IP Addressing Table

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP Address</th>
<th>Subnet Mask</th>
<th>Default Gateway</th>
<th>Switch Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1</td>
<td>FA0/0</td>
<td>209.165.200.233</td>
<td>255.255.255.248</td>
<td>N/A</td>
<td>ASA E0/0</td>
</tr>
<tr>
<td></td>
<td>S0/0/0 (DCE)</td>
<td>10.10.10.1</td>
<td>255.255.255.252</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Loopback 1</td>
<td>172.20.1.1</td>
<td>255.255.255.0</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>R2</td>
<td>S0/0/0</td>
<td>10.10.10.2</td>
<td>255.255.255.252</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>S0/0/1 (DCE)</td>
<td>10.20.20.2</td>
<td>255.255.255.252</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>R3</td>
<td>FA0/1</td>
<td>172.30.3.1</td>
<td>255.255.255.0</td>
<td>N/A</td>
<td>S3 FA0/5</td>
</tr>
<tr>
<td>Device</td>
<td>Interface</td>
<td>IP Address</td>
<td>Subnet Mask</td>
<td>Default Gateway</td>
<td>Switch Port</td>
</tr>
<tr>
<td>--------</td>
<td>-----------</td>
<td>-------------</td>
<td>--------------</td>
<td>-----------------</td>
<td>--------------</td>
</tr>
<tr>
<td>S0/0/1</td>
<td></td>
<td>10.20.20.1</td>
<td>255.255.255.252</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>S1</td>
<td>VLAN 1</td>
<td>192.168.10.11</td>
<td>255.255.255.0</td>
<td>192.168.10.1</td>
<td>N/A</td>
</tr>
<tr>
<td>S2</td>
<td>VLAN 1</td>
<td>192.168.10.12</td>
<td>255.255.255.0</td>
<td>192.168.10.1</td>
<td>N/A</td>
</tr>
<tr>
<td>S3</td>
<td>VLAN 1</td>
<td>172.30.3.11</td>
<td>255.255.255.0</td>
<td>172.30.3.1</td>
<td>N/A</td>
</tr>
<tr>
<td>ASA</td>
<td>VLAN 1 (E0/1)</td>
<td>192.168.10.1</td>
<td>255.255.255.0</td>
<td>NA</td>
<td>S2 FA0/24</td>
</tr>
<tr>
<td>ASA</td>
<td>VLAN 2 (E0/0)</td>
<td>209.165.200.234</td>
<td>255.255.255.248</td>
<td>NA</td>
<td>R1 FA0/0</td>
</tr>
<tr>
<td>PC-A</td>
<td>NIC</td>
<td>192.168.10.2</td>
<td>255.255.255.0</td>
<td>192.168.10.1</td>
<td>S1 FA0/6</td>
</tr>
<tr>
<td>PC-B</td>
<td>NIC</td>
<td>192.168.10.3</td>
<td>255.255.255.0</td>
<td>192.168.10.1</td>
<td>S2 FA0/18</td>
</tr>
<tr>
<td>PC-C</td>
<td>NIC</td>
<td>172.30.3.3</td>
<td>255.255.255.0</td>
<td>172.30.3.1</td>
<td>S3 FA0/18</td>
</tr>
</tbody>
</table>

Objectives

Part 1: Verify Basic Device Settings

Part 2: Configure Secure Router Administrative Access

- Configure encrypted passwords and a login banner.
- Configure EXEC timeout on console and VTY lines.
- Configure login failure rates and VTY login enhancements.
- Configure SSH access and disable Telnet.
- Configure local AAA authentication.

Part 3: Configure a Site-to-Site VPN between ISRs

- Configure an IPsec site-to-site VPN between R1 and R3 using CCP.

Part 4: Configure an ISR firewall

- Configure a zone-based policy (ZPF) firewall on an ISR using CCP.

Part 5: Secure Network Switches

- Configure passwords and a login banner.
- Configure management VLAN access.
- Secure trunk ports.
- Secure access ports.
- Protect against STP attacks.
- Configure port security and disable unused ports.

Part 6: Configure ASA Basic Settings and Firewall

- Configure basic settings, passwords, date and time.
- Configure the inside and outside VLAN interfaces.
- Configure port address translation (PAT) for the inside network.
- Configure a DHCP server for the inside network.
- Configure administrative access via Telnet and SSH.
- Configure a static default route for the ASA.
- Configure Local AAA user authentication.
- Verify address translation and firewall functionality

**Part 7: Configure ASA Clientless SSL VPN Remote Access**
- Configure a remote access SSL VPN using ASDM.
- Verify SSL VPN access to the portal.

**Exam Overview**

This skills-based assessment is the final practical exam of Academy student training for the CCNA Security course. The exam is divided into six parts. The parts should be completed sequentially. In Part 1 you verify that the basic device settings have been preconfigured by the instructor. In Part 2, you secure a network router using the CLI to configure various IOS features including AAA and SSH. In Part 3 you configure a site-to-site VPN between R1 and R3 through the ISP router (R2). In Part 4 you configure a ZPF firewall and IPS on an ISR. Part 5 configures network switches using the CLI. In Parts 6 and 7 you configure the ASA firewall functionality and clientless SSL VPN remote access.

**Note:** The router commands and CCP output in this SBA are from Cisco 1841 routers with Cisco IOS Release 12.4(20)T (Advanced IP image). The switch commands and output are from Cisco WS-C2960-24TT-L switches with Cisco IOS Release 12.2(46)SE (C2960-LANBASEK9-M image). The ASA is a 5505 with OS version 8.4(2) and ASDM version 6.4(5). Other routers, switches, and Cisco IOS versions may be used. See the Router Interface Summary table at the end of the SBA to determine which interface identifiers to use based on the equipment in the SBA. Depending on the router or switch model and Cisco IOS version, the commands available and output produced might vary from what is shown in this SBA.

**Required Resources**

- 2 routers (Cisco 1841 with Cisco IOS Release 12.4(20)T1 Advanced IP Service or comparable)
- 1 router (Cisco 1841 with Cisco IOS Release 12.4(20)T1 IP Base or comparable)
- 3 switches (Cisco 2960 with Cisco IOS Release 12.2(46)SE C2960-LANBASEK9-M image or comparable)
- 1 ASA 5505 (OS version 8.4(2) and ASDM version 6.4(5) and Base license or comparable)
- PC-A: Windows XP, Vista, or Windows 7 with CCP, PuTTy SSH client (Web and FTP server optional) (flash drive optional)
- PC-B: Windows XP, Vista, or Windows 7 with PuTTy SSH client and Java version 6.x or higher (ASDM loaded on the PC is optional)
- PC-C: Windows XP, Vista, or Windows 7 with CCP, PuTTy SSH client, TFTP server and IPS files. (flash drive optional)
- Serial and Ethernet cables as shown in the topology
- Rollover cables to configure the routers, switches and ASA via the console
Part 1: Verify Basic Device Settings

**Important Note:** Prior to starting the exam, verify that the basic test environment is built as described below. Contact your instructor if the following devices and settings have not been pre-configured.

- Network cabled as shown in the topology.
- **Basic settings for all routers configured.**
  - Host names, interface IP addresses, serial interface DCE clock rate.
  - DNS lookup disabled on each router.
- **Static default routes on routers R1, R2 and R3 configured.**
  - Static default route from R1 to R2 and from R3 to R2.
  - Static routes from R2 to the R1 simulated LAN (Loopback 1), the R1 Fa0/0-to-ASA subnet and the R3 LAN.
- **Basic settings for each switch configured.**
  - Host names, VLAN 1 management address, IP default gateway.
  - DNS lookup disabled on each switch.
- **PC host IP settings configured.**
  - Static IP address, subnet mask, and default gateway for each PC.
- **Verify connectivity between PC-C and R1 Lo1 and Fa0/0.**

Part 2: Configure Secure Router Administrative Access

**Task 1: Configure Settings for R1 and R2.**

**Step 1:** Configure a minimum password length of 10 characters on R1.

**Step 2:** Configure the enable secret password on R1.

Use an enable secret password of **ciscoenapa55**.

**Step 3:** Encrypt plaintext passwords on R1.

**Step 4:** Configure the console lines on R1.

Configure a console password of **ciscoconpa55** and enable login. Set the exec-timeout to log out after 15 minutes of inactivity. Prevent console messages from interrupting command entry.

**Note:** The vty lines for R1 are configured for SSH in Task 3.

**Step 5:** Configure a login warning banner on R1.

Configure a warning to unauthorized users with a message-of-the-day (MOTD) banner that says: “Unauthorized access strictly prohibited and prosecuted to the full extent of the law!”.
Step 6: Configure the vty lines and enable password on R2.
   a. Configure the password for vty lines to be ciscovtypa55 and enable login. Set the exec-timeout so a
      session is logged out after 15 minutes of inactivity.
   b. Use an enable secret password of ciscoenapa55.

Step 7: Enable HTTP access on router R2.
      Enable the HTTP server on R2 to simulate an Internet target for later testing.

Task 2: Configure Local Authentication with AAA on R1.

Step 1: Configure the local user database.
       Create a local user account of Admin01 with a secret password of Admin01pa55 and a privilege level of 15.

Step 2: Enable AAA services.

Step 3: Implement AAA services using the local database.
       Create the default login authentication method list using case-sensitive local authentication as the first
       option and the enable password as the backup option to use if an error occurs in relation to local
       authentication.

Task 3: Configure the SSH Server on Router R1.

Step 1: Configure the domain name ccnasecurity.com.

Step 2: Configure the incoming vty lines.
       Specify that the router vty lines will accept only SSH connections.

Step 3: Generate the RSA encryption key pair.
       Configure the RSA keys with 1024 as the number of modulus bits.

Step 4: Configure the SSH version.
       Specify that the router accept only SSH version 2 connections.

Step 5: Verify SSH connectivity to R1 from PC-C.
       Launch the SSH client on PC-C and test SSH connectivity to R1 and login in as Admin01 with the
       password Admin01pa55.

Task 4: Secure against login attacks on R1.

Step 1: Configure enhanced login security on R1.
       If a user fails to login twice within a 30 second time span, then disable logins for 1 minute. Log all failed
       login attempts.
Part 3: Configure a Site-to-Site IPsec VPN between ISRs

In Part 3 of this SBA, you use CCP to configure an IPsec VPN tunnel between R1 and R3 that passes through R2.

Task 1: Configure the site-to-site VPN between R1 and R3.

Step 1: Configure the enable secret password and HTTP access on R3 prior to starting CCP.
   a. From the CLI, configure an enable secret password of ciscoenapa55 for use with CCP on R3.
   b. Enable the HTTP server on R3.
   c. Add user Admin01 to the local database with a privileged level of 15, and a password of Admin01pa55.
   d. Configure local database authentication of HTTP sessions.

Step 2: Access CCP and discover R3.
   From PC-C run CCP and access R3.

Step 3: Use the CCP VPN wizard to configure R3.
   Use the Quick Setup option to configure the R3 side of the site-to-site VPN.

Step 4: Configure basic VPN connection information settings.
   a. Specify R3 S0/0/1 as the interface for the connection and R1 interface S0/0/0 as the remote peer static IP address.
   b. Specify the pre-shared VPN key cisco12345.
   c. Encrypt traffic between the R3 LAN and the R1 Loopback 1 simulated LAN.

Step 5: Generate a mirror configuration from R3 and apply it to R1.
   a. On R3, generate a mirror configuration for application to router R1 and save it to the desktop or flash drive. Edit the file as necessary and apply the mirrored commands to R1.
   b. Apply the crypto map to the R1 VPN interface.

Task 2: Test the Site-to-Site IPsec VPN using CCP
   a. On R3 (PC-C), use CCP to test the IPsec VPN tunnel between the two routers.
   b. Ping from PC-C to the R1 Lo1 interface at 172.16.1.1 to generate some interesting traffic.
   c. Issue the show crypto isakmp sa command on R3 to view the security association created.
   d. Issue the show crypto ipsec sa command on R1 to verify packets are being received from R3 and decrypted by R1.

Part 4: Configure an ISR Firewall

In Part 4, you configure a zone-based policy firewall and IPS on R3 using CCP.
Task 1: Configure a ZPF Firewall on R3 using CCP.

Step 1: Use the CCP Firewall wizard to configure a zone-based firewall.
   a. Configure a Basic firewall with Fa0/1 interface as the Inside interface and S0/0/1 as the Outside interface.
   b. Use the Low Security setting, and complete the Firewall wizard.

Step 2: Verify Firewall functionality.
   a. From PC-C, ping external router R2. The pings should be successful.
   b. From external router R2, ping PC-C. The pings should NOT be successful.

Part 5: Secure Network Switches

Task 1: Configure Passwords and a Login Banner on S1.

Step 1: Configure the enable secret password of ciscoenapa55.

Step 2: Encrypt plaintext passwords.

Step 3: Configure the console and VTY lines.
   a. Configure a console password of ciscoconpa55 and set the exec-timeout to log out after 5 minutes of inactivity. Prevent console messages from interrupting command entry.
   b. Configure a vty lines password of ciscovtypa55 and set the exec-timeout to log out after 5 minutes of inactivity.

Step 4: Configure a login warning banner.
   Configure a warning to unauthorized users with a message-of-the-day (MOTD) banner that says “Unauthorized access strictly prohibited and prosecuted to the full extent of the law!”. 
Step 5: Disable HTTP access.

Task 2: Secure Trunk and Access Ports on S1 and S2.

Step 1: Configure trunk ports on S1 and S2.

Step 2: Change the native VLAN to 99 for the trunk ports on S1 and S2.

Step 3: Prevent the use of DTP on S1 and S2 trunk ports.

Step 4: Verify the trunking configuration on S1 and S2.

Step 5: Enable storm control for broadcasts on S1 and S2 trunk ports.

Step 6: Disable trunking on S1 access ports that are in use.

Step 7: Enable PortFast on S1 access ports that are in use.

Step 8: Enable BPDU guard on S1 access ports that are in use.

Task 3: Configure Port Security and Disable Unused Ports.

Step 1: Configure basic port security for the S1 access port.

Use the default port security options (set maximum MAC addresses to 1 and violation action to shutdown). Allow the secure MAC address that is dynamically learned on a port be added to the switch running configuration.

Step 2: Disable unused ports on S1.

As a further security measure, disable any ports not being used.

Part 6: Configure ASA Basic Settings and Firewall

Task 1: Prepare the ASA for ASDM access.

Step 1: Clear the previous ASA configuration settings.

Step 2: Bypass Setup Mode and configure the VLAN interfaces using CLI.

a. The VLAN 1 logical interface will be used by PC-B to access ASDM on ASA physical interface E0/1. Configure interface VLAN 1 and name it “inside”. Specify IP address 192.168.10.1 and subnet mask 255.255.255.0. Verify that the security level is set to 100.

b. Pre-configure interface VLAN 2 and name it “outside”, and add physical interface E0/0 to VLAN 2. You will assign the IP address using ASDM. Verify that the security level is set to 0.

c. Test Connectivity to the ASA by pinging from PC-B to ASA interface VLAN 1 IP address 192.168.10.1. The pings should be successful.

Step 3: Configure and verify access to the ASA from the inside network.

a. Configure the ASA to accept HTTPS connections and to allow access to ASDM from any host on the inside network 192.168.10.0/24.

b. Open a browser on PC-B and test the HTTPS access to the ASA ASDM GUI.
Task 2: Configure basic ASA settings using the ASDM Startup Wizard.

Step 1: Access the Configuration menu and launch the Startup wizard.

Step 2: Configure hostname, domain name, and enable password.

Configure the ASA host name CCNAS-ASA and domain name of ccnasecurity.com. Change the enable mode password to ciscoenapa55.

Step 3: Configure the outside VLAN interface.

Enter an outside IP address of 209.165.200.234 and mask 255.255.255.248.

Step 4: Configure DHCP, address translation and administrative access.

a. Enable the DHCP server on the Inside Interface and specify a starting IP address of 192.168.10.5 and ending IP address of 192.168.10.30. Enter the DNS server 1 address of 10.3.3.3 and domain name ccnasecurity.com.

b. Configure the ASA to use port address translation (PAT) using the IP address of the outside interface.

c. Add Telnet access to the ASA for the inside network 192.168.10.0 with a subnet mask of 255.255.255.0. Add SSH access to the ASA from host 172.30.3.3 on the outside network.

Step 5: Test Telnet access to the ASA.

a. From a command prompt or GUI Telnet client on PC-B, Telnet to the ASA inside interface at IP address 192.168.10.1.

Task 3: Configuring ASA Settings from the ASDM Configuration Menu.

Step 1: Set the ASA Date and Time.

Set the time zone, current date and time and apply the commands to the ASA.

Step 2: Configure a static default route for the ASA.

Add a static route for the outside interface and specify Any for the network object and a Gateway IP of 209.165.200.233. Use Ping from the ASDM Tools menu to test connectivity to the IP address of router R1 S0/0/0 (10.10.10.1). The ping should succeed.

Step 3: Test access to an external website from PC-B.

Open a browser on PC-B and enter the IP address of the R2 S0/0/0 interface (10.10.10.2) to simulate access to an external website. The R2 HTTP server was previously enabled so you should be prompted with a user authentication login dialog box from the R2 GUI device manger. Exit the browser.

Step 4: Configure AAA for SSH client access.

a. Create a new user named admin with a password of cisco123. Allow this user Full access (ASDM, SSH, Telnet, and console) and set the privilege level to 15.

b. Require authentication for HTTP/ASDM, SSH and Telnet connections and specify the “LOCAL” server group for each connection type.

c. From PC-C, open an SSH client such as PuTTY and attempt to access the ASA outside interface at 209.165.200.234. You should be able to establish the connection.
Part 7: Configure ASA Clientless SSL VPN Remote Access

Step 1: Configure the SSL VPN user interface.
Configure VPN-Con-Prof as the Connection Profile Name, and specify outside as the interface to which outside users will connect.

Step 2: Configure AAA user authentication.
Use the local user database to authenticate remote access users and create a new user named VPNuser with a password of remote.

Step 3: Configure the VPN group policy.
Create a new group policy named VPN-Grp-Pol.

Step 4: Configure the bookmark list.
- Add a bookmark list and name it WebServer-XX (where XX is your initials).
- Add a new Bookmark with Web Mail as the Bookmark Title. Specify the server destination IP address of PC-B 192.168.10.3 (simulating a web server).

Step 5: Verify VPN access from the remote host.
Open the browser on PC-C and enter the login URL for the SSL VPN into the address field (https://209.165.200.234). The Logon window should appear. Enter the previously configured user name VPNuser and password remote and click Logon to continue. The Web Portal window should display.