DECLARAÇÃO

A Fundação de Apoio à Tecnologia, o Centro Paula Souza e a Cisco Networking Academy América Latina declaram que **Bruno Sa Oliveira Arantes**, portador(a) do Cadastro de Pessoa Física Nº 33173164890, participou do curso **CISCO - CCNA1 - PREPARATIVO PARA SEGURANÇA EM REDES,** com 96 horas de duração, no período de 03/10/2022 a 18/12/2022.

São Paulo, 20 de dezembro de 2022.

DocuSigned by:
106230FDCDA747F...
Cesar Silva
Diretor Presidente

DocuSigned by:
B36F118BB8AC4B8...
Emilena Lorenzon Bianco
Vice-diretora Superintendente
Centro Paula Souza

DocuSigned by:
João Carlos Lopes Fernandes
2045D484773740C...
João Carlos Lopes Fernandes
Manager ASC CISCO - CPS

DocuSigned by:
Leandro dos Santos Franco
C5CBB5E893FE44A...
Leandro dos Santos Franco
Coordenador de Ensino Técnico e
Profissionalizante - Secretaria de
Desenvolvimento Econômico

FUNDAÇÃO FAT

CPS Centro Paula Souza — GOVERNO DO ESTADO DE SÃO PAULO

Networking Academy
CISCO.

MINHA CHANCE

SÃO PAULO
GOVERNO DO ESTADO
Secretaria de Desenvolvimento Econômico

Cisco CCNA (92 horas)

O Curso Cisco CCNA apresenta arquiteturas, modelos, protocolos e elementos de rede, te preparando para criar LANs simples, executar configurações básicas para roteadores e switches, implementar esquemas de endereçamento IPv4 e IPv6 e segurança.

1.Fundamentos de Redes

1.1.Explicar funções dos componentes de redes
1.2.Descrever as características de arquitetura de redes
1.3.Comparação de interfaces físicas e tipos de cabeamento
1.4.Identificar problemas de interfaces e cabos (Colisões erros incompatibilidade duplex / velocidade)
1.5.Verificar parâmetros de IP para o SO e Clients (Windows, MAC, Linux e etc...)
1.6.Descrever os princípios de redes sem fio Fundamentos de virtualização (Máquinas virtuais)

2.Descrever Conceitos de Switchs Acesso a Rede

2.1.Configurar e verificar VLANs Configurar e verificar conexões entre switchs
2.2.Configurar e verificar protocolos de descobertas de camada 2 (CDP e LLDP)
2.3.Configurar e verificar EtherChannel (Camada 2 e 3)
2.4.Descrever a necessidade e as operações básicas do spanning tree protocol
2.5.Arquitetura wireless cisco e modos dos Access Points
2.6.Descrever as conexões de infraestrutura física dos componentes WLAN (AP, WLC, portas de acesso / tronco e LAG)
2.7.Descrever conexões de acesso de gerenciamento de AP e WLC (Telnet, SSH, HTTP, HTTPS, console e TACACS + / RADIUS)

3.Conectividade IP

3.1.Interpretar os componentes da tabela de roteamento
3.2.Determinar como um roteador toma uma decisão de encaminhamento por padrão Configurar e verificar o roteamento estático IPv4 e IPv6
3.3.Configurar e verificar OSPFv2 de área única
3.4.Descrever a finalidade do HSRP (protocolo de redundância)

4.Serviços IP

4.1.Configurar e verificar NAT usando configuração estática e pools
4.2.Configurar e verificar NTP operando em modo cliente e servidor
4.3.Explicar a função do DHCP e DNS na rede
4.4.Explicar a função do SNMP nas operações de rede
4.5.Descrever o uso de recursos do syslog, incluindo recursos e níveis
4.6.Configurar e verificar o cliente DHCP e DHCP Relay
4.7.Configurar dispositivos de rede para acesso remoto usando SSH
4.8.Descrever as capacidades e funções do TFTP / FTP na rede

5.Fundamentos de Segurança

5.1.Definir os principais conceitos de segurança (ameaças, vulnerabilidades, explorações e técnicas de mitigação)
5.2.Descrever os elementos do programa de segurança (conscientização do usuário, treinamento e controle de acesso físico)
5.3.Configurar o controle de acesso ao dispositivo usando senhas locais
5.4.Descrever os elementos das políticas de senha de segurança, como gerenciamento, complexidade e alternativas de senha (autenticação multifator, certificados e biometria)
5.5.Descreva o acesso remoto e VPNs site a site
5.6.Configurar e verificar listas de controle de acesso
5.7.Configurar recursos de segurança da Camada 2 (rastreamento de DHCP, inspeção ARP dinâmica e segurança de porta)
5.8.Diferenciar conceitos de autenticação, autorização e contabilidade (Triplo AAA)
5.9.Descrever os protocolos de segurança sem fio (WPA, WPA2 e WPA3)
5.10.Configurar WLAN usando WPA2 PSK usando a interface gráfica

6.Automação e Programação

6.1.Explicação como a automação afeta o gerenciamento de rede
6.2.Comparação de redes tradicionais com rede baseadas em controlador
6.3.Descrever arquiteturas baseadas em controlador e definidas por software (overlay, underlay e fabric)
6.4.Compare o gerenciamento de dispositivo de campus tradicional com o gerenciamento de dispositivo habilitado para Cisco DNA Center
6.5.Descrever as características das APIs baseadas em REST (CRUD, verbos HTTP e codificação de dados)
6.6.Reconhecer as capacidades dos mecanismos de gerenciamento de configuração Puppet, Chef e Ansible
6.7.Interpretar dados codificados JSON

Soft Skill (8 horas)