CONCORSO PUBBLICO, PER ESAMI, A N. 1 POSTO DI CATEGORIA C, POSIZIONE ECONOMICA C1, AREA TECNICA, TECNICO-SCIENTIFICA ED ELABORAZIONE DATI, PER LE ESIGENZE DEL CENTRO DI ATENEO PER I SERVIZI INFORMATIVI (CSI) DELL'UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II (COD. RIF. 2217), INDETTO CON DECRETO DEL DIRETTORE GENERALE N. 766 DEL 21.07.2022 E PUBBLICATO SULLA G.U. IV SERIE SPECIALE N. 67 DEL 23.08.2022

Tracce estratte alla prova orale del 04.11.2022

Traccia 1

l candidato descriva gli aspetti più importanti legati al networking in una rete di ampie dimensioni e con forte distribuzione territoriale con particolare riferimento alla configurazione e gestione degli apparati di rete wireless

l candidato descriva gli aspetti salienti dei sistemi di identità digitale applicati in un contesto organizzativo complesso;

CHAPTER 3

802.1x Authentication

802.1x authentication allows a remote Cisco IOS router to connect authenticated VPN users to a secure network through a VPN tunnel that is up at all times. The Cisco IOS router will authenticate users through a RADIUS server on the secure network.

802.1x authentication is applied to switch ports or Ethernet (routed) ports, but not to both types of interfaces. If 802.1x authentication is applied to an Ethernet port, non-authenticated users can be routed outside the VPN tunnel to the Internet.

802.1x authentication is configured on interfaces by using the LAN wizard. However, before you can enable 802.1x on any interface, AAA must be enabled on your Cisco IOS router. If you attempt to use the LAN wizard before AAA is enabled, a window appears asking if you want to enable AAA. If you choose to enable AAA, then the 802.1x configuration screens will appear as part of the LAN wizard. If you choose to *not* enable AAA, then the 802.1x configuration screens will *not* appear.

LAN Wizard: 802.1x Authentication (Switch Ports)

This window allows you to enable 802.1x authentication on the switch port or ports you selected for configuration using the LAN wizard.

Enable 802.1x Authentication

Check **Enable 802.1x Authentication** to enable 802.1x authentication on the switch port.

Traccia 2

Il candidato illustri e successivamente indichi le differenze che esistono tra lo stack protocollare ISO-OSI e quello TCP-IP

Il candidato descriva gli aspetti legati all'amministrazione dei sistemi operativi client più diffusi, sia on premise che in ambiente cloud, con particolare riferimento al sistema Microsoft Windows

CHAPTER 4

Create Connection Wizards

The Create Connection wizards let you configure LAN and WAN connections for all Cisco SDM-supported interfaces.

Create Connection

This window allows you to create new LAN and WAN connections.

Note You cannot use Cisco SDM to create WAN connections for Cisco 7000 series routers.

Create a New Connection

Choose a connection type to configure on the physical interfaces available on your router. Only interfaces that have not been configured are available. When you click the radio button for a connection type, a use case scenario diagram appears illustrating that type of connection. If all interfaces have been configured, this area of the window is not displayed.

If the router has Asynchronous Transfer Mode (ATM) or serial interfaces, multiple connections can be configured from a single interface because Cisco Router and Security Device Manager II (Cisco SDM) configures subinterfaces for each interface of that type.

Traccia 4

Il candidato descriva in dettaglio la gestione di server: con particolare riferimento alla gestione delle utenze;

Il candidato descriva gli aspetti più importanti legati al networking in una rete di ampie dimensioni e con forte distribuzione territoriale con particolare riferimento alla configurazione e gestione degli apparati di rete wired;

How Do I Configure Dial-on-Demand Routing for My ISDN or Asynchronous Interface?

ISDN BRI and asynchronous connections are dial-up connections, meaning that in order to establish a connection, the router must dial a preconfigured phone number. Because the cost of these types of connections is usually determined by the amount of time that a connection was established, and in the case of an asynchronous connection, that a phone line will be tied up, it is often desirable to configure Dial-on-Demand Routing (DDR) for these connection types.

Cisco SDM can help you configure DDR by:

- Letting you associate a rule (or ACL) with the connection, which causes the router to establish the connection only when it recognizes network traffic that you have identified as interesting with the associated rule.
- Setting idle timeouts, which cause the router to end a connection after a specified amount of time when there is no activity on the connection.
- Enabling multilink PPP, which causes an ISDN BRI connection to use only one of the two B channels unless a specified percentage of bandwidth is exceeded on the first B channel. This has the advantage of saving costs when network traffic is low and the second B channel is not needed, but letting you utilize the full bandwidth of your ISDN BRI connection when needed.

To configure DDR on an existing ISDN BRI or asynchronous connection:

Step 1 Click **Configure** on the Cisco SDM toolbar.

Step 2 Click **Interfaces and Connections** in the left frame.

Step 3 Click the ISDN or asynchronous interface on which you want to configure DDR.

Step 4 Click **Edit**.

The Connection tab appears.

Step 5 Click **Options**.

The Edit Dialer Option dialog box appears.

Step 6 If you want the router to establish the connection only when it recognizes specific IP traffic, click the **Filter traffic based on selected ACL** radio button, and either enter a rule (ACL) number that will identify which IP traffic should cause the router to dial out, or click the **...** button to browse the list of rules and choose the rule that you want to use to identify IP traffic from that list.

Traccia 5

I candidato descriva le caratteristiche della virtualizzazione di una macchina server indicando nello specifico quali sono le caratteristiche principali e le configurazioni da realizzare

Il candidato descriva gli aspetti più importanti legati al networking in una rete di ampie dimensioni e con forte distribuzione territoriale con particolare riferimento agli aspetti legati alla autenticazione degli utenti

CHAPTER 5

Edit Interface/Connection

This window displays the router's interfaces and connections. The window also enables you to add, edit, and delete connections, and to enable or disable connections.

Add

When you choose an unconfigured physical interface and click **Add**, the menu contains choices for adding a connection on that interface. Click **Add** to create a new loopback or tunnel interface. If the Cisco IOS image on the router supports Virtual Template Interfaces (VTI), the context menu contains an option to add a VTI. If there are switch ports present on the router, you can add a new VLAN.

If you want to reconfigure an interface, and see no choices except Loopback and Tunnel when you click **Add**, choose the interface and click **Delete**. All the types of connections available for that kind of interface will appear in the Add menu. Click **Available Interface Configurations** to see what configurations are available for an interface.

Edit

When you choose an interface and click **Edit**, a dialog appears. If the interface is a supported and configured interface and is not a switch port, the dialog will have the following tabs:

- Connection
- Association tab
- NAT tab

Traccia 7

Il candidato descriva le caratteristiche delle reti LAN, WAN e MAN, con particolare riferimento all' Indirizzamento IP e subnetting

Il candidato descriva le principali tecniche di salvaguardia del funzionamento dei sistemi esplicando nel dettaglio le differenze che intercorrono tra HA, business continuity e disaster recovery

QoS

The QoS Status window allows you to monitor the performance of the traffic on QoS configured interfaces (see Associating a QoS Policy With an Interface). This window also allows you to monitor bandwidth utilization and bytes-sent for interfaces with no QoS configuration. Monitoring inbound traffic on QoS interfaces shows the statistics only at a protocol level. Protocol-level statistics for non-QoS interfaces are collected for traffic in both directions.

This window allows you to monitor the following statistics:

- Bandwidth utilization for Cisco SDM defined traffic types
  - Bandwidth utilization per class under each traffic type
  - Bandwidth utilization for protocols under each class

  Bandwidth utilization is shown in Kbps.
- Total incoming and outgoing bytes for each traffic type
  - Incoming and outgoing bytes for each class defined under the traffic type
  - Incoming and outgoing bytes for each protocol for each class

  If the value is more than 1,000,000, then the graph may show the bytes as a multiple of 10^6. If the value is more than 1,000,000,000, then the graph may show the bytes as a multiple of 10^9.
- Packets dropped statistics for each traffic type

Interface—IP/Mask—Slot/Port—Description

This area lists the interfaces with associated QoS policies, their IP addresses and subnet masks, slot/port information if applicable, and available descriptions.

Select the interface that you want to monitor from this list.

View Interval

Select the interval at which statistics should be gathered:

- Now—Statistics are gathered when you click **Start Monitoring**.
- Every 1 minute—Statistics are gathered when you click **Start Monitoring**, and refreshed at 1-minute intervals.