Test Project

IT Network System Administration

Module C – Commissioning of data and voice networks

Submitted by:

José Daniel Medeiros PT
Aleksandr Gorbachev RU
Christian Schöndorfer AT
Andrei Varuyeu BY
Sonia E Cardenas Urrea CO
Almut Leykauff-Bothe DE
Benjamin Callar FR
Silvio Papić HR
Svetlana Lapenko KZ
Te Chao Liang TW
Joe Motsapi ZA

Contents

Introduction to Test Project

Contents

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

1. WSC2019_TP39_ModuleC_pre_EN.docx
2. Physical_and_Logical_Topology.pdf

Introduction

Network technology knowledge is becoming 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 service the network infrastructure for any multi-branch enterprise.

Description of project and tasks

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

- Campus and branch LAN
- Public internet
- Enterprise routing
- Services integration
- Unified communications infrastructure

Some tasks are quite simple and straightforward while others may be more complex. 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 PPP 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

1. Read all tasks in each section before proceeding with any configuration. The completion of any item may require the completion of any previous or later item.

2. Before starting the test project, confirm that all devices in your topology are in working order. During the test project, if any device is locked or inaccessible for any reason, **you must recover it**. When you complete this test project, ensure that all devices are accessible to the grading Experts. A device that is not accessible for grading cannot be marked and may cause you to lose substantial points.

3. Knowledge of implementation and troubleshooting techniques is part of the skills being tested in the configuration section of the Test Project.

4. Points are awarded for working configurations only. Test the functionality of all the requirements before you submit the test project. Be careful, because as you configure one part, you may break a previous requirement or configuration.

5. No partial points can be granted for any aspect; all requirements need to be fulfilled to receive the points for the aspect. Some requirements depend on other aspect's requirements, either before or after the current aspect.

6. Save your configurations frequently; accidents do and will happen.

7. Use alpha-numeric characters only in any variable name (access-list, prefix-list, route-map, etc); that is, do not use any punctuation or special characters (.,;:'/|\?!_-(){}*&^%$#@).

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

9. Whenever you are required to configure a password, use password **cisco** if otherwise is not stated.

10. All virtual machines are pre-installed. Use **admin\Passw0rd$** local credentials to access windows virtual machines (**administrator\Passw0rd$** for domain administrator) and **root\Passw0rd$** to access linux virtual machines. Do not change these passwords.

11. DO NOT configure any authentication on **console lines** of cisco devices (including cisco virtual machines).

12. Implement all tasks to the best of your ability, in line with industry best practices (in terms of security, high availability and scalability) within the limitations imposed by the equipment.

13. Complete self assessment questionnaire. Answers in this questionnaire will be used by experts as a time saver for judgment marking. If you mark a section as **Not implemented** (or no answer \ details specified) configuration check for this section will be skipped. If you mark a section as done (or any answer \ details specified) experts will double check your configuration against your answer.

Equipment, machinery, installations and materials required

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

Marking Scheme

According to the WorldSkills Standards Specifications within current Technical Description all marks for this test project module fall into section 7 «Configuring network devices» which has a maximum mark of 25.

Test Project objectives

Verify basic configuration

1. Hostnames for all devices and virtual machines are preconfigured according to the topology diagrams.
2. Virtual and physical switching is preconfigured according to the topology diagrams. VLAN numbers on physical switches are used in accordance with SVI numbers in each subnet.
3. Network devices (except for IP phones) and virtual machines are preconfigured with static IP addresses. For each subnet the gateway device assigned with the last IP address in this subnet and the client device assigned with the first IP address in this subnet. If there are more than one client\gateway device in a subnet, each next device is using next available IP address. E.g. in **Tyumen** subnet **TJM-01** is assigned with last address in this subnet (.254), **TJM-02** — next available from the end (.253), **DC** — first available in this subnet (.1), **CA** — next available (.2) and **NetOps** — next available (.3).
4. Network equipment and virtual machines are preconfigured with default static routing towards the internet as well as basic NAT/PAT.
5. Server VMs are preconfigured with following roles and services:

Virtual machine	Roles \ Services
DC	Active Directory Domain Services (tnk-bp.ru), DNS (tnk-bp.ru, rosatom.ru), DHCP, Network Policy Server
CA	Enterprise Certificate Authority
NetOps	Observium network monitoring platform (observium.tnk-bp.ru), SNMP server, TFTP server
ROSATOM	IIS webserver (rosatom.ru)
Yandex	Apache2 web server (ya.ru), BIND9 DNS server

Campus and Branch LAN

1. Configure VLAN distribution feature on **DSW-01**. When adding any new VLAN to **DSW-01**, this VLAN should be automatically distributed to **DSW-02**, **ASW-01** and **ASW-02**.
2. **DSW-01** should be the root bridge for all VLANs and **DSW-02** should take over in case DSW-01 fails.
3. Configure link aggregation between **DSW-01** and **DSW-02**. Use any LAG protocol.
4. During normal network operation **DSW-01** should act as a next hop for **HQ** subnet. In case of **DSW-01** crash or physical links failure, **DSW-02** should act as the next hop.
5. Implement layer 2 security features on the access switches at the Moscow site.

Public Internet

1. **ya.ru** and **observium.tnk-bp.ru** must be accessible on public internet from any client virtual machine.
2. Implement necessary security measures on **Moscow** site border to expose minimum services towards public internet.
3. **rosatom.ru** should not be accessible on public internet — only inside enterprise routing domain.

Enterprise Routing Domain

1. Ensure end-to-end connectivity between all virtual machines inside enterprise routing domain.
2. All traffic between sites must be encrypted with IPsec while traversing via public internet.
3. Serial links must serve as a routing failover to branch networks and internet access in case of public internet is down. Implement a secure layer 2 protocol on this link.
4. Implement secure remote access for **Boris** so he can securely access all services inside enterprise routing domain. Add A record **vpn.tnk-bp.ru** with IP address of VPN termination device to **Yandex** DNS server.
5. **TJM-02** should act as stateless failover for all traffic from **Tyumen** towards the internet and enterprise routing domain and vice versa. In case of **TJM-01** failure **TJM-02** should take over all roles of **TJM-01** so all network services will continue normal operation.

Services Integration

1. Synchronize time on all network equipment using NTP (time zone KZN +3). Use **RTK** as the root NTP server. In case you are configuring hierarchical NTP infrastructure use **MOW** as a corporate NTP server.
2. Client machines in **Yakutsk** and **Kirov**, as well as IP phones in **HQ**, should receive IP addresses via DHCP service.
3. Add **MOW** router and **DSW-01** switch to the Observium network monitoring platform via SNMP.
4. For **MOW** router Implement configuration backup to TFTP server located on **NetOps** virtual machine. New backup copy should be created each time configuration is saved on a device.
5. Implement local user **wsc2019\Passw0rd$** with privilege level 15 on all network devices (only for VTY lines).
6. For **TJM-01** and **TJM-02** only users of **DL-Net-Admins** group in **tnk-bp.ru** domain must be able to login remotely. After login users should automatically land in privileged mode (level 15). Use local authentication in case remote authentication server is not available.

Unified Communications Infrastructure

Configure Call Manager Express on **MOW** router:

1. Configure a custom system message.
2. Configure Local Directory Services so that users can lookup other users' extension number via the Directory catalog.
3. Configure conferencing services to support at least three parties in a conference call.
4. Configure Call Park on extension 999 to allow any user to park the call so that any user can pick up the call upon dialing the call park extension.
5. On **Kremlin** phone upon pressing second line-button, **Ivan**'s phone should automatically answer the call in speakerphone mode with mute activated and **Ivan** should hear **Kremlin**'s conversation.
6. Both **KGB** and **Kremlin** should automatically answer the call-in speakerphone mode when dialing extension 888.
7. On **Yuri** configure second line-button to speed dial **Ivan**.
8. When **KGB** and **Kremlin** are on or park, they should hear music. Use MOH.au file located on **MOW** router flash.
9. While remotely connected to the enterprise routing domain, **Boris** must be able to register softphone on **MOW** router and communicate with all sites normally.

Optional self assessment questionnaire

Campus and branch LAN implementation

How did you implement dynamic VLAN distribution at Moscow site?

□ Not implemented □ VTP v1 □ VTP v2 □ VTP v3

□ Other (please specify):

Which spanning tree protocol did you implement at Moscow site?

□ Default □ RPVST+ □ MST

□ Other (please specify):

Any additional Layer 2 features are used at Moscow site?

□ DTP disable (specify details):

□ Non-default native VLAN (specify details):

□ Blackhole VLAN (specify details):

□ Portfast (specify details):

□ BPDU guard (specify details):

□ Root guard (specify details):

□ Port security (specify details):

□ DHCP snooping (specify details):

□ Dynamic ARP inspection (specify details):

How did you implement link aggregation at Moscow site?

□ Not implemented □ Static (L2) □ Static (L3) □ LACP □ PAgP

□ Other (please specify):

How did you implement failover at Moscow site?

□ Not implemented □ HSRP □ VRRP

□ Other (please specify):

Public internet implementation

Briefly describe the restrictions for the traffic destined for each site that passes through the public Internet (specify ALL if there are no restrictions configured).

□ MOW:

How did you implement routing on the public internet?

□ Not implemented □ Static \ Default routes □ RIP v1/2 □ OSPF □ EIGRP □ BGP

□ Other (please specify):

Enterprise routing domain implementation

How did you implement site-to-site VPN(s) between MOW, KVX, YKS, TJM-01 and TJM-02?

□ Not implemented □ Full mesh GRE □ Hub-and-spoke GRE □ Full mesh IPsec □ Hub-and-spoke IPsec

□ DMVPN Phase 1 □ DMVPN Phase 2 □ DMVPN Phase 3

□ Other (please specify):

How did you implement site-to-site VPN(s) between TOF and the rest of enterprise routing domain?

□ Not implemented □ Hub-and-spoke IPsec □ Point-to-Point IPsec (specify peer):

□ Other (please specify):

Specify components that are used for IPsec

Internet Key Exchange protocol:	□ IKE v1	□ IKE v2
Authentication:	□ Pre-shared key	□ RSA
Payload security:	□ AH	□ ESP
Other \ Details (please specify):		

How did you implement routing inside enterprise routing domain?

□ Not implemented □ Static routes □ RIP □ OSPF □ EIGRP □ BGP

□ Other \ Details (please specify):

How did you implement remote access VPN?

□ Not implemented □ PPTP □ L2TP □ IPsec □ AnyConnect

□ Other (please specify):

Which entry point(s) is used for remote access VPN?

□ Not implemented □ MOW □ YKS □ KVX □ TOF

□ FW-01 □ TJM-01 □ TJM-02

□ Other \ Details (please specify):

How did you implement security for serial links?

□ Not implemented □ One-way PAP □ Two-way PAP □ One-way CHAP □ Two-way CHAP

□ Other (please specify):

Services implementation

How did you implement NTP synchronization?

□ Not implemented □ Authentication is used □ Single NTP server

□ Hierarchical NTP infrastructure (please specify):

□ Other (please specify):

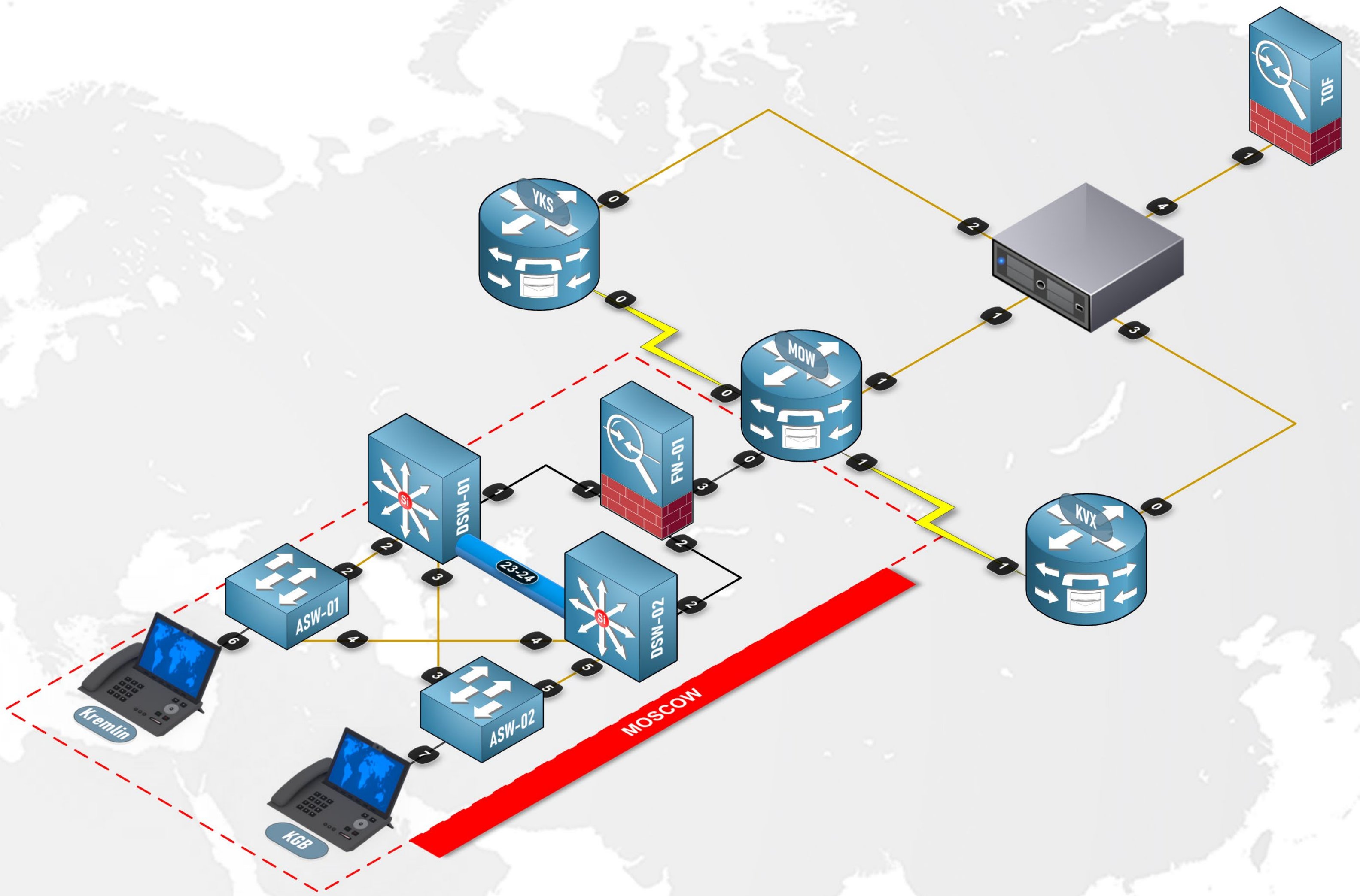
How did you implement network monitoring?

□ Not implemented □ SNMPv1 □ SNMPv2 □ SNMPv3

□ Other (please specify):

Diagrams

PHYSICAL CONNECTIONS AND VIRTUAL SWITCHING



ESXi port-groups

Yakutsk
VLAN ID: 10
Virtual machines:
Ivan
ESXi uplink:
VMNIC2

Kirov
VLAN ID: 20
Virtual machines:
Yuri
ESXi uplink:
VMNIC3

Tomsk
VLAN ID: 30
Virtual machines:
ROSATOM
ESXi uplink:
VMNIC4

Tyumen
VLAN ID: 40
Virtual machines:
TJM-01 (Gi1) TJM-02 (Gi1)
DC CA NetOps
ESXi uplink:
None

Sakhalin
VLAN ID: 50
Virtual machines:
Boris
RTK (Gi6)
ESXi uplink:
None

RT-MOW
VLAN ID: 100
Virtual machines:
RTK (Gi1)
ESXi uplink:
VMNIC1

RT-YKS
VLAN ID: 110
Virtual machines:
RTK (Gi2)
ESXi uplink:
VMNIC2

RT-KVX
VLAN ID: 120
Virtual machines:
RTK (Gi3)
ESXi uplink:
VMNIC3

RT-TOF
VLAN ID: 130
Virtual machines:
RTK (Gi4)
ESXi uplink:
VMNIC4

RT-TJM
VLAN ID: 140
Virtual machines:
RTK (Gi5)
TJM-01 (Gi2) TJM-02 (Gi2)
ESXi uplink:
None

Yandex
VLAN ID: 60
Virtual machines:
Yandex
RTK (Gi7)
ESXi uplink:
None

CSR_MGMT
VLAN ID: 999
Virtual machines:
TJM-01 (Gi0) TJM-02 (Gi0)
RTK
ESXi uplink:
VMNIC0

Legend

Router
ISR 4321
IOS-XE 16.6.6

Switch
Catalyst 3650
IOS-XE 16.6.5

Switch
Catalyst 2960
IOS 15.2.4

Firewall
ASA 5506-X
9.10.1

IP Phone
7945G
9.4(2)

Router
CSR 1000v
IOS-XE 3.9.15.3.2

Virtual Machine
Windows 10

Virtual Machine
Debian 9.8

Virtual Machine
Windows Server 2016

Etherchannel
LACP / PAgP

Serial Link

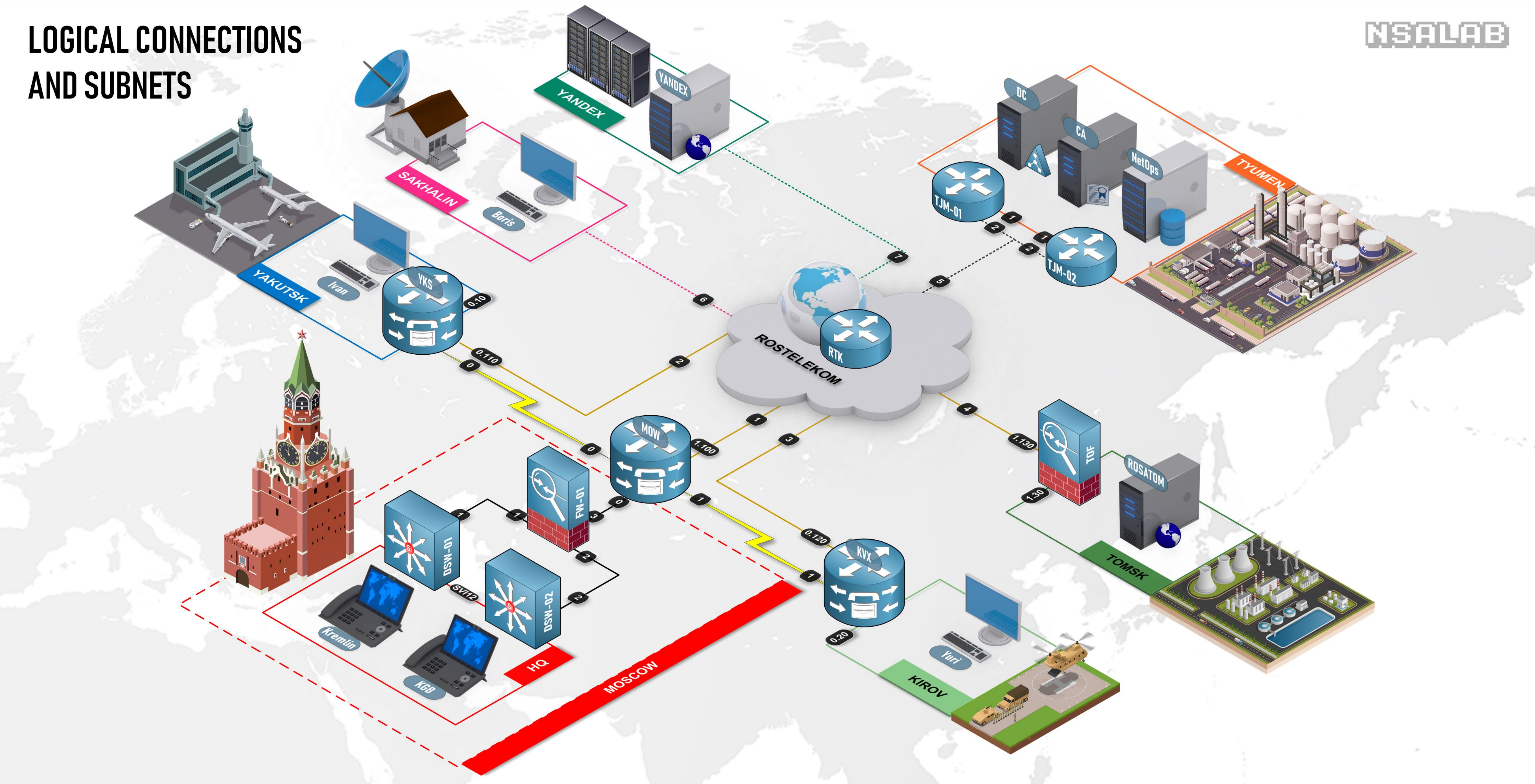
Hypervisor
VMware ESXi
6.7u2

Ethernet
IEEE 802.3
Access Link

Ethernet
IEEE 802.1Q
Trunk Link

Port number
Gi [0/0/X] Fa [0/X]
Ser [0/0/X] SVI [XX] VMNIC [X]

LOGICAL CONNECTIONS AND SUBNETS



Enterprise routing domain

YAKUTSK 172.16.10.0 /24	TOMSK 172.16.30.0 /24
KIROV 172.16.20.0 /24	TYUMEN 172.16.40.0 /24
DSW-01 – FW-01 172.20.1.0 /30	DSW-02 – FW-01 172.20.2.0 /30
HQ 172.20.3.0 /24	FW-01 - MOW 172.20.4.0 /30
MOW-YKS 10.0.10.0 /30	MOW-KVX 10.0.20.0 /30

Internet routing domain

RT-YKS 100.10.9.4 /30	RT-KVX 94.121.72.0 /24
RT-TOF 65.32.147.0 /24	RT-TJM 18.31.192.0 /24
RT-MOW 132.87.2.0 /24	Loopback8888 8.8.8.8 /32
SAKHALIN 100.71.60.252 /30	YANDEX 87.250.250.0 /24

Legend

Router
ISR 4321
IOS-XE 16.6.6

Switch
Catalyst 3650
IOS-XE 16.6.5

Switch
Catalyst 2960
IOS 15.2.4

Firewall
ASA 5506-X
9.10.1

IP Phone
7945G
9.4(2)

Router
CSR 1000v
IOS-XE 3.9.15.3.2

Virtual Machine
Windows 10

Virtual Machine
Debian 9.8

Virtual Machine
Windows Server 2016

SUBNET **Network Location**
L3 Subnet

Serial Link

Hypervisor
VMware ESXi
6.7u2

Ethernet
IEEE 802.3
Access Link

Ethernet
IEEE 802.1Q
Trunk Link

Ethernet
IEEE 802.1Q
VLAN

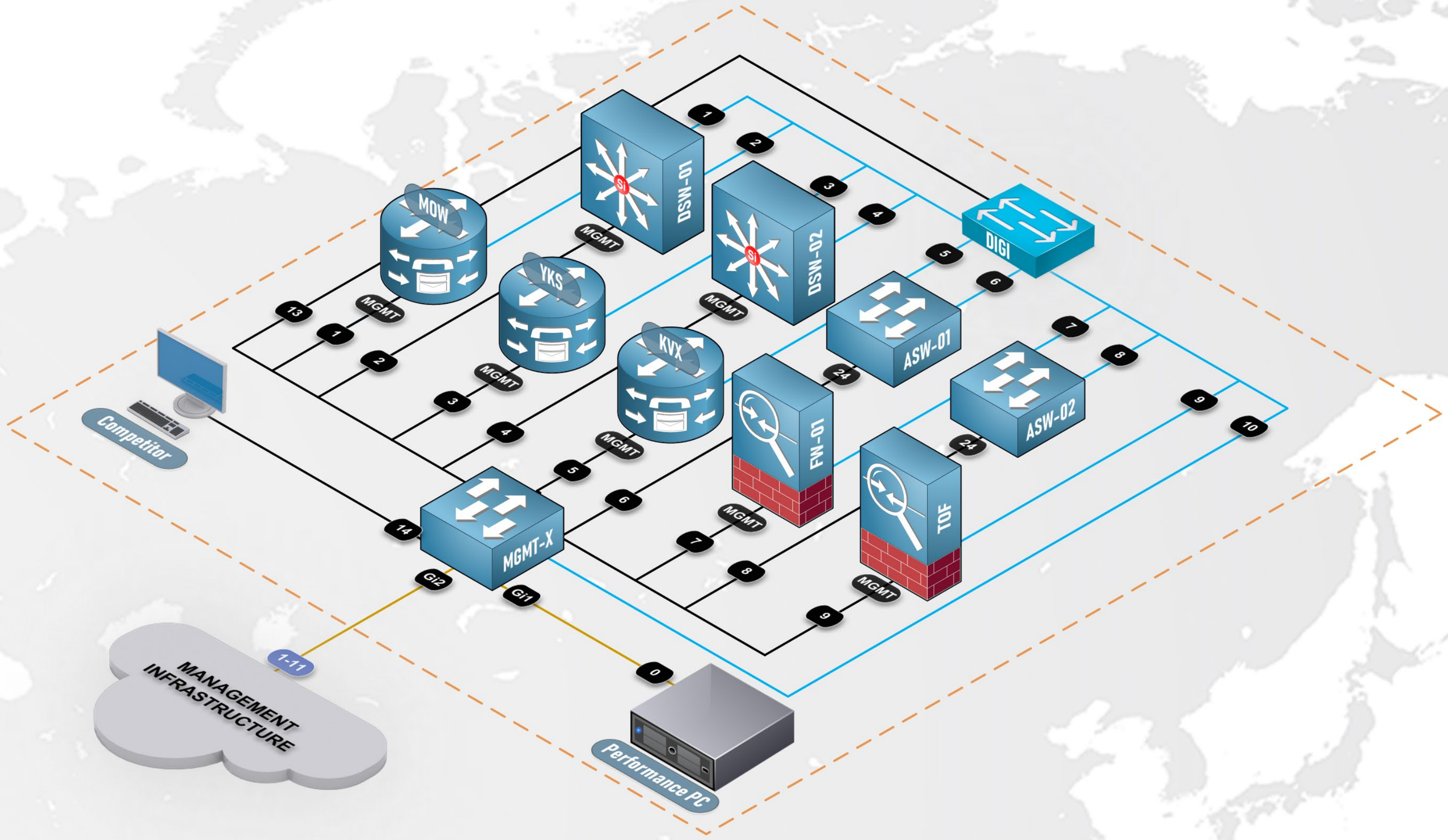
Etherchannel
LACP / PAgP

EGP
Routing Domain

1 **Port number**
Gi [0/0/X] Fa [0/X]
Ser [0/0/X] SVI [XX] VMNIC [X]

POD MANAGEMENT CONNECTIONS

NSALAB



POD Management IP addressing (10.0.0.0 /24)

MOW 10.0.0.1 Gi0	YKS 10.0.0.3 Gi0	KVX 10.0.0.5 Gi0	FW-01 10.0.0.7 Management1/1	TOF 10.0.0.9 Management1/1	TJM-01 10.0.0.11 Gi3	DIGI 10.0.0.13 Eth
DSW-01 10.0.0.2 Gi0/0	DSW-02 10.0.0.4 Gi0/0	ASW-01 10.0.0.6 SVI 999	ASW-02 10.0.0.8 SVI 999	RTK 10.0.0.10 Gi8	TJM-02 10.0.0.12 Gi3	Competitor 10.0.0.14 NIC

DIGI SSH PORTS (10.0.0.13)

MOW 7001	YKS 7003	KVX 7005	FW-01 7007	TOF 7009
DSW-01 7002	DSW-02 7004	ASW-01 7006	ASW-02 7008	Digi credentials competitor / P@ssw0rd