Configure a numbered standard ACL.  
a. Configure the ACL on R3. Use 1 for the access list number.  
R3(config)# access-list 1 remark Allow R1 LANs Access  
R3(config)# access-list 1 permit 192.168.10.0 0.0.0.255  
R3(config)# access-list 1 permit 192.168.20.0 0.0.0.255  
R3(config)# access-list 1 deny any

a. Create the standard named ACL BRANCH-OFFICE-POLICY on R1.  
R1(config)# ip access-list standard BRANCH-OFFICE-POLICY  
R1(config-std-nacl)# permit host 192.168.30.3  
R1(config-std-nacl)# permit 192.168.40.0 0.0.0.255  
R1(config-std-nacl)# 30 permit 209.165.200.224 0.0.0.31  
R1(config-std-nacl)# 40 deny any

SSH

R3(config)# ip domain-name cisco.com  
R3(config)# crypto key generate rsa modulus 1024  
R3(config)# line vty 0 4  
R3(config-line)# login local  
R3(config-line)# transport input ssh

Configure the policy on R3. Name the ACL WEB-POLICY.

R1(config)# access-list 100 remark Allow Web & SSH Access  
R1(config)# access-list 100 permit tcp host 192.168.10.3 host 10.2.2.1 eq 22  
R1(config)# access-list 100 permit tcp 192.168.10.0 0.0.0.255 any eq 80

Configure the policy on R3. Name the ACL WEB-POLICY.

R3(config)# ip access-list extended WEB-POLICY  
R3(config-ext-nacl)# permit tcp 192.168.30.0 0.0.0.255 host 10.1.1.1 eq 80  
R3(config-ext-nacl)# permit tcp 192.168.30.0 0.0.0.255 209.165.200.224 0.0.0.31 eq 80

global configuration mode and modify the ACL on R1.

R1(config)# ip access-list extended 100  
R1(config-ext-nacl)# 30 permit ip 192.168.10.0 0.0.0.255 192.168.30.0  
0.0.0.255

nter global configuration mode and modify the ACL on R3.  
R3(config)# ip access-list extended WEB-POLICY  
R3(config-ext-nacl)# 30 permit ip 192.168.30.0 0.0.0.255 192.168.10.0  
0.0.0.255

Step 2: Set the time.  
R1# clock set 9:39:00 05 july 2013  
Step 3: Configure the NTP master.  
R1(config)# ntp master 5  
b. point to the IP address or hostname of the NTP server.  
R2(config)# ntp server 10.1.1.1

Step 4: Configure R2 to log messages to the syslog server.  
R2(config)# logging host 172.16.2.3

Use the logging trap ? command to determine the various trap levels availability. When configuring a level, the messages sent to the syslog server are the trap level configured and any lower levels.  
R2(config)# logging trap ?  
<0-7> Logging severity level  
alerts Immediate action needed (severity=1)  
critical Critical conditions (severity=2)  
debugging Debugging messages (severity=7)  
emergencies System is unusable (severity=0)  
errors Error conditions (severity=3)  
informational Informational messages (severity=6)  
notifications Normal but significant conditions (severity=5)  
warnings Warning conditions (severity=4)  
b. Change the logging severity level to 4.  
R2(config)# logging trap warnings or  
R2(config)# logging trap 4  
Step 1: Configure NetFlow capture.  
R2(config)# interface g0/1  
R2(config-if)# ip flow ingress  
R2(config-if)# ip flow egress  
R2(config-if)# interface g0/2  
R2(config-if)# ip flow ingress  
R2(config-if)# ip flow egress  
Step 2: Configure NetFlow data export.  
R2(config)# ip flow-export destination 192.168.2.3 9996  
Step 3: Configure the NetFlow export version..  
R2(config)# ip flow-export version 9