Abhinav Dinesh Srivatsa

21BDS0340

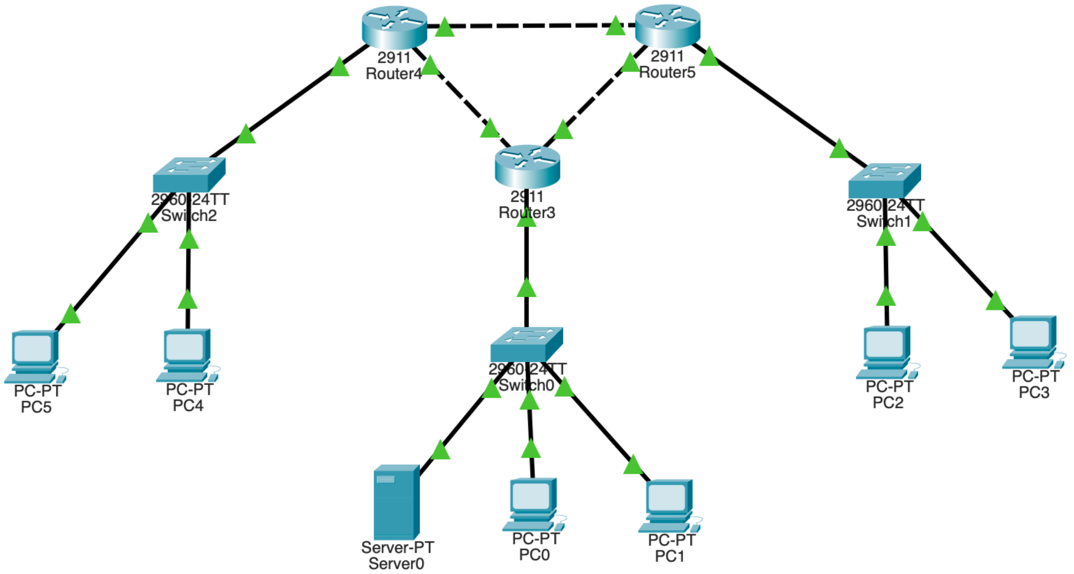
Information Security Management

Assignment – II

Aim

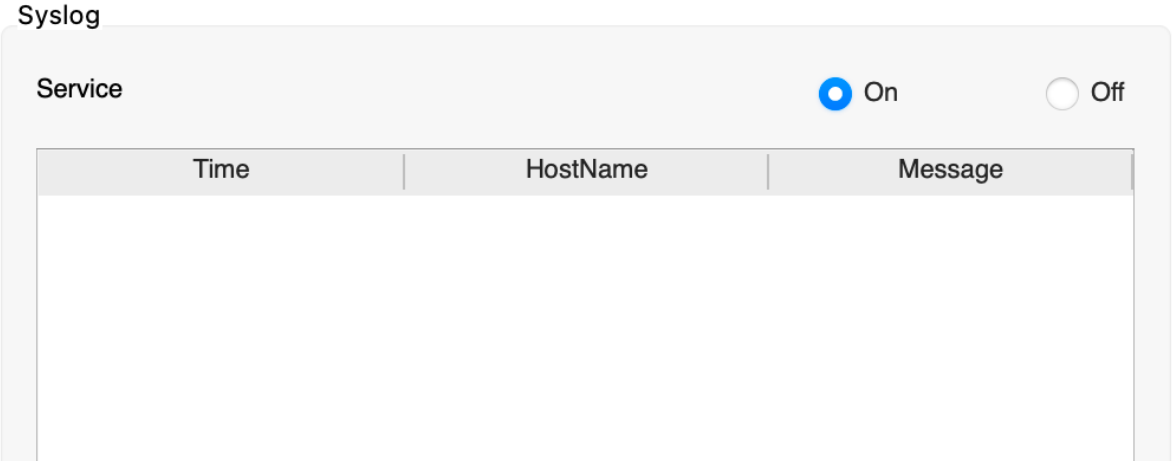
To configure IPS for dynamically connected PCs on a network.

Layout



All IP addresses have been configured using DHCP from the server via RIP dynamic routing.

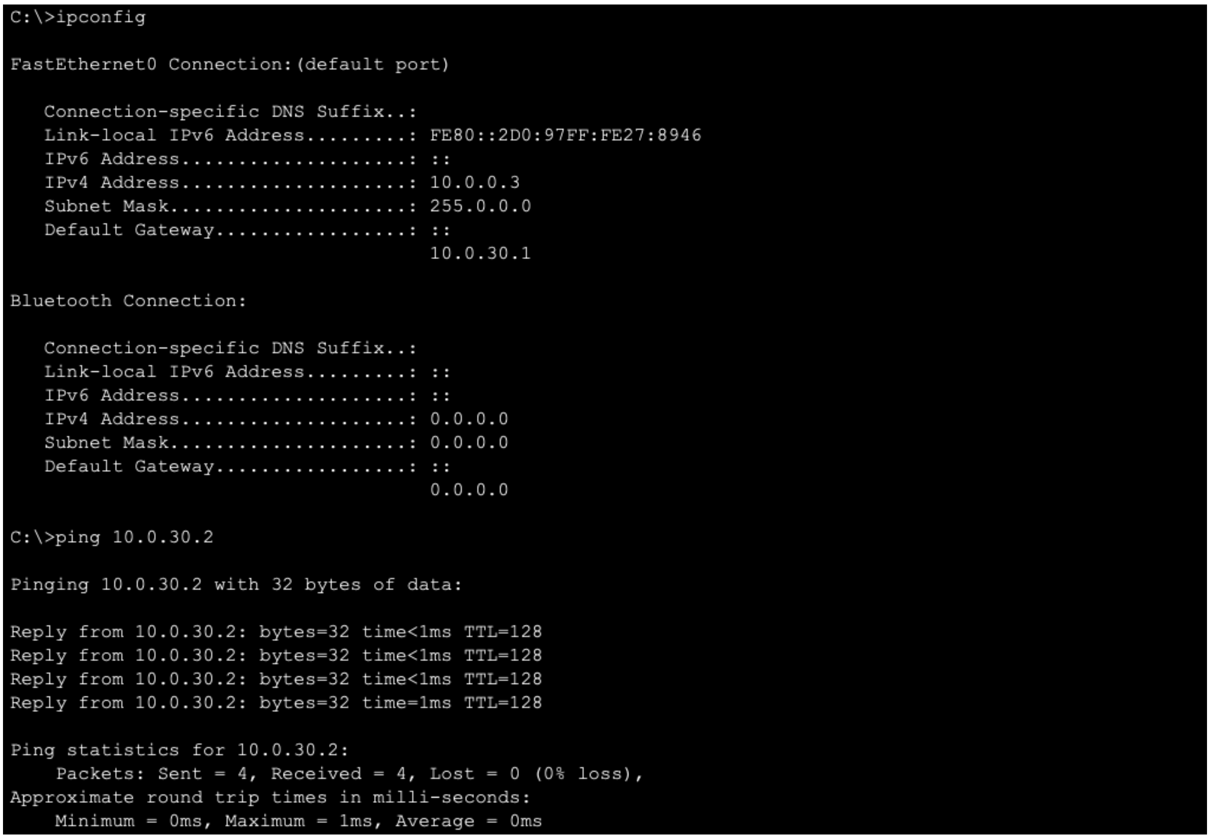
Before IPS Configuration



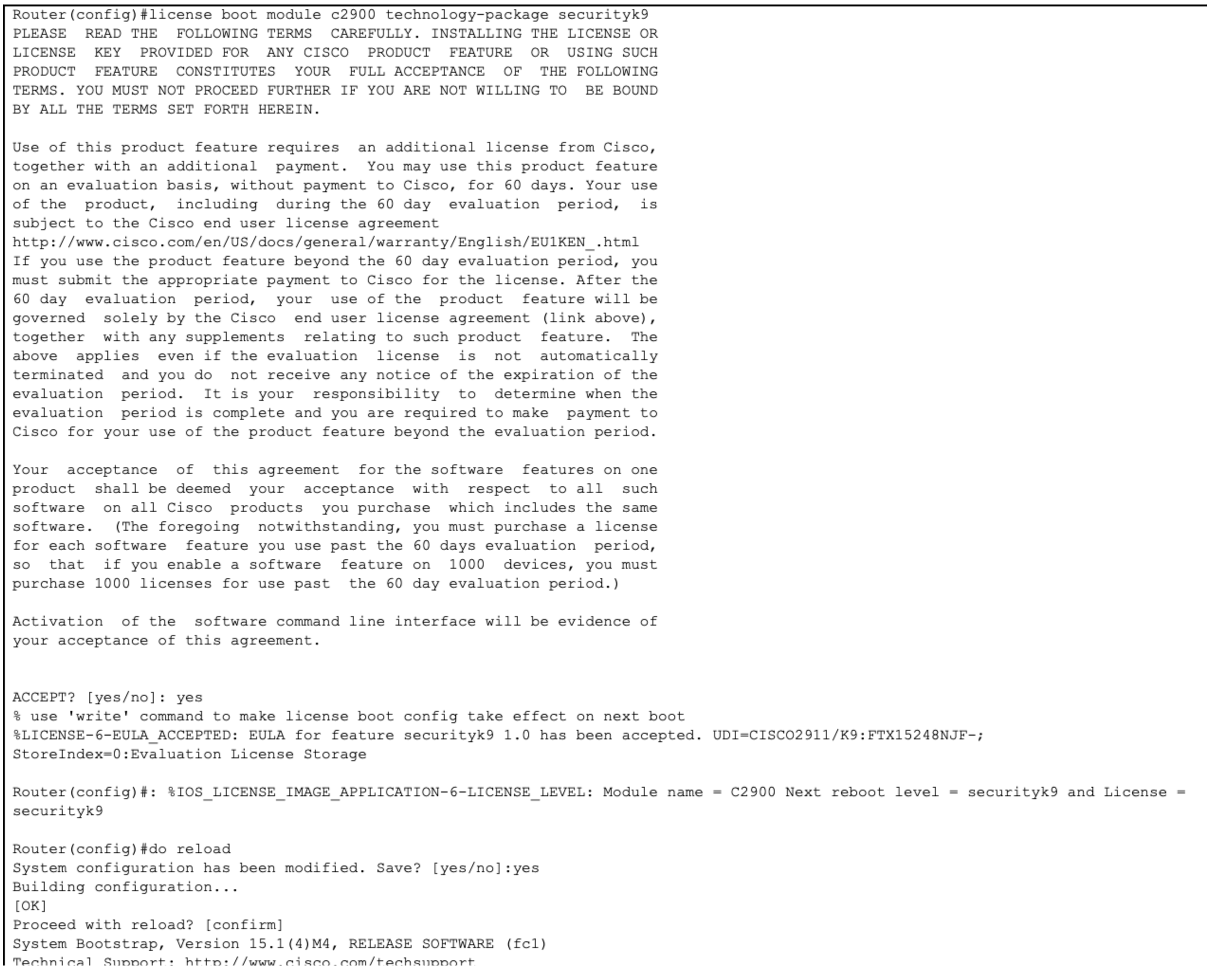
Syslog

Service ● On ○ Off

Time	HostName	Message

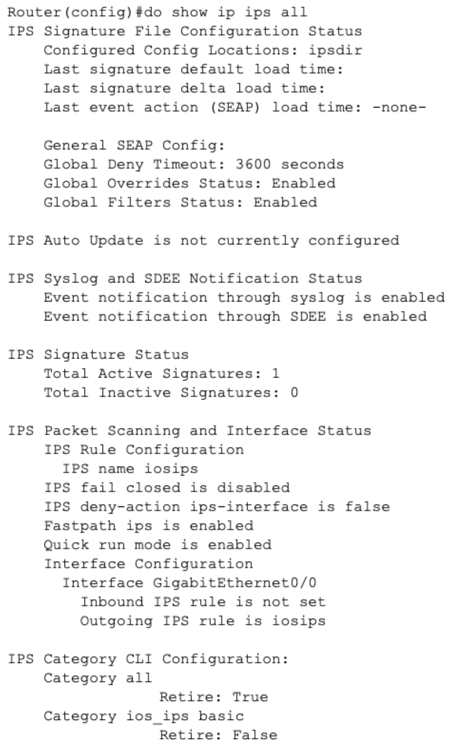


```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: FE80::2D0:97FF:FE27:8946
   IPv6 Address....................: ::
   IPv4 Address....................: 10.0.0.3
   Subnet Mask.....................: 255.0.0.0
   Default Gateway.................: ::
                                     10.0.30.1

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0

C:\>ping 10.0.30.2

Pinging 10.0.30.2 with 32 bytes of data:

Reply from 10.0.30.2: bytes=32 time<1ms TTL=128
Reply from 10.0.30.2: bytes=32 time<1ms TTL=128
Reply from 10.0.30.2: bytes=32 time<1ms TTL=128
Reply from 10.0.30.2: bytes=32 time=1ms TTL=128

Ping statistics for 10.0.30.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```



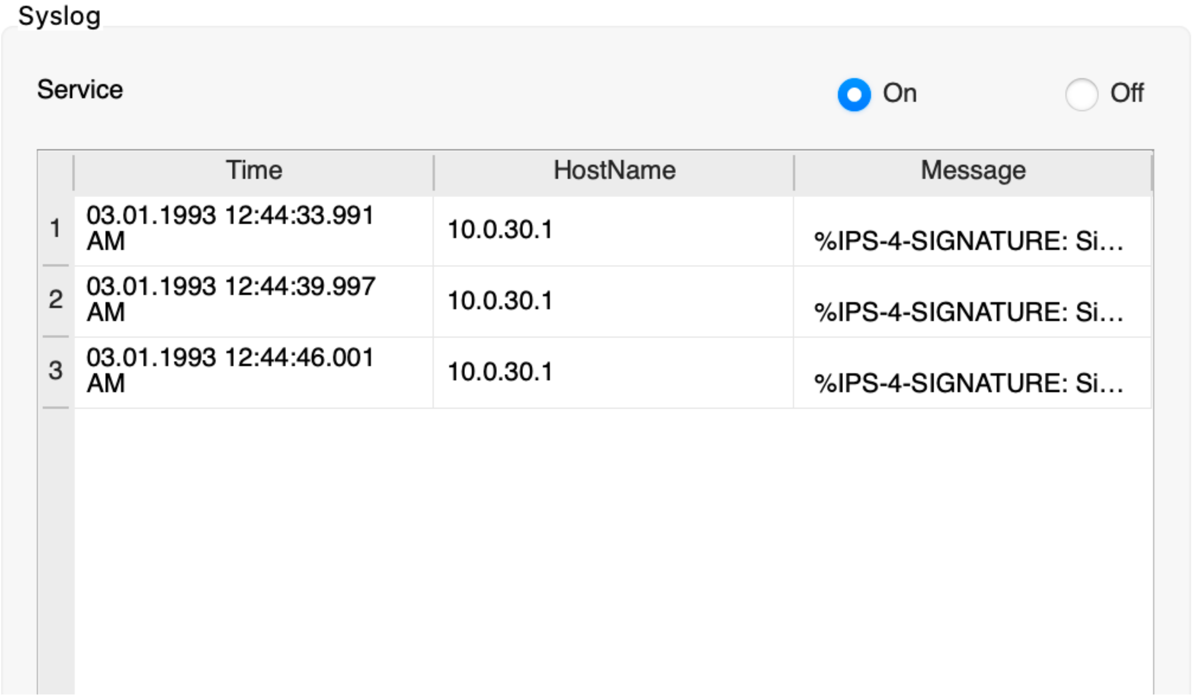
```
Router(config)#license boot module c2900 technology-package securityk9
PLEASE  READ THE  FOLLOWING TERMS  CAREFULLY. INSTALLING THE LICENSE OR
LICENSE  KEY  PROVIDED FOR  ANY CISCO  PRODUCT  FEATURE  OR  USING SUCH
PRODUCT  FEATURE  CONSTITUTES  YOUR  FULL ACCEPTANCE  OF  THE FOLLOWING
TERMS. YOU MUST NOT PROCEED FURTHER IF YOU ARE NOT WILLING TO  BE BOUND
BY ALL THE TERMS SET FORTH HEREIN.

Use of this product feature requires  an additional license from Cisco,
together with an additional  payment.  You may use this product feature
on an evaluation basis, without payment to Cisco, for 60 days. Your use
of the  product,  including  during the 60 day  evaluation  period,  is
subject to the Cisco end user license agreement
http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html
If you use the product feature beyond the 60 day evaluation period, you
must submit the appropriate payment to Cisco for the license. After the
60 day  evaluation  period,  your  use of the  product  feature will be
governed  solely by the Cisco  end user license agreement (link above),
together  with any supplements  relating to such product  feature.  The
above  applies  even if the evaluation  license  is  not  automatically
terminated  and you do  not receive any notice of the expiration of the
evaluation  period.  It is your  responsibility  to  determine when the
evaluation  period is complete and you are required to make  payment to
Cisco for your use of the product feature beyond the evaluation period.

Your  acceptance  of  this agreement  for the software  features on one
product  shall be deemed  your  acceptance  with  respect  to all  such
software  on all Cisco  products  you purchase  which includes the same
software.  (The foregoing  notwithstanding, you must purchase a license
for each software  feature you use past the 60 days evaluation  period,
so  that  if you enable a software  feature on  1000  devices, you must
purchase 1000 licenses for use past  the 60 day evaluation period.)

Activation  of the  software command line interface will be evidence of
your acceptance of this agreement.


ACCEPT? [yes/no]: yes
% use 'write' command to make license boot config take effect on next boot
%LICENSE-6-EULA_ACCEPTED: EULA for feature securityk9 1.0 has been accepted. UDI=CISCO2911/K9:FTX15248NJF-;
StoreIndex=0:Evaluation License Storage

Router(config)#: %IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL: Module name = C2900 Next reboot level = securityk9 and License =
securityk9

Router(config)#do reload
System configuration has been modified. Save? [yes/no]:yes
Building configuration...
[OK]
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
```

```
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco CISCO2911/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
3 Gigabit Ethernet interfaces
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

Press RETURN to get started!



Router>en
Router#mkdir ipsdir
Create directory filename [ipsdir]?
Created dir flash:ipsdir

Router#ip ips config location ipsdir
          ^
% Invalid input detected at '^' marker.

Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip ips config location ipsdir
Router(config)#ip ips name iosips
Router(config)#ip ips signature-category
Router(config-ips-category)#category all
Router(config-ips-category-action)#retired true
Router(config-ips-category-action)#exit
Router(config-ips-category)#category ios_ips basic
Router(config-ips-category-action)#retired false
Router(config-ips-category-action)#exit
Router(config-ips-category)#exit
Do you want to accept these changes? [confirm]
Applying Category configuration to signatures ...
%IPS-6-ENGINE_BUILDING: atomic-ip - 288 signatures - 6 of 13 engines
%IPS-6-ENGINE_READY: atomic-ip - build time 30 ms - packets for this engine will be scanned


Router(config)#in gigabitEthernet 0/0
Router(config-if)#
Router(config)#
Router(config)#interface GigabitEthernet0/2
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip ips iosips?
WORD
Router(config-if)#ip ips iosips out
Router(config-if)#
 %IPS-6-ENGINE_BUILDS_STARTED:  00:04:42 UTC Mar 01 1993

 %IPS-6-ENGINE_BUILDING: atomic-ip - 3 signatures - 1 of 13 engines

 %IPS-6-ENGINE_READY: atomic-ip - build time 8 ms - packets for this engine will be scanned

 %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 8 ms

Router(config-if)#exit
Router(config)#logging host 10.0.30.2
Router(config)#service timestamps log datetime sec
                                               ^
% Invalid input detected at '^' marker.

Router(config)#service timestamps log datetime msec
Router(config)#ip ips signature-definition
Router(config-sigdef)#signature 2004 0
Router(config-sigdef-sig)#status
Router(config-sigdef-sig-status)#retired false
Router(config-sigdef-sig-status)#enabled true
Router(config-sigdef-sig-status)#exit
Router(config-sigdef-sig)#engine
Router(config-sigdef-sig-engine)#event-action produce-alert
Router(config-sigdef-sig-engine)#event-action deny-packet-inline
Router(config-sigdef-sig-engine)#exit
Router(config-sigdef-sig)#exit
Router(config-sigdef)#exit
Do you want to accept these changes? [confirm]
%IPS-6-ENGINE_BUILDS_STARTED:
%IPS-6-ENGINE_BUILDING: atomic-ip - 303 signatures - 3 of 13 engines
%IPS-6-ENGINE_READY: atomic-ip - build time 480 ms - packets for this engine will be scanned
%IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 648 ms
```



```
Router(config)#do show ip ips all
IPS Signature File Configuration Status
    Configured Config Locations: ipsdir
    Last signature default load time:
    Last signature delta load time:
    Last event action (SEAP) load time: -none-

    General SEAP Config:
    Global Deny Timeout: 3600 seconds
    Global Overrides Status: Enabled
    Global Filters Status: Enabled

IPS Auto Update is not currently configured

IPS Syslog and SDEE Notification Status
    Event notification through syslog is enabled
    Event notification through SDEE is enabled

IPS Signature Status
    Total Active Signatures: 1
    Total Inactive Signatures: 0

IPS Packet Scanning and Interface Status
    IPS Rule Configuration
      IPS name iosips
    IPS fail closed is disabled
    IPS deny-action ips-interface is false
    Fastpath ips is enabled
    Quick run mode is enabled
    Interface Configuration
      Interface GigabitEthernet0/0
        Inbound IPS rule is not set
        Outgoing IPS rule is iosips

IPS Category CLI Configuration:
    Category all
                Retire: True
    Category ios_ips basic
                Retire: False
```

After IPS Configuration



Syslog

Service ● On ○ Off

	Time	HostName	Message
1	03.01.1993 12:44:33.991 AM	10.0.30.1	%IPS-4-SIGNATURE: Si…
2	03.01.1993 12:44:39.997 AM	10.0.30.1	%IPS-4-SIGNATURE: Si…
3	03.01.1993 12:44:46.001 AM	10.0.30.1	%IPS-4-SIGNATURE: Si…

Result

IPS intrusion detection has been enabled in the router and logs out any detection to the server connected on the network.