use three available drives to create a RAID-5 array; assign letter D:\ to it.

**Active Directory**

* configure the server as a secondary controller for the Moscow.ru domain;
* the controller must not be a global catalogue server.

**DHCP**

* configure the DHCP protocol to automatically configure hosts;
* configure failover: mode – Load balancer, partner server – DC-M, state switchover – 10 min;

**DNS**

* make the server a secondary DNS-server for Moscow.ru domain;
* download all forward and reverse lookup zones form DC-M.

**Shared folders**

* create shared folders for the organizational units (Competitors, Experts and Managers) at FILES-M→d:\shares\departments;
* ensure, that the shared folder of the organizational unit is attached to the corresponding group as disk G:\;
* create a shared project folder at FILES-M→d:\shares\projects;
* create the following folders inside d:\shares\projects folder: Budget, Intranet, Logistics; configure the permissions for these folders according with Table 2;
* assign this shared project folder as disk P:\ to all users except the Visitors group; the users must see only those folders inside disk P:\ that they have permission to access.

**Quotes/File Screening**

* set maximum home folder size (U:\) to 5Gb each;
* forbid storing files with .exe and .cmd extensions in home folders; note, that user should be allowed to store files of all other types in their home folders.

**IIS**

* create a site for company managers (use the htm file provided as the default document);
* the site must be accessible only by the domain name of managers.moscow.ru, only via HTTPS protocol and exclusively to the members of Managers group based on their user certificates.

**ROOTCA-M configuration**

**Basic сonfiguration**

* rename the computer to ROOTCA-M;
* configure the network according to table 1;
* ensure that ICMP protocol is working (to use ping)
* do not add the computer to any domains.

**Certification services**

* install certification services;
* configure a standalone root certification authority (key length and crypto algorithms are irrelevant);
* name of the certification authority - Moscow Root CA;
* certificate should be valid for 10 years;
* CRL location: http://SUBCA-М.Moscow.ru/certenroll/<caname><crlnamesuffix><deltacrlallowed>.crl
* AIA location: http://SUBCA-M.Moscow.ru/certenroll/<serverdnsname>\_<caname><certificatename>.crt
* create a certificate revocation list and a root certificate for the SUBCA-M;
* issue a subordinate CA certificate for SUBCA-M by approving the corresponding request;
* disable the network interface after performing all the necessary configurations.

**SUBCA-M configuration**

**Basic сonfiguration**

* rename the computer to SUBCA-M;
* configure the network according to table 1;
* ensure that ICMP protocol is working (to use ping)
* add the computer to the Moscow.ru domain.

**Certification services**

* install certification services;
* configure a subordinate certification authority;
* the certification authority name - Moscow Sub CA;
* certificate should be valid for 5 years;
* import and publish the CRL from ROOTCA-M;
* configure a template for client computer certificates named *MoscowClients*: *subject name=common name*, automatic request for all client computers in the domain;
* configure a certificate template for the Managers group named *MoscowUsers*: *subject name=common name*, automatic request only for members of the Managers group.

**CLIENT-M configuration**

**Basic сonfiguration**

* rename the computer to CLIENT-M;
* ensure that ICMP protocol is working (to use ping)
* add the computer to Moscow.ru domain;
* install the Remote Server Administration Tools (RSAT);
* disable the sleep mode;
* use the computer to test the configuration of the Moscow.ru domain: users, shared folders, group policies, including testing the Direct Access connections (by temporarily moving the computer to the Internet network).

**DC-IZ configuration**

**Access recovery**

* gain (recover) access to the domain controller and Active Directory replica; remember - the server contains important information, and because of this you are not allowed to reinstall the operating system!

**User and resources search**

* find all domain users in Izhevsk.ru domain, that have *Expert* in the *Job title* field;
* move all found users to a special organizational unit named Migration (create it if necessary) and disable the accounts in the Izhevsk.ru domain;
* find all home folders of the users found earlier in the Izhevsk.ru domain, and copy them to FILES-M→d:\shares\migrated;
* create new user accounts in the Migrated organizational unit of the Moscow.ru domain (create the OU if necessary) for all corresponding user accounts that you have found and disabled on the previous steps; set a password *NewP@ssw0rd* for them;
* for the newly created user accounts ensure that their home folders are mounted as disk S:\; ensure that all the newly created users in the Moscow.ru domain can access the files, that were copied from their home folders in the Izhevsk.ru domain.

**DNS**

* make all the necessary configurations to ensure working trust with the Moscow.ru domain (if new DNS servers are introduced, they must get the settings required for working trust automatically).
* ensure that site names www.moscow.ru and www.izhevsk.ru are resolved.

**Remote Desktop Services**

* deploy a remote desktop server, do not install or configure licensing components;
* Configure RemoteApp web-access for terminal services;
* Publish *Wordpad* on the web-portal of RemoteApp for the members of Domain Admins group;
* Publish *Notepad* on the web-portal of RemoteApp for the members of Domain Users;
* The web-interface must be configured so users should automatically access the RDS login page when accessing http://rds.izhevsk.ru and https://rds.izhevsk.ru;
* On the SUBCA-M 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.izhevsk.ru from any computer in the Izhevsk.ru or Moscow.ru domains, the certificate must be recognized as trusted and valid.

**IIS-IZ configuration**

**IIS**

* create a site named www.moscow.ru (use the htm file provided as the default page);
* create a site named www.izhevsk.ru (use the htm file provided as the default page);
* both sites should be accessible via HTTPS protocol using the certificates issued by SUBCA-M.

**CLIENT-IZ configuration**

**Basic сonfiguration**

* rename the computer to CLIENT-IZ;
* ensure that ICMP protocol is working (to use ping)
* add the computer to Izhevsk.ru domain;
* disable the sleep mode;
* use the computer to test the configuration of the Izhevsk.ru domain.

**INET configuration**

**Basic сonfiguration**

* rename the computer to INET;
* configure the network according to table 1;
* ensure that ICMP protocol is working (to use ping)
* do not add the computer to any domains.

**DNS/IIS**

* configure Internet emulation, considering the operating system versions;
* create corresponding records on the DNS server to allow remote client access to the Direct Access server in the Moscow.ru domain, as well as the records for external clients to access www.moscow.ru and www.izhevsk.ru sites.

**DHCP**

* configure DHCP protocol for the Internet clients;
* allocated address pool: .170-190/24;
* configure the rest of the options as you see fit.

**EDGE-IZ configuration**

**Basic сonfiguration**

* rename the computer to EDGE-IZ;
* configure the network according to table 1;
* ensure that ICMP protocol is working (to use ping)
* add the computer to the Izhevsk.ru domain.

**RRAS configuration**

* install RRAS service;
* configure a secure VPN connection to the Moscow.ru domain using computer certificates for authentication; the certificates must be issued by SUBCA-M; all the traffic between domains must be sent through this connection;
* configure port forwarding for remote client access (checked from the Internet) to www.moscow.ru and www.izhevsk.ru sites that are deployed on IIS-IZ.

**EDGE-M configuration**

**Basic сonfiguration**

* rename the computer to EDGE-M;
* configure the network according to table 1;
* ensure that ICMP protocol is working (to use ping)
* add the computer to the Moscow.ru domain.

**RRAS configuration**

* install RRAS service;
* configure a secure VPN connection to the Izhevsk.ru domain using computer certificates for authentication; the certificates must be issued by SUBCA-M; all the traffic between domains must be sent through this connection.

**Direct Access configuration**

* make CLIENT-M and REMOTE-M computer accounts members of the DAClients group;
* only members of the DAClients group should be able to connect using Direct Access;
* name of the connection - *DA-Moscow*
* use FILES-M as the NCA;
* use name *connect.moscow.ru* for external clients connections;
* use the certificate issued by SUBCA-M for configuration (using self-signed certificates is not allowed);
* Direct Access clients must have full access to all shared resources in both offices.

**REMOTE-M configuration**

**Basic сonfiguration**

* rename the computer to REMOTE-M;
* ensure that ICMP protocol is working (to use ping)
* disable the sleep mode;
* without changing the network settings (the NIC must be connected to the Internet network) connect the computer to the Moscow.ru domain in the OFFLINE mode;
* save the offline metadata file created on DC-M in the C:\Remote.txt folder.

*Table 1*

|  |  |  |
| --- | --- | --- |
| **Computer name** | **Domain name** | **IP addresses** |
| DC-IZ | Izhevsk.ru | 172.19.0.1/24 |
| CLIENT-IZ | DHCP |
| IIS-IZ | 172.19.0.3/24 |
| EDGE-IZ | 172.19.0.250/24  200.100.50.101/24 |
| DC-M | Moscow.ru | 172.16.0.1/24 |
| FILES-M | 172.16.0.2/24 |
| SUBCA-M | 172.16.0.4/24 |
| EDGE-M | 172.16.0.250/24  200.100.50.100/24 |
| CLIENT-M | DHCP |
| REMOTE-M | DHCP |
| ROOTCA-M | None | 172.16.0.3/24 |
| INET | 200.100.50.200/24 |

*Table 2.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Shared resource name** | **Location** | **Read-only access** | **Read-write access** |
| Budget | FILES-M→D:\shares\projects | RU-Budget-R | RU-Budget-W |
| Intranet | RU-Intranet-R | RU-Intranet-W |
| Logistics | RU-Logistics-R | RU-Logistics-W |