CISCO CCST Networking – Syllabus Esame di Certificazione

La **Certificazione CISCO CCST Networking** convalida le conoscenze e le competenze relative a concetti e argomenti di rete a livello base, per supportare e assistere attività tra cui mostrare il funzionamento delle reti, inclusi i dispositivi, i supporti e i protocolli che consentono le comunicazioni di rete.

La Certificazione **CCST Networking** è un primo passo verso altre Certificazioni CISCO, come ad esempio la Certificazione **CISCO CCNA**.

Saranno a breve rese disponibili risorse gratuite ONLINE per aiutare i Candidati a prepararsi per la Certificazione, al seguente link: https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/entry/ccst-certifications.html?ccid=ccst&dtid=blog&oid=blog-new-entry-level-cisco-certifications-to-start-your-it-career#~ccst-certifications

Per ottenere la Certificazione **CCST Networking** si deve superare il relativo Esame, attualmente disponibile in lingua inglese. L'Esame di Certificazione è di tipo LINEAR, ovvero test a risposta multipla, multi risposta con più risposte valide, elenco, corrispondenza, drag and drop e click map. L'Esame dura circa 50 minuti ed è composto da circa 45 domande.

Gli argomenti dell'Esame di Certificazione **CCST Networking** verificano la conoscenza su sei principali aree di skill sulla sicurezza informatica, che sono le seguenti:

1.0 STANDARD E CONCETTI

2.0 INDIRIZZAMENTO E FORMATI DI SOTTORETE

3.0 ENDPOINT E TIPI DI MEDIA

4.0 INFRASTRUTTURE

5.0 DIAGNOSI DEI PROBLEMI

6.0 SICUREZZA

Syllabus Esame di Certificazione
CISCO CCST Networking

1. STANDARD E CONCETTI

1.1. - Identificare gli elementi costitutivi concettuali fondamentali delle reti.

- Modello TCP/IP, modello OSI, frame e pacchetti, indirizzamento.

1.2. - Differenza tra larghezza di banda e throughput.

- Latenza, ritardo, test di velocità rispetto a Iperf.

1.3. Differenziare tra LAN, WAN, MAN, CAN, PAN e WLAN.

- Identificare e illustrare le topologie comuni di rete fisiche e logiche.

1.4. Confrontare e contrastare applicazioni e servizi cloud e on-premise.

- Pubblico, privato, ibrido, SaaS, PaaS, IaaS, lavoro remoto/lavoro ibrido.

1.5. Descrivere le applicazioni e i protocolli di rete comuni.

- TCP vs. UDP (orientato alla connessione vs. senza connessione), FTP, SFTP, TFTP, HTTP, HTTPS, DHCP, DNS, ICMP, NTP.

2. INDIRIZZAMENTO E FORMATI DI SOTTORETE

2.1. Confrontare e contrastare indirizzi privati e indirizzi pubblici.

- Classi di indirizzi, concetti NAT.

2.2. Identifica gli indirizzi IPv4 e i formati di subnet.

- Concetti di sottorete, calcolatore di sottorete, notazione barra e maschera di sottorete; dominio di trasmissione.

2.3. Identifica gli indirizzi IPv6 e i formati dei prefissi.

- Tipi di indirizzi, concetti di prefisso.

3. ENDPOINT E TIPI DI MEDIA

3.1. Identifica cavi e connettori comunemente usati nelle reti locali.

- Tipi di cavi: fibra, rame, doppino intrecciato; Tipi di connettori: coassiale, RJ-45, RJ-11, fibra.

3.2. Differenziare tra tecnologie di rete Wi-Fi, cellulare e cablata.

- Rame, comprese le fonti di interferenza; fibra; wireless, incluso 802.11 (senza licenza, 2,4 GHz, 5 GHz, 6 GHz), cellulare (con licenza), fonti di interferenza.

3.3. Descrivi i dispositivi endpoint.

- Dispositivi Internet of Things (IoT), computer, dispositivi mobili, telefono IP, stampante, server.

3.4. Dimostrare come configurare e controllare la connettività di rete su Windows, Linux, Mac OS, Android e Apple iOS.

- Utilità di rete su sistemi operativi Windows, Linux, Android e Apple; come eseguire i comandi per la risoluzione dei problemi; impostazioni client wireless (SSID, autenticazione, modalità WPA).

4. INFRASTRUTTURE

4.1. Identifica le spie di stato su un dispositivo Cisco in base alle istruzioni di un tecnico.

- Colore e stato della spia di collegamento (lampeggiante o fissa).

4.2. Utilizzare uno schema di rete fornito da un tecnico per collegare i cavi appropriati.

- Cavi patch, switch e router, piccole topologie, alimentazione, layout rack.

4.3. Identificare le varie porte sui dispositivi di rete.

- Porta console, porta seriale, porta in fibra, porte Ethernet, SFP, porta USB, PoE.

4.4. Spiegare i concetti di routing di base.

- Gateway predefinito, switch di livello 2 e livello 3, rete locale e rete remota.

4.5. Spiegare i concetti di commutazione di base.

- Tabelle di indirizzi MAC, filtraggio indirizzi MAC, VLAN.

5. DIAGNOSI DEI PROBLEMI

5.1. Dimostrare metodologie di risoluzione dei problemi efficaci e best practice dell'help desk, inclusi l'apertura di un ticket, documentazione e raccolta di informazioni.

- Politiche e procedure, documentazione accurata e completa, prioritizzazione.

5.2. Esegui un'acquisizione di pacchetti con Wireshark e salvala in un file.

- Scopo dell'utilizzo di un analizzatore di pacchetti, salvataggio e apertura di un file .pcap.

5.3. Eseguire i comandi diagnostici di base e interpretare i risultati.

- ping, ipconfig/ifconfig/ip, tracert/traceroute, nslookup; riconoscere come i firewall possono influenzare il risultato.

5.4. Differenziare tra diversi modi per accedere e raccogliere dati sui dispositivi di rete.

- Accesso remoto (RDP, SSH, telnet), VPN, emulatori di terminale, Console, Rete, Sistemi di Gestione, rete gestita dal cloud (Meraki), script.

5.5. Esegui comandi show di base su un dispositivo di rete Cisco.

- Show run, show cdp neighbors, show ip interface brief, show ip route, show version, show inventory, show switch, show mac address-table, show interface, mostra interfaccia x, show interface status, livelli di privilegio; guida ai comandi e completamento automatico.

6. SICUREZZA

6.1. Descrivere come operano i firewall per filtrare il traffico.

- Firewall (porte e protocolli bloccati); le regole che negano o consentono l'accesso.

6.2. Descrivere i concetti di sicurezza fondamentali.

- Riservatezza, integrità e disponibilità (CIA); autenticazione, autorizzazione e contabilità (AAA); Autenticazione a più fattori (MFA); crittografia, certificati e complessità della password; archivi/database di identità (Active Directory); minacce e vulnerabilità; spam, phishing, malware e denial of service

6.3. Configurare la sicurezza wireless di base su un router domestico (WPAx).

- WPA, WPA2, WPA3; scegliendo tra Personale e Impresa; concetti di sicurezza del Wi-Fi

Per maggiori informazioni sulle Certificazioni CISCO CCST, contattare TESI Automazione ai seguenti recapiti: https://www.tesiautomazione.it/it_it/contatti o accedere al sito www.tesiautomazione.it

DISCLAIMER - Clausola di Esclusione di Responsabilità

Le informazioni e disposizioni presenti nel presente documento possono essere non esaustive e subire variazioni senza preavviso su indicazioni dei proprietari dei diritti intellettuali, relativamente ai prodotti e servizi trattati.