Ütemterv

Számítógép hálózat üzemeltetési alapismeretek I.

Tárgy kódja: GEIAL30I-B, GEIAL30GB
Szak: mérnök informatikus alapszak, villamosmérnök alapszak.
Típusa: szakirányban választható
Oktató, előadó: dr. Kovács Szilveszter
Tárgyfelelős: dr. Kovács Szilveszter
Félév: 2018/2019 tavasz

Hét	Elmélet	Gyakorlat
1.	Bevezetés.	Labor ismertetés.
2.	OSI rétegek	Packet Tracer szimulacios gyakorlatok
3.	Ethernet	Packet Tracer szimulacios gyakorlatok
4.	Hálózattervezés és kábelezés	Packet Tracer szimulacios gyakorlatok
5.	Hálózati címzés; IPv4	Packet Tracer szimulacios gyakorlatok
6.	Hálózat konfiguráció és tesztelés.	Packet Tracer szimulacios gyakorlatok
7.	Forgalomirányító protokollok és módszerek, statikus forgalomirányítás. Évközi zárthelyi dolgozat	Packet Tracer szimulacios gyakorlatok
8.	Dinamikus forgalomirányítás, távolság vektor és él-állapot módszerek.	Packet Tracer szimulacios gyakorlatok
9.	RIP v1, VLSM és CIDR, forgalomirányító táblázat.	Packet Tracer szimulacios gyakorlatok
10.	RIPv2, EIGRP	Packet Tracer szimulacios gyakorlatok
11.	Él-állapot módszerek, OSPF	Packet Tracer szimulacios gyakorlatok
12.	Évközi zárthelyi dolgozat	Packet Tracer szimulacios gyakorlatok

Kötelező irodalom

- Kovács Szilveszter honlapján található előadásjegyzet (www.iit.uni-miskolc.hu/~szkovacs)

Ajánlott irodalom

- Tanenbaum, A.S.: Számítógép-hálózatok, Panem, 2003, ISBN 963 545 384 1

- Cisco Certified Networking Associate (CCNA) Routing and Switching tananyag (magyar nyelvű).
- Cisco Certified Networking Associate (CCNA) Routing and Switching tananyag (angol nyelvű).

A tárgy lezárásának módja:

- aláírás, gyakorlati jegy

Évközi számonkérés:

- témaköröket záró rövid teszt feladatok
- két évközi zárthelyi dolgozat, amely a nagyobb tananyagegységek zárásaként íródik.

Az aláírás megszerzésének feltételei:

- Az ME SzMSz III. kötet 38§ (6) pontja alapján, ha a hallgató nem igazolt hiányzása a gyakorlatokon eléri a gyakorlatok darabszámának 50%-át, a tantárgy aláírása nem szerezhető meg.
- Az aláírás megszerzésének további feltétele a témaköröket záró rövid teszt feladatok sikeres teljesítése.

Az gyakorlati jegy megszerzésének feltételei:

- Az aláírás megszerzése és a zárthelyi dolgozatok legalább elégséges szintű megírása.

Pótlási lehetőségek:

A gyakorlatok, egyéni feladatok és a zárhelyi dolgozatok egyszer pótolhatók, melyek egyenkénti (vagy összevont) pótlásra az ME SzMSz III. kötet 38§ (5) pontja alapján legkésőbb a szorgalmi időszak utolsó hetében kerülhet sor. A feladatok pótvédése határidő mulasztással jár, ezért különeljárási díjat kell fizetni.

Általános rendelkezések:

Az ME SzMSz III. kötet 96§ alapján a tárgyakhoz kapcsolódó valamennyi számonkérési alkalomnál a nem engedélyezett segédeszközök használata (puskázás) vagy más munkájának sajátként történő feltüntetése (plagizálás) fegyelmi vétségnek minősül, mely tanulmányi szankciókat vagy fegyelmi eljárást von maga után.

Tanulmányi szankció az évközi számonkéréseknél a számonkérés sikertelen minősítése. A számonkérés ilyen esetekben nem pótolható.

Tanulmányi szankció a vizsgaidőszakban a vizsga elégtelen minősítése, és hogy ismételt vizsgát a hallgató a tanszék által kijelölt időpontban, kijelölt vizsgabizottság előtt, szóbeli vizsga formájában tehet.

A puskázás és/vagy plagizálás tényét a tanszék a hallgató tanulmányi ideje alatt nyilvántartja, és ismételt előfordulás esetén a ME SzMSz III. kötet 96§ által előírt fegyelmi eljárást kezdeményez.

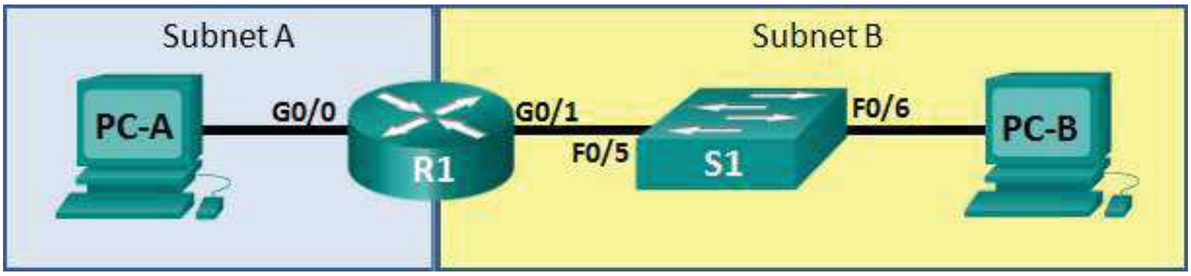
Miskolc, 2019. február 13.

Dr. Kovács Szilveszter

CCNA: Introduction to Networks

Skills Assessment – Student Training Exam

Topology



Assessment Objectives

Part 1: Develop the IPv4 Address Scheme (15 points, 20 minutes)

Part 2: Initialize and Reload Devices (10 points, 5 minutes)

Part 3: Configure Device IPv4 and Security Settings (30 points, 20 minutes)

Part 4: Test and Verify IPv4 End-to-End Connectivity (8 points, 10 minutes)

Part 5: Configure IPv6 Addressing on R1 (10 points, 10 minutes)

Part 6: Test and Verify IPv6 End-to-End Connectivity (7 points, 10 minutes)

Part 7: Use the IOS CLI to Gather Device Information (10 points, 10 minutes)

Part 8: Save the R1 Configuration to a TFTP Server (10 points, 10 minutes)

Scenario

In this Skills Assessment (SA) you will configure the devices in a small network. You must configure a router, switch and PCs to support both IPv4 and IPv6 connectivity. You will configure security, including SSH, on the router. You will test and document the network using common CLI commands. Finally, you will save the router configuration to a TFTP server.

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cable to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Instructor Note: Part 8 requires a TFTP server. Tftpd32 is recommended and must be preinstalled on PC-A.

Instructor Note: If Windows XP hosts are used, it may be necessary to install IPv6. Refer to Lab 0.0.0.2: *Installing the IPv6 Protocol with Windows XP* in the Instructor Lab Manual.

Part 1: Develop the IPv4 Addressing Scheme

Total points: 15

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Time: 20 minutes

Given an IP address and mask of ______________________________________ (address / mask), design an IP addressing scheme that satisfies the following requirements. Network address/mask and the number of hosts for Subnets A and B will be provided by your instructor.

Subnet	Number of Hosts
Subnet A	
Subnet B	

The 0th subnet is used. No subnet calculators may be used. All work must be shown on the other side of this page.

Subnet A		
Specification	**Student Input**	**Points**
Number of bits in the subnet		(5 points)
IP mask (binary)		
New IP mask (decimal)		
Maximum number of usable subnets (including the 0th subnet)		
Number of usable hosts per subnet		
IP Subnet		
First IP Host address		
Last IP Host address		

Subnet B		
Specification	**Student Input**	**Points**
Number of bits in the subnet		(5 points)
IP mask (binary)		
New IP mask (decimal)		
Maximum number of usable subnets (including the 0th subnet)		
Number of usable hosts per subnet		
IP Subnet		
First IP Host address		
Last IP Host address		

Host computers will use the first IP address in the subnet. The network router will use the LAST network host address. The switch will use the second to the last network host address.

Write down the IP address information for each device:

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Device	IP address	Subnet Mask	Gateway	Points
PC-A				(5 points)
R1-G0/0			N/A	
R1-G0/1			N/A	
S1			N/A	
PC-B				

Before proceeding, verify your IP addresses with the instructor.

Instructor Sign-off Part 1: ______________________

Points: _________ of 15

Part 2: Initialize and Reload Devices

Total points: 10

Time: 5 minutes

Step 1: Initialize and reload router and switch. (10 points)

Erase the startup configurations and VLANs from the router and switch and reload the devices.

Before proceeding, have your instructor verify device initializations.

Task	IOS Command	Points
Erase the startup-config file on the Router.		(2 point)
Reload the Router.		(2 point)
Erase the startup-config file on the Switch.		(2 point)
Delete the vlan.dat file on the Switch		(2 point)
Reload the Switch.		(2 point)

Instructor Sign-off Part 2: _________________________

Points: __________ of 10

Part 3: Configure Device IPv4 and Security Settings

Total points: 30

Time: 20 minutes

Step 1: Configure host computers.

After configuring each host computer, record the host network settings with the **ipconfig /all** command.

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

PC-A Network Configuration		Points
Description		(2 points)
Physical Address		
IP Address		
Subnet Mask		
Default Gateway		

PC-B Network Configuration		Points
Description		(2 points)
Physical Address		
IP Address		
Subnet Mask		
Default Gateway		

Step 2: Configure R1.

Configuration tasks for R1 include the following:

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Task	Specification	Points
Disable DNS lookup		(1 point)
Router name	R1	(1 point)
Domain name	ccna-lab.com	(1 point)
Encrypted privileged exec password	ciscoenpass	(1 point)
Console access password	ciscoconpass	(1 point)
Telnet access password	ciscovtypass	(1 point)
Set the minimum length for passwords	10 characters	(2 points)
Create an administrative user in the local database	Username: admin Password: admin1pass	(2 points)
Set login on VTY lines to use local database		(1 point)
Set VTY lines to accept ssh and telnet connections only		(2 points)
Encrypt the clear text passwords		(1 point)
MOTD Banner		(1 point)
Interface G0/0	Set the description Set the Layer 3 IPv4 address Activate Interface	(2 points)
Interface G0/1	Set the description Set the Layer 3 IPv4 address Activate Interface	(2 points)
Generate a RSA crypto key	1024 bits modulus	(2 points)

Step 3: Configure S1.

Configuration tasks for R1 include the following:

Task	Specification	Points
Switch name	S1	(1 point)
Configure Management Interface (SVI)	Set the Layer 3 IPv4 address	(1 point)
Encrypted privileged exec password	ciscoenpass	(1 point)
Console access password	ciscoconpass	(1 point)
Telnet access password	ciscovtypass	(1 point)

Instructor Sign-off Part 3: ______________________

Points: _________ of 30

Part 4: Test and Verify IPv4 End-to-End Connectivity

Total points: 8

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Time: 10 minutes

Step 1: Verify network connectivity.

Use the ping command to test connectivity between all network devices.

Note: If pings to host computers fail, temporarily disable the computer firewall and retest. To disable a Windows 7 firewall, select Start > Control Panel > System and Security > Windows Firewall > Turn Windows Firewall on or off, select **Turn off Windows Firewall**, and click **OK**.

Use the following table to methodically verify connectivity with each network device. Take corrective action to establish connectivity if a test fails:

From	To	IP Address	Ping Results	Points
PC-A	R1, G0/0			(1 point)
PC-A	R1, G0/1			(1 point)
PC-A	S1 VLAN 1			(1 point)
PC-A	PC-B			(1 point)
PC-B	R1, G0/1			(1 point)
PC-B	R1, G0/0			(1 point)
PC-B	S1 VLAN 1			(1 point)

In addition to the ping command, what other command is useful in displaying network delay and breaks in the path to the destination? (1 point)

____

tracert or traceroute

Instructor Sign-off Part 4: ______________________

Points: _________ of 8

Part 5: Configure IPv6 Addressing on R1

Total points: 10

Time: 10 minutes

Given an IPv6 network address of **2001:DB8:ACAD::/48**, configure IPv6 addresses for the Gigabit interfaces on R1. Use **FE80::1** as the link-local address on both interfaces.

Step 1: Configure R1.

Configuration tasks for R1 include the following:

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Task	Specification	Points
Configure G0/0 to use the first address in subnet A.	Assign the IPv6 unicast address Assign the IPv6 link-local address	(4 points)
Configure G0/1 to use the first address in subnet B.	Assign the IPv6 unicast address Assign the IPv6 link-local address	(4 points)
Enable IPv6 unicast routing.		(2 points)

Instructor Sign-off Part 5: ______________________

Points: _________ of 10

Part 6: Test and Verify IPv6 End-to-End Connectivity

Total points: 7

Time: 10 minutes.

Step 1: Obtain the IPv6 address assigned to host PCs.

PC-A IPv6 Network Configuration		Points
Description		(1 point)
Physical Address		
IPv6 Address		
Default Gateway		

PC-B IPv6 Network Configuration		Points
Description		(1 point)
Physical Address		
IPv6 Address		
IPv6 Default Gateway		

Step 2: Use the ping command to verify network connectivity.

IPv6 network connectivity can be verified with the ping command. Use the following table to methodically verify connectivity with each network device. Take corrective action to establish connectivity if a test fails:

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

From	To	IP Address	Ping Results	Points
PC-A	R1, G0/0			(1 point)
PC-A	R1, G0/1			(1 point)
PC-A	PC-B			(1 point)
PC-B	R1, G0/1			(1 point)
PC-B	R1, G0/0			(1 point)

Instructor Sign-off Part 6: ______________________

Points: _________ of 7

Part 7: Use the IOS CLI to Gather Device Information

Total points: 10

Time: 10 minutes

Step 1: Issue the appropriate command to discover the following information:

Description	Student Input	Points
Router Model		(2 points)
IOS Image File		
Total RAM		
Total Flash Memory		
Configuration Register		
CLI Command Used		

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Step 2: Enter the appropriate CLI command needed to display the following on R1:

Command Description	Student Input (command)	Points
Display a summary of important information about the interfaces on R1.		(1 point)
Display the IPv4 routing table.		(1 point)
Display the Layer 2 to Layer 3 mapping of addresses on R1.		(1 point)
Display detailed IPv4 information about interface G0/0 on R1.		(1 point)
Display the IPv6 routing table.		(1 point)
Display a summary of IPv6 interface addresses and status.		(1 point)
Display information about the devices connected to R1. Information should include Device ID, Local Interface, Hold time, Capability, Platform, and Port ID.		(1 point)
Save the current configuration so it will be used the next time the router is started.		(1 point)

Instructor Sign-off Part 7: ______________________

Points: _________ of 10

Part 8: Save the R1 Configuration to a TFTP Server.

Total points: 10

Time: 10 minutes

Save the current configuration for R1 to the TFTP Server on PC-A. Tftpd32 software has been installed on PC-A. You will need to start this program before you begin. Document the command used below:

Description	Student Input	Points
CLI Command		(5 Points)
Address of remote host		
Destination Filename		

Instructor Sign-off Part 8: ______________________

Points: _________ of 10

Part 9: Cleanup

NOTE: DO NOT PROCEED WITH CLEANUP UNTIL YOUR INSTRUCTOR HAS GRADED YOUR SKILLS EXAM AND HAS INFORMED YOU THAT YOU MAY BEGIN CLEANUP.

Unless directed otherwise by the instructor, restore host computer network connectivity, and then turn off power to the host computers.

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Before turning off power to the router and switch, remove the NVRAM configuration files (if saved) from both devices.

Disconnect and neatly put away all LAN cables that were used in the Final.

Router Interface Summary Table

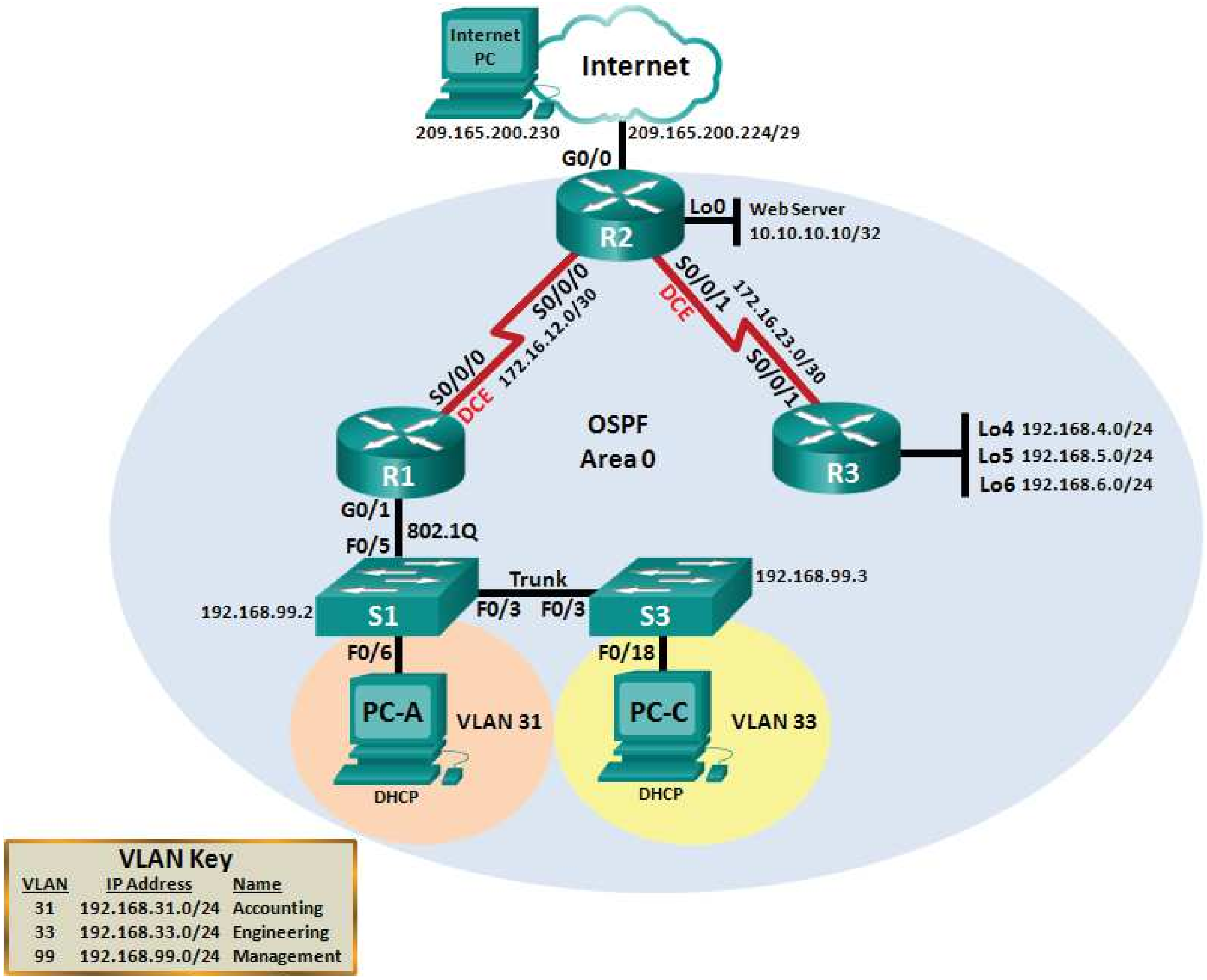
Router Interface Summary				
Router Model	**Ethernet Interface #1**	**Ethernet Interface #2**	**Serial Interface #1**	**Serial Interface #2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

CCNA: Routing and Switching Essentials

Skills Assessment – Student Training Exam

Topology



VLAN Key

VLAN	IP Address	Name
31	192.168.31.0/24	Accounting
33	192.168.33.0/24	Engineering
99	192.168.99.0/24	Management

Assessment Objectives

Part 1: Initialize Devices (8 points, 5 minutes)

Part 2: Configure Device Basic Settings (28 points, 30 minutes)

Part 3: Configure Switch Security, VLANs, and Inter-VLAN Routing (14 points, 15 minutes)

Part 4: Configure OSPFv2 Dynamic Routing Protocol (24 points, 25 minutes)

Part 5: Implement DHCP and NAT (13 points, 25 minutes)

Part 6: Configure and Verify Access Control Lists (ACLs) (13 points, 25 minutes)

Scenario

In this Skills Assessment (SA) you will configure a small network. You will configure routers, switches, and PCs to support IPv4 connectivity, switch security, and inter VLAN routing. You will then configure the devices with OSPFv2, DHCP, and dynamic and static NAT. Access control lists (ACLs) will be applied for added security. You will test and document the network using common CLI commands throughout the assessment.

Required Resources

- 3 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 3 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cable to configure the Cisco IOS devices via the console ports
- Ethernet and Serial cables as shown in the topology

Part 1: Initialize Devices

Total points: 8

Time: 5 minutes

Step 1: Initialize and reload the routers and switches.

Erase the startup configurations reload the devices.

Before proceeding, have your instructor verify device initializations.

Task	IOS Command	Points
Erase the startup-config file on all routers.		1½ points (½ point per router)
Reload all routers.		1 ½ points (½ point per router)
Erase the startup-config file on all switches and remove the old VLAN database.		2 points (1 point per switch)
Reload both switches.		2 points (1 point per switch)
Verify VLAN database is absent from flash on both switches.		1 point (½ point per switch)

Instructor Sign-off Part 1: ________________________

Points: __________ of 8

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Part 2: Configure Device Basic Settings

Total points: 28

Time: 30 minutes

Step 1: Configure the Internet PC.

Configuration tasks for the Internet PC include the following (Refer to Topology for IP address information):

Configuration Item or Task	Specification	Points
IP Address		(1/2 point)
Subnet Mask		(1/2 point)
Default Gateway	209.165.200.225	

Note: It may be necessary to disable the PC firewall for pings to be successful later in this lab.

Step 2: Configure R1.

Configuration tasks for R1 include the following:

Configuration Item or Task	Specification	Points
Disable DNS lookup		(1/2 point)
Router name	R1	(1/2 point)
Encrypted privileged exec password	class	(1/2 point)
Console access password	cisco	(1/2 point)
Telnet access password	cisco	(1/2 point)
Encrypt the clear text passwords		(1/2 point)
MOTD banner	Unauthorized Access is Prohibited!	(1/2 point)
Interface S0/0/0	Set the description Set the Layer 3 IPv4 address. Use the first available address in the subnet. Set the clocking rate to 128000 Activate Interface	(1/2 point)
Default route	Configure a default route out S0/0/0.	(1/2 point)

Note: Do not configure G0/1 at this time.

Step 3: Configure R2.

Configuration tasks for R2 include the following:

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Configuration Item or Task	Specification	Points
Disable DNS lookup		(1/2 point)
Router name	R2	(1/2 point)
Encrypted privileged exec password	class	(1/2 point)
Console access password	cisco	(1/2 point)
Telnet access password	cisco	(1/2 point)
Encrypt the clear text passwords		(1/2 point)
Enable HTTP server		(1/2 point)
MOTD banner	Unauthorized Access is Prohibited!	(1/2 point)
Interface S0/0/0	Set the description Set the Layer 3 IPv4 address. Use the next available address in the subnet. Activate Interface	(1 point)
Interface S0/0/1	Set the description Set the Layer 3 IPv4 address. Use the first available address in the subnet. Set clocking rate to 128000 Activate Interface	(1 point)
Interface G0/0 (Simulated Internet)	Set the Description Set the Layer 3 IPv4 address. Use the first available address in the subnet. Activate Interface	(1 point)
Interface Loopback 0 (Simulated Web Server)	Set the description. Set the Layer 3 IPv4 address.	(1/2 point)
Default route	Configure a default route out G0/0.	(1/2 point)

Step 4: Configure R3.

Configuration tasks for R3 include the following:

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Configuration Item or Task	Specification	Points
Disable DNS lookup		(1/2 point)
Router name	R3	(1/2 point)
Encrypted privileged exec password	class	(1/2 point)
Console access password	cisco	(1/2 point)
Telnet access password	cisco	(1/2 point)
Encrypt the clear text passwords		(1/2 point)
MOTD banner	Unauthorized Access is Prohibited!	(1/2 point)
Interface S0/0/1	Set the description Set the Layer 3 IPv4 address. Use the next available address in the subnet. Activate Interface	(1/2 point)
Interface Loopback 4	Set the Layer 3 IPv4 address. Use the first available address in the subnet.	(1/2 point)
Interface Loopback 5	Set the Layer 3 IPv4 address. Use the first available address in the subnet.	(1/2 point)
Interface Loopback 6	Set the Layer 3 IPv4 address. Use the first available address in the subnet.	(1/2 point)
Default route	Configure a default route out S0/0/1.	(1/2 point)

Step 5: Configure S1.

Configuration tasks for S1 include the following:

Configuration Item or Task	Specification	Points
Disable DNS lookup		(1/2 point)
Switch name	S1	(1/2 point)
Encrypted privileged exec password	class	(1/2 point)
Console access password	cisco	(1/2 point)
Telnet access password	cisco	(1/2 point)
Encrypt the clear text passwords		(1/2 point)
MOTD banner	Unauthorized Access is Prohibited!	(1/2 point)

Step 6: Configure S3

Configuration tasks for S3 include the following:

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Configuration Item or Task	Specification	Points
Disable DNS lookup		(1/2 point)
Switch name	S3	(1/2 point)
Encrypted privileged exec password	class	(1/2 point)
Console access password	cisco	(1/2 point)
Telnet access password	cisco	(1/2 point)
Encrypt the clear text passwords		(1/2 point)
MOTD banner	Unauthorized Access is Prohibited!	(1/2 point)

Step 7: Verify network connectivity.

Use the **ping** command to test connectivity between network devices.

Use the following table to methodically verify connectivity with each network device. Take corrective action to establish connectivity if a test fails:

From	To	IP Address	Ping Results	Points
R1	R2, S0/0/0			(1/2 point)
R2	R3, S0/0/1			(1/2 point)
Internet PC	Default Gateway			(1/2 point)

Note: It may be necessary to disable the PC firewall for pings to be successful.

Instructor Sign-off Part 2: ______________________

Points: _________ of 28

Part 3: Configure Switch Security, VLANS, and Inter VLAN Routing

Total points: 14

Time: 15 minutes

Step 1: Configure S1.

Configuration tasks for S1 include the following:

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Configuration Item or Task	Specification	Points
Create the VLAN database	Use Topology VLAN Key table to create and name each of the listed VLANS.	(1 point)
Assign the management IP address.	Assign the Layer 3 IPv4 address to the Management VLAN. Use the IP address assigned to S1 in the Topology diagram.	(1/2 point)
Assign the default-gateway	Assign the first IP address in the subnet as the default-gateway.	(1/2 point)
Force trunking on Interface F0/3	Use VLAN 1 as the native VLAN.	(1/2 point)
Force trunking on Interface F0/5	Use VLAN 1 as the native VLAN.	(1/2 point)
Configure all other ports as access ports	Use the interface range command.	(1/2 point)
Assign F0/6 to VLAN 31		(1/2 point)
Shutdown all unused ports.		(1/2 point)

Step 2: Configure S3.

Configuration tasks for S3 include the following:

Configuration Item or Task	Specification	Points
Create the VLAN database	Use Topology VLAN Key Table to create each of the listed VLANS. Name each VLAN.	(1 point)
Assign the management IP address.	Assign the Layer 3 IPv4 address to the Management VLAN. Use the IP address assigned to S3 in the Topology diagram.	(1/2 point)
Assign the default-gateway	Assign the first IP address in the subnet as the default-gateway	(1/2 point)
Force trunking on Interface F0/3	Use VLAN 1 as the native VLAN.	(1/2 point)
Configure all other ports as access ports	Use the interface range command.	(1/2 point)
Assign F0/18 to VLAN 33		(1/2 point)
Shutdown all unused ports.		(1/2 point)

Step 3: Configure R1.

Configuration tasks for R1 include the following:

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Configuration Item or Task	Specification	Points
Configure 802.1Q subinterface .31 on G0/1	Description Accounting LAN Assign VLAN 31. Assign the first available address to this interface.	(1 point)
Configure 802.1Q subinterface .33 on G0/1	Description Engineering LAN Assign VLAN 33. Assign the first available address to this interface.	(1 point)
Configure 802.1Q subinterface .99 on G0/1	Description Management LAN Assign VLAN 99. Assign the first available address to this interface.	(1 point)
Activate Interface G0/1		(1/2 point)

Step 4: Verify network connectivity.

Use the **ping** command to test connectivity between the switches and R1.

Use the following table to methodically verify connectivity with each network device. Take corrective action to establish connectivity if a test fails:

From	To	IP Address	Ping Results	Points
S1	R1, VLAN 99 address			(1/2 point)
S3	R1, VLAN 99 address			(1/2 point)
S1	R1, VLAN 31 address			(1/2 point)
S3	R1, VLAN 33 address			(1/2 point)

Instructor Sign-off Part 2: ______________________

Points: _________ of 14

Part 4: Configure OSPFv2 Dynamic Routing Protocol

Total points: 24

Time: 25 minutes

Step 1: Configure OSPFv2 on R1.

Configuration tasks for R1 include the following:

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Configuration Item or Task	Specification	Points
OSPF Process ID	1	(1/2 point)
Router ID	1.1.1.1	(1/2 point)
Advertise directly connected Networks	Use classless network addresses Assign all directly connected networks to Area 0	(1 point)
Set all LAN interfaces as passive		(1 point)
Change the default cost reference bandwidth to support Gigabit interface calculations	1000	(1 point)
Set the serial interface bandwidth	128 Kb/s	(1 point)
Adjust the metric cost of S0/0/0	Cost: 7500	(1 point)

Step 2: Configure OSPFv2 on R2.

Configuration tasks for R2 include the following:

Configuration Item or Task	Specification	Points
OSPF Process ID	1	(1 point)
Router ID	2.2.2.2	(1 point)
Advertise directly connected Networks	Use classless network addresses **Note:** Omit the G0/0 network.	(1 point)
Set the LAN (Loopback) interface as passive		(1 point)
Change the default cost reference bandwidth to allow for Gigabit interfaces	1000	(1 point)
Set the bandwidth on all serial interfaces	128 Kb/s	(1 point)
Adjust the metric cost of S0/0/0	Cost: 7500	(1 point)

Step 3: Configure OSPFv2 on R3.

Configuration tasks for R3 include the following:

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Configuration Item or Task	Specification	Points
OSPF Process ID	1	(1/2 point)
Router ID	3.3.3.3	(1/2 point)
Advertise directly connected Networks	Use classless network addresses Assign interfaces to Area 0 Use a single summary address for the LAN (loopback) interfaces.	(1 point)
Set all LAN (Loopback) interfaces as passive		(1 point)
Change the default cost reference bandwidth to support Gigabit interface calculations	1000	(1 point)
Set the serial interface bandwidth	128 Kb/s	(1 point)

Step 4: Verify OSPF information.

Verify that OSPF is functioning as expected. Enter the appropriate CLI command to discover the following information:

Question	Response	Points
What command will display all connected OSPFv2 routers?		(1 point)
What command displays a summary list of OSPF interfaces that includes a column for the cost of each interface?		(1 point)
What command displays the OSPF Process ID, Router ID, Address summarizations, Routing Networks, and passive interfaces configured on a router?		(1 point)
What command displays only OSPF routes?		(1 point)
What command displays detail information about the OSPF interfaces, including the authentication method?		(1 point)
What command displays the OSPF section of the running-configuration?		(1 point)

Instructor Sign-off Part 3: ______________________

Points: _________ of 24

Part 5: Implement DHCP and NAT for IPv4

Total points: 13

Time: 25 minutes

Step 1: Configure R1 as the DHCP server for VLANs 31 and 33.

Configuration tasks for R1 include the following:

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Configuration Item or Task	Specification	Points
Reserve the first 20 IP addresses in VLAN 31 for static configurations		(1 point)
Reserve the first 20 IP addresses in VLAN 33 for static configurations		(1 point)
Create a DHCP pool for VLAN 31	Name: ACCT DNS-Server: 10.10.10.11 Domain-Name: ccna-sba.com Set the default gateway.	(1 point)
Create a DHCP pool for VLAN 33	Name: ENGNR DNS-Server: 10.10.10.11 Domain-Name: ccna-sba.com Set the default gateway.	(1 point)

Step 2: Configure Static and Dynamic NAT on R2.

Configuration tasks for R2 include the following:

Configuration Item or Task	Specification	Points
Create a local database with 1 user account	Username: **webuser** Password: **cisco12345** Privilege level: **15**	(1 point)
Enable HTTP server service		(1/2 point)
Configure the HTTP server to use the local database for authentication		(1/2 point)
Create a static NAT to the Web Server	Inside Global Address: **209.165.200.229**	(1 point)
Assign the inside and outside interface for the static NAT		(1 point)
Configure the dynamic NAT inside private ACL	Access List: 1 Allow the Accounting and Engineering networks on R1 to be translated. Allow a summary of the LANs (loopback) networks on R3 to be translated.	(1 point)
Define the pool of usable public IP addresses	Pool Name: **INTERNET** Pool of addresses include: **209.165.200.225 – 209.165.200.228**	(1 point)
Define the dynamic NAT translation		(1 point)

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Step 3: Verify DHCP and Static NAT.

Use the following tasks to verify that DHCP and Static NAT settings are functioning correctly. It may be necessary to disable the PC firewall for pings to be successful:

Test	Results	Points
Verify that PC-A acquired IP information from the DHCP server		(1/2 point)
Verify that PC-C acquired IP information from the DHCP server		(1/2 point)
Verify that PC-A can ping PC-C. **Note**: It may be necessary to disable the PC firewall		(1/2 point)
Use a Web browser on the Internet PC to access the Web server (209.165.200.229). Login with Username: **webuser**, Password: **cisco12345**		(1/2 point)

Note: Verification of dynamic NAT will be performed in Part 6.

Instructor Sign-off Part 2: ______________________

Points: _________ of 13

Part 6: Configure and Verify Access Control Lists (ACLs)

Total points: 13

Time: 25 minutes

Step 1: Restrict access to VTY lines on R2.

Configuration Item or Task	Specification	Points
Configure a named access list to only allow R1 to telnet to R2.	ACL Name: **ADMIN-MGT**	(2 points)
Apply the named ACL to the VTY lines		(1 point)
Verify ACL is working as expected,		(1 point)

Step 2: Secure the network from Internet traffic.

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Configuration Item or Task	Specification	Points
Configure an Extended ACL to: • Allow Internet hosts WWW access to the simulated web server on R2 by accessing the static NAT address (209.165.200.229) that you configured in Part 3. • Prevent traffic from the Internet from pinging internal networks, while continuing to allow LAN interfaces to ping the Internet PC.	ACL No.: **101**	(2 points)
Apply ACL to the appropriate interface(s)		(1 point)
Verify ACL is working as expected	From the Internet PC: • Ping PC-A (Pings should be unreachable.) • Ping PC-C (Pings should be unreachable.) From R1, Ping the Internet PC (Pings should be successful.)	(1 point)

Note: It may be necessary to disable the PC firewall for pings to be successful.

Step 3: Enter the appropriate CLI command needed to display the following:

Command Description	Student Input (command)	Points
Display the matches an access-list has received since the last reset.		(1 point)
Reset access-list counters.		(1 point)
What command is used to display what ACL is applied to an interface and the direction that it is applied		(1 point)
What command displays the NAT translations?	**Note**: The translations for PC-A and PC-C were added to the table when the Internet PC attempted to ping these PCs in Step 2. Pinging the Internet PC from PC-A or PC-C will not add the translations to the table because of the way the Internet is being simulated on the network.	(1 point)
What command is used to clear dynamic NAT translations?		(1 point)

Instructor Sign-off Part 4: ______________________

Points: _________ of 13

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Part 7: Cleanup

NOTE: DO NOT PROCEED WITH CLEANUP UNTIL YOUR INSTRUCTOR HAS GRADED YOUR SKILLS EXAM AND HAS INFORMED YOU THAT YOU MAY BEGIN CLEANUP.

Before turning off power to the routers, remove the NVRAM configuration files (if saved) from all devices.

Disconnect and neatly put away all cables that were used in the Final.

Router Interface Summary Table

Router Interface Summary				
Router Model	**Ethernet Interface #1**	**Ethernet Interface #2**	**Serial Interface #1**	**Serial Interface #2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/0/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

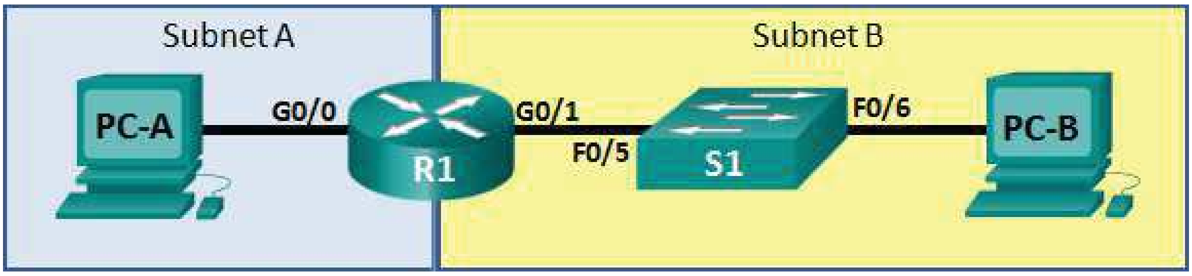
© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

CCNA: Introduction to Networks

Skills Assessment – Student Training (Answer Key)

Instructor Note: Red font color or Gray highlights indicate text that appears in the instructor copy only.

Topology



Assessment Objectives

Part 1: Develop the IPv4 Address Scheme (15 points, 20 minutes)

Part 2: Initialize and Reload Devices (10 points, 5 minutes)

Part 3: Configure Device IPv4 and Security Settings (30 points, 20 minutes)

Part 4: Test and Verify IPv4 End-to-End Connectivity (8 points, 10 minutes)

Part 5: Configure IPv6 Addressing on R1 (10 points, 10 minutes)

Part 6: Test and Verify IPv6 End-to-End Connectivity (7 points, 10 minutes)

Part 7: Use the IOS CLI to Gather Device Information (10 points, 10 minutes)

Part 8: Save the R1 Configuration to a TFTP Server (10 points, 10 minutes)

Scenario

In this Skills Assessment (SA) you will configure the devices in a small network. You must configure a router, switch and PCs to support both IPv4 and IPv6 connectivity. You will configure security, including SSH, on the router. You will test and document the network using common CLI commands. Finally, you will save the router configuration to a TFTP server.

Instructor Note: For the student version of this exam, the instructor should build the network and connect devices prior to the student starting the exam. This will save time and reduce wear on cables and equipment. The student will need to initialize and reload devices. Scoring is adjusted accordingly.

Instructor Note: The router used with this SA is a Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switch used is a Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the SA. Refer to the **Hiba! A hivatkozási forrás nem található.** at the end of the lab for the correct interface identifiers.

Instructor Note: For the initial SBA setup, the router and switch should have a startup-configuration saved with hostnames (Rtr & Sws). The router should also have a loopback address configured and the switch should have vlan 99 configured. These configurations will be used to verify that the student initialized the devices correctly in Part 2, Step 3. It is recommended that these configurations are saved to flash as SBA_Init and used to reset the device for the next student.

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Instructor Note: Sample scoring and estimated times for each exam part are provided. These can be adjusted by the instructor as necessary to suit the testing environment. Total points for the exam are 100 and total time is estimated at 100 minutes. The instructor may elect to deduct points if excessive time is taken for a part of the assessment.

Instructor Note: In the first task, enter in an IP address / mask, and fill in an appropriate value of hosts per subnet. Appropriate IP address / mask values can be taken from the following table:

IP Address			
Start	**End**	**Subnet Mask**	**Bits**
10.0.0.0	10.255.255.255	255.0.0.0	8
172.16.0.0	172.31.255.255	255.240.0.0	12
192.168.0.0	192.168.0.255	255.255.255.0	24
209.165.200.224	209.165.200.255	255.255.255.224	27
209.165.201.0	209.165.201.31	255.255.255.224	27
209.165.202.128	209.165.202.159	255.255.255.224	27

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cable to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Instructor Note: Part 8 requires a TFTP server. Tftpd32 is recommended It must be preinstalled on PC-A.

Instructor Note: If Windows XP hosts are used, it may be necessary to install IPv6. Refer to Lab 0.0.0.2: *Installing the IPv6 Protocol with Windows XP* in the Instructor Lab Manual.

Part 1: Develop the IPv4 Addressing Scheme

Ref labs: 8.2.1.3 Lab - Designing and Implementing a Subnetted IPv4 Addressing Scheme

8.2.1.4 Lab - Designing and Implementing a VLSM Addressing Scheme

Total points: 15

Time: 20 minutes

Given an IP address and mask of ____ (address / mask), design an IP addressing scheme that satisfies the following requirements:

Subnet	Number of Hosts
Subnet A	
Subnet B	

The 0th subnet is used. No subnet calculators may be used. All work must be shown on the other side of this page.

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Subnet A		
Specification	**Student Input**	**Points**
Number of bits in the subnet	Answers will vary.	(5 points)
IP mask (binary)	Answers will vary.	
New IP mask (decimal)	Answers will vary.	
Maximum number of usable subnets (including the 0th subnet)	Answers will vary.	
Number of usable hosts per subnet	Answers will vary.	
IP Subnet	Answers will vary.	
First IP Host address	Answers will vary.	
Last IP Host address	Answers will vary.	

Subnet B		
Specification	**Student Input**	**Points**
Number of bits in the subnet	Answers will vary.	(5 points)
IP mask (binary)	Answers will vary.	
New IP mask (decimal)	Answers will vary.	
Maximum number of usable subnets (including the 0th subnet)	Answers will vary.	
Number of usable hosts per subnet	Answers will vary.	
IP Subnet	Answers will vary.	
First IP Host address	Answers will vary.	
Last IP Host address	Answers will vary.	

Host computers will use the first IP address in the subnet. The network router will use the LAST network host address. The switch will use the second to the last network host address.

Write down the IP address information for each device:

Device	IP address	Subnet Mask	Gateway	Points
PC-A				(5 points)
R1-G0/0			N/A	
R1-G0/1			N/A	
S1			N/A	
PC-B				

Before proceeding, verify your IP addresses with the instructor.

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Instructor Sample: Given an IP address and mask of `192.168.25.0/24 (address/mask)`, design an IP addressing scheme that satisfies the following requirements:

Subnet	Number of Hosts
Subnet A	2
Subnet B	Between 20 and 30

Subnet A		
Specification	**Student Input**	**Points**
Number of bits in the subnet	6	(5 points)
IP mask (binary)	11111111.11111111.11111111.11111100	
New IP mask (decimal)	255.255.255.252	
Maximum Number of usable hosts per subnet	2	
IP Subnet	192.168.25.32	
First IP Host address	192.168.25.33	
Last IP Host address	192.168.25.34	

Subnet B		
Specification	**Student Input**	**Points**
Number of bits in the subnet	3	(5 points)
IP mask (binary)	11111111.11111111.11111111.11100000	
New IP mask (decimal)	255.255.255.224	
Number of usable hosts per subnet	30	
IP Subnet	192.168.25.0	
First IP Host address	192.168.25.1	
Last IP Host address	192.168.25.30	

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Device	IP address	Mask	Gateway	Points
PC-A	192.168.25.33	255.255.255.252	192.168.25.34	(5 points)
Router1-G0/0	192.168.25.34	255.255.255.252	N/A	
Router1-G0/1	192.168.25.30	255.255.255.224	N/A	
S1-VLAN1	192.168.25.29	255.255.255.224	N/A	
PC-B	192.168.25.1	255.255.255.224	192.168.25.30	

Instructor Sign-off Part 1: ______________________

Points: _________ of 15

Part 2: Initialize and Reload Devices

Ref lab: 0.0.0.1 Lab - Initializing and Reloading a Router and Switch

Total points: 10

Time: 5 minutes

Step 1: Initialize and reload router and switch. (10 points)

Erase the startup configurations and VLANs from the router and switch and reload the devices.

Before proceeding, have your instructor verify device initializations.

Task	IOS Command	Points
Erase the startup-config file on the Router.	Rtr# **erase startup-config**	(2 point)
Reload the Router.	Rtr# **reload** (Verify by using **show run** command to see if loopback address is missing. Hostname should be reset back to **Router**.)	(2 point)
Erase the startup-config file on the Switch.	Sws# **erase startup-config**	(2 point)
Delete the vlan.dat file on the Switch	Sws# **del vlan.dat** (Verify by using the **show vlan** command and look for vlan 99, if vlan.dat file was deleted vlan 99 will not be listed.)	(2 point)
Reload the Switch.	Sws# **reload** (To verify check to see if hostname is reset back to **Switch**.)	(2 point)

Instructor Sign-off Part 2: _________________________

Points: __________ of 10

Part 3: Configure Device IPv4 and Security Settings

Ref lab: 11.2.4.6 Lab - Securing Network Devices

Total points: 30

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Time: 20 minutes

Step 1: Configure host computers.

After configuring each host computer, record the host network settings with the **ipconfig /all** command.

PC-A Network Configuration		Points
Description	Answers will vary.	(2 points)
Physical Address	Answers will vary.	
IP Address	Answers will vary.	
Subnet Mask	Answers will vary.	
Default Gateway	Answers will vary.	

PC-B Network Configuration		Points
Description	Answers will vary.	(2 points)
Physical Address	Answers will vary.	
IP Address	Answers will vary.	
Subnet Mask	Answers will vary.	
Default Gateway	Answers will vary.	

Step 2: Configure R1.

Configuration tasks for R1 include the following:

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Task	Specification	Points
Disable DNS lookup		(1 point)
Router name	R1	(1 point)
Domain name	ccna-lab.com	(1 point)
Encrypted privileged exec password	ciscoenpass	(1 point)
Console access password	ciscoconpass	(1 point)
Telnet access password	ciscovtypass	(1 point)
Set the minimum length for passwords	10 characters	(2 points)
Create an administrative user in the local database	Username: admin Password: admin1pass	(2 points)
Set login on VTY lines to use local database		(1 point)
Set VTY lines to accept ssh and telnet connections only		(2 points)
Encrypt the clear text passwords		(1 point)
MOTD Banner		(1 point)
Interface G0/0	Set the description Set the Layer 3 IPv4 address Activate Interface	(2 points)
Interface G0/1	Set the description Set the Layer 3 IPv4 address Activate Interface	(2 points)
Generate a RSA crypto key	1024 bits modulus	(2 points)

Instructor Note: Have the student connect to R1, and then verify the proper configuration.

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Task	Specification	IOS Commands
Disable DNS lookup		R1# **show run** (Look for: **no ip domain lookup**)
Router name	R1	(Look for : **R1>** or **R1#** command prompt)
Domain name	ccna-lab.com	R1# **show run** (Look for: **ip domain-name ccna-lab.com**)
Encrypted privileged exec password	ciscoenpass	R1> **enable** (Type in privileged exec password)
Console access password	ciscoconpass	R1# **exit** (Type in access password)
Telnet access password	ciscovtypass	R1# **show run** (Look under line VTY 0 4 for: **password 7 00071A1507541D1216314D5D1A**)
Set the minimum length for passwords	10 characters	R1# **show run** (Look for: **security passwords min-length 10**)
Create an administrative user the in local database	User: admin Password: admin1pass	R1# **telnet 192.168.25.34** (G0/0 interface IP address) (Type in the username and password. Type exit to leave telnet session.)
Set login on VTY lines to use local database		R1# **show run** (Look under VTY 0 4 for: **login local**)
Set VTY lines to accept ssh and telnet connections only		R1# **show run** (Look under line VTY 0 4 for: **transport input telnet ssh**)
Encrypt the plain text passwords		R1# **show run** (Look for: **service password-encryption**)
MOTD Banner		(Verify banner during above step)
Interface G0/0	Set the description Set the Layer 3 IPv4 address Activate Interface	Router1# **show ip interface g0/0** (Look for IP address, description, and verify that interface is not administratively down.)
Interface G01	Set the description Set the Layer 3 IPv4 address Activate Interface	Router1# **show ip interface g0/1** (Look for IP address, description, and verify that interface is not administratively down.)
Generate a RSA crypto key.	1024 bits modulus	R1# **show crypto key mypubkey rsa** (Look for Key name= R1.ccna-lab.com.)

Step 3: Configure S1.

Configuration tasks for R1 include the following:

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Task	Specification	Points
Switch name	S1	(1 point)
Configure Management Interface (SVI)	Set the Layer 3 IPv4 address	(1 point)
Encrypted privileged exec password	ciscoenpass	(1 point)
Console access password	ciscoconpass	(1 point)
Telnet access password	ciscovtypass	(1 point)

Instructor Note: Have the student connect to S1, and then verify the proper configuration.

Task	**Specification**	**IOS Commands**
Switch name	S1	(Look for : **S1>** or **S1#** command prompt)
Console access password	ciscoconpass	S1> **exit** (Type in access password)
Encrypted privileged exec password	ciscoenpass	S1> **enable** (Type in privileged exec password)
Telnet access password	ciscovtypass	S1# **show run** (Look under line VTY 0 4 for: **password 7 00071A1507541D1216314D5D1A**)
Configure Management Interface (SVI)	Set the Layer 3 IPv4 address	S1# **show ip interface brief** (Look at interface VLAN1 and verify that the correct IP address has been assigned.)

Instructor Sign-off Part 3: ______________________

Points: _________ of 30

Part 4: Test and Verify IPv4 End-to-End Connectivity

Ref lab: 7.3.2.7 Lab - Testing Network Connectivity with Ping and Traceroute

Total points: 8

Time: 10 minutes

Step 1: Verify network connectivity.

Use the ping command to test connectivity between all network devices.

Note: If pings to host computers fail, temporarily disable the computer firewall and retest. To disable a Windows 7 firewall, select Start > Control Panel > System and Security > Windows Firewall > Turn Windows Firewall on or off, select **Turn off Windows Firewall**, and click **OK**.

Use the following table to methodically verify connectivity with each network device. Take corrective action to establish connectivity if a test fails:

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

From	To	IP Address	Ping Results	Points
PC-A	R1, G0/0	Answers will vary.	Should be successful.	(1 point)
PC-A	R1, G0/1	Answers will vary.	Should be successful.	(1 point)
PC-A	S1 VLAN 1	Answers will vary.	Should be successful.	(1 point)
PC-A	PC-B	Answers will vary.	Should be successful.	(1 point)
PC-B	R1, G0/1	Answers will vary.	Should be successful.	(1 point)
PC-B	R1, G0/0	Answers will vary.	Should be successful.	(1 point)
PC-B	S1 VLAN 1	Answers will vary.	Should be successful.	(1 point)

In addition to the ping command, what other command is useful in displaying network delay and breaks in the path to the destination? (1 point)

____

tracert or traceroute

Instructor Sign-off Part 4: ______________________

Points: _________ of 8

Part 5: Configure IPv6 Addressing on R1

Lab ref: 7.2.5.5 Lab - Configuring IPv6 Addresses on Network Devices

Total points: 10

Time: 10 minutes

Given an IPv6 network address of **2001:DB8:ACAD::/48**, configure IPv6 addresses for the Gigabit interfaces on R1. Use **FE80::1** as the link-local address on both interfaces.

Instructor Note: This will allow the PCs to obtain their IP address and default gateway information automatically using Stateless Address Autoconfiguration (SLAAC). The instructor may wish to have students configure the PC IP address and default gateway manually.

Step 1: Configure R1.

Configuration tasks for R1 include the following:

Task	Specification	Points
Configure G0/0 to use the first address in subnet A.	Assign the IPv6 unicast address Assign the IPv6 link-local address	(4 points)
Configure G0/1 to use the first address in subnet B.	Assign the IPv6 unicast address Assign the IPv6 link-local address	(4 points)
Enable IPv6 unicast routing.		(2 points)

Instructor Note: Have the student connect to R1, and then verify the proper configuration.

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Task	Specification	IOS Commands
Configure G0/0 to use the first address in subnet A.	**2001:DB8:ACAD:A::1/64** **FE80::1**	R1# **sh ipv6 interface g0/0** (Verify that the link-local and global unicast address is set correctly.)
Configure G0/1 to use the first address in subnet B.	**2001:DB8:ACAD:B::1/64** **FE80::1**	R1# **sh ipv6 interface g0/1** (Verify that the link-local and global unicast address is set correctly.)
Enable IPv6 unicast routing.	**ipv6 unicast-routing**	R1# **show ipv6 interface g0/1** (Verify that **FF02::02** is listed in the Joined Group Addresses. You can also use **show run** to verify that the command is present in the running configuration.)

Instructor Sign-off Part 5: ______________________

Points: _________ of 10

Part 6: Test and Verify IPv6 End-to-End Connectivity

Instructor Note: If students were instructed to configure the PC-A and PC-B IP address and default gateway manually, verify the correct addressing accordingly.

Lab ref: 7.2.5.5 Lab - Configuring IPv6 Addresses on Network Devices

Total points: 7

Time: 10 minutes

Step 1: Obtain the IPv6 address assigned to host PCs.

PC-A IPv6 Network Configuration		Points
Description	Answers will vary.	(1 point)
Physical Address	Answers will vary.	
IPv6 Address	Answers will vary but will start with: 2001:DB8:ACAD:A:x:x:x:x **Instructor Note:** Student may have configured the IP address manually based on instructions.	
Default Gateway	Should be FE80::1%11 **Instructor Note:** Student may have configured the default gateway IP address manually based on instructions.	

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

PC-B IPv6 Network Configuration		Points
Description	Answers will vary.	(1 point)
Physical Address	Answers will vary.	
IPv6 Address	Answers will vary but will start with: 2001:DB8:ACAD:B:x:x:x:x **Instructor Note:** Student may have configured the IP address manually based on instructions.	
IPv6 Default Gateway	Should be FE80::1%11 **Instructor Note:** Student may have configured the default gateway IP address manually based on instructions.	

Step 2: Use the ping command to verify network connectivity.

IPv6 network connectivity can be verified with the ping command. Use the following table to methodically verify connectivity with each network device. Take corrective action to establish connectivity if a test fails:

From	To	IP Address	Ping Results	Points
PC-A	R1, G0/0	Answers will vary.	Should be successful.	(1 point)
PC-A	R1, G0/1	Answers will vary.	Should be successful.	(1 point)
PC-A	PC-B	Answers will vary.	Should be successful.	(1 point)
PC-B	R1, G0/1	Answers will vary.	Should be successful.	(1 point)
PC-B	R1, G0/0	Answers will vary.	Should be successful.	(1 point)

Instructor Sign-off Part 6: ______________________

Points: _________ of 7

Part 7: Use the IOS CLI to Gather Device Information

Ref lab: 11.3.4.6 Lab - Using the CLI to Gather Network Device Information

Total points: 10

Time: 10 minutes

Step 1: Issue the appropriate command to discover the following information:

Instructor Note: Answers for step 1 will vary based on router model and IOS.

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Description	Student Input	Points
Router Model	Cisco 1941 Router	(2 points)
IOS Image File	C1900-universalk9-mz.SPA.152-4.M1.bin	
Total RAM	512 MB	
Total Flash Memory	250880K bytes	
Configuration Register	0x2102	
CLI Command Used	show version	

Step 2: Enter the appropriate CLI command needed to display the following on R1:

Command Description	Student Input (command)	Points
Display a summary of important information about the interfaces on R1.	show ip interface brief	(1 point)
Display the IPv4 routing table.	show ip route	(1 point)
Display the Layer 2 to Layer 3 mapping of addresses on R1.	show arp	(1 point)
Display detailed IPv4 information about interface G0/0 on R1.	show interface g0/0	(1 point)
Display the IPv6 routing table.	show ipv6 route	(1 point)
Display a summary of IPv6 interface addresses and status.	show ipv6 interface brief	(1 point)
Display information about the devices connected to R1. Information should include Device ID, Local Interface, Hold time, Capability, Platform, and Port ID.	show cdp neighbor	(1 point)
Save the current configuration so it will be used the next time the router is started.	copy running-config startup-config	(1 point)

Instructor Sign-off Part 7: ______________________

Points: _________ of 10

Part 8: Save the R1 Configuration to a TFTP Server.

Ref lab: 11.4.2.7 Lab - Managing Device Configuration Files Using TFTP, Flash and USB

Total points: 10

Time: 10 minutes

Save the current configuration for R1 to the TFTP Server on PC-A. Tftpd32 software has been installed on PC-A. You will need to start this program before you begin. Document the command used below:

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Description	Student Input	Points
CLI Command	R1# copy running-config tftp:	(5 Points)
Address of remote host	Answers will vary, should be PC-A IPv4 address.	
Destination Filename	Answers may vary, "r1-confg" is the default name.	

Instructor Sign-off Part 8: ______________________

Points: _________ of 10

Part 9: Cleanup

NOTE: DO NOT PROCEED WITH CLEANUP UNTIL YOUR INSTRUCTOR HAS GRADED YOUR SKILLS EXAM AND HAS INFORMED YOU THAT YOU MAY BEGIN CLEANUP.

Unless directed otherwise by the instructor, restore host computer network connectivity, and then turn off power to the host computers.

Before turning off power to the router and switch, remove the NVRAM configuration files (if saved) from both devices.

Disconnect and neatly put away all LAN cables that were used in the Final.

Router Interface Summary Table

Router Interface Summary				
Router Model	**Ethernet Interface #1**	**Ethernet Interface #2**	**Serial Interface #1**	**Serial Interface #2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				

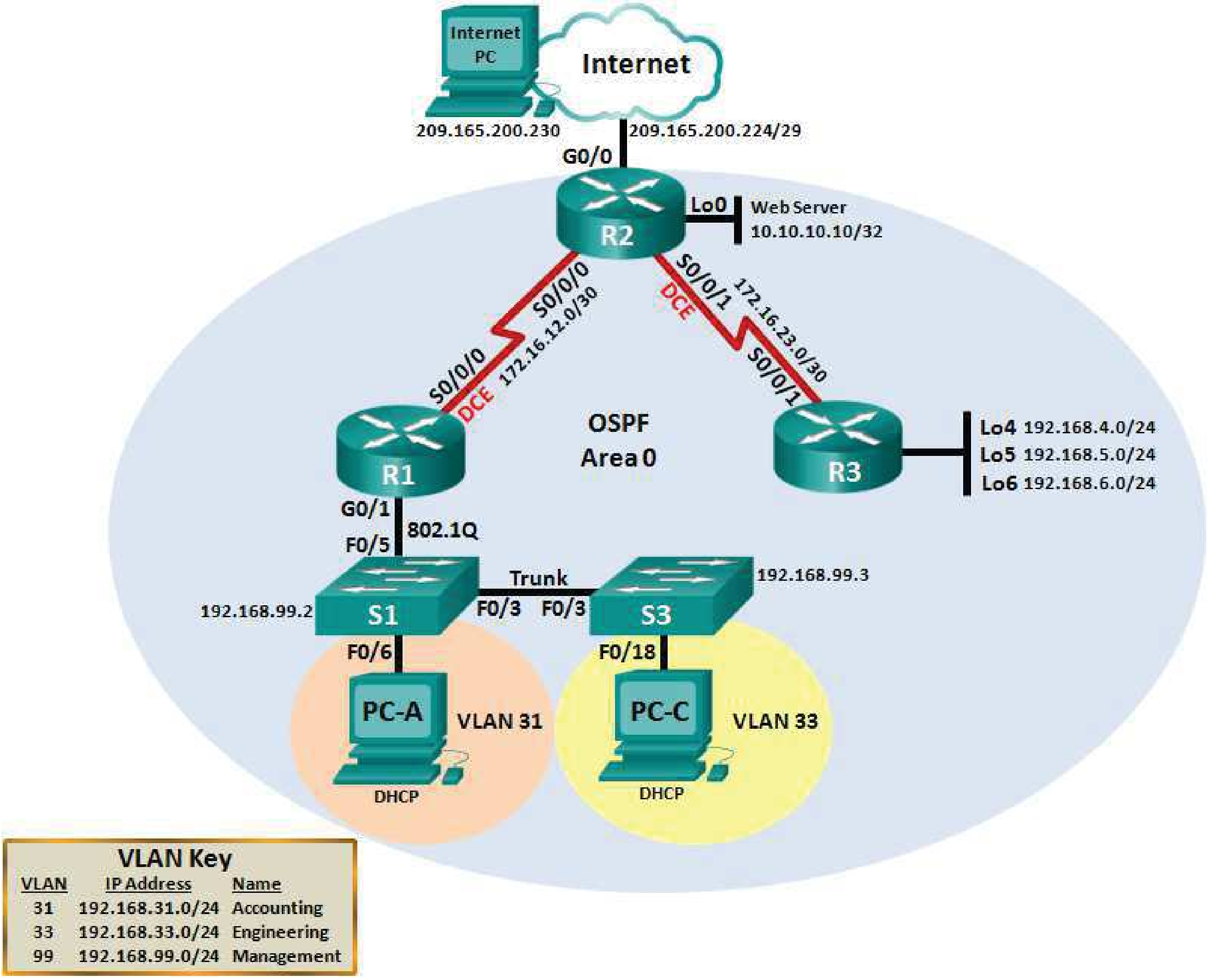
© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

CCNA: Routing and Switching Essentials

Skills Assessment – Student Training (Answer Key)

Instructor Note: Red font color or Gray highlights indicate text that appears in the instructor copy only.

Topology



VLAN Key

VLAN	IP Address	Name
31	192.168.31.0/24	Accounting
33	192.168.33.0/24	Engineering
99	192.168.99.0/24	Management

Assessment Objectives

Part 1: Initialize Devices (8 points, 5 minutes)

Part 2: Configure Device Basic Settings (28 points, 30 minutes)

Part 3: Configure Switch Security, VLANs, and Inter-VLAN Routing (14 points, 15 minutes)

Part 4: Configure OSPFv2 Dynamic Routing Protocol (24 points, 25 minutes)

Part 5: Implement DHCP and NAT (13 points, 25 minutes)

Part 6: Configure and Verify Access Control Lists (ACLs) (13 points, 25 minutes)

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Scenario

In this Skills Assessment (SA) you will configure a small network. You will configure routers, switches, and PCs to support IPv4 connectivity, switch security, and inter VLAN routing. You will then configure the devices with OSPFv2, DHCP, and dynamic and static NAT. Access control lists (ACLs) will be applied for added security. You will test and document the network using common CLI commands throughout the assessment.

Instructor Note: For the student version of this exam, the instructor should build the network and connect devices prior to the student starting the exam. This will save time and reduce wear on cables and equipment. The student will need to initialize and reload devices. Scoring is adjusted accordingly.

Instructor Note: The routers used with this SA are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). Other routers and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the SA. Refer to the Router Interface Summary Table at the end of the lab for the correct interface identifiers.

Instructor Note: For the initial SBA setup, the routers should have a startup-configuration saved with a hostname (Rtr). The router should also have a loopback address configured. The switches should have a startup-configuration saved with a hostname (Sw) and have VLAN 99 created. These configurations will be used to verify that the student initialized the devices correctly in Part 1, Step 1. It is recommended that these configurations are saved to flash as SBA_Init and used to reset the device for the next student.

Instructor Note: Sample scoring and estimated times for each exam part are provided. These can be adjusted by the instructor as necessary to suit the testing environment. Total points for the exam are 100 and total time is estimated at 125 minutes. The instructor may elect to deduct points if excessive time is taken for a part of the assessment.

Required Resources

- 3 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 3 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cable to configure the Cisco IOS devices via the console ports
- Ethernet and Serial cables as shown in the topology

Part 1: Initialize Devices

Total points: 8

Time: 5 minutes

Step 1: Initialize and reload the routers and switches.

Erase the startup configurations reload the devices.

Before proceeding, have your instructor verify device initializations.

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Task	IOS Command	Points
Erase the startup-config file on all routers.	R1# **erase startup-config**	1½ points (½ point per router)
Reload all routers.	R1# **reload** (Hostnames should be reset back to **Router**.)	1 ½ points (½ point per router)
Erase the startup-config file on all switches and remove the old VLAN database.	S1# **erase startup-config** S1# **del vlan.dat**	2 points (1 point per switch)
Reload both switches.	S1# **reload** (Hostnames should be reset back to **Switch**.)	2 points (1 point per switch)
Verify VLAN database is absent from flash on both switches.	S1# **show flash** (Have student execute the CLI command on the switch.)	1 point (½ point per switch)

Instructor Sign-off Part 1: ________________________

Points: __________ of 8

Part 2: Configure Device Basic Settings

Ref lab: 2.1.1.6 Lab - Configuring Basic Switch Settings

Ref lab: 4.1.4.6 Lab – Configuring Basic Router Settings with IOS CLI

Total points: 28

Time: 30 minutes

Step 1: Configure the Internet PC.

Configuration tasks for the Internet PC include the following (Refer to Topology for IP address information):

Configuration Item or Task	Specification	Points
IP Address	209.165.200.230	(1/2 point)
Subnet Mask	255.255.255.248	(1/2 point)
Default Gateway	209.165.200.225	

Note: It may be necessary to disable the PC firewall for pings to be successful later in this lab.

Step 2: Configure R1.

Configuration tasks for R1 include the following:

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Configuration Item or Task	Specification	Points
Disable DNS lookup		(1/2 point)
Router name	R1	(1/2 point)
Encrypted privileged exec password	class	(1/2 point)
Console access password	cisco	(1/2 point)
Telnet access password	cisco	(1/2 point)
Encrypt the clear text passwords		(1/2 point)
MOTD banner	Unauthorized Access is Prohibited!	(1/2 point)
Interface S0/0/0	Set the description Set the Layer 3 IPv4 address. Use the first available address in the subnet. Set the clocking rate to 128000 Activate Interface	(1/2 point)
Default route	Configure a default route out S0/0/0.	(1/2 point)

Note: Do not configure G0/1 at this time.

Instructor Note: Ask the student to connect to R1, and then verify the proper configuration.

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Configuration Item or Task	**Specification**	**IOS Commands**
Disable DNS lookup	no ip domain lookup	R1# **show run** (Look for: **no ip domain lookup**)
Router name	R1	(Look for : **R1>** or **R1#** command prompt)
Encrypted privileged exec password	class	R1> **enable** (Type in privileged exec password)
Console access password	cisco	R1# **exit** (Type in access password)
Telnet access password	cisco	R1# **show run** (Look under line VTY 0 4 for: **password 7 121A0C041104**)
Encrypt the plain text passwords	service password-encryption	R1# **show run** (Look for: **service password-encryption**)
MOTD banner	banner motd @ Unauthorized Access is Prohibited! @	(Verify banner during above step)
Interface S0/0/0	interface s0/0/0 description Connection to R2 ip address 172.16.12.1 255.255.255.252 clock rate 128000 no shutdown	R1# **show interface S0/0/0** (Look for Description, Internet address, and verify that interface is not administratively down.) R1# **show controllers S0/0/0** (Look for DCE V.35, clock rate 128000)
Default router	ip route 0.0.0.0 0.0.0.0 s0/0/0	R1# **show ip route** (Look for: **Gateway of last resort is 0.0.0.0 to network 0.0.0.0** **S* 0.0.0.0/0 is directly connected, Serial0/0/0**)

Step 3: Configure R2.

Configuration tasks for R2 include the following:

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Configuration Item or Task	Specification	Points
Disable DNS lookup		(1/2 point)
Router name	R2	(1/2 point)
Encrypted privileged exec password	class	(1/2 point)
Console access password	cisco	(1/2 point)
Telnet access password	cisco	(1/2 point)
Encrypt the clear text passwords		(1/2 point)
Enable HTTP server		(1/2 point)
MOTD banner	Unauthorized Access is Prohibited!	(1/2 point)
Interface S0/0/0	Set the description Set the Layer 3 IPv4 address. Use the next available address in the subnet. Activate Interface	(1 point)
Interface S0/0/1	Set the description Set the Layer 3 IPv4 address. Use the first available address in the subnet. Set clocking rate to 128000 Activate Interface	(1 point)
Interface G0/0 (Simulated Internet)	Set the Description Set the Layer 3 IPv4 address. Use the first available address in the subnet. Activate Interface	(1 point)
Interface Loopback 0 (Simulated Web Server)	Set the description. Set the Layer 3 IPv4 address.	(1/2 point)
Default route	Configure a default route out G0/0.	(1/2 point)

Instructor Note: Ask the student to connect to R2, and then verify the proper configuration.

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Configuration Item or Task	**Specification**	**IOS Commands**
Disable DNS lookup	no ip domain lookup	R2# **show run** (Look for: **no ip domain lookup**)
Router name	R2	(Look for : **R2>** or **R2#** command prompt)
Encrypted privileged exec password	class	R2> **enable** (Type in privileged exec password)
Console access password	cisco	R2# **exit** (Type in access password)
Telnet access password	cisco	R2# **show run** (Look under line VTY 0 4 for: **password 7 121A0C041104**)
Encrypt the plain text passwords	service password-encryption	R2# **show run** (Look for: **service password-encryption**)
Enable HTTP server	ip http server	R2# **show run | include http** (Look for **ip http server**)
MOTD banner	banner motd @ Unauthorized Access is Prohibited! @	(Verify banner during above step)
Interface S0/0/0	interface s0/0/0 description Connection to R1 ip add 172.16.12.2 255.255.255.252 no shutdown	R2# **show interface S0/0/0** (Look for Description, Internet address, and verify that interface is not administratively down.)
Interface S0/0/1	interface s0/0/1 description Connection to R3 ip add 172.16.23.1 255.255.255.252 clock rate 128000 no shutdown	R2# **show interface S0/0/1** (Look for Description, Internet address, and verify that interface is not administratively down.) R2# **show controllers S0/0/1** (Look for DCE V.35, clock rate 128000)
Interface G0/0	interface g0/0 description Connection to ISP ip address 209.165.200.225 255.255.255.248 no shutdown	R2# **show ip interface G0/0** (Look for IP address and correct subnet mask)
Interface Loopback 0	interface lo0 description Simulated Web Server ip address 10.10.10.10 255.255.255.255	R2# **show ip interface lo0** (Look for IP address and correct subnet mask)

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Default router	ip route 0.0.0.0 0.0.0.0 g0/0	R2# **show ip route** (Look for: **Gateway of last resort is 0.0.0.0 to network 0.0.0.0** **S* 0.0.0.0/0 is directly connected, GigabitEthernet0/0**)

Step 4: Configure R3.

Configuration tasks for R3 include the following:

Configuration Item or Task	Specification	Points
Disable DNS lookup		(1/2 point)
Router name	R3	(1/2 point)
Encrypted privileged exec password	class	(1/2 point)
Console access password	cisco	(1/2 point)
Telnet access password	cisco	(1/2 point)
Encrypt the clear text passwords		(1/2 point)
MOTD banner	Unauthorized Access is Prohibited!	(1/2 point)
Interface S0/0/1	Set the description Set the Layer 3 IPv4 address. Use the next available address in the subnet. Activate Interface	(1/2 point)
Interface Loopback 4	Set the Layer 3 IPv4 address. Use the first available address in the subnet.	(1/2 point)
Interface Loopback 5	Set the Layer 3 IPv4 address. Use the first available address in the subnet.	(1/2 point)
Interface Loopback 6	Set the Layer 3 IPv4 address. Use the first available address in the subnet.	(1/2 point)
Default route	Configure a default route out S0/0/1.	(1/2 point)

Instructor Note: Ask the student to connect to R3, and then verify the proper configuration.

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Configuration Item or Task	Specification	IOS Commands
Disable DNS lookup	no ip domain lookup	R3# **show run** (Look for: **no ip domain lookup**)
Router name	R3	(Look for : **R3>** or **R3#** command prompt)
Encrypted privileged exec password	class	R3> **enable** (Type in privileged exec password)
Console access password	cisco	R3# **exit** (Type in access password)
Telnet access password	cisco	R3# **show run** (Look under line VTY 0 4 for: **password 7 121A0C041104**)
Encrypt the plain text passwords	service password-encryption	R3# **show run** (Look for: **service password-encryption**)
MOTD banner	banner motd @ Unauthorized Access is Prohibited! @	(Verify banner during above step)
Interface S0/0/1	interface s0/0/1 description Connection to R2 ip address 172.16.23.2 255.255.255.252 no shutdown	R3# **show interface S0/0/1** (Look for Description, Internet address, and verify that interface is not administratively down.)
Interface Loopback 4	interface lo4 ip address 192.168.4.1 255.255.255.0	R3# **show ip interface lo4** (Look for IP address and correct subnet mask)
Interface Loopback 5	interface lo5 ip address 192.168.5.1 255.255.255.0	R3# **show ip interface lo5** (Look for IP address and correct subnet mask)
Interface Loopback 6	interface lo6 ip address 192.168.6.1 255.255.255.0	R3# **show ip interface lo6** (Look for IP address and correct subnet mask)
Default router	ip route 0.0.0.0 0.0.0.0 s0/0/1	R3# **show ip route** (Look for: **Gateway of last resort is 0.0.0.0 to network 0.0.0.0** **S* 0.0.0.0/0 is directly connected, Serial0/0/1**)

Step 5: Configure S1.

Configuration tasks for S1 include the following:

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Configuration Item or Task	Specification	Points
Disable DNS lookup		(1/2 point)
Switch name	S1	(1/2 point)
Encrypted privileged exec password	class	(1/2 point)
Console access password	cisco	(1/2 point)
Telnet access password	cisco	(1/2 point)
Encrypt the clear text passwords		(1/2 point)
MOTD banner	Unauthorized Access is Prohibited!	(1/2 point)

Instructor Note: Ask the student to connect to S1, and then verify the proper configuration.

Configuration Item or Task	Specification	IOS Commands
Disable DNS lookup	no ip domain lookup	S1# **show run** (Look for: **no ip domain lookup**)
Switch name	S1	(Look for : **S1>** or **S1#** command prompt)
Encrypted privileged exec password	class	R3> **enable** (Type in privileged exec password)
Console access password	cisco	S1# **exit** (Type in access password)
Telnet access password	cisco	S1# **show run** (Look under line VTY 0 4 for: **password 7 121A0C041104**)
Encrypt the plain text passwords	service password-encryption	S1# **show run** (Look for: **service password-encryption**)
MOTD banner	banner motd @ Unauthorized Access is Prohibited! @	(Verify banner during above step)

Step 6: Configure S3

Configuration tasks for S3 include the following:

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Configuration Item or Task	Specification	Points
Disable DNS lookup		(1/2 point)
Switch name	S3	(1/2 point)
Encrypted privileged exec password	class	(1/2 point)
Console access password	cisco	(1/2 point)
Telnet access password	cisco	(1/2 point)
Encrypt the clear text passwords		(1/2 point)
MOTD banner	Unauthorized Access is Prohibited!	(1/2 point)

Instructor Note: Ask the student to connect to S3, and then verify the proper configuration.

Configuration Item or Task	**Specification**	**IOS Commands**
Disable DNS lookup	no ip domain lookup	S3# **show run** (Look for: **no ip domain lookup**)
Switch name	S3	(Look for : **S3>** or **S3#** command prompt)
Encrypted privileged exec password	class	S3> **enable** (Type in privileged exec password)
Console access password	cisco	S3# **exit** (Type in access password)
Telnet access password	cisco	S3# **show run** (Look under line VTY 0 4 for: **password 7 121A0C041104**)
Encrypt the plain text passwords	service password-encryption	S3# **show run** (Look for: **service password-encryption**)
MOTD banner	banner motd @ Unauthorized Access is Prohibited! @	(Verify banner during above step)

Step 7: Verify network connectivity.

Use the **ping** command to test connectivity between network devices.

Use the following table to methodically verify connectivity with each network device. Take corrective action to establish connectivity if a test fails:

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

From	To	IP Address	Ping Results	Points
R1	R2, S0/0/0	172.16.12.2	Should be successful.	(1/2 point)
R2	R3, S0/0/1	172.16.23.2	Should be successful.	(1/2 point)
Internet PC	Default Gateway	209.165.200.225	Should be successful.	(1/2 point)

Note: It may be necessary to disable the PC firewall for pings to be successful.

Instructor Sign-off Part 2: ______________________

Points: _________ of 28

Part 3: Configure Switch Security, VLANS, and Inter VLAN Routing

Ref lab: 2.2.4.10 Lab – Configuring Switch Security Features

Ref lab: 3.2.2.5 Lab – Configuring VLANS and Trunking

Ref lab: 3.3.2.5 Lab – Implementing VLAN Security

Ref lab: 5.1.3.7 Lab – Configuring 802.1Q Trunk-Based Inter-VLAN Routing

Total points: 14

Time: 15 minutes

Step 1: Configure S1.

Configuration tasks for S1 include the following:

Configuration Item or Task	Specification	Points
Create the VLAN database	Use Topology VLAN Key table to create and name each of the listed VLANS.	(1 point)
Assign the management IP address.	Assign the Layer 3 IPv4 address to the Management VLAN. Use the IP address assigned to S1 in the Topology diagram.	(1/2 point)
Assign the default-gateway	Assign the first IP address in the subnet as the default-gateway.	(1/2 point)
Force trunking on Interface F0/3	Use VLAN 1 as the native VLAN.	(1/2 point)
Force trunking on Interface F0/5	Use VLAN 1 as the native VLAN.	(1/2 point)
Configure all other ports as access ports	Use the interface range command.	(1/2 point)
Assign F0/6 to VLAN 31		(1/2 point)
Shutdown all unused ports.		(1/2 point)

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Configuration Item or Task	Specification	IOS Commands
Create the VLAN database	vlan 31 name Accounting vlan 33 name Engineering vlan 99 name Management	S1# **show vlan** (Look for vlans listed in VLAN Key. Verify that a VLAN name has been assigned to each vlan.)
Assign the management IP address	interface vlan 99 ip address 192.168.99.2 255.255.255.0	S1# **show interface vlan 99** (Look for the ip address and subnet mask).
Assign the default-gateway	ip default-gateway 192.168.99.1	S1# **show run | section default** (Look for **ip default-gateway 192.168.99.1**)
Force trunking on Interface F0/3	interface F0/3 switchport mode trunk switchport trunk native vlan 1 **Note:** VLAN 1 is the native VLAN by default, the previous command is not necessary.	S1# **show interface trunk** (Look to see if F0/3 is listed. If not listed check to see if interface is active.) S1# **show run interface f0/3**
Force trunking on Interface F0/5	interface F0/5 switchport mode trunk switchport trunk native vlan 1 **Note:** vlan is the native VLAN, the previous command is not necessary.	S1# **show interface trunk** (Look to see if F0/3 is listed. If not listed check to see if interface is active.)
Configure all other ports as access ports	interface range F0/1-2, F0/4, F0/6-24, G0/1-2 switchport mode access	S1# **show run | begin interface** (Look to see if all unused interfaces are access switchports.)
Assign F0/6 to VLAN 31	interface F0/6 switchport access vlan 31	S1# **show run interface f0/6** (Look for: **switchport access vlan 31**)
Shutdown all unused ports.	interface range F0/1-2, F0/4, F0/7-24, G0/1-2 shutdown	S1# **show ip interface brief** (Look to see if all unused ports are administratively down.)

Step 2: Configure S3.

Configuration tasks for S3 include the following:

Configuration Item or Task	Specification	Points
Create the VLAN database	Use Topology VLAN Key Table to create each of the listed VLANS. Name each VLAN.	(1 point)
Assign the management IP address.	Assign the Layer 3 IPv4 address to the Management VLAN. Use the IP address assigned to S3 in the Topology diagram.	(1/2 point)
Assign the default-gateway	Assign the first IP address in the subnet as the default-gateway	(1/2 point)
Force trunking on Interface F0/3	Use VLAN 1 as the native VLAN.	(1/2 point)
Configure all other ports as access ports	Use the interface range command.	(1/2 point)
Assign F0/18 to VLAN 33		(1/2 point)
Shutdown all unused ports.		(1/2 point)

Configuration Item or Task	Specification	IOS Commands
Create VLAN database	vlan 31 name Accounting vlan 33 name Engineering vlan 99 name Management	S3# **show vlan** (Look for vlans listed in VLAN Key. Verify that a VLAN name has been assigned to each vlan.)
Assign the management IP address	interface vlan 99 ip address 192.168.99.3 255.255.255.0	S3# **show interface vlan 99** (Look for the ip address and subnet mask).
Assign default-gateway	ip default-gateway 192.168.99.1	S3# **show run | section default** (Look for **ip default-gateway 192.168.99.1**)
Force trunking on Interface F03	interface F0/3 switchport mode trunk switchport trunk native vlan 1	S3# **show interface trunk** (Look to see if F0/3 is listed. If not listed check to see if interface is active.) S3# **show run interface f0/3**
Assign all other ports as access ports	interface range F0/1-2, F0/4, F0/6-24, G0/1-2 switchport mode access	S3# **show run | begin interface** (Look to see if all unused interfaces are access switchports.)
Assign F0/18 to VLAN 33	interface F0/18 switchport access vlan 33	S3# **show run interface f0/18** (Look for: **switchport access vlan 33**)
Shutdown all unused ports.	interface range F0/1-2, F0/4, F0/6-17, F0/19-24, G0/1-2 shutdown	S3# **show ip interface brief** (Look to see if all unused ports are administratively down.)

Step 3: Configure R1.

Configuration tasks for R1 include the following:

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Configuration Item or Task	Specification	Points
Configure 802.1Q subinterface .31 on G0/1	Description Accounting LAN Assign VLAN 31. Assign the first available address to this interface.	(1 point)
Configure 802.1Q subinterface .33 on G0/1	Description Engineering LAN Assign VLAN 33. Assign the first available address to this interface.	(1 point)
Configure 802.1Q subinterface .99 on G0/1	Description Management LAN Assign VLAN 99. Assign the first available address to this interface.	(1 point)
Activate Interface G0/1		(1/2 point)

Configuration Item or Task	Specification	IOS Commands
Configure 802.1Q subinterface .31 on G0/1	interface g0/1.31 description Accounting LAN encapsulation dot1q 31 ip address 192.168.31.1 255.255.255.0	R1# **show ip interface brief** (Look to see if the .31 subinterface has the correct IP address and has an up/up status.)
Configure 802.1Q subinterface .33 on G0/1	interface g0/1.33 description Engineering LAN encapsulation dot1q 33 ip address 192.168.33.1 255.255.255.0	R1# **show ip interface brief** (Look to see if the .33 subinterface has the correct IP address and has an up/up status.)
Configure 802.1Q subinterface .99 on G0/1	interface g0/1.99 description Management LAN encapsulation dot1q 99 ip address 192.168.99.1 255.255.255.0	R1# **show ip interface brief** (Look to see if the .99 subinterface has the correct IP address and has an up/up status.)
Activate Interface G0/1	interface g0/1 no shutdown	(See above)

Step 4: Verify network connectivity.

Use the **ping** command to test connectivity between the switches and R1.

Use the following table to methodically verify connectivity with each network device. Take corrective action to establish connectivity if a test fails:

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

From	To	IP Address	Ping Results	Points
S1	R1, VLAN 99 address	192.168.99.1	Should be successful.	(1/2 point)
S3	R1, VLAN 99 address	192.168.99.1	Should be successful.	(1/2 point)
S1	R1, VLAN 31 address	192.168.31.1	Should be successful.	(1/2 point)
S3	R1, VLAN 33 address	192.168.33.1	Should be successful.	(1/2 point)

Instructor Sign-off Part 2: ______________________

Points: _________ of 14

Part 4: Configure OSPFv2 Dynamic Routing Protocol

Ref lab: 8.2.4.5 Lab – Configuring Basic Single-Area OSPFv2

Total points: 24

Time: 25 minutes

Step 1: Configure OSPFv2 on R1.

Configuration tasks for R1 include the following:

Configuration Item or Task	Specification	Points
OSPF Process ID	1	(1/2 point)
Router ID	1.1.1.1	(1/2 point)
Advertise directly connected Networks	Use classless network addresses Assign all directly connected networks to Area 0	(1 point)
Set all LAN interfaces as passive		(1 point)
Change the default cost reference bandwidth to support Gigabit interface calculations	1000	(1 point)
Set the serial interface bandwidth	128 Kb/s	(1 point)
Adjust the metric cost of S0/0/0	Cost: 7500	(1 point)

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Configuration Item or Task	Specification	IOS Commands
OSPF Process ID	router ospf 1	R1# **show ip protocols** (Look for: **Routing Protocol is "ospf 1"**)
Router ID	router-id 1.1.1.1	(From output from previous command, look for: **Router-ID: 1.1.1.1**)
Advertise directly connected Networks	network 172.16.12.0 0.0.0.3 area 0 network 192.168.31.0 0.0.0.255 area 0 network 192.168.33.0 0.0.0.255 area 0 network 192.168.99.0 0.0.0.255 area 0	R1# **show run | section router ospf** (Compare network commands to specifications.) Can also use **show ip protocols** command.
Set all LAN interfaces as passive	passive-interface g0/1.31 passive-interface g0/1.33 passive-interface g0/1.99	R1# **show ip protocols** (Look at passive interface section at bottom of output. If not there then either the Loopback network wasn't added or the passive interface command was not applied. Use the **show run | section router ospf** command to verify.)
Change the default cost reference bandwidth to support Gigabit interface calculations	auto-cost reference-bandwidth 1000	R1# **show run | section router** (Look for: auto-cost reference-bandwidth 1000)
Set the serial interface bandwidths	interface s0/0/0 bandwidth 128	R1# **show interface s0/0/0** (Look for **BW 128 Kbit/sec**,)
Adjust the metric cost of S0/0/0	ip ospf cost 7500	R1# **show ip ospf interface brief** (Look for: Se0/0/0 1 0 172.16.12.1/30 **7500** P2P 1/1)

Step 2: Configure OSPFv2 on R2.

Configuration tasks for R2 include the following:

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Configuration Item or Task	Specification	Points
OSPF Process ID	1	(1 point)
Router ID	2.2.2.2	(1 point)
Advertise directly connected Networks	Use classless network addresses **Note:** Omit the G0/0 network.	(1 point)
Set the LAN (Loopback) interface as passive		(1 point)
Change the default cost reference bandwidth to allow for Gigabit interfaces	1000	(1 point)
Set the bandwidth on all serial interfaces	128 Kb/s	(1 point)
Adjust the metric cost of S0/0/0	Cost: 7500	(1 point)

Instructor Note: Ask the student to connect to R2, and then verify the proper configuration.

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Configuration Item or Task	**Specification**	**IOS Commands**
OSPF Process ID	router ospf 1	R2# **show ip protocols** (Look for: **Routing Protocol is "ospf 1"**)
Router ID	router-id 2.2.2.2	(From output from previous command, look for: **Router-ID: 1.1.1.1**)
Advertise directly connected Networks	network 172.16.12.0 0.0.0.3 area 0 network 172.16.23.0 0.0.0.3 area 0 network 10.10.10.10 0.0.0.0 area 0	R2# **show run | section router ospf** (Compare network commands to specifications.) Can also use **show ip protocols** command.
Set the LAN (Loopback) interface as passive	passive-interface lo0	R2# **show ip protocols** (Look at passive interface section at bottom of output. If not there then either the Loopback network wasn't added or the passive interface command was not applied. Use the **show run | section router ospf** command to verify.)
Change the default cost reference bandwidth to support Gigabit interface calculations	auto-cost reference-bandwidth 1000	R2# **show run | section router** (Look for: **auto-cost reference-bandwidth 1000**)
Set the bandwidth on all serial interfaces	interface s0/0/0 bandwidth 128 interface s0/0/1 bandwidth 128	R2# **show interface s0/0/0** R2# **show interface s0/0/1** (Look for **BW 128 Kbit/sec**,)
Adjust the metric cost of S0/0/0	interface s0/0/0 ip ospf cost 7500	R2# **show ip ospf interface brief** (Look for: Se0/0/0 1 0 172.16.12.1/30 **7500** P2P 1/1)

Step 3: Configure OSPFv2 on R3.

Configuration tasks for R3 include the following:

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Configuration Item or Task	Specification	Points
OSPF Process ID	1	(1/2 point)
Router ID	3.3.3.3	(1/2 point)
Advertise directly connected Networks	Use classless network addresses Assign interfaces to Area 0 Use a single summary address for the LAN (loopback) interfaces.	(1 point)
Set all LAN (Loopback) interfaces as passive		(1 point)
Change the default cost reference bandwidth to support Gigabit interface calculations	1000	(1 point)
Set the serial interface bandwidth	128 Kb/s	(1 point)

Instructor Note: Ask the student to connect to R3, and then verify the proper configuration.

Configuration Item or Task	Specification	IOS Commands
OSPF Process ID	router ospf 1	R3# **show ip protocols** (Look for: **Routing Protocol is "ospf 1"**)
Router-ID	router-id 3.3.3.3	(From output from previous command, look for: **Router-ID: 1.1.1.1**)
Advertise directly connected Networks	network 172.16.23.0 0.0.0.3 area 0 network 192.168.4.0 0.0.3.255 area 0	R3# **show run | section router ospf** (Compare network commands to specifications. Can also use **show ip protocols** command.)
Set all LAN (Loopback) interfaces as passive	passive-interface lo4 passive-interface lo5 passive-interface lo6	R3# **show ip protocols** (Look at passive interface section at bottom of output. If not there then either the Loopback network wasn't added or the passive interface command was not applied. Use the **show run | section router ospf** command to verify.)
Change the default cost reference bandwidth to support Gigabit interface calculations	auto-cost reference-bandwidth 1000	R3# **show run | section router** (Look for: **auto-cost reference-bandwidth 1000**)
Set the serial interface bandwidth	interface s0/0/1 bandwidth 128	R3# **show interface s0/0/1** (Look for **BW 128 Kbit/sec**,)

Step 4: Verify OSPF information.

Verify that OSPF is functioning as expected. Enter the appropriate CLI command to discover the following information:

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Question	Response	Points
What command will display all connected OSPFv2 routers?	show ip ospf neighbor	(1 point)
What command displays a summary list of OSPF interfaces that includes a column for the cost of each interface?	show ip ospf interface brief	(1 point)
What command displays the OSPF Process ID, Router ID, Address summarizations, Routing Networks, and passive interfaces configured on a router?	show ip protocols	(1 point)
What command displays only OSPF routes?	show ip route ospf	(1 point)
What command displays detail information about the OSPF interfaces, including the authentication method?	show ip ospf interface	(1 point)
What command displays the OSPF section of the running-configuration?	show run | section router OSPF	(1 point)

Instructor Sign-off Part 3: ______________________

Points: _________ of 24

Part 5: Implement DHCP and NAT for IPv4

Ref lab: 10.1.2.5 Lab – Configure Basic DHCPv4 on a router

Ref lab: 11.2.2.6 Lab – Configure dynamic and static NAT

Total points: 13

Time: 25 minutes

Step 1: Configure R1 as the DHCP server for VLANs 31 and 33.

Configuration tasks for R1 include the following:

Configuration Item or Task	Specification	Points
Reserve the first 20 IP addresses in VLAN 31 for static configurations		(1 point)
Reserve the first 20 IP addresses in VLAN 33 for static configurations		(1 point)
Create a DHCP pool for VLAN 31	Name: ACCT DNS-Server: 10.10.10.11 Domain-Name: ccna-sba.com Set the default gateway.	(1 point)
Create a DHCP pool for VLAN 33	Name: ENGNR DNS-Server: 10.10.10.11 Domain-Name: ccna-sba.com Set the default gateway.	(1 point)

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Configuration Item or Task	Specification	IOS Commands
Reserve the first 20 IP addresses in VLAN 31 for static configurations	ip dhcp excluded-address 192.168.31.1 192.168.31.20	R1# **show run | section dhcp** (Look for excluded-address.)
Reserve the first 20 IP addresses in VLAN 33 for static configurations	ip dhcp excluded-address 192.168.33.1 192.168.33.20	R1# **show run | section dhcp** (Look for excluded-address.)
Create a DHCP pool for VLAN 31	ip dhcp pool ACCT network 192.168.31.0 255.255.255.0 dns-server 10.10.10.11 domain-name ccna-sba.com default-router 192.168.31.1	R1# **show run | section dhcp** (Review pool information.) R1# **show ip dhcp bindings** (Verify binding with PC-A)
Create a DHCP pool for VLAN 33	ip dhcp pool ENGNR network 192.168.33.0 255.255.255.0 dns-server 10.10.10.11 domain-name ccna-sba.com default-router 192.168.33.1	R1# **show run | section dhcp** (Review pool information.) R1# **show ip dhcp bindings** (Verify binding with PC-C)

Step 2: Configure Static and Dynamic NAT on R2.

Configuration tasks for R2 include the following:

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Configuration Item or Task	Specification	Points
Create a local database with 1 user account	Username: **webuser** Password: **cisco12345** Privilege level: **15**	(1 point)
Enable HTTP server service		(1/2 point)
Configure the HTTP server to use the local database for authentication		(1/2 point)
Create a static NAT to the Web Server	Inside Global Address: **209.165.200.229**	(1 point)
Assign the inside and outside interface for the static NAT		(1 point)
Configure the dynamic NAT inside private ACL	Access List: 1 Allow the Accounting and Engineering networks on R1 to be translated. Allow a summary of the LANs (loopback) networks on R3 to be translated.	(1 point)
Define the pool of usable public IP addresses	Pool Name: **INTERNET** Pool of addresses include: **209.165.200.225 – 209.165.200.228**	(1 point)
Define the dynamic NAT translation		(1 point)

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Configuration Item or Task	Specification	IOS Commands
Create a local database with 1 user account	username webuser privilege 15 secret cisco12345	R2# **show run | section username**
Enable HTTP server service on R2	ip http server	R2# **show run | section ip http**
Configure the HTTP server to use the local database for authentication	ip http authentication local	R2# **show run | section ip http**
Create a static NAT to the Web Server	ip nat inside source static 10.10.10.10 209.165.200.229	R2# **show ip nat translations** (Verify the Inside global and local addresses.)
Assign the inside and outside interface for the static NAT	interface lo0 ip nat inside interface g0/0 ip nat outside	R2# **show run | begin interface** (Look for **ip nat** information.)
Configure the dynamic NAT inside private ACL	access-list 1 permit 192.168.31.0 0.0.0.255 access-list 1 permit 192.168.33.0 0.0.0.255 access-list 1 permit 192.168.4.0 0.0.3.255	R2# **show access-lists** (Look for: Standard IP access list 1 10 permit 192.168.31.0, wildcard bits 0.0.0.255 20 permit 192.168.33.0, wildcard bits 0.0.0.255)
Define the pool of usable public IP addresses	ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248	R2# **show run | section ip nat**
Define the dynamic NAT translation	ip nat inside source list 1 pool INTERNET	R2# **show run | section ip nat**

Step 3: Verify DHCP and Static NAT.

Use the following tasks to verify that DHCP and Static NAT settings are functioning correctly. It may be necessary to disable the PC firewall for pings to be successful:

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Test	Results	Points
Verify that PC-A acquired IP information from the DHCP server	C:\> **ipconfig /all** (Look at settings to determine if dhcp provided the correct network information.)	(1/2 point)
Verify that PC-C acquired IP information from the DHCP server	C:\> **ipconfig /all** (Look at settings to determine if dhcp provided the correct network information.)	(1/2 point)
Verify that PC-A can ping PC-C. **Note**: It may be necessary to disable the PC firewall	C:\> **ping 192.168.33.21** Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.31.21, timeout is 2 seconds: !!!!!	(1/2 point)
Use a Web browser on the Internet PC to access the Web server (209.165.200.229). Login with Username: **webuser**, Password: **cisco12345**	(Browser should present a Windows Security window. Username: **webuser**, Password: **cisco12345**)	(1/2 point)

Note: Verification of dynamic NAT will be performed in Part 6.

Instructor Sign-off Part 2: ______________________

Points: _________ of 13

Part 6: Configure and Verify Access Control Lists (ACLs)

Total points: 13

Time: 25 minutes

Step 1: Restrict access to VTY lines on R2.

Ref lab: 9.2.3.4 Configuring and Verifying VTY Restrictions

Configuration Item or Task	Specification	Points
Configure a named access list to only allow R1 to telnet to R2.	ACL Name: **ADMIN-MGT**	(2 points)
Apply the named ACL to the VTY lines		(1 point)
Verify ACL is working as expected,		(1 point)

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Configuration Item or Task	**Specification**	**IOS Commands**
Configure a named access list to only allow R1 to telnet to R2.	ip access-list standard ADMIN-MGT permit host 172.16.12.1	R2# **show access-lists** (Look for: **Standard IP access list ADMIN-MGT** **10 permit 172.16.12.1**)
Apply the named ACL to the VTY lines	line vty 0 4 access-class ADMIN-MGT in	R2# **show run | sec line vty** (Look to see if ADMIN-MGT has been applied correctly)
Verify ACL is working as expected		R1# **telnet 172.16.12.2** (You should only be able to telnet from R1 to R2. The Internet PC and R3 should not be able to telnet to R2.)

Step 2: Secure the network from Internet traffic.

Ref lab: 9.3.2.13 Configuring and Verifying Extended ACLs

Configuration Item or Task	Specification	Points
Configure an Extended ACL to: • Allow Internet hosts WWW access to the simulated web server on R2 by accessing the static NAT address (209.165.200.229) that you configured in Part 3. • Prevent traffic from the Internet from pinging internal networks, while continuing to allow LAN interfaces to ping the Internet PC.	ACL No.: **101**	(2 points)
Apply ACL to the appropriate interface(s)		(1 point)
Verify ACL is working as expected	From the Internet PC: • Ping PC-A (Pings should be unreachable.) • Ping PC-C (Pings should be unreachable.) From R1, Ping the Internet PC (Pings should be successful.)	(1 point)

Note: It may be necessary to disable the PC firewall for pings to be successful.

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Configuration Item or Task	Specification	IOS Commands
Configure an Extended ACL that prevents traffic from the Internet from pinging internal interfaces, while continuing to allow LAN interfaces to ping the Internet PC. Internet hosts should be granted WWW access to the simulated web server (Lo0) on R2.	access-list 101 permit tcp any host 209.165.200.229 eq www access-list 101 permit icmp any any echo-reply access-list 101 deny ip any any	R2# **show access-lists** (Look for: **Extended IP access list 101** **10 permit tcp any host 10.10.10.10 eq www (20 matches)** **20 permit icmp any any echo-reply (22 matches)** **30 deny ip any any (31 matches)** **Note:** the last line can be omitted as it is implied, but explicitly adding it is useful to be able to see matches.)
Apply ACL to the appropriate interface(s)	Interface g0/0 ip access-group 101 in	R2# **show run interface g0/0** (Look to see if **ip access-group 101 in** has been applied to interface.)
Verify ACL is working as expected	Test from Internet PC.	C:\> **ping 192.168.31.21** C:\> **ping 192.168.33.21** (Look to see if you receive **Destination net unreachable** messages to both networks.) R1# **ping 209.165.200.230** (This ping should work.) **Using a browser on the Internet PC, go to 209.165.200.229.** An **Authentication Required** window requesting a User Name and Password should appear. Sign in using user: **webuser**, password: **cisco12345**.

Step 3: Enter the appropriate CLI command needed to display the following:

Command Description	Student Input (command)	Points
Display the matches an access-list has received since the last reset.	show access-lists	(1 point)
Reset access-list counters.	clear ip access-list counters	(1 point)
What command is used to display what ACL is applied to an interface and the direction that it is applied	show ip interface	(1 point)

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

What command displays the NAT translations?	show ip nat translations (Pro Inside global Inside local Outside local Outside global --- 209.165.200.229 10.10.10.10 --- --- --- **209.165.200.225** **192.168.31.21** --- --- --- **209.165.200.226** **192.168.33.21** --- ---) **Note**: The translations for PC-A and PC-C were added to the table when the Internet PC attempted to ping these PCs in Step 2. Pinging the Internet PC from PC-A or PC-C will not add the translations to the table because of the way the Internet is being simulated on the network.	(1 point)
What command is used to clear dynamic NAT translations?	clear ip nat translations *	(1 point)

Instructor Sign-off Part 4: ______________________

Points: _________ of 13

Part 7: Cleanup

NOTE: DO NOT PROCEED WITH CLEANUP UNTIL YOUR INSTRUCTOR HAS GRADED YOUR SKILLS EXAM AND HAS INFORMED YOU THAT YOU MAY BEGIN CLEANUP.

Before turning off power to the routers, remove the NVRAM configuration files (if saved) from all devices.

Disconnect and neatly put away all cables that were used in the Final.

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Router Interface Summary Table

Router Interface Summary				
Router Model	**Ethernet Interface #1**	**Ethernet Interface #2**	**Serial Interface #1**	**Serial Interface #2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/0/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.