# Packet Tracer - Skills Integration Challenge

|  |  |
| --- | --- |
| 1.3.1.3 Packet Tracer - Skills Integration Challenge.pka | Connect Console cable from User-01 (RS 232) to ASw-1 (Console)  ASw-1 -> Startup Config  Switch>enable  Switch(config)#copy running-config startup-config  ENTER  ASw-1 -> Banner MOTD  Switch(config)#banner motd "Warning, you must be admin"  ASw-1 -> Console Line -> Password  Switch(config)#line console 0  Switch(config-line)#password xAw6k  Switch(config-line)#exit  ASw-1 -> Enable Secret  Switch(config)#enable secret 6EBUp  ASw-1 -> Host Name  Switch(config)#hostname ASw-1  ASw-1 -> Ports -> Vlan1 -> IP Address/Subnet Mask  Switch#configure terminal  ASw-1(config)#interface vlan 1  ASw-1(config-if)#ip address 10.10.10.100 255.255.255.0  ASw-1 -> Ports -> Vlan1 -> Port Status  Switch(config-if)#no shutdown  Switch(config-if)#exit  ASw-1 -> Service Password Encryption  ASw-1(config)#service password-encryption  ASw-1 -> VTY Lines -> VTY Line 0 -> Password  ASw-1(config)#line vty 0  ASw-1(config-line)#password xAw6k  ASw-1(config-line)#exit  Connect Console cable from User-02 (RS 232) to ASw-2 (Console)  Do all ASw-1 steps (except hostname = ASw-2 and Vlan1 = ip address 10.10.10.150 255.255.255.0)  Open “IP Configuration” for User-01  IP Address: 10.10.10.4  Subnet Mask: 255.255.255.0  Open “IP Configuration” for User-02  IP Address: 10.10.10.5  Subnet Mask: 255.255.255.0 |
| 2.3.1.2 Packet Tracer - Skills Integration Challenge.pka | Click Switch -> CLI  S1 -> Banner MOTD  Switch>enable  Switch#configure terminal  Switch(config)#banner motd "Warning, you must be admin"  S1 -> Console Line -> Password & Login  Switch(config)#line console 0  Switch(config-line)#password cisco  Switch(config-line)#login  Switch(config-line)#exit  S1 -> Enable Secret  Switch(config)#enable secret class  S1 -> Host Name  Switch(config)#hostname S1  S1 -> IP Domain Name  S1(config)#ip domain-name cisco.com  S1 -> Ports -> FastEthernet0/x -> Port Status  S1(config)#interface range FastEthernet0/1-24  S1(config-if-range)#shutdown  S1(config-if-range)#exit  S1 -> Ports -> FastEthernet0/1 & 2 -> Port Security -> Enabled & Port Security Violation  S1(config-if-range)#interface range FastEthernet0/1-2  S1(config-if-range)#switchport mode access  S1(config-if-range)#switchport port-security  S1 -> Ports -> FastEthernet0/1 &2 -> Port Security -> Maximum Static MACs  (config-if-range)#switchport port-security maximum 2  S1 -> Ports -> FastEthernet0/1 & 2 -> Port Security -> Sticky Enabled  S1(config-if-range)#switchport port-security mac-address sticky  S1(config-if-range)#exit  S1 -> Ports -> GigabitEthernet0/1 & 2 -> Port Status  S1(config)#interface range GigabitEthernet0/1-2  S1(config-if-range)#shutdown  S1(config-if-range)#exit  S1 -> Ports -> Vlan 1 -> IP Address & Subnet Mask  S1(config)#interface vlan 1  S1(config-if)#ip address 10.10.10.2 255.255.255.0  S1 -> Ports -> Vlan 1 -> Port Status  S1(config-if)#no shutdown  S1(config-if)#exit  S1 -> Service Password Encryption  (config)# service password-encryption  ---  Generate RSA 768 bits token  S1(config)#crypto key generate rsa  How many bits in the modulus [512]: 768  % Generating 768 bit RSA keys, keys will be non-exportable...[OK]  ---  S1 -> SSH Server -> SSH Version  S1(config)#ip ssh version 2  S1 -> Usernames -> Username (hit “secret password”)  S1(config)#username admin secret ccna  S1 -> VTY Lines -> VTY Line 0 -> Login  S1(config)#line vty 0  S1(config-line)#login local  S1 -> VTY Lines -> VTY Line 0 -> Transport Input  S1(config-line)#transport input ssh  S1(config-line)#exit  Restart only two ports  S1(config)#interface range FastEthernet0/1-2  S1(config-if-range)#no shutdown  Open PC1 and PC2 -> Desktop -> IP Configuration  Set IP Address: 10.10.10.10 or 10.10.10.11  Subnet Mask: 255.255.255.0  Gateway: 10.10.10.1  Open Command Prompt  Ping: 10.10.10.2 (Switch)  Ping 10.10.10.10 (PC1)  Ping 10.10.10.11 (PC2) |
| 2.5.1.2\_Packet\_Tracer\_-\_Configure\_Cisco\_Routers  for\_Syslog,\_NTP,\_and\_SSH\_Operations[1].pka | R1 -> Logging -> Service timestamp log  R1>enable  Password: (ciscoenpa55)  R1#configure terminal  R1(config)#service timestamps log datetime msec  (Check on the Dashboard IP Address of “NTP Server”)  R1 -> NTP Client -> NTP Server Information -> IP  R1(config)#ntp server 192.168.1.5  R1 -> NTP Client -> NTP Server Information -> Update Calendar  R1(config)#ntp update-calendar  (Verify: R1(config)#do show ntp status)  (Verify: R1(config)#do show clock)  R1 -> SYSLOG Client -> Server Addresses  R1(config)#logging host 192.168.1.6  (Verify: R1(config)#do show logging)  Click on “Syslog Server” -> Services -> SYSLOG  Type in R1 -> CLI : R1(config)#exit  Do the same steps in R2 and R3 routers  ---  R3 -> IP Domain Name  R3(config)#ip domain-name ccnasecurity.com  ---  Generate RSA 1024 bits token (see notes)  S1(config)#crypto key generate rsa  How many bits in the modulus [512]: 1024  % Generating 768 bit RSA keys, keys will be non-exportable...[OK]  Verify: R3(config)#do show ip ssh)  ---  R3 -> SSH Server -> SSH Authentication Retries  R3(config)#ip ssh authentication-retries 2  R3 -> SSH Server -> SSH Timeout  R3(config)#ip ssh time-out 90  R3 -> SSH Server -> SSH Version  R3(config)#ip ssh version 2  R3 -> User Names -> Username  (Verify: R3(config)#username SSHadmin privilege ?  <0-15> User privilege level)  R3(config)#username SSHadmin privilege 15 secret ciscosshpa55  R3 -> VTY Lines -> VTY Line 0 to 4 -> Login  R3(config)#line vty 0 4  R3(config-line)#login local  R3 -> VTY Lines -> VTY Line 0 to 4 -> Transport Input  R3(config-line)#transport input ssh  R3(config-line)#exit  Open PC-C -> Desktop -> Command Prompt  C:\>telnet 192.168.3.1  Trying 192.168.3.1 ...Open  [Connection to 192.168.3.1 closed by foreign host]  C:\>ssh -l SSHadmin 192.168.3.1  Password: (ciscosshpa55)  R3#exit |
| 3.3.3.3\_Packet\_Tracer\_-\_Explore\_a\_Network[1].pka | It’s simulator demo from “Sales” PC |
| 3.4.1.2 Skills Integration Challenge.pka | Only S3 CLI is available we use connect console cables.  Open S3 CLI (some conflict Gig0/2 connection, temporary shutdown)  S3>enable  S3#configure terminal  S3(config)#  S3(config)#interface GigabitEthernet0/2  S3(config-if)#shutdown  S3(config-if)#exit  S3 -> Banner MOTD  S3(config)#banner motd "Authorized Access Only!!"  S3 -> Console Line -> Password  S3(config)#line console 0  S3(config-line)#password letmein  S3(config-line)#exit  S3 -> Default Gateway  S3(config)# ip default-gateway 172.31.88.1  S3 -> Enable Secret  S3(config)#enable secret itsasecret  S3 -> Ports -> FastEthernet0/11 -> Access VLAN  S3(config)#interface range FastEthernet0/7-12  S3(config-if-range)#switchport access vlan 10  S3(config-if-range)#exit  S3 -> Ports -> FastEthernet0/18 -> Access VLAN  S3(config)#interface range FastEthernet0/13-20  S3(config-if-range)#switchport access vlan 20  S3(config-if-range)#exit  S3 -> Ports -> FastEthernet0/6 -> Access VLAN  S3(config)#interface range FastEthernet0/1-6  S3(config-if-range)#switchport access vlan 30  S3 -> Ports -> FastEthernet0/6 -> Port Security -> Enabled  S3(config-if-range)#switchport mode access  S3(config-if-range)#switchport port-security  S3 -> Ports -> FastEthernet0/6 -> Port Security -> Maximum Static MACs  (config-if-range)#switchport port-security maximum 2  S3 -> Ports -> FastEthernet0/6 -> Port Security -> Port Security Violation  S3(config-if-range)#switchport port-security violation restrict  S3 -> Ports -> FastEthernet0/6 -> Port Security -> Sticky Enabled  S3(config-if-range)#switchport port-security mac-address sticky  S3(config-if-range)#exit  S3 -> Ports -> FastEthernet0/4 & 0/14 & 0/24 -> Port Status  S3(config)#interface range FastEthernet0/1-24  S3(config-if-range)#shutdown  S3(config-if-range)#exit  Check Dashboard - enable F0/6 & F0/11 & F0/18  S3(config)#interface FastEthernet0/6  S3(config-if)#no shutdown  S3(config-if)#exit  …  S3 -> Ports -> GigabitEthernet0/2 -> Native VLAN  S3(config)#interface GigabitEthernet0/2  S3(config-if)#switchport trunk native vlan 99  S3 -> Ports -> GigabitEthernet0/2 -> Nonegotiate  S3(config-if)# switchport nonegotiate  S3 -> Ports -> GigabitEthernet0/2 -> Port Mode  S3(config-if)#switchport mode trunk  S3 -> Ports -> GigabitEthernet0/2 -> Trunk VLANs -> 10 & 20 & 30 & 88 & 99  S3(config-if)#switchport trunk allowed vlan 10  etc. or  S3(config-if)#switchport trunk allowed vlan all  S3(config-if)#exit  S3 -> Ports -> Vlan88 -> Port Status  S3(config)#interface vlan 88  S3(config-if)#no shutdown  S3 -> Ports -> Vlan88 -> IP Address / Subnet Mask  S3(config-if)#ip address 172.31.88.4 255.255.255.0  S3(config-if)#exit  S3 -> Service Password Encryption  (config)# service password-encryption  S3 -> VLANS -> VLAN 10 -> VLAN Name  S3(config)#vlan 10  S3(config-vlan)#name Sales  S3(config-vlan)#exit  (Assign name for other VLANs)  S3 -> VTY Lines -> VTY Line 0 -> Password  S3(config)#line vty 0  S3(config-line)#password c1$c0  S3(config-line)#exit  Restart GigabitEthernet0/2  S3(config)#interface GigabitEthernet0/2  S3(config-if)#no shutdown |
| 3.6.1.2\_Packet\_Tracer\_-\_Configure\_AAA\_Authentication\_on\_Cisco\_Routers[1].pka  A close up of text on a white background  Description automatically generated | R1 -> AAA -> New-model  R1>enable  Password: (ciscoenpa55)  R1#configure terminal  R1(config)#aaa new-model  R1 -> AAA -> Authentication -> Authen Command 1  R1(config)#aaa authentication login TELNET-LOGIN local  R1 -> AAA -> Authentication -> Authen Command 2  R1(config)#aaa authentication login default local  R1 -> Console Line -> AAA Method List Name  R1(config-line)#line console 0  R1(config-line)#login authentication default  R1(config-line)#exit  R1 -> User Names -> Username  username Admin1 secret admin1pa55  R1 -> VTY Lines -> VTY Line 0 to 4 -> AAA Method List Name  R1(config)#line vty 0 4  R1(config-line)#login authentication TELNET-LOGIN  R1(config-line)#exit  Router R2  R2 -> AAA -> New-model  R2>enable  Password: (ciscoenpa55)  R2#configure terminal  R2(config)#aaa new-model  R2 -> AAA -> Authentication -> Authen Command 1  R2(config)#aaa authentication login default group tacacs+ local  R2 -> Console Line -> AAA Method List Name  R2(config-line)#login authentication default  R2(config-line)#exit  R2 -> TACACS Client -> TACAS Server Hosts -> 0  tacacs-server host 192.168.2.2  R2 -> TACACS Client -> TACAS server key  R2(config)#tacacs-server key tacacspa55  R2 -> User Names -> Username  R2(config)#username Admin2 secret admin2pa55  Router R3  R3 -> AAA -> New-model  R3>enable  Password: (ciscoenpa55)  R3#configure terminal  R3(config)#aaa new-model  R3 -> AAA -> Authentication -> Authen Command 1  R3(config)#aaa authentication login default group radius local  R3 -> Console Line -> AAA Method List Name  R3(config-line)#login authentication default  R3(config-line)#exit  R3 -> RADIUS Client -> RADIUS Server Hosts -> 0  R3(config)#radius-server host 192.168.3.2  R3 -> RADIUS Client -> RADIUS server key  R3(config)# radius-server key radiuspa55  R3 -> User Names -> Username  R3(config)#username Admin3 secret admin3pa55 |
| 5.4.1.2 Packet Tracer - Skills Integration Challenge.pka  A screenshot of a cell phone  Description automatically generated | R1(config)#interface G0/0  R1(config-if)#ip address 172.17.25.2 255.255.255.252  R1(config-if)#no shutdown  R1(config-if)#exit  R1 -> Ports -> GigabitEthernet0/1.10 -> 802.1Q -> VLAN ID  R1(config-if)#interface G0/1.10  R1(config-subif)#encapsulation dot1Q 10  R1 -> Ports -> GigabitEthernet0/1.10 -> 802.1Q -> IP Address & Subnet Mask  R1(config-subif)#ip address 172.17.10.1 255.255.255.0  R1(config-subif)#exit  R1 -> Ports -> GigabitEthernet0/1.20 -> 802.1Q -> VLAN ID  R1(config-if)#interface G0/1.20  R1(config-subif)#encapsulation dot1Q 20  R1 -> Ports -> GigabitEthernet0/1.20 -> 802.1Q -> IP Address & Subnet Mask  R1(config-subif)#ip address 172.17.20.1 255.255.255.0  R1(config-subif)#exit  R1 -> Ports -> GigabitEthernet0/1.30 -> 802.1Q -> VLAN ID  R1(config-if)#interface G0/1.30  R1(config-subif)#encapsulation dot1Q 30  R1 -> Ports -> GigabitEthernet0/1.30 -> 802.1Q -> IP Address & Subnet Mask  R1(config-subif)#ip address 172.17.30.1 255.255.255.0  R1(config-subif)#exit  R1 -> Ports -> GigabitEthernet0/1.88 -> 802.1Q -> VLAN ID  R1(config-if)#interface G0/1.88  R1(config-subif)#encapsulation dot1Q 88  R1 -> Ports -> GigabitEthernet0/1.88 -> 802.1Q -> IP Address & Subnet Mask  R1(config-subif)#ip address 172.17.88.1 255.255.255.0  R1(config-subif)#exit  R1 -> Ports -> GigabitEthernet0/1.99 -> 802.1Q -> VLAN ID  R1(config-if)#interface G0/1.99  R1(config-subif)#encapsulation dot1Q 99  R1 -> Ports -> GigabitEthernet0/1.99 -> 802.1Q -> IP Address & Subnet Mask  R1(config-subif)#ip address 172.17.99.1 255.255.255.0  R1(config-subif)#exit  R1 -> Ports -> GigabitEthernet0/1 -> Port Status  R1(config-subif)#interface G0/1  R1(config-if)#no shutdown  Switch S1  S1 -> Default Gateway  S1>enable  S1#configure terminal  S1(config)#ip default-gateway 172.17.99.1  S1 -> Ports -> FastEthernet0/10 -> Access VLAN  S1(config)#interface range F0/6-10  S1(config-if-range)#switchport mode access  S1(config-if-range)#switchport access vlan 30  S1(config-if-range)#exit  S1 -> Ports -> FastEthernet0/11 -> Access VLAN  S1(config)#interface range F0/11-17  S1(config-if-range)#switchport mode access  S1(config-if-range)#switchport access vlan 10  S1(config-if-range)#exit  S1 -> Ports -> FastEthernet0/18 -> Access VLAN  S1(config)#interface range F0/18-24  S1(config-if-range)#switchport mode access  S1(config-if-range)#switchport access vlan 20  S1(config-if-range)#exit  S1 -> Vlan99 -> Post Status  S1(config)#interface vlan 99  S1 -> Vlan99 -> IP Address & Subnet Mask  S1(config-if)#ip address 172.17.99.10 255.255.255.0  S1(config-if)#exit  S1 -> VLANS -> VLAN 10 -> VLAN Name  S1(config)#vlan 10  S1(config-vlan)#name Faculty/Staff  S1 -> VLANS -> VLAN 20 -> VLAN Name  S1(config)#vlan 20  S1(config-vlan)#name Students  S1 -> VLANS -> VLAN 30 -> VLAN Name  S1(config)#vlan 30  S1(config-vlan)#name Guest(Default)  S1(config-vlan)#exit  S1 -> VLANS -> VLAN 88 -> VLAN Name  S1(config)#vlan 88  S1(config-vlan)#name Native  S1(config-vlan)#exit  S1 -> VLANS -> VLAN 99 -> VLAN Name  S1(config)#vlan 99  S1(config-vlan)#name Management  S1(config-vlan)#exit  S1 -> Ports -> GigabitEthernet0/1  S1(config)#interface G0/1  S1(config-if)#switchport trunk native vlan 88  S1(config-if)#exit  Additional Requirements to shutdown all not assigned ports  S1(config)#ip default-gateway 172.17.99.1  S1(config)#interface range F0/1-5, G0/2  S1(config-if-range)#shutdown  S1(config-if-range)#exit |
| 6.6.1.2 Packet Tracer - Skills Integration Challenge.pka  A close up of text on a white background  Description automatically generated | HQ -> Routes -> Static Routes -> Route0  HQ>enable  HQ# configure terminal  HQ(config)#ip route 172.31.10.0 255.255.255.0 S0/0/0  HQ -> Routes -> Static Routes -> Route1  HQ(config)#ip route 172.31.20.0 255.255.255.0 S0/0/0  HQ -> Routes -> Static Routes -> Route2  HQ(config)#ip route 172.31.30.0 255.255.255.0 S0/0/0  HQ -> Routes -> Static Routes -> Route3  HQ(config)#ip route 172.31.88.0 255.255.255.0 S0/0/0  HQ -> Routes -> Static Routes -> Route4  HQ(config)#ip route 209.165.200.0 255.255.255.224 Serial0/1/0  HQ -> Routes -> Static Routes -> Route5  HQ(config)#ip route 209.165.200.0 255.255.255.224 Serial0/1/1 10  ISP -> Routes -> Static Routes ->Route1  ISP>enable  ISP#configure terminal  ISP(config)#  ISP(config)#ip route 172.31.0.0 255.255.128.0 Serial0/1/1  ISP -> Routes -> Static Routes ->Route2  ISP(config)#ip route 172.31.0.0 255.255.128.0 Serial0/1/0 25  R1 -> Ports -> GigabitEthernet0/0 -> Port Status  R1>enable  R1#configure terminal  R1(config-if)#no shutdown  R1(config-if)#exit  R1 -> Ports -> GigabitEthernet0/0.10 -> 802.1Q -> VLAN ID  R1(config-if)#interface G0/0.10  R1(config-subif)#encapsulation dot1Q 10  R1 -> Ports -> GigabitEthernet0/0.10 -> 802.1Q -> IP Address & Subnet Mask  R1(config-subif)#ip address 172.31.10.1 255.255.255.0  R1(config-subif)#exit  R1 -> Ports -> GigabitEthernet0/0.20 -> 802.1Q -> VLAN ID  R1(config-if)#interface G0/0.20  R1(config-subif)#encapsulation dot1Q 20  R1 -> Ports -> GigabitEthernet0/0.20 -> 802.1Q -> IP Address & Subnet Mask  R1(config-subif)#ip address 172.31.20.1 255.255.255.0  R1(config-subif)#exit  R1 -> Ports -> GigabitEthernet0/0.30 -> 802.1Q -> VLAN ID  R1(config-if)#interface G0/0.30  R1(config-subif)#encapsulation dot1Q 30  R1 -> Ports -> GigabitEthernet0/0.30 -> 802.1Q -> IP Address & Subnet Mask  R1(config-subif)#ip address 172.31.30.1 255.255.255.0  R1(config-subif)#exit  R1 -> Ports -> GigabitEthernet0/0.88 -> 802.1Q -> VLAN ID  R1(config-if)#interface G0/0.88  R1(config-subif)#encapsulation dot1Q 88  R1 -> Ports -> GigabitEthernet0/0.88 -> 802.1Q -> IP Address & Subnet Mask  R1(config-subif)#ip address 172.31.88.1 255.255.255.0  R1(config-subif)#exit  R1 -> Ports -> GigabitEthernet0/0.99 -> 802.1Q -> VLAN ID  R1(config-if)#interface G0/0.99  R1(config-subif)# encapsulation dot1Q 99 native  R1 -> Ports -> GigabitEthernet0/0.99 -> 802.1Q -> IP Address & Subnet Mask  R1(config-subif)#ip address 172.31.99.1 255.255.255.0  R1(config-subif)#exit  R1 -> Routes -> Static Routes -> Route0  R1(config)#ip route 0.0.0.0 0.0.0.0 Serial0/0/0  R1 -> Ports -> GigabitEthernet0/0 -> Port Status  R1(config-subif)#interface G0/0  R1(config-if)#no shutdown  R1(config-if)#exit  S1 -> Ports -> GigabitEthernet0/1 -> Native VLAN  S1>enable  S1#configure terminal  S1(config)#interface G0/1  S1(config-if)#switchport mode trunk  S1(config-if)#switchport trunk native vlan 99 |
| 8.7.1.4\_Packet\_Tracer\_-\_Configure\_and\_Verify\_a\_Site-to-Site\_IPsec\_VPN\_Using\_CLI[1].pka  A close up of text on a white background  Description automatically generated | User Access Verification  Password: (ciscoconpa55)  R1>enable  Password: (ciscoenpa55)  R1#configure terminal  R1 -> AGL -> 100  R1(config)#access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255  R1 -> IKE -> Crypto IpSec Transform Sets -> Set VPN-SET -> Name  R1(config-isakmp)#crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac  R1 -> IKE -> Crypto ISAKMP Key Address Pairs -> vpnpa55  R1(config)#crypto isakmp key vpnpa55 address 10.2.2.2  R1 -> IKE -> Crypto ISAKMP Policy -> Authentication type  R1(config)#crypto isakmp policy 10  R1(config-isakmp)#authentication pre-share  R1 -> IKE -> Crypto ISAKMP Policy -> Encryption  R1(config-isakmp)#encryption aes  R1 -> IKE -> Crypto ISAKMP Policy -> Group  R1(config-isakmp)#group 2  ---  (Create the crypto map VPN-MAP)  R1(config)#crypto map VPN-MAP 10 ipsec-isakmp  R1(config-crypto-map)#description VPN connection to R3  R1(config-crypto-map)#set peer 10.2.2.2  R1(config-crypto-map)#set transform-set VPN-SET  R1(config-crypto-map)#match address 110  R1(config-crypto-map)#exit  R1(config)#interface S0/0/0  R1(config-if)#crypto map VPN-MAP  R1(config-if)#exit  ---  Do the same for R3  Do next changes:  a. R3(config)#access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255  b. R3(config)#crypto isakmp key vpnpa55 address 10.1.1.2 |
| 9.3.2.10 Configuring Extended ACLs Scenario 1.pka  A screenshot of a cell phone  Description automatically generated | R1 -> ACL -> 100  R1>enable  R1#configure terminal  R1(config)#access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp  R1(config)#access-list 100 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62  R1 -> ACL -> HTTP\_ONLY  R1(config)#ip access-list extended HTTP\_ONLY  R1(config-ext-nacl)#permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq www  R1(config-ext-nacl)#permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62  R1(config-ext-nacl)#exit  R1 -> GigabitEthernet0/0 -> Access-group in  R1(config)#interface range G0/0  R1(config-if)#ip access-group 100 in  R1(config-if)#exit  R1 -> GigabitEthernet0/1 -> Access-group in  R1(config)#interface G0/1  R1(config-if)#ip access-group HTTP\_ONLY in  R1(config-if)#exit  PC2 -> From Browser:  <http://172.22.34.62> (OK)  PC2 -> Command Prompt:  C:\>ping 172.22.34.62. (OK)  PC2 -> Command Prompt:  C:\>ftp 172.22.34.62  Trying to connect...172.22.34.62  %Error opening ftp://172.22.34.62/ (Timed out)  PC1 -> From Browser:  <http://172.22.34.62> -> Request Timeout  PC1 -> Command Prompt:  C:\>ping 172.22.34.62. (OK)  PC1 -> Command Prompt:  C:\>ftp 172.22.34.62  Trying to connect...172.22.34.62  Connected to 172.22.34.62  220- Welcome to PT Ftp server  Username: cisco Password: cisco |
| 9.4.1.2\_Packet\_Tracer\_-\_Skills\_Integration\_Challenge[1](1).pka  A close up of text on a white background  Description automatically generated  A close up of text on a white background  Description automatically generated | Open Branch-A Router  Branch-A -> Console Line -> Login & Password  Router>enable  Router# config terminal  Router(config)#line console 0  Router(config-line)#password cisco  Router(config-line)#login  Router(config-line)#exit  Branch-A -> Enable Secret  Router(config)#enable secret class  Branch-A -> Host Name  Router(config)# hostname Branch-A  Branch-A -> Ports -> Gig0/0 -> IP Address & Mask  Branch-A(config-if)#ip address 172.20.16.1 255.255.254.0  Branch-A -> Ports -> Gig0/0 -> Port Status  Branch-A(config-if)#no shutdown  Branch-A -> Ports -> Gig0/1 -> IP Address & Mask  Branch-A(config-if)#interface G0/1  Branch-A(config-if)#ip address 172.20.18.1 255.255.255.0  Branch-A -> Ports -> Gig0/1 -> Port Status  Branch-A(config-if)#no shutdown  Branch-A -> Ports -> Gig0/2 -> IP Address & Mask  Branch-A(config-if)#interface G0/2  Branch-A(config-if)#ip address 172.20.31.254 255.255.255.252  Branch-A -> Ports -> Gig0/2 -> Port Status  Branch-A(config-if)#no shutdown  Branch-A(config-if)#exit  Branch-A -> Service Password Encryption  Branch-A(config)#service password-encryption  Branch-A -> VTY Lines -> VTY Line 0 -> Password  Branch-A(config)#line vty 0 15  Branch-A(config-line)#password cisco  Branch-A(config-line)#exit  Open Branch-B Router  Branch-B -> Console Line -> Login & Password  Router>enable  Router# config terminal  Router(config)#line console 0  Router(config-line)#password cisco  Router(config-line)#login  Router(config-line)#exit  Branch-B -> Enable Secret  Router(config)#enable secret class  Branch-B -> Host Name  Router(config)# hostname Branch-B  Branch-B -> Ports -> G0/0 -> IPv6 Addresses -> 2001:DB8:FADE:00FF::1  Branch-B(config)#interface G0/0  Branch-B(config-if)#ipv6 address 2001:DB8:FADE:00FF::1/64  Branch-B -> Ports -> G0/0 -> IPv6 Addresses -> Link Local  Branch-B(config-if)#ipv6 address FE80::B link-local  Branch-B -> Ports -> G0/0 -> IPv6 Addresses -> Port Status  Branch-B(config-if)#no shutdown  Branch-B(config-if)#exit  Branch-B -> Ports -> G0/1 -> IPv6 Addresses -> 2001:DB8:FADE:100::2  Branch-B(config)#interface G0/1  Branch-B(config-if)#ipv6 address 2001:DB8:FADE:100::1/64  Branch-B -> Ports -> G0/1 -> IPv6 Addresses -> Link Local  Branch-B(config-if)#ipv6 address FE80::B link-local  Branch-B -> Ports -> G0/1 -> IPv6 Addresses -> Port Status  Branch-B(config-if)#no shutdown  Branch-B(config-if)#exit  Branch-B -> Ports -> G0/2 -> IPv6 Addresses -> 2001:DB8:FFFF:FFFF::2  Branch-B(config)#interface G0/2  Branch-B(config-if)#ipv6 address 2001:DB8:FFFF:FFFF::2/64  Branch-B -> Ports -> G0/2 -> IPv6 Addresses -> Link Local  Branch-B(config-if)#ipv6 address FE80::B link-local  Branch-B -> Ports -> G0/2 -> IPv6 Addresses -> Port Status  Branch-B(config-if)#no shutdown  Branch-B(config-if)#exit  Branch-B -> Service Password Encryption  Branch-B(config)#service password-encryption  Branch-B -> VTY Lines -> VTY Line 0 -> Password  Branch-B(config)#line vty 0 15  Branch-B(config-line)#password cisco  Branch-B(config-line)#exit  PC-A1 -> (all)  Open PC-A1 -> Desktop -> IP Configuration  IP Address: 172.20.17.254  Subnet Mask: 255.255.254.0  Default Gateway: 172.20.16.1  DNS Server: 172.20.32.10  PC-A2 -> (all)  Open PC-A1 -> Desktop -> IP Configuration  IP Address: 172.20.18.254  Subnet Mask: 255.255.255.0  Default Gateway: 172.20.18.1  DNS Server: 172.20.32.10  PC-B1 -> (all)  Open PC-A1 -> Desktop -> IP Configuration  IPv6 Address: 2001:DB8:FADE:00FF::10 / 64  IPv6 Gateway: FE80::B  IPv6 DNS Server: 2001:DB8:FADE:1000::10  PC-B1 -> (all)  Open PC-A1 -> Desktop -> IP Configuration  IPv6 Address: 2001:DB8:FADE:0100::10 / 64  IPv6 Gateway: FE80::B  IPv6 DNS Server: 2001:DB8:FADE:1000::10 |