د افغان تیلي کـــام مخابراتي شرکت لـوی ریاست
د مالــــــــــی او اداری مـــــــعاونیـــت
د تــــدارکـــــــــــاتـو ریاست
د پیرودلولـــــــــوی مـــدیریت
د اجناسو او خدماتو پیرودلو مـدیریت

(موضوع: اجراء برنامه های آموزشی کارمندان ریاست تکنالوژی معلوماتی)

شماره درخواست نرخدهی: { 616 }

تاریخ صدور درخواست نرخدهی: {1445/3/ 25}

جنس فوق ضرورت : ریاست منابع بشری

تاریخ ترتیب استعلام : (25 / 3 / 1445)

(1) اداره {نام اداره تدارکاتی را درج کنید} تخصیص بودجه لازم برای تدارک اجناس/ خدمات غیر مشورتی مندرج این درخواست را دارد.

(2) آفر سربسته شما الی {تاریخ و وقت را درج کنید} یا قبل ازآن به دفتر {مدیریت خریداري امریت تهیه و تدارکات شرکت افغان تیلیکام } تسلیم داده شود.

(3) آفر ها ئیکه بعد از میعاد تسلیمی ارائه گردند، بدون اینکه بازشود مسترد می گردد. پاکت حاوی آفر باید به صورت واضح عبارت نرخ برای {نام اجناس /خدمات غیر مشورتی را درج کنید} نشانی شده باشد.

(4) آفر ارائه شده در آفرها باید الی مدت (30) روز تقویمی سر از تاریخ ختم میعاد تسلیمی آفرها اعتبار داشته باشد.

(5) در صورت تغیر در مقدار نیازمندی، اداره می تواند مقدار نیازمندی تقاضا شده را الی (25) فیصد زیاد و یا کم نماید، مشروط به اینکه قیمت مجموعی آن از حدود صلاحیت پولی برای درخواست نرخ گیری تجاوز ننماید.

(6) ترجیح داخلی مطابق حکم چهارم طرزالعمل تدارکات قابل اجرا است. {مورد ترجیح داخلی و فیصدی آنرا درج نمائید}.

(7) آفر گشائی در محضر عام حتمی نبوده و فرمایش دهنده مکلف به قبول نازلترین نرخ نمی باشد. در صورت رد هر یک یا تمام آفرها فرمایش دهنده کدام مسؤلیت در قبال داوطلب تهیه/ارائه کننده ندارد.

(8) آفر دهنده اسناد ذیل را با آفر خویش ضمیمه می نماید:

1- جواز تجارتی/ فعالیت/کار قابل اعتبار؛

2- نمبرتشخیصیه مالیه؛

3- اجازه نامه تولید کننده (درصورت لزوم).

4-

(9) سند نرخ گیری تکمیل و توسط شخص با صلاحیت تهیه/ ارائه کننده در هر صفحه مهر امضاء شده باشد.

نام کارمند صادر کننده درخواست نرخ گیری:

امضاء هیت   امضاء هیت   امضاء هیت

جدول اقلام و قیمت ها

قمیت مجموعی به افغانی	قیمت فی واحد به افغانی	مقدار	واحد	اسم و تشریح با مشخصات تخنیکی اقلام	شماره
		2	**Person**	**MCSE 216 -2022**	1
		8	**Person**	**RHCE**	2
		17	**Person**	**Oracle Database Certified Associate**	3
		10	**Person**	**Red Hat System Administration || (RH 134)**	4
		3	**Person**	**CCNA Security 210-260**	5
		11	**Person**	**CCNP and CCIE Enterprise Core ENCOR 350-401 & CCNP 300-410 ENARSI**	6

مجموع قیمت به ارقام بشمول مالیات :عدد
مجموع قیمت به حروف بشمول مالیات:
مجموع مبلغ مالیات به ارقام و حروف:
مجموع قیمت به ارقام بدون مالیات:عدد (قابل پرداخت)
مجموع قیمت به حروف بدون مالیات (قابل پرداخت)
مدت ضمانت (ورانتی/ گرنتی) بعد از تاریخ اکمال:
مشخصات ضم پیشنهاد می باشد:
یاداشت : هرگاه شرکت میخواهند انصراف کند باید از تاریخ استعلام نرخگیری الی دو یوم انصراف خود را بطور رسمی ارایه نماید. **شرکت برنده مکلف است که بعد از برنده شدن باید جنس را در ظرف یک هفته ارایه نماید.**

مشخصات تخنیکی اجناس

مشخصات	اقلام	شماره
		آدرس مشخص شرکت: **ایمیل آدرس شــــرکت:**

شماره	اقلام	مشخصات
	اسم تهیه/ ارائه کننده:	مهر تهیه/ارائه کننده
	اسم شخص یا نماینده با صلاحیت تهیه/ارائه کننده:	
	امضای شخص یا نماینده تهیه/ارائه کننده:	
	تاریخ:	
	شماره تیلفون حتمی:	

یادداشت: فرمایش گیرنده کاپی رهنمود، ساخت و مودل، بروشور و یا فهرست تجهیزات یا خدماتی را که اکمال   می نماید   ضمیمه نماید.   معلومات فوق جهت ارزیابی مؤثر آفرها استفاده می گردد.

شرایط تدارک و پرداخت

شرایط ذیل صرف با موافقه تحریری فرمایش دهنده قابل تغییر می باشد.

(1) تهیه کننده مکلف به پرداخت تأمینات و تضمینات می باشد ، تامینات از سر جمع پول 5 الی 15 فیصد اخذ میگردد و بعد از تکمیل وارنتی به اکانت شرکت انتقال میگردد.

(2) بعد از اکمال خدمات غیر مشورتی/ تهیه اجناس، تهیه/ارائه کننده باید نسخه اصلی و (2) کاپی بل (Invoice) را به فرمایش دهنده تسلیم نماید؛

(3) پرداخت توسط فرمایش دهنده، طی مدت (30) روز کاری درمقابل مقدار واقعی اجناس/خدمات غیر مشورتی تهیه شده صورت می گیرد.

(4) فرمایش دهنده میتواند در حالات ذیل با ارسال اطلاعیه کتبی به تهیه/ارائه کننده، امرخریداری را کاملاً یا قسماً فسخ نماید:

1- تهیه/ارائه کننده موفق به تحویل بخش یا تمام اجناس درظرف مدت معینه در امرخریداری نشود؛

2- تهیه /ارائه کننده موفق به اجرای مکلفیت های دیگر تحت امر خریداری نشود.

3- هرگاه در اجناس اکمال شده یا خدمات ارائه شده نواقص و یا کاستی ها مشاهده گردد، تهیه/ارائه کننده مکلف به رفع نواقص و کاستی ها در مدت (3) روز کاری بعد از دریافت اطلاعیه در مورد می باشد، در غیر آن فرمایش دهنده می تواند امر خریداری را فسخ نماید.

4- هرگاه تهیه/ارائه کننده، در جریان داوطلبی و یا حین اجرای وظایف محوله تحت امر خریداری اقدام به فساد و تقلب نموده باشد.

(5) هرگاه در درخواست نرخ گیری میعاد ضمانت (وارنتی/ گرنتی) تصریح گردیده باشد، تهیه/ارائه کننده مکلف به تعویض در طول مدت معینه می باشد.

اصلاح اشتباهات محاسبوی

(1) اشتباهات محاسبوی طور ذیل تصحیح می گردد:

1- درصورت تفاوت میان مبلغ به ارقام و حروف، مبلغ به حروف قابل اعتبار می باشد؛

2- درصورتیکه تفاوت میان قیمت فی واحد و قیمت مجموعی وجود داشته باشد، قیمت فی واحد برای ارزیابی قیمت ها و ترتیب امر خریداری قابل اعتبار می باشد؛

3- درصورت موجودیت تفاوت میان نرخ فی واحد و قیمت مجموعی (حاصل ضرب مقدار در نرخ فی واحد)، نرخ فی واحد قابل اعتبار می باشد، هرگاه از نظر فرمایش دهنده اشتباه در نقاط اعشاری در قیمت فی واحد برجسته باشد، دراین صورت قیمت مجموعی اقلام طوریکه نرخ داده شده است قابل اعتبار بوده و قیمت فی واحد باید اصلاح شود.

4- فرمایش دهنده مطابق مندرجات فوق اشتباهات محاسبوی را اصلاح و بعد از اخذ موافقه کتبی داوطلب در قیمت مجموعی آفر محاسبه می نماید.

5- داوطلب مکلف به پذیرش اشتباهات محاسبوی در آفر خویش می باشد. در صورت عدم پذیرش اشتباهات محاسبوی توسط داوطلب، آفر وی رد می گردد.

Capacity Building Program

This program is the first cycle of an ongoing capacity building program for Billing department employees:

Course Title	Start Date	End date	Internal Exam Date
Red Hat System Administration II (RH134)	19-08-2023	19-10-2023	21-10-2023
Oracle Database SQL Certified Associate	19-08-2023	19-10-2023	21-10-2023

Red Hat System Administration II (RH134) outline

The Red Hat System Administration II (RH134) course is part of Red Hat's official training program for system administrators who work with Red Hat Enterprise Linux. The course builds upon the concepts covered in the RH124 (Red Hat System Administration I) course and focuses on more advanced system administration tasks. Here is a general outline of the course content:

Module 1: Automating Installation with Kickstart

- Creating and using Kickstart files to automate installations.

- Performing unattended installations using Kickstart.

Module 2: Using Regular Expressions with grep

- Understanding regular expressions.

- Using grep to search for patterns in text.

Module 3: Creating and Editing Text Files with vim

- Understanding the vim text editor.

- Creating, editing, and saving text files using vim.

Module 4: Scheduling Future Linux Tasks

- Using the **at** and **cron** utilities to schedule one-time and recurring tasks.

- Managing scheduled tasks.

Module 5: Managing Priority of Linux Processes

- Understanding process priority and nice values.

- Using the **nice** and **renice** commands to control process priorities.

Module 6: Controlling Access to Files with Access Control Lists (ACLs)

- Understanding traditional Unix permissions and limitations.

- Implementing ACLs to provide more fine-grained control over file access.

Module 7: Managing SELinux Security

- Understanding SELinux concepts.

- Managing SELinux policies and contexts.

Module 8: Connecting to Network-Defined Users and Groups

- Using Network Information Service (NIS) to manage users and groups across a network.

- Implementing LDAP authentication.

Module 9: Adding Disks, Partitions, and File Systems to a Linux System

- Managing disks, partitions, and filesystems.

- Creating and resizing partitions using **fdisk** and **parted**.

Module 10: Managing Logical Volume Management (LVM) Storage

- Understanding LVM concepts.

- Creating, resizing, and managing logical volumes.

Module 11: Accessing Network Attached Storage with Network File System (NFS)

- Configuring NFS to share files and directories over the network.

- Mounting NFS shares on client systems.

Module 12: Accessing Network Storage with SMB

- Configuring Samba to share files with Windows systems.

- Mounting SMB shares on Linux clients.

Module 13: Controlling and Troubleshooting the Red Hat Enterprise Linux Boot Process

- Managing GRUB bootloader configurations.

- Troubleshooting boot-related issues.

Oracle Database SQL Certified Associate outline:

The Oracle Database SQL Certified Associate certification is designed to validate your skills and knowledge in using SQL (Structured Query Language) to work with Oracle databases effectively. This certification is a great starting point for individuals who want to demonstrate their expertise in using SQL to manage and query Oracle databases. Please note that details might have changed since my last update in September 2021, so make sure to visit the official Oracle certification website for the most up-to-date information. Here's a general overview of the certification:

Exam Information:

- **Exam Code:** 1Z0-071

- **Exam Name:** Oracle Database SQL

Exam Topics: The exam covers a range of topics related to SQL and Oracle database concepts. Here's a general breakdown of the topics you can expect to encounter on the exam:

1. **SQL SELECT Statements:**

   - Retrieve data from one or more tables using SELECT statements.

   - Use various types of SELECT statements to query data.

2. **SQL Sorting and Filtering:**

   - Sort and order the result set.

   - Filter data using WHERE clauses.

3. **Single-Row Functions:**

   - Use various single-row functions to modify and manipulate data.

   - Utilize string, numeric, and date functions.

4. **Conversion Functions and Conditional Expressions:**

   - Convert data types using conversion functions.

   - Implement conditional expressions using CASE statements.

5. **Reporting Aggregated Data Using the Group Functions:**

   - Use group functions to summarize data.

   - Apply the GROUP BY clause to group data.

6. **Displaying Data from Multiple Tables:**

   - Write queries involving multiple tables using JOIN operations.

   - Combine result sets using set operators.

7. **Using Subqueries to Solve Queries:**

   - Write queries using subqueries.

   - Utilize single-row and multiple-row subqueries.

8. **Using the SET Operators:**

   - Perform set operations (UNION, UNION ALL, INTERSECT, MINUS).

9. **Manipulating Data:**

- Insert, update, and delete data using DML statements.

- Control transactions using COMMIT and ROLLBACK.

10. **Using DDL Statements to Create and Manage Tables:**

    - Create, modify, and drop tables using DDL statements.

11. **Managing Schema Objects:**

    - Create, modify, and drop schema objects.

    - Manage constraints and indexes.

12. **Managing Data in Different Time Zones:**

    - Understand and work with data in different time zones.

13. **Retrieving Data Using Subqueries and Reporting Aggregated Data:**

    - Combine subqueries and group functions to retrieve specific data.

The Red Hat System Administration II (RH134) course is part of Red Hat's official training program for system administrators who work with Red Hat Enterprise Linux. The course builds upon the concepts covered in the RH124 (Red Hat System Administration I) course and focuses on more advanced system administration tasks. Here is a general outline of the course content:

RED HAT PART-1:

Module 1: Automating Installation with Kickstart

- Creating and using Kickstart files to automate installations.
- Performing unattended installations using Kickstart.

Module 2: Using Regular Expressions with grep

- Understanding regular expressions.
- Using grep to search for patterns in text.

Module 3: Creating and Editing Text Files with vim

- Understanding the vim text editor.
- Creating, editing, and saving text files using vim.

Module 4: Scheduling Future Linux Tasks

- Using the **at** and **cron** utilities to schedule one-time and recurring tasks.
- Managing scheduled tasks.

Module 5: Managing Priority of Linux Processes

- Understanding process priority and nice values.
- Using the **nice** and **renice** commands to control process priorities.

Module 6: Controlling Access to Files with Access Control Lists (ACLs)

- Understanding traditional Unix permissions and limitations.
- Implementing ACLs to provide more fine-grained control over file access.

Module 7: Managing SELinux Security

- Understanding SELinux concepts.
- Managing SELinux policies and contexts.

Module 8: Connecting to Network-Defined Users and Groups

- Using Network Information Service (NIS) to manage users and groups across a network.
- Implementing LDAP authentication.

Module 9: Adding Disks, Partitions, and File Systems to a Linux System

- Managing disks, partitions, and filesystems.
- Creating and resizing partitions using **fdisk** and **parted**.

Module 10: Managing Logical Volume Management (LVM) Storage

- Understanding LVM concepts.
- Creating, resizing, and managing logical volumes.

Module 11: Accessing Network Attached Storage with Network File System (NFS)

- Configuring NFS to share files and directories over the network.
- Mounting NFS shares on client systems.

Module 12: Accessing Network Storage with SMB

- Configuring Samba to share files with Windows systems.
- Mounting SMB shares on Linux clients.

Module 13: Controlling and Troubleshooting the Red Hat Enterprise Linux Boot Process

- Managing GRUB bootloader configurations.
- Troubleshooting boot-related issues.

RED HAT PART-2:

Linux Red Hat Certified Engineer (RHCE - EX294)

- Benefits and Key Terms of Ansible
- How Ansible Automation Works
- Lab Design
- Install Oracle VirtualBox and Setup Ansible Node on Linux
- Option 2 - Install Linux on AWS Cloud
- Additional Ansible Clients
- Install Ansible Automation
- Ansible Configuration File
- YAML File Syntax and Example
- Writing First Ansible Playbook
- Output Playbook
- Creating Multiple Tasks playbook
- Install and Start a Service from a Playbook
- Hosts File Syntax
- Setup Connection to Remote Clients
- Remote Clients Connectivity Status
- Copy Files to Remote Clients
- Change File Permissions
- Check File or Directory Status
- Create Dir/File and Remove File

- Create a File and Add Text
- Setup Apache and Open Firewall Port
- Run Shell Scripts on Remote Clients
- Schedule a job (crontab)
- Download Package from a URL
- Create and Mount New Storage
- User Account Management
- Add or Update User Password
- Kill a Running Process
- Pick and Choose Steps
- Ansible Ad-Hoc Commands
- Handlers
- Conditions
- Loops
- Ansible Roles
- Roles by Application
- Roles on Ansible Galaxy
- Tags
- Variables
- Variables in Inventory File
- Ansible Vault
- Encrypt Strings within a Playbook
- Other Automation tools
- Free source Ansible and Red Hat Ansible
- Ansible AWX and Tower
- Ansible Additional Commands
- Documentation and Community Help

The Oracle Database SQL Certified Associate certification is designed to validate your skills and knowledge in using SQL (Structured Query Language) to work with Oracle databases effectively. This certification is a great starting point for individuals who want to demonstrate their expertise in using SQL to manage and query Oracle databases. Please note that details might have changed since my last update in September 2021, so make sure to visit the official Oracle certification website for the most up-to-date information. Here's a general overview of the certification:

Exam Information:

- **Exam Code:** 1Z0-071
- **Exam Name:** Oracle Database SQL

Exam Topics: The exam covers a range of topics related to SQL and Oracle database concepts. Here's a general breakdown of the topics you can expect to encounter on the exam:

1. **SQL SELECT Statements:**
   - Retrieve data from one or more tables using SELECT statements.

- Use various types of SELECT statements to query data.

2. **SQL Sorting and Filtering:**
   - Sort and order the result set.
   - Filter data using WHERE clauses.

3. **Single-Row Functions:**
   - Use various single-row functions to modify and manipulate data.
   - Utilize string, numeric, and date functions.

4. **Conversion Functions and Conditional Expressions:**
   - Convert data types using conversion functions.
   - Implement conditional expressions using CASE statements.

5. **Reporting Aggregated Data Using the Group Functions:**
   - Use group functions to summarize data.
   - Apply the GROUP BY clause to group data.

6. **Displaying Data from Multiple Tables:**
   - Write queries involving multiple tables using JOIN operations.
   - Combine result sets using set operators.

7. **Using Subqueries to Solve Queries:**
   - Write queries using subqueries.
   - Utilize single-row and multiple-row subqueries.

8. **Using the SET Operators:**
   - Perform set operations (UNION, UNION ALL, INTERSECT, MINUS).

9. **Manipulating Data:**
   - Insert, update, and delete data using DML statements.
   - Control transactions using COMMIT and ROLLBACK.

10. **Using DDL Statements to Create and Manage Tables:**
    - Create, modify, and drop tables using DDL statements.

11. **Managing Schema Objects:**
    - Create, modify, and drop schema objects.
    - Manage constraints and indexes.

12. Managing Data in Different Time Zones:

- Understand and work with data in different time zones.

13. Retrieving Data Using Subqueries and Reporting Aggregated Data:

- Combine subqueries and group functions to retrieve specific data.

Implementing Cisco Network Security Exam (210-260)

Exam Description: The Implementing Cisco Network Security (IINS) exam (210-260) is a 90-minute assessment with 60–70 questions. This exam tests the candidate's knowledge of secure network infrastructure, understanding core security concepts, managing secure access, VPN encryption, firewalls, intrusion prevention, web and email content security, and endpoint security. This exam validates skills for installation, troubleshooting, and monitoring of a secure network to maintain integrity, confidentiality, and availability of data and devices. This exam also shows competency in the technologies that Cisco uses in its security infrastructure. Candidates can prepare for this exam by taking the Implementing Cisco Network Security (IINS) course.

The following topics are general guidelines for the content likely to be included on the exam. However, other related topics may also appear on any specific delivery of the exam. In order to better reflect the contents of the exam and for clarity purposes, the guidelines below may change at any time without notice.

12%	**1.0**	**Security Concepts**
	1.1	Common security principles
		1.1.a Describe confidentiality, integrity, availability (CIA)
		1.1.b Describe SIEM technology
		1.1.c Identify common security terms
		1.1.d Identify common network security zones
	1.2	Common security threats
		1.2.a Identify common network attacks
		1.2.b Describe social engineering
		1.2.c Identify malware
		1.2.d Classify the vectors of data loss/exfiltration

14% **2.0** **Secure Access**

2.1 Secure management

2.1.a Compare in-band and out-of band
2.1.b Configure secure network management
2.1.c Configure and verify secure access through SNMP v3 using an ACL
2.1.d Configure and verify security for NTP
2.1.e Use SCP for file transfer

2.2 AAA concepts

2.2.a Describe RADIUS and TACACS+ technologies
2.2.b Configure administrative access on a Cisco router using TACACS+
2.2.c Verify connectivity on a Cisco router to a TACACS+ server
2.2.d Explain the integration of Active Directory with AAA
2.2.e Describe authentication and authorization using ACS and ISE

2.3 802.1X authentication

2.3.a Identify the functions 802.1X components

2.4 BYOD

2.4.a Describe the BYOD architecture framework
2.4.b Describe the function of mobile device management (MDM)

17% **3.0** **VPN**

3.1 VPN concepts

3.1.a Describe IPsec protocols and delivery modes (IKE, ESP, AH, tunnel mode, transport mode)
3.1.b Describe hairpinning, split tunneling, always-on, NAT traversal

3.2 Remote access VPN

3.2.a Implement basic clientless SSL VPN using ASDM
3.2.b Verify clientless connection
3.2.c Implement basic AnyConnect SSL VPN using ASDM
3.2.d Verify AnyConnect connection
3.2.e Identify endpoint posture assessment

3.3 Site-to-site VPN

3.3.a Implement an IPsec site-to-site VPN with pre-shared key authentication on Cisco routers and ASA firewalls
3.3.b Verify an IPsec site-to-site VPN

18% **4.0** **Secure Routing and Switching**

4.1 Security on Cisco routers

4.1.a Configure multiple privilege levels
4.1.b Configure Cisco IOS role-based CLI access
4.1.c Implement Cisco IOS resilient configuration

4.2 Securing routing protocols

4.2.a Implement routing update authentication on OSPF

4.3   Securing the control plane
        4.3.a   Explain the function of control plane policing

4.4   Common Layer 2 attacks
        4.4.a   Describe STP attacks
        4.4.b   Describe ARP spoofing
        4.4.c   Describe MAC spoofing
        4.4.d   Describe CAM table (MAC address table) overflows
        4.4.e   Describe CDP/LLDP reconnaissance
        4.4.f   Describe VLAN hopping
        4.4.g   Describe DHCP spoofing

4.5   Mitigation procedures
        4.5.a   Implement DHCP snooping
        4.5.b   Implement Dynamic ARP Inspection
        4.5.c   Implement port security
        4.5.d   Describe BPDU guard, root guard, loop guard
        4.5.e   Verify mitigation procedures

4.6   VLAN security
        4.6.a   Describe the security implications of a PVLAN
        4.6.b   Describe the security implications of a native VLAN

18% 5.0   Cisco Firewall Technologies
        5.1   Describe operational strengths and weaknesses of the different firewall technologies
        5.1.a   Proxy firewalls
        5.1.b   Application firewall
        5.1.c   Personal firewall

        5.2   Compare stateful vs. stateless firewalls
        5.2.a   Operations
        5.2.b   Function of the state table

        5.3   Implement NAT on Cisco ASA 9.x
        5.3.a   Static
        5.3.b   Dynamic
        5.3.c   PAT
        5.3.d   Policy NAT
        5.3 e   Verify NAT operations

        5.4   Implement zone-based firewall
        5.4.a   Zone to zone
        5.4.b   Self zone

        5.5   Firewall features on the Cisco Adaptive Security Appliance (ASA) 9.x
        5.5.a   Configure ASA access management
        5.5.b   Configure security access policies

5.5.c	Configure Cisco ASA interface security levels
5.5.d	Configure default Cisco Modular Policy Framework (MPF)
5.5.e	Describe modes of deployment (routed firewall, transparent firewall)
5.5.f	Describe methods of implementing high availability
5.5.g	Describe security contexts
5.5.h	Describe firewall services

9%   **6.0**   **IPS**

6.1	Describe IPS deployment considerations
6.1.a	Network-based IPS vs. host-based IPS
6.1.b	Modes of deployment (inline, promiscuous - SPAN, tap)
6.1.c	Placement (positioning of the IPS within the network)
6.1.d	False positives, false negatives, true positives, true negatives

6.2	Describe IPS technologies
6.2.a	Rules/signatures
6.2.b	Detection/signature engines
6.2.c	Trigger actions/responses (drop, reset, block, alert, monitor/log, shun)
6.2.d	Blacklist (static and dynamic)

12%   **7.0**   **Content and Endpoint Security**

| 7.1 | Describe mitigation technology for email-based threats |
| 7.1.a | SPAM filtering, anti-malware filtering, DLP, blacklisting, email encryption |

7.2	Describe mitigation technology for web-based threats
7.2.a	Local and cloud-based web proxies
7.2.b	Blacklisting, URL filtering, malware scanning, URL categorization, web application filtering, TLS/SSL decryption

7.3	Describe mitigation technology for endpoint threats
7.3.a	Anti-virus/anti-malware
7.3.b	Personal firewall/HIPS
7.3.c	Hardware/software encryption of local data

CISCO.

Implementing Cisco Enterprise Advanced Routing and Services v1.0 (300-410)

Exam Description: Implementing Cisco Enterprise Advanced Routing and Services v1.0 (ENARSI 300-410) is a 90-minute exam associated with the CCNP Enterprise Certification. This exam certifies a candidate's knowledge for implementation and troubleshooting of advanced routing technologies and services including Layer 3, VPN services, infrastructure security, infrastructure services, and infrastructure automation. The course, Implementing Cisco Enterprise Advanced Routing and Services, helps candidates to prepare for this exam.

The following topics are general guidelines for the content likely to be included on the exam. However, other related topics may also appear on any specific delivery of the exam. To better reflect the contents of the exam and for clarity purposes, the guidelines below may change at any time without notice.

35%	1.0	Layer 3 Technologies

1.1 Troubleshoot administrative distance (all routing protocols)

1.2 Troubleshoot route map for any routing protocol (attributes, tagging, filtering)

1.3 Troubleshoot loop prevention mechanisms (filtering, tagging, split horizon, route poisoning)

1.4 Troubleshoot redistribution between any routing protocols or routing sources

1.5 Troubleshoot manual and auto-summarization with any routing protocol

1.6 Configure and verify policy-based routing

1.7 Configure and verify VRF-Lite

1.8 Describe Bidirectional Forwarding Detection

1.9 Troubleshoot EIGRP (classic and named mode)

    1.9.a Address families (IPv4, IPv6)

    1.9.b Neighbor relationship and authentication

    1.9.c Loop-free path selections (RD, FD, FC, successor, feasible successor, stuck in active)

    1.9.d Stubs

    1.9.e Load balancing (equal and unequal cost)

    1.9.f Metrics

1.10 Troubleshoot OSPF (v2/v3)

    1.10.a Address families (IPv4, IPv6)

    1.10.b Neighbor relationship and authentication

    1.10.c Network types, area types, and router types

        1.10.c (i) Point-to-point, multipoint, broadcast, nonbroadcast

        1.10.c (ii) Area type: backbone, normal, transit, stub, NSSA, totally stub

        1.10.c (iii) Internal router, backbone router, ABR, ASBR

        1.10.c (iv) Virtual link

    1.10.d Path preference

1.11 Troubleshoot BGP (Internal and External)

1.11.a   Address families (IPv4, IPv6)
1.11.b   Neighbor relationship and authentication (next-hop, mulithop, 4-byte AS, private AS, route refresh, synchronization, operation, peer group, states and timers)
1.11.c   Path preference (attributes and best-path)
1.11.d   Route reflector (excluding multiple route reflectors, confederations, dynamic peer)
1.11.e   Policies (inbound/outbound filtering, path manipulation)

20%   2.0   VPN Technologies

2.1   Describe MPLS operations (LSR, LDP, label switching, LSP)
2.2   Describe MPLS Layer 3 VPN
2.3   Configure and verify DMVPN (single hub)
2.3.a   GRE/mGRE
2.3.b   NHRP
2.3.c   IPsec
2.3.d   Dynamic neighbor
2.3.e   Spoke-to-spoke

20%   3.0   Infrastructure Security

3.1   Troubleshoot device security using IOS AAA (TACACS+, RADIUS, local database)
3.2   Troubleshoot router security features
3.2.a   IPv4 access control lists (standard, extended, time-based)
3.2.b   IPv6 traffic filter
3.2.c   Unicast reverse path forwarding (uRPF)
3.3   Troubleshoot control plane policing (CoPP) (Telnet, SSH, HTTP(S), SNMP, EIGRP, OSPF, BGP)
3.4   Describe IPv6 First Hop security features (RA guard, DHCP guard, binding table, ND inspection/snooping, source guard)

25%   4.0   Infrastructure Services

4.1   Troubleshoot device management
4.1.a   Console and VTY
4.1.b   Telnet, HTTP, HTTPS, SSH, SCP
4.1.c   (T)FTP
4.2   Troubleshoot SNMP (v2c, v3)
4.3   Troubleshoot network problems using logging (local, syslog, debugs, conditional debugs, timestamps)
4.4   Troubleshoot IPv4 and IPv6 DHCP (DHCP client, IOS DHCP server, DHCP relay, DHCP options)
4.5   Troubleshoot network performance issues using IP SLA (jitter, tracking objects, delay, connectivity)
4.6   Troubleshoot NetFlow (v5, v9, flexible NetFlow)
4.7   Troubleshoot network problems using Cisco DNA Center assurance (connectivity, monitoring, device health, network health)