Computer Networking: Concepts, Practice and Introduction to Security – J0HJ 34

Student Name	: Erya A
Logbook	: Assessment 2, 3 and 4

Contents

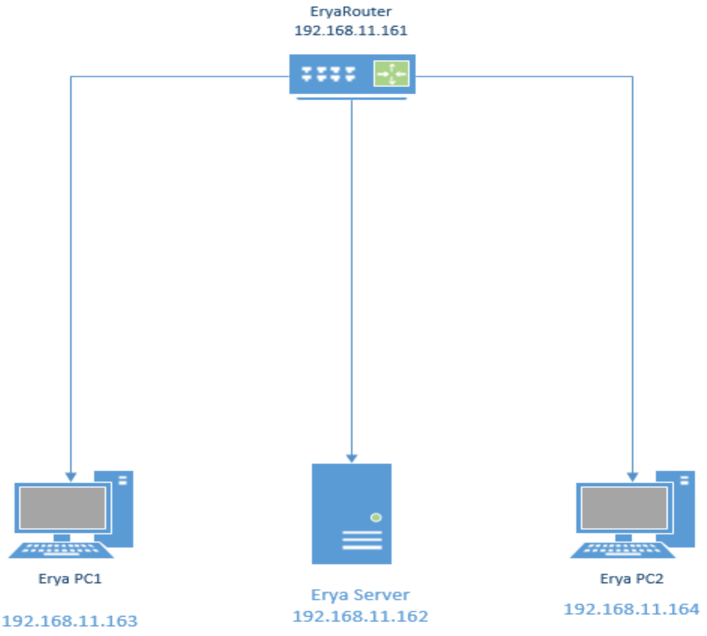
Assessment 2

Create a client server switched local area network, with secure endpoints.

Assessment Instructions

Scenario- You have been tasked with the setting up and configuring of a small local area network. This network should be set up with an emphasis on securing the endpoints of the network. To comply with this requirement, you can choose any suitable network operating system. You should be provided with suitable working hardware to allow this task to be completed.

Stage 1 – Select a suitable contemporary network topology

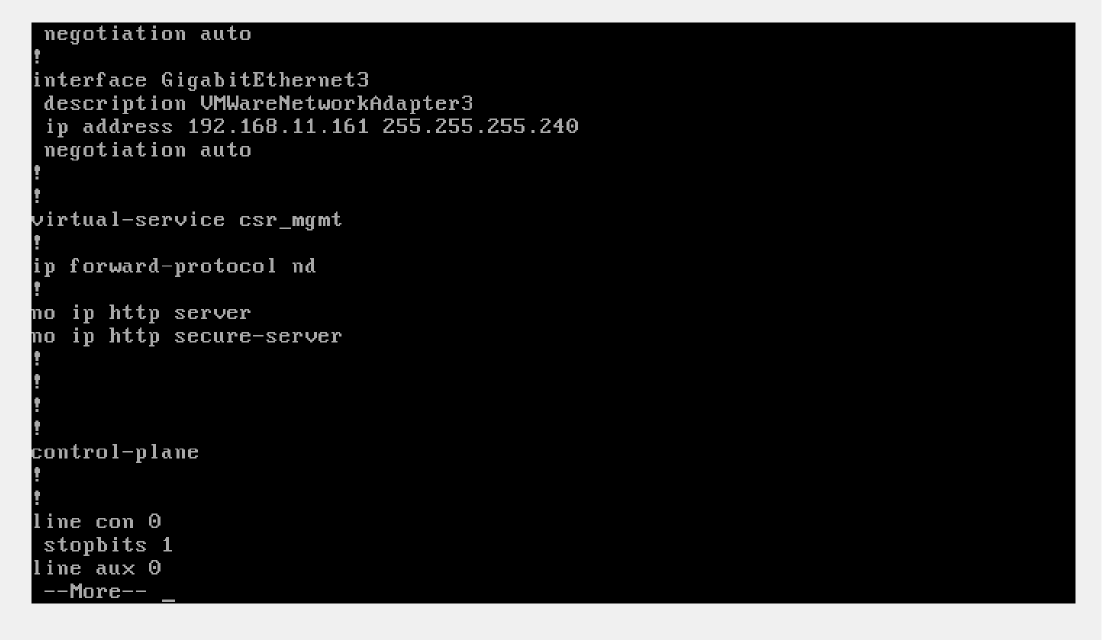


The diagram shown the represents a simple network topology set up for a small Local Area Network. Router – 192.168.11.161. this device serves as the central point for managing traffic and connectivity in the network. It assigns that the IP addresses, enables communication between the devices and could also provide a firewall security.

PC1 [192.168.11.163] and PC2 [192.168.11.164] these represents a workstation or endpoint in the network. Lastly, server with IP addresses 192.168.11.162, the server provides centralised services to other devices on the network. It acts as a resource hub or service provider, depending on how its configuring.

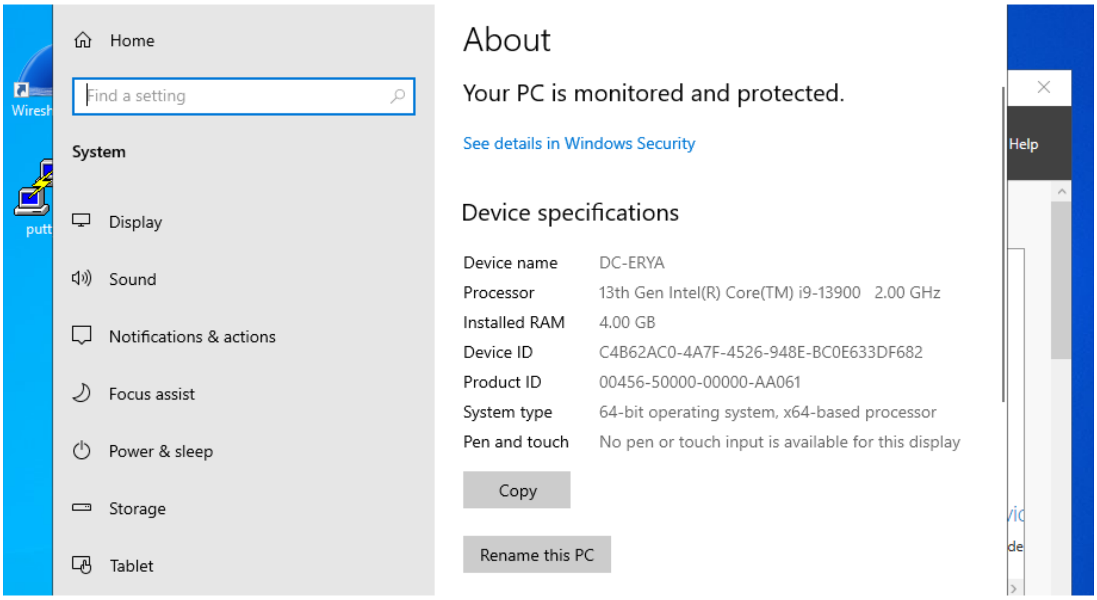
Stage 2 – Device a suitable naming convention for the network hosts/nodes

Device	IP Address	Host Name
Router	192.168.11.161	Erya Router
Server	192.168.11.162	DC ERYA
PC 1	192.168.11.163	C1ERYA
PC 2	192.168.11.164	C2-ERYA



```
 negotiation auto
!
interface GigabitEthernet3
 description VMWareNetworkAdapter3
 ip address 192.168.11.161 255.255.255.240
 negotiation auto
!
!
virtual-service csr_mgmt
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
!
control-plane
!
!
line con 0
 stopbits 1
line aux 0
 --More-- _
```

Router – Erya Router [192.168.11.161]



About

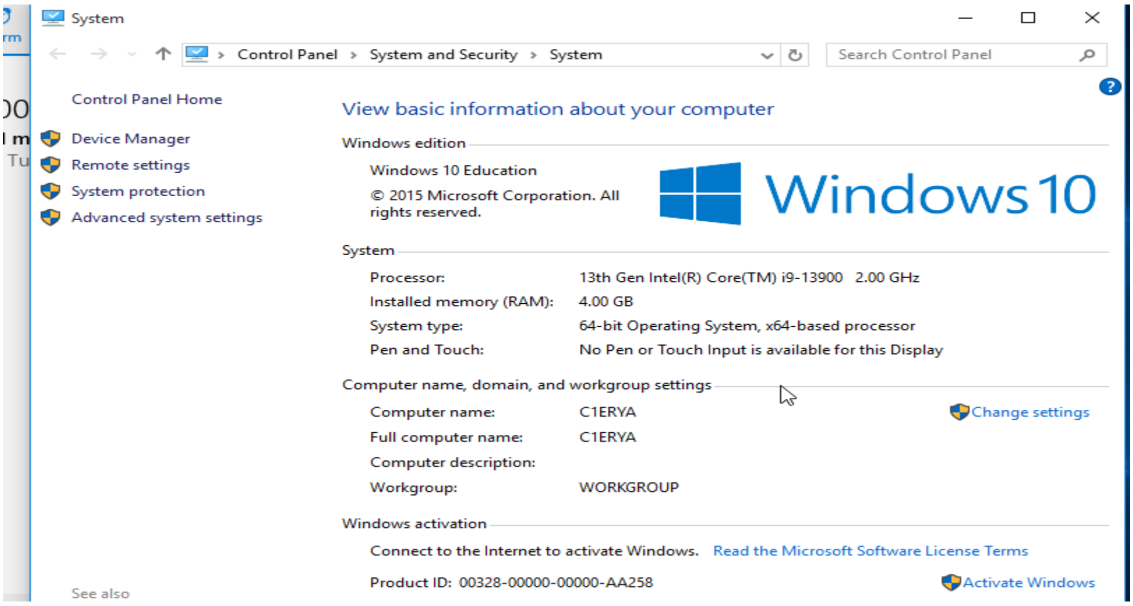
Your PC is monitored and protected.

See details in Windows Security

Device specifications

Device name	DC-ERYA
Processor	13th Gen Intel(R) Core(TM) i9-13900 2.00 GHz
Installed RAM	4.00 GB
Device ID	C4B62AC0-4A7F-4526-948E-BC0E633DF682
Product ID	00456-50000-00000-AA061
System type	64-bit operating system, x64-based processor
Pen and touch	No pen or touch input is available for this display

Server – DC ERYA [192.168.11.162]



View basic information about your computer

Windows edition

Windows 10 Education

© 2015 Microsoft Corporation. All rights reserved.

Windows 10

System

Processor: 13th Gen Intel(R) Core(TM) i9-13900 2.00 GHz

Installed memory (RAM): 4.00 GB

System type: 64-bit Operating System, x64-based processor

Pen and Touch: No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

Computer name: C1ERYA

Full computer name: C1ERYA

Computer description:

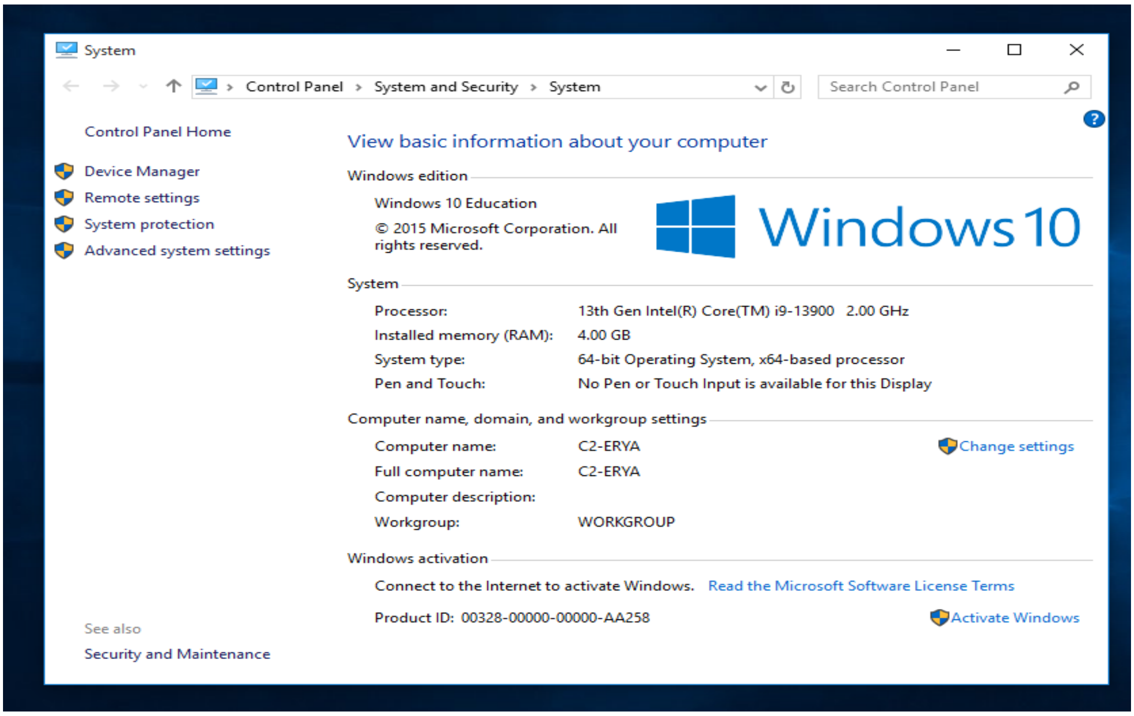
Workgroup: WORKGROUP

Windows activation

Connect to the Internet to activate Windows. Read the Microsoft Software License Terms

Product ID: 00328-00000-00000-AA258

PC 1 – C1ERYA [192.168.11.163]



View basic information about your computer

Windows edition

Windows 10 Education

© 2015 Microsoft Corporation. All rights reserved.

Windows 10

System

Processor: 13th Gen Intel(R) Core(TM) i9-13900 2.00 GHz

Installed memory (RAM): 4.00 GB

System type: 64-bit Operating System, x64-based processor

Pen and Touch: No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

Computer name: C2-ERYA

Full computer name: C2-ERYA

Computer description:

Workgroup: WORKGROUP

Windows activation

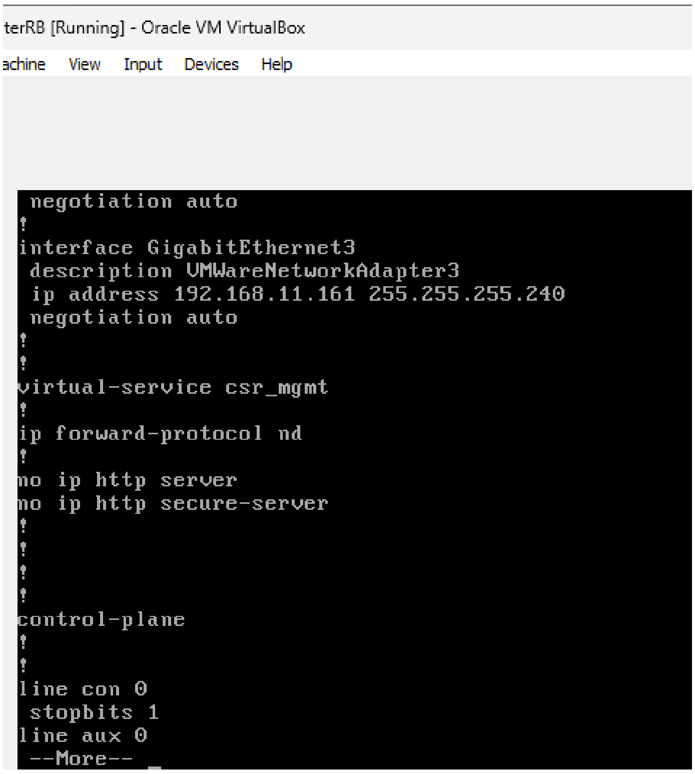
Connect to the Internet to activate Windows. Read the Microsoft Software License Terms

Product ID: 00328-00000-00000-AA258

PC 2 – C2-ERYA [192.168.11.164]

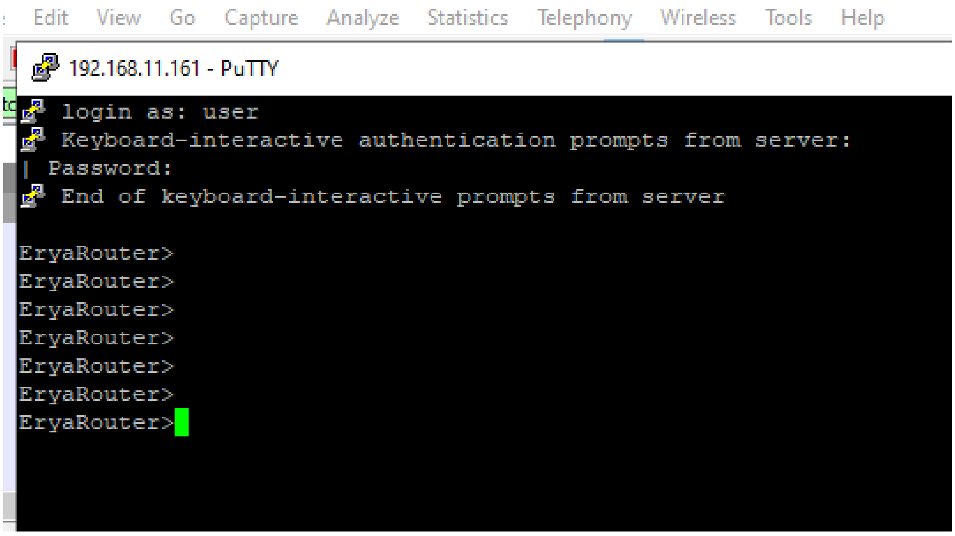
Stage 3 – Devise a suitable logical addressing structure for the network hosts/nodes

Static IP addressing scheme screenshots of all devices (including router)

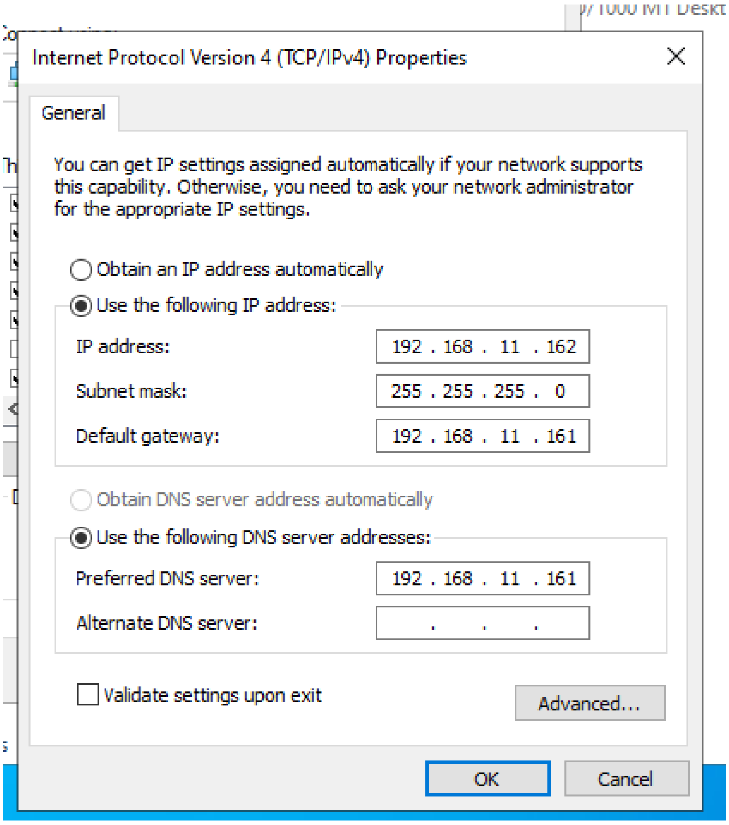

terRB [Running] - Oracle VM VirtualBox
achine View Input Devices Help

```
 negotiation auto
!
interface GigabitEthernet3
 description VMWareNetworkAdapter3
 ip address 192.168.11.161 255.255.255.240
 negotiation auto
!
!
virtual-service csr_mgmt
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
!
control-plane
!
!
line con 0
 stopbits 1
line aux 0
 --More-- _
```

Erya Router: 192.168.11.161


Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
192.168.11.161 - PuTTY

```
 login as: user
 Keyboard-interactive authentication prompts from server:
| Password:
 End of keyboard-interactive prompts from server

EryaRouter>
EryaRouter>
EryaRouter>
EryaRouter>
EryaRouter>
EryaRouter>
EryaRouter>
```



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 11 . 162

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 11 . 161

○ Obtain DNS server address automatically

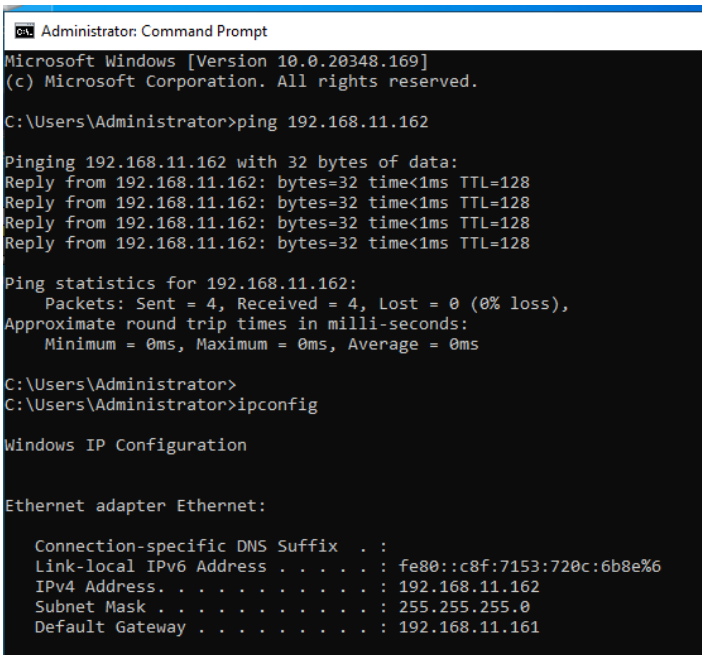
● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 11 . 161

Alternate DNS server: . . .

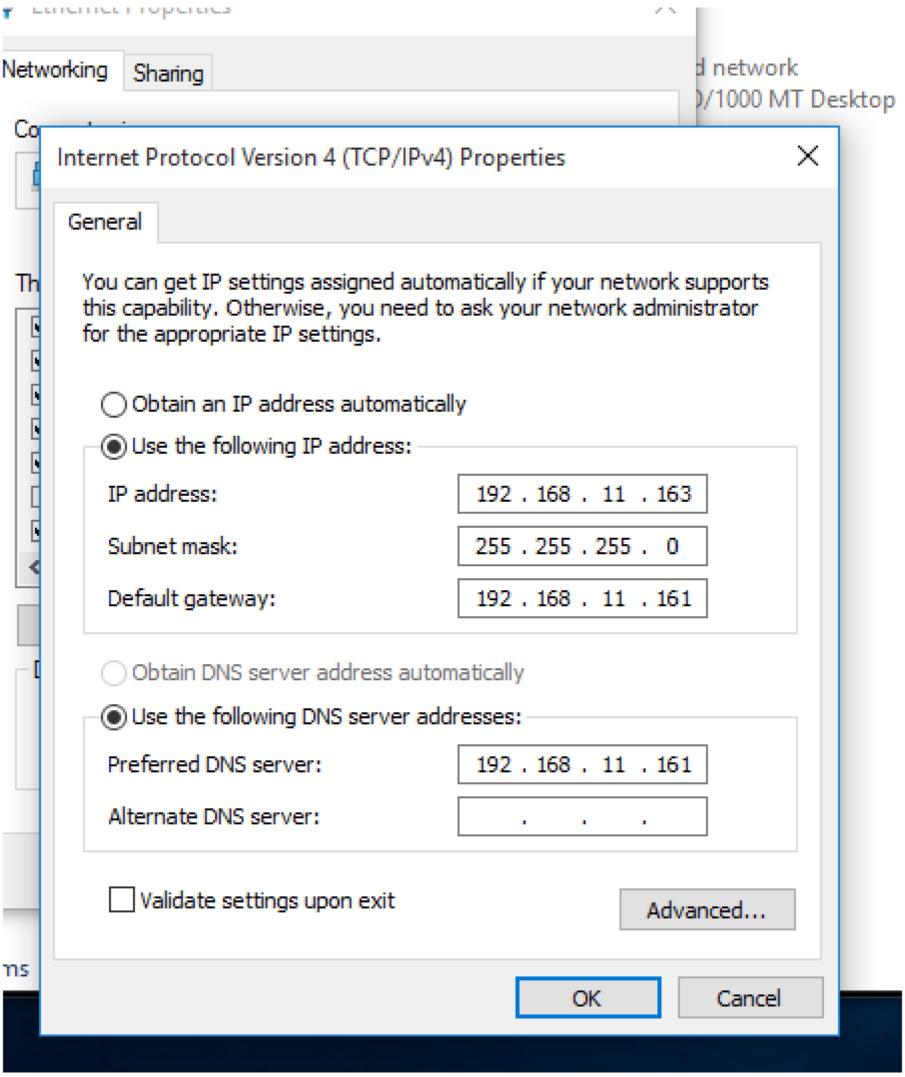
□ Validate settings upon exit

For the server DC ERYA - 192.168.11.162



Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.20348.169]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 192.168.11.162

Pinging 192.168.11.162 with 32 bytes of data:
Reply from 192.168.11.162: bytes=32 time<1ms TTL=128
Reply from 192.168.11.162: bytes=32 time<1ms TTL=128
Reply from 192.168.11.162: bytes=32 time<1ms TTL=128
Reply from 192.168.11.162: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.11.162:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>
C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::c8f:7153:720c:6b8e%6
   IPv4 Address. . . . . . . . . . . : 192.168.11.162
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.11.161
```



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 11 . 163

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 11 . 161

○ Obtain DNS server address automatically

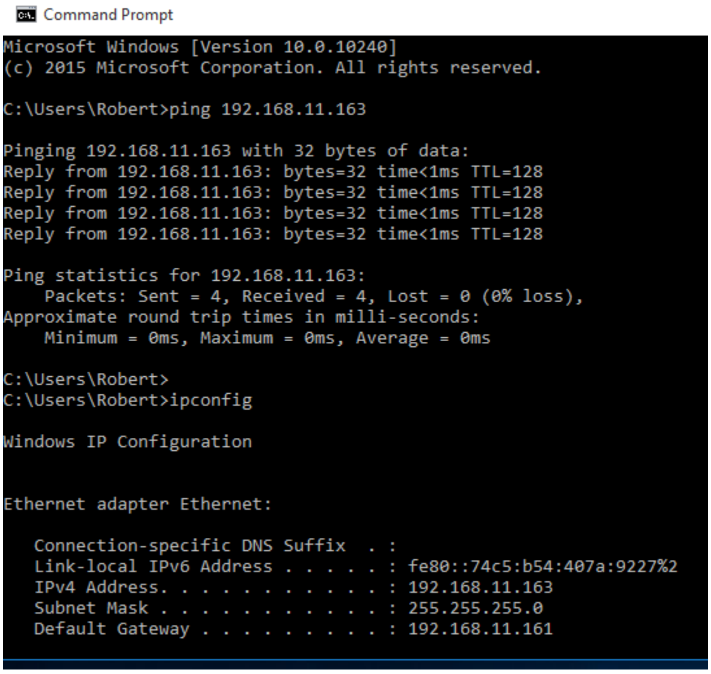
● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 11 . 161

Alternate DNS server: . . .

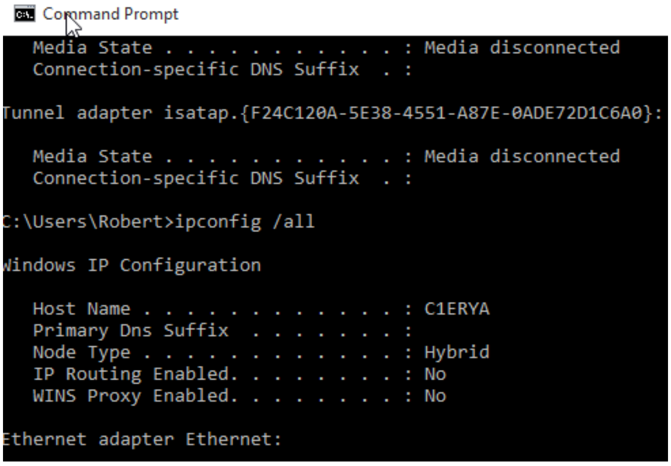
□ Validate settings upon exit

For the server C1ERYA - 192.168.11.163



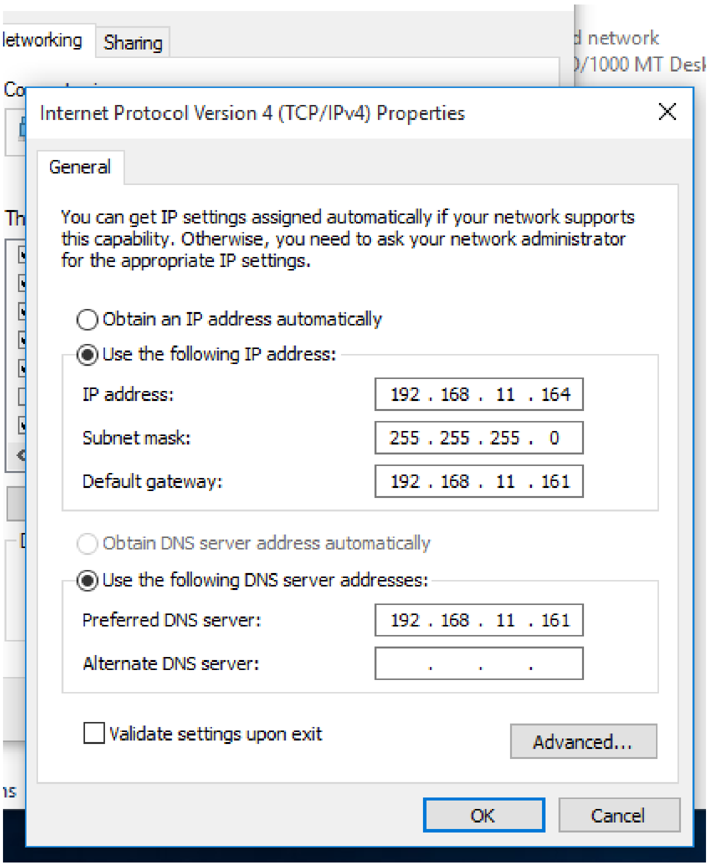
Command Prompt

```
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\Robert>ping 192.168.11.163

Pinging 192.168.11.163 with 32 bytes of data:
Reply from 192.168.11.163: bytes=32 time<1ms TTL=128
Reply from 192.168.11.163: bytes=32 time<1ms TTL=128
Reply from 192.168.11.163: bytes=32 time<1ms TTL=128
Reply from 192.168.11.163: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.11.163:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Robert>
C:\Users\Robert>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::74c5:b54:407a:9227%2
   IPv4 Address. . . . . . . . . . . : 192.168.11.163
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.11.161
```



Command Prompt

```
   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter isatap.{F24C120A-5E38-4551-A87E-0ADE72D1C6A0}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Robert>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : C1ERYA
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:
```



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 11 . 164

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 11 . 161

○ Obtain DNS server address automatically

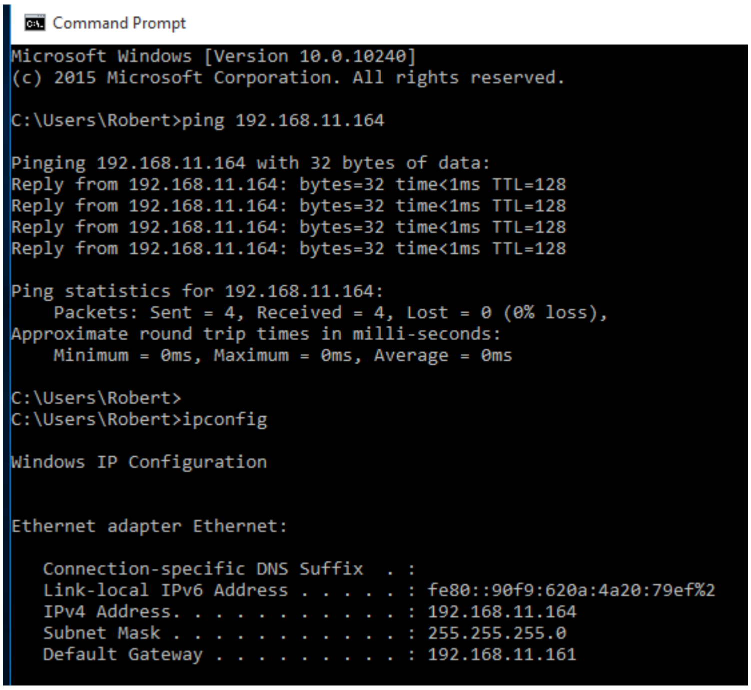
● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 11 . 161

Alternate DNS server: . . .

□ Validate settings upon exit

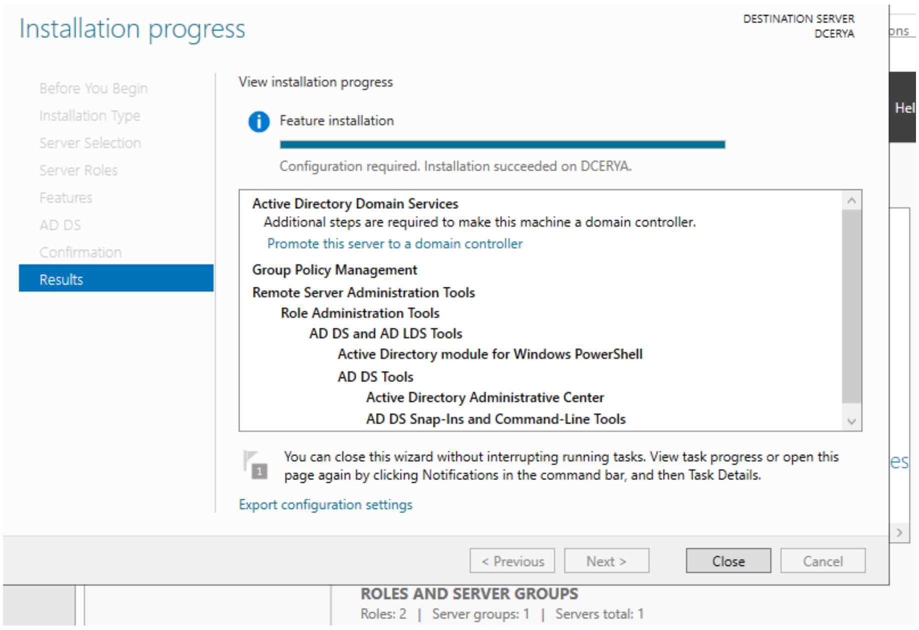
For the server C2-ERYA - 192.168.11.164


Command Prompt

```
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\Robert>ping 192.168.11.164

Pinging 192.168.11.164 with 32 bytes of data:
Reply from 192.168.11.164: bytes=32 time<1ms TTL=128
Reply from 192.168.11.164: bytes=32 time<1ms TTL=128
Reply from 192.168.11.164: bytes=32 time<1ms TTL=128
Reply from 192.168.11.164: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.11.164:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Robert>
C:\Users\Robert>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::90f9:620a:4a20:79ef%2
   IPv4 Address. . . . . . . . . . . : 192.168.11.164
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.11.161
```

Stage 4 – Configure appropriate network authentication services and name resolution

DNS Screenshots on Server and DNS


Installation progress

DESTINATION SERVER
DCERYA

View installation progress

Feature installation

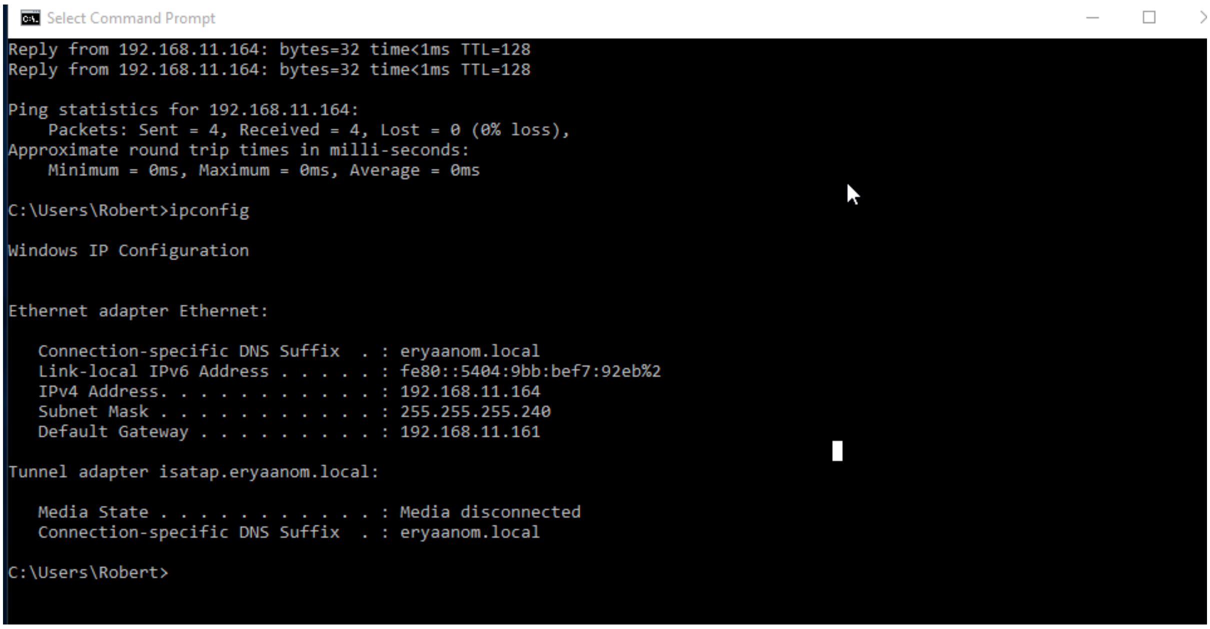
Configuration required. Installation succeeded on DCERYA.

Active Directory Domain Services
Additional steps are required to make this machine a domain controller.
Promote this server to a domain controller
Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools
Active Directory Administrative Center
AD DS Snap-Ins and Command-Line Tools

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

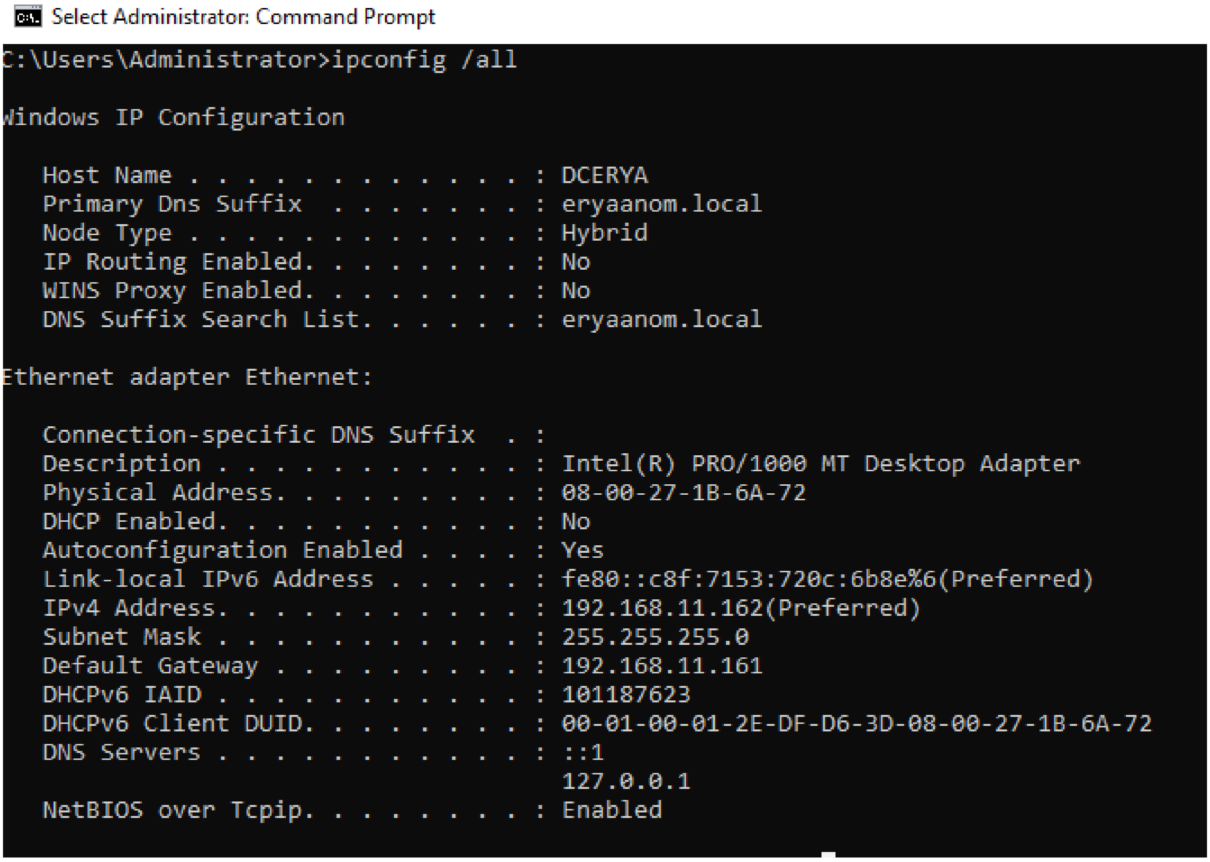
Export configuration settings

ROLES AND SERVER GROUPS
Roles: 2 | Server groups: 1 | Servers total: 1

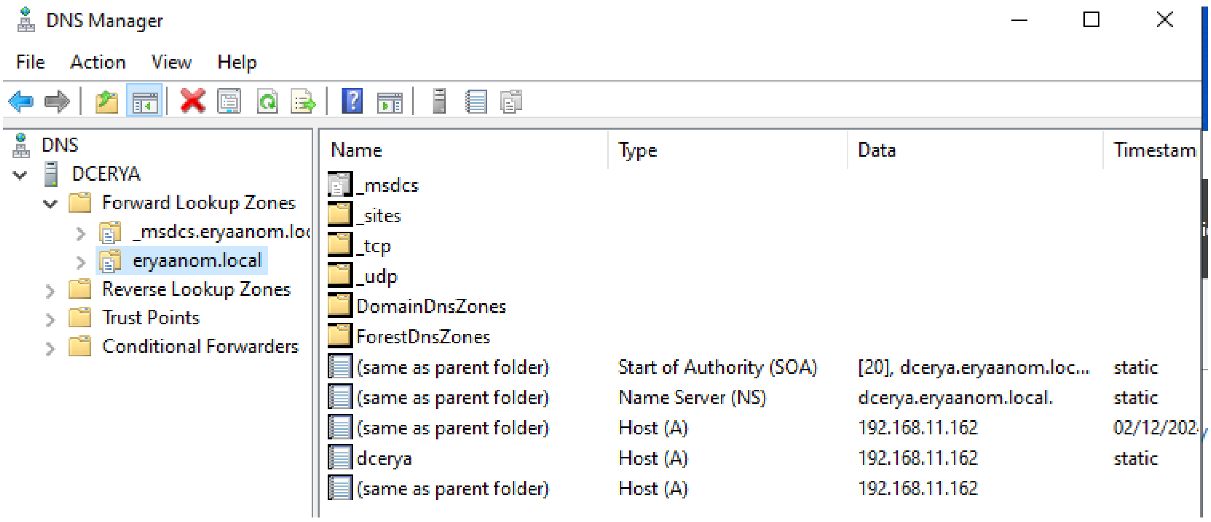


```
Reply from 192.168.11.164: bytes=32 time<1ms TTL=128
Reply from 192.168.11.164: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.11.164:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Robert>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : eryaanom.local
   Link-local IPv6 Address . . . . . : fe80::5404:9bb:bef7:92eb%2
   IPv4 Address. . . . . . . . . . . : 192.168.11.164
   Subnet Mask . . . . . . . . . . . : 255.255.255.240
   Default Gateway . . . . . . . . . : 192.168.11.161

Tunnel adapter isatap.eryaanom.local:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : eryaanom.local

C:\Users\Robert>
```

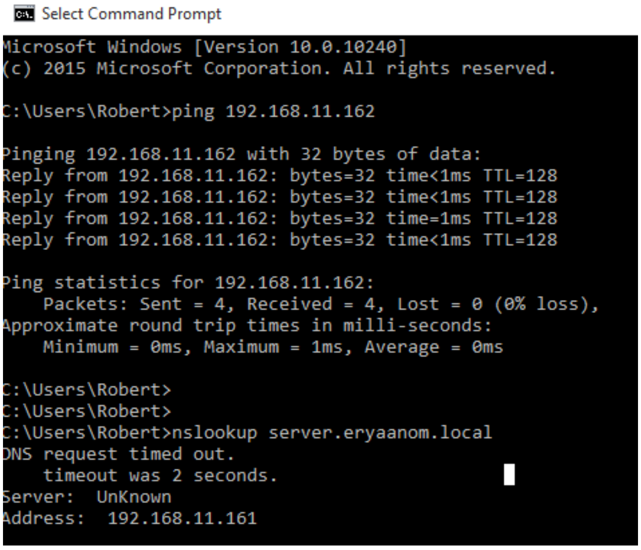
Active Directory Domain Services AD DS are used to authenticate and authorize users, devices and applications with the network. It will provide centralised management of user accounts, security policies and access to resources.



```
C:\Users\Administrator>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DCERYA
   Primary Dns Suffix  . . . . . . . : eryaanom.local
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : eryaanom.local

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
   Physical Address. . . . . . . . . : 08-00-27-1B-6A-72
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::c8f:7153:720c:6b8e%6(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.11.162(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.11.161
   DHCPv6 IAID . . . . . . . . . . . : 101187623
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2E-DF-D6-3D-08-00-27-1B-6A-72
   DNS Servers . . . . . . . . . . . : ::1
                                       127.0.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

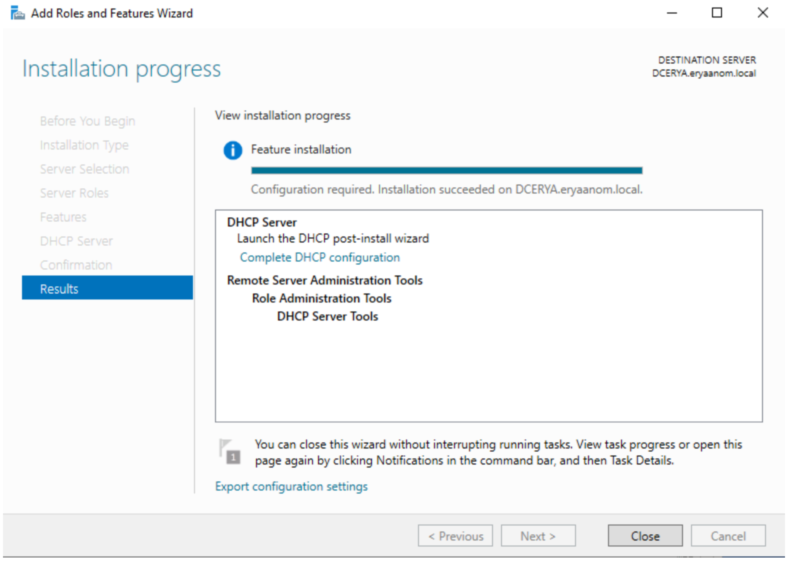


Name	Type	Data	Timestam
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(same as parent folder)	Start of Authority (SOA)	[20], dcerya.eryaanom.loc...	static
(same as parent folder)	Name Server (NS)	dcerya.eryaanom.local.	static
(same as parent folder)	Host (A)	192.168.11.162	02/12/202
dcerya	Host (A)	192.168.11.162	static
(same as parent folder)	Host (A)	192.168.11.162	



```
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\Robert>ping 192.168.11.162

Pinging 192.168.11.162 with 32 bytes of data:
Reply from 192.168.11.162: bytes=32 time<1ms TTL=128
Reply from 192.168.11.162: bytes=32 time<1ms TTL=128
Reply from 192.168.11.162: bytes=32 time=1ms TTL=128
Reply from 192.168.11.162: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.11.162:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Robert>
C:\Users\Robert>
C:\Users\Robert>nslookup server.eryaanom.local
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  192.168.11.161
```

Testing DNS Resolution



Installation progress

DESTINATION SERVER
DCERYA.eryaanom.local

View installation progress

Feature installation

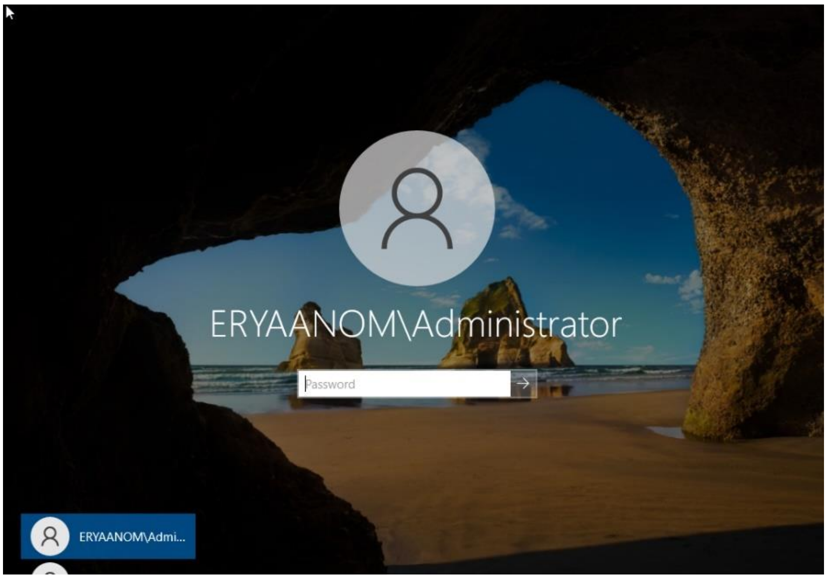
Configuration required. Installation succeeded on DCERYA.eryaanom.local.

DHCP Server
Launch the DHCP post-install wizard
Complete DHCP configuration
Remote Server Administration Tools
Role Administration Tools
DHCP Server Tools

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings

DHCP Server Installation



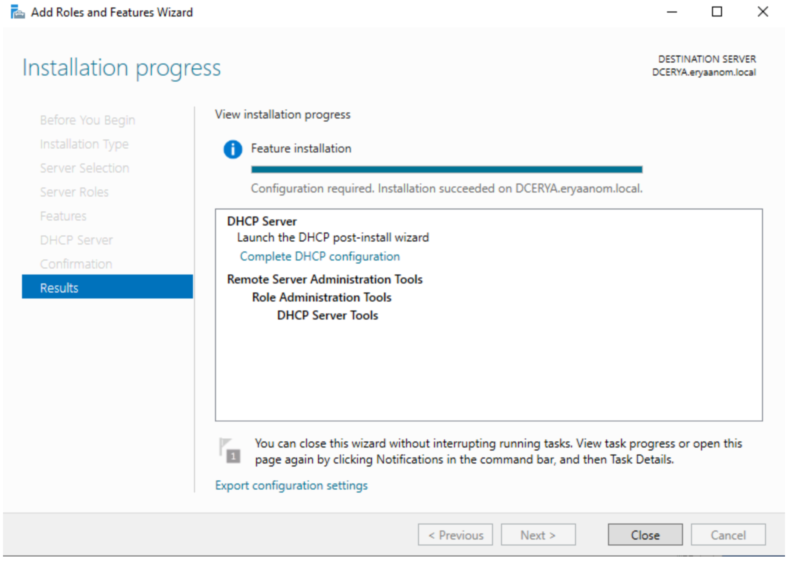
Testing Domain Authentication, by capturing the login screen showing the domain name.

Stage 5 – Using the addressing scheme provided at stage 3, implement network DHCP services within the LAN

Screenshots of DHCP on Server and Clients

Addressing Scheme:

Device	IP Address	Host Name
Router	192.168.11.161	Erya Router
Server	192.168.11.162	DC ERYA
PC 1	192.168.11.163	C1ERYA
PC 2	192.168.11.164	C2-ERYA



Installation progress

DESTINATION SERVER
DCERYA.eryaanom.local

View installation progress

Feature installation

Configuration required. Installation succeeded on DCERYA.eryaanom.local.

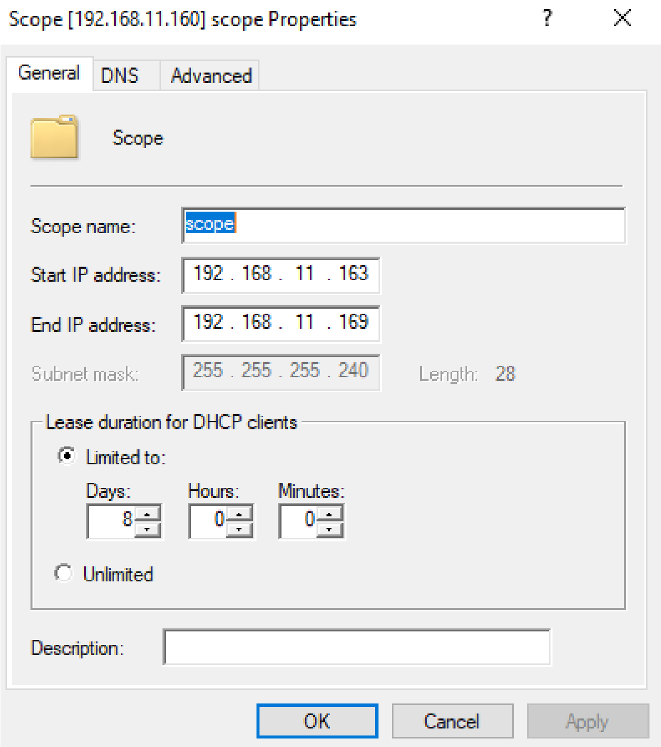
DHCP Server
Launch the DHCP post-install wizard
Complete DHCP configuration

Remote Server Administration Tools
Role Administration Tools
DHCP Server Tools

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings

DHCP Server Installation



Scope name: scope

Start IP address: 192 . 168 . 11 . 163

End IP address: 192 . 168 . 11 . 169

Subnet mask: 255 . 255 . 255 . 240 Length: 28

Lease duration for DHCP clients

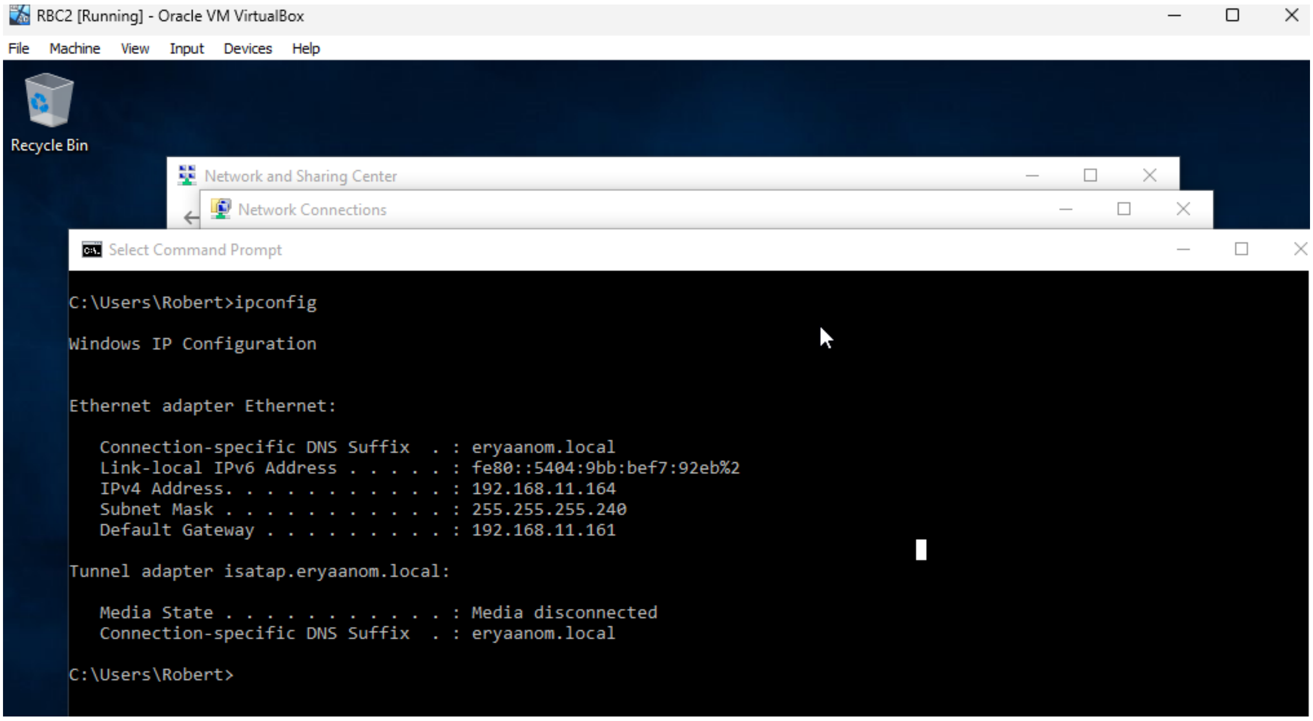
● Limited to:

Days: 8 Hours: 0 Minutes: 0

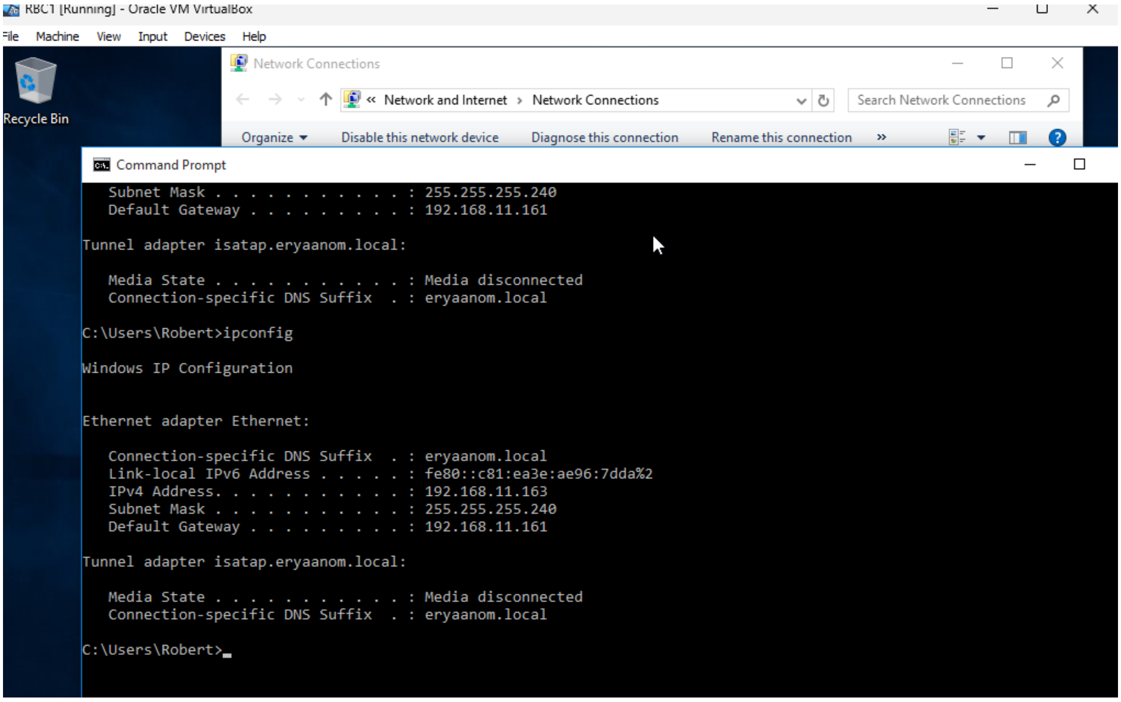
○ Unlimited

Description:

Create a Scope



```
C:\Users\Robert>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : eryaanom.local
   Link-local IPv6 Address . . . . . : fe80::5404:9bb:bef7:92eb%2
   IPv4 Address. . . . . . . . . . . : 192.168.11.164
   Subnet Mask . . . . . . . . . . . : 255.255.255.240
   Default Gateway . . . . . . . . . : 192.168.11.161

Tunnel adapter isatap.eryaanom.local:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : eryaanom.local

C:\Users\Robert>
```

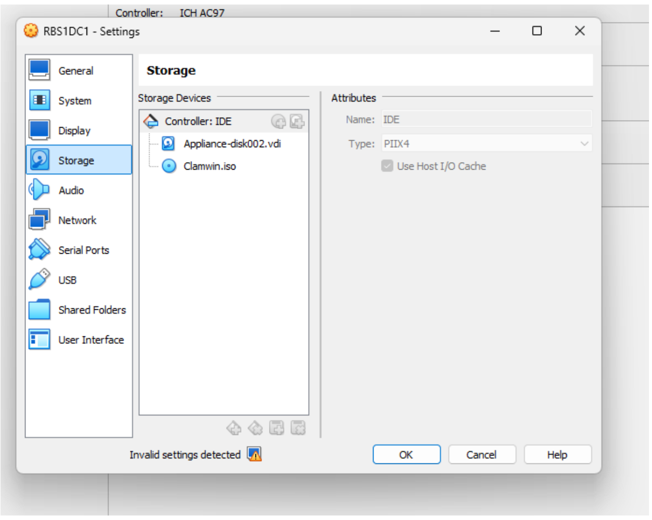

RBC1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Network Connections
« Network and Internet › Network Connections
Search Network Connections
Organize ▾ Disable this network device Diagnose this connection Rename this connection »
Command Prompt

```
   Subnet Mask . . . . . . . . . . . : 255.255.255.240
   Default Gateway . . . . . . . . . : 192.168.11.161

Tunnel adapter isatap.eryaanom.local:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : eryaanom.local

C:\Users\Robert>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : eryaanom.local
   Link-local IPv6 Address . . . . . : fe80::c81:ea3e:ae96:7dda%2
   IPv4 Address. . . . . . . . . . . : 192.168.11.163
   Subnet Mask . . . . . . . . . . . : 255.255.255.240
   Default Gateway . . . . . . . . . : 192.168.11.161

Tunnel adapter isatap.eryaanom.local:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : eryaanom.local

C:\Users\Robert>_
```

There several advantages of using DHCP, firstly, automatically assigns IP addresses, reducing administrative overhead. Secondly, easy to accommodates new devices in the network without manual configuration and lastly, consistency to managed.

Stage 6 – Harden the endpoint devices/hosts by installing virus checking software

Screenshot of install and run clamwin



Storage

Storage Devices

- Controller: IDE
  - Appliance-disk002.vdi
  - Clamwin.iso

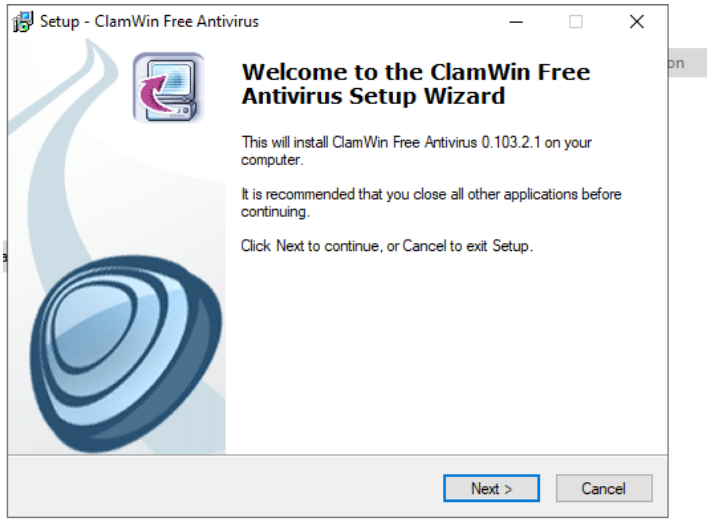
Attributes

Name: IDE

Type: PIIX4

☑ Use Host I/O Cache

Invalid settings detected

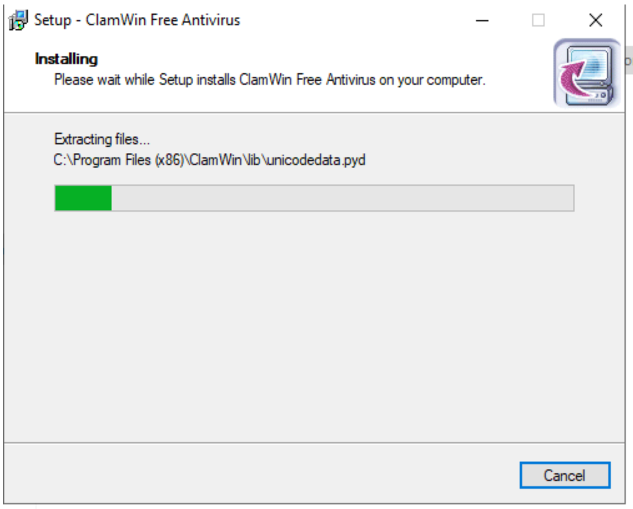


Welcome to the ClamWin Free Antivirus Setup Wizard

This will install ClamWin Free Antivirus 0.103.2.1 on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

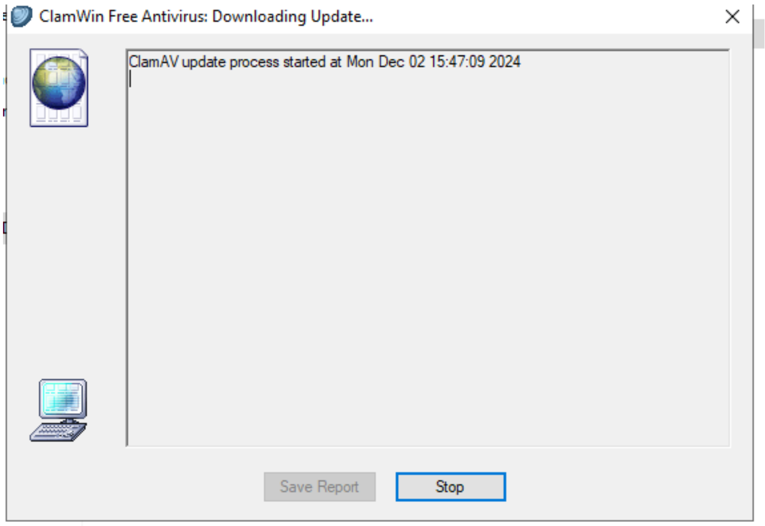


Installing

Please wait while Setup installs ClamWin Free Antivirus on your computer.

Extracting files...

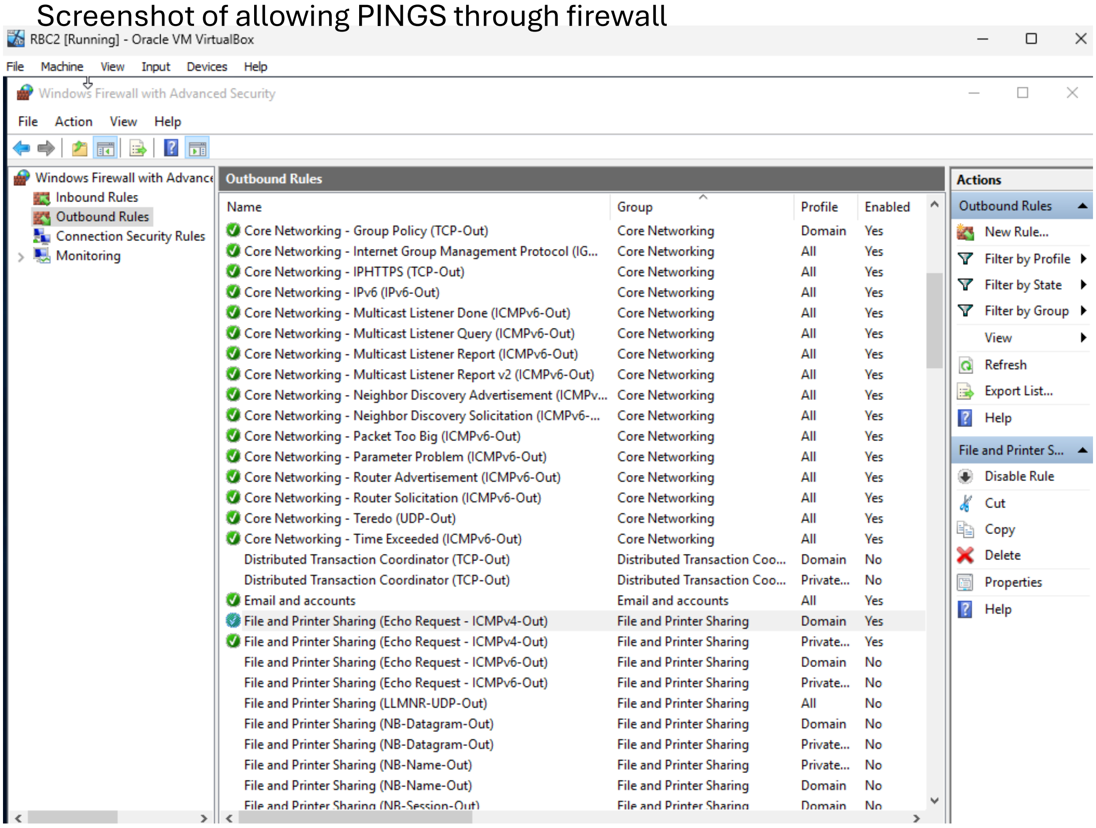
C:\Program Files (x86)\ClamWin\lib\unicodedata.pyd



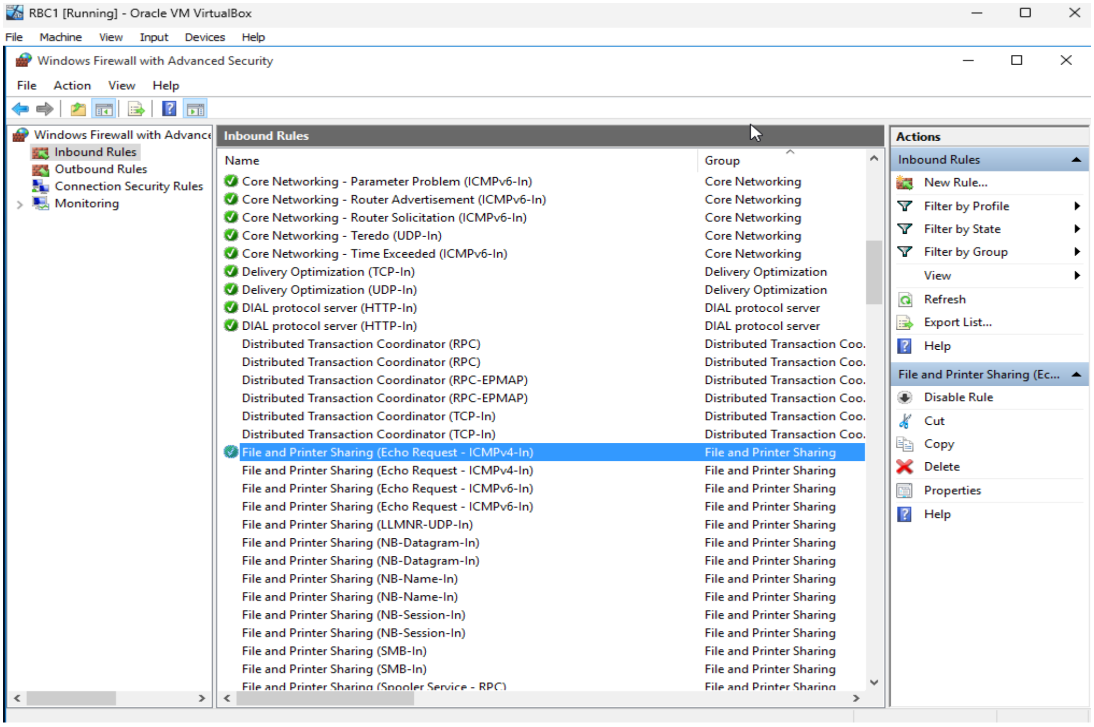
```
ClamAV update process started at Mon Dec 02 15:47:09 2024
```

Stage 7 – Configure endpoint devices firewalls to allow network hosts to each other

Screenshot of allowing PINGS through firewall



Name	Group	Profile	Enabled
Core Networking - Group Policy (TCP-Out)	Core Networking	Domain	Yes
Core Networking - Internet Group Management Protocol (IG...	Core Networking	All	Yes
Core Networking - IPHTTPS (TCP-Out)	Core Networking	All	Yes
Core Networking - IPv6 (IPv6-Out)	Core Networking	All	Yes
Core Networking - Multicast Listener Done (ICMPv6-Out)	Core Networking	All	Yes
Core Networking - Multicast Listener Query (ICMPv6-Out)	Core Networking	All	Yes
Core Networking - Multicast Listener Report (ICMPv6-Out)	Core Networking	All	Yes
Core Networking - Multicast Listener Report v2 (ICMPv6-Out)	Core Networking	All	Yes
Core Networking - Neighbor Discovery Advertisement (ICMPv...	Core Networking	All	Yes
Core Networking - Neighbor Discovery Solicitation (ICMPv6-...	Core Networking	All	Yes
Core Networking - Packet Too Big (ICMPv6-Out)	Core Networking	All	Yes
Core Networking - Parameter Problem (ICMPv6-Out)	Core Networking	All	Yes
Core Networking - Router Advertisement (ICMPv6-Out)	Core Networking	All	Yes
Core Networking - Router Solicitation (ICMPv6-Out)	Core Networking	All	Yes
Core Networking - Teredo (UDP-Out)	Core Networking	All	Yes
Core Networking - Time Exceeded (ICMPv6-Out)	Core Networking	All	Yes
Distributed Transaction Coordinator (TCP-Out)	Distributed Transaction Coo...	Domain	No
Distributed Transaction Coordinator (TCP-Out)	Distributed Transaction Coo...	Private...	No
Email and accounts	Email and accounts	All	Yes
File and Printer Sharing (Echo Request - ICMPv4-Out)	File and Printer Sharing	Domain	Yes
File and Printer Sharing (Echo Request - ICMPv4-Out)	File and Printer Sharing	Private...	Yes
File and Printer Sharing (Echo Request - ICMPv6-Out)	File and Printer Sharing	Domain	No
File and Printer Sharing (Echo Request - ICMPv6-Out)	File and Printer Sharing	Private...	No
File and Printer Sharing (LLMNR-UDP-Out)	File and Printer Sharing	All	No
File and Printer Sharing (NB-Datagram-Out)	File and Printer Sharing	Domain	No
File and Printer Sharing (NB-Datagram-Out)	File and Printer Sharing	Private...	No
File and Printer Sharing (NB-Name-Out)	File and Printer Sharing	Private...	No
File and Printer Sharing (NB-Name-Out)	File and Printer Sharing	Domain	No
File and Printer Sharing (NB-Session-Out)	File and Printer Sharing	Domain	No



Name	Group
✓ Core Networking - Parameter Problem (ICMPv6-In)	Core Networking
✓ Core Networking - Router Advertisement (ICMPv6-In)	Core Networking
✓ Core Networking - Router Solicitation (ICMPv6-In)	Core Networking
✓ Core Networking - Teredo (UDP-In)	Core Networking
✓ Core Networking - Time Exceeded (ICMPv6-In)	Core Networking
✓ Delivery Optimization (TCP-In)	Delivery Optimization
✓ Delivery Optimization (UDP-In)	Delivery Optimization
✓ DIAL protocol server (HTTP-In)	DIAL protocol server
✓ DIAL protocol server (HTTP-In)	DIAL protocol server
Distributed Transaction Coordinator (RPC)	Distributed Transaction Coo...
Distributed Transaction Coordinator (RPC)	Distributed Transaction Coo...
Distributed Transaction Coordinator (RPC-EPMAP)	Distributed Transaction Coo...
Distributed Transaction Coordinator (RPC-EPMAP)	Distributed Transaction Coo...
Distributed Transaction Coordinator (TCP-In)	Distributed Transaction Coo...
Distributed Transaction Coordinator (TCP-In)	Distributed Transaction Coo...
✓ File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing
File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing
File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing
File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing
File and Printer Sharing (LLMNR-UDP-In)	File and Printer Sharing
File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing
File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing
File and Printer Sharing (NB-Name-In)	File and Printer Sharing
File and Printer Sharing (NB-Name-In)	File and Printer Sharing
File and Printer Sharing (NB-Session-In)	File and Printer Sharing
File and Printer Sharing (NB-Session-In)	File and Printer Sharing
File and Printer Sharing (SMB-In)	File and Printer Sharing
File and Printer Sharing (SMB-In)	File and Printer Sharing
File and Printer Sharing (Spooler Service - RPC)	File and Printer Sharing

Stage 8 – show evidence that stages 4-7 have been completed and are operational

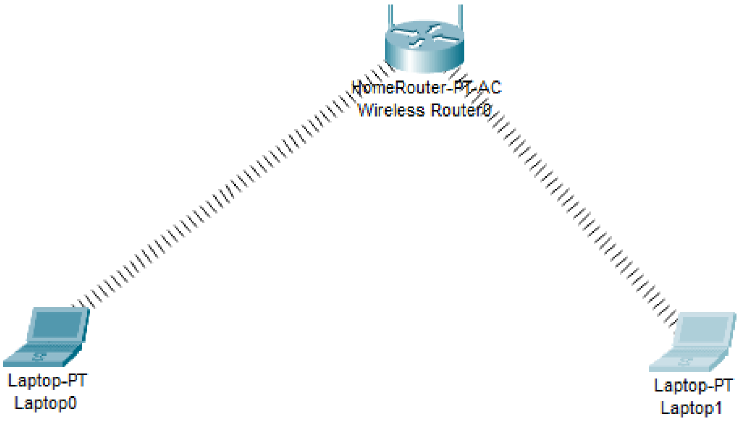
Assessment 3

Assessment instructions

Create a secure wireless network

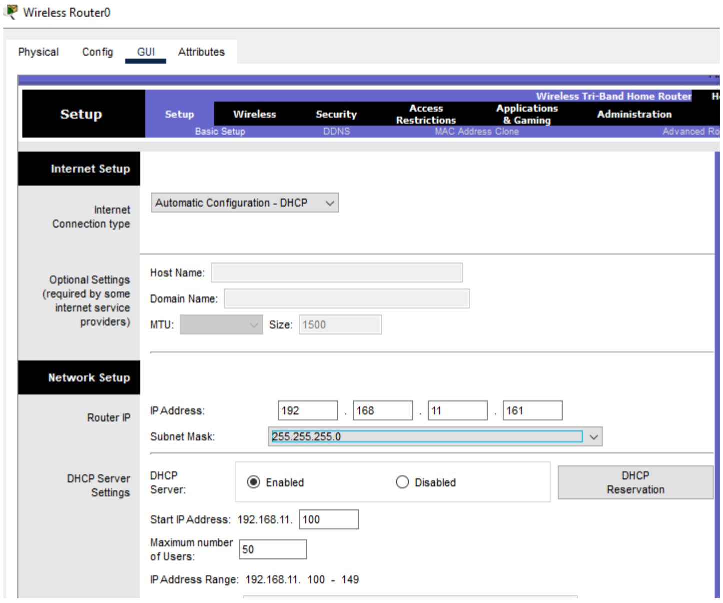
Scenario – you have been tasked with setting up a secure wireless network for a local charity.

Stage 1 — Devise a list of equipment that will be required to allow wireless technology to be implemented within the local charity



in this stage, need to identify the equipment to set up the wireless network. Firstly, wireless router or access points. Central devices that broadcast the wireless signals. Secondly, end devices with two laptops used by charity staff or visitors. Firewall. A hardware or software firewall to protect the network from external threats and lastly, cables, ethernet cables to connect devices like access point to the switch or router.

Stage 2 — Obtain and setup the wireless equipment, describe/log/picture log/vlog the steps to achieve this build



Internet Setup

Internet Connection type: Automatic Configuration - DHCP

Optional Settings (required by some internet service providers)

Host Name:

Domain Name:

MTU: Size: 1500

Network Setup

Router IP

IP Address: 192 . 168 . 11 . 161

Subnet Mask: 255.255.255.0

DHCP Server Settings

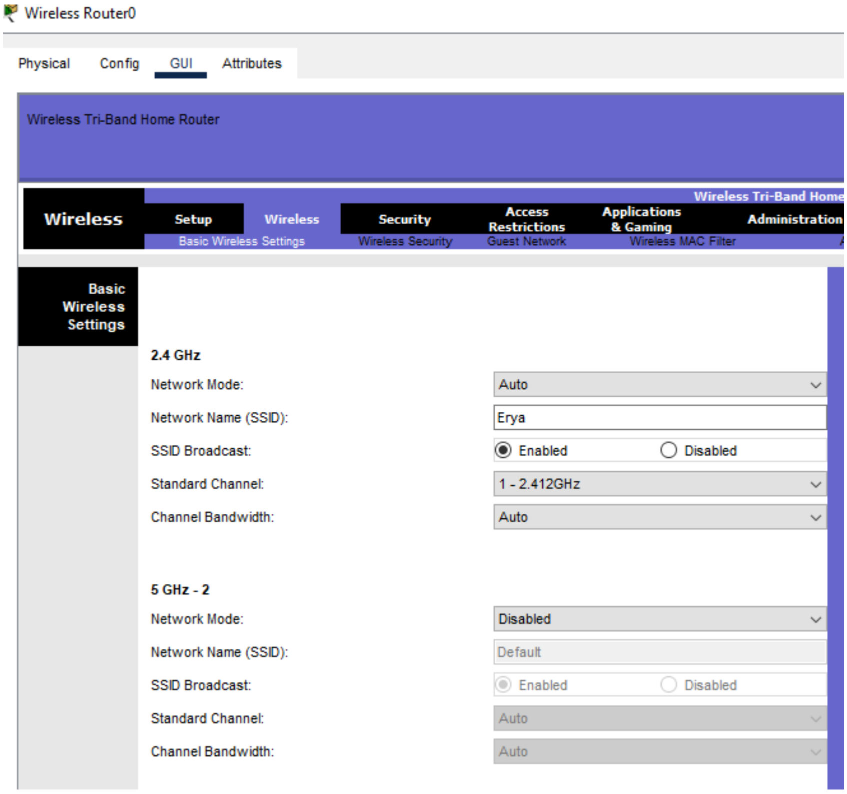
DHCP Server: ● Enabled ○ Disabled

Start IP Address: 192.168.11. 100

Maximum number of Users: 50

IP Address Range: 192.168.11. 100 - 149

This stage involved setting up the wireless equipment. Connect the router and configure the wireless and setting up the IP address scheme by configure DHCP to assign IP address to devices. Router IP: 192.168.11.161 and DHCP Range: 192.168.11.100 – 192.168.0.149. and setting up wireless, Network Mode > Auto Network Name > Erya > Enable > 1-2412GHz >save setting



Basic Wireless Settings

2.4 GHz

Network Mode: Auto

Network Name (SSID): Erya

SSID Broadcast: ● Enabled ○ Disabled

Standard Channel: 1 - 2.412GHz

Channel Bandwidth: Auto

5 GHz - 2

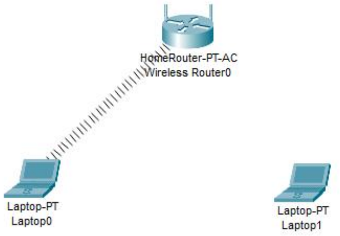
Network Mode: Disabled

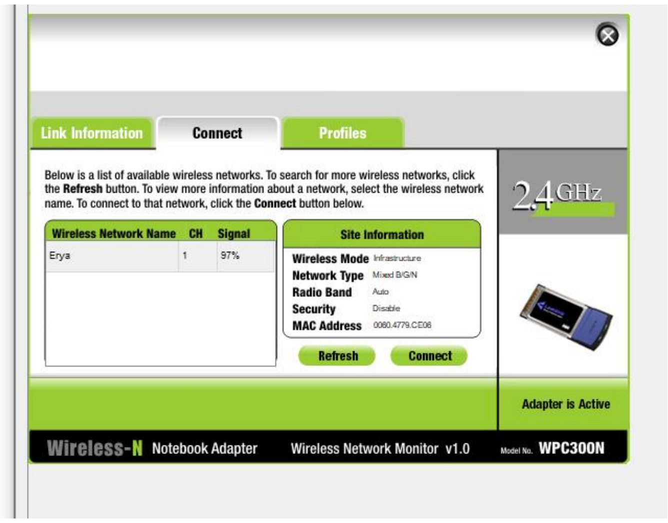
Network Name (SSID): Default

SSID Broadcast: ● Enabled ○ Disabled

Standard Channel: Auto

Channel Bandwidth: Auto



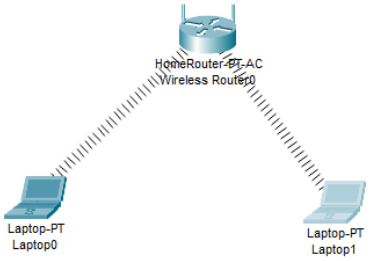


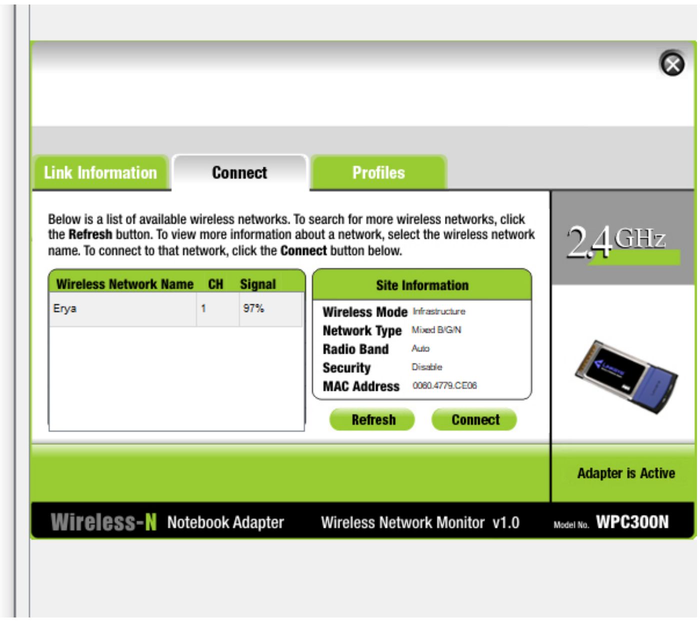
Below is a list of available wireless networks. To search for more wireless networks, click the **Refresh** button. To view more information about a network, select the wireless network name. To connect to that network, click the **Connect** button below.

Wireless Network Name	CH	Signal
Erya	1	97%

Site Information

Wireless Mode	Infrastructure
Network Type	Mixed B/G/N
Radio Band	Auto
Security	Disable
MAC Address	0060.4779.CE06





Below is a list of available wireless networks. To search for more wireless networks, click the **Refresh** button. To view more information about a network, select the wireless network name. To connect to that network, click the **Connect** button below.

Wireless Network Name	CH	Signal
Erya	1	97%

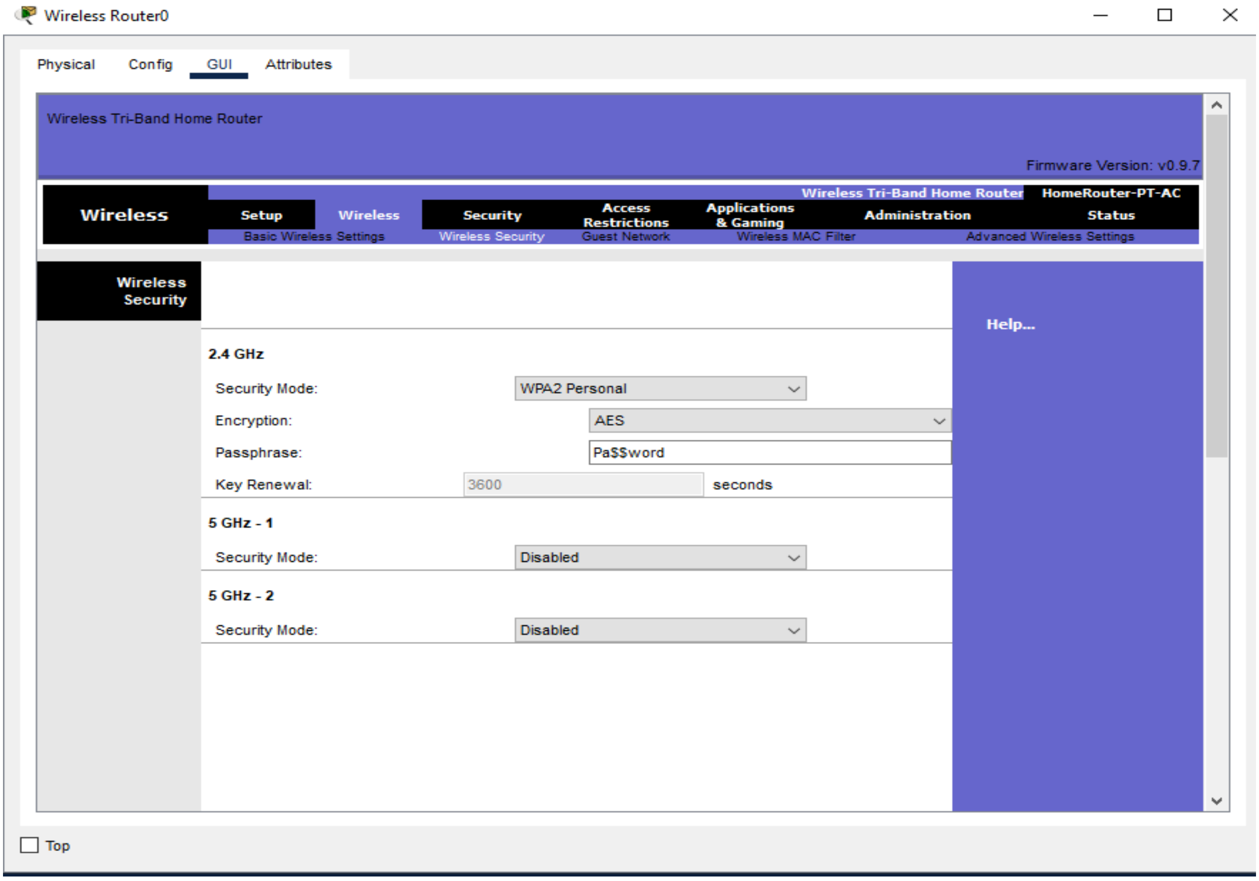
Site Information

Wireless Mode	Infrastructure
Network Type	Mixed B/G/N
Radio Band	Auto
Security	Disable
MAC Address	0060.4779.CE06

Test connectivity: make sure devices can connect to the network and access the internet.

Stage 3 — Devise and implement a suitable authentication and encryption scheme to allow users to use the wireless network

In this stage must secure the wireless network with appropriate authentication and encryption to make sure only authorized users can access it. Choose wireless security protocol and set up a strong password.



2.4 GHz

Security Mode: WPA2 Personal

Encryption: AES

Passphrase: Pa$$word

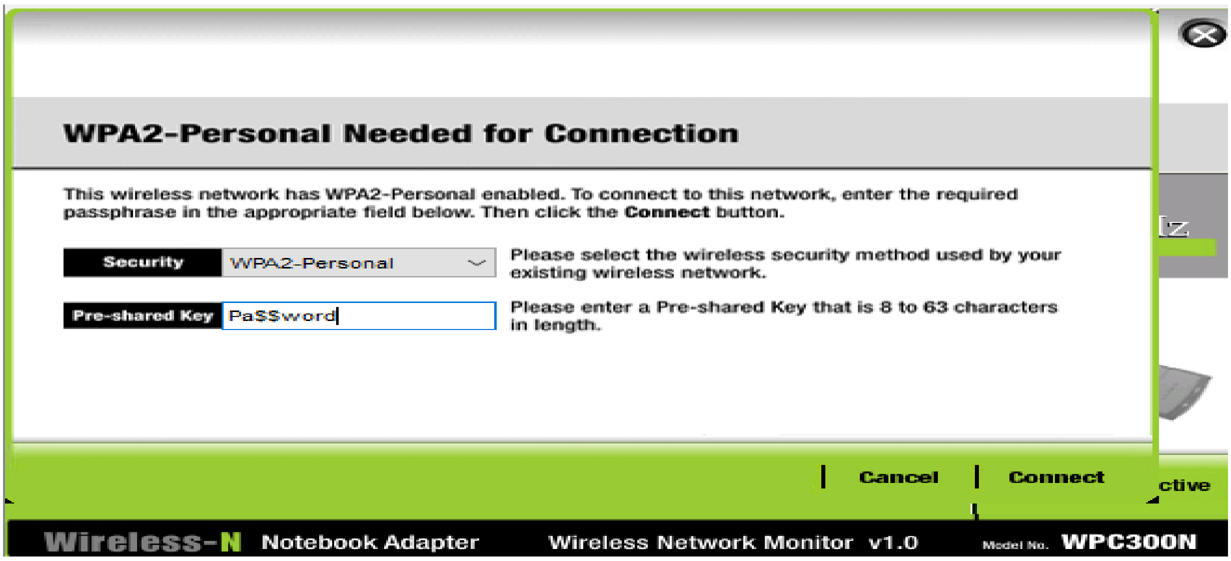
Key Renewal: 3600 seconds

5 GHz - 1

Security Mode: Disabled

5 GHz - 2

Security Mode: Disabled



WPA2-Personal Needed for Connection

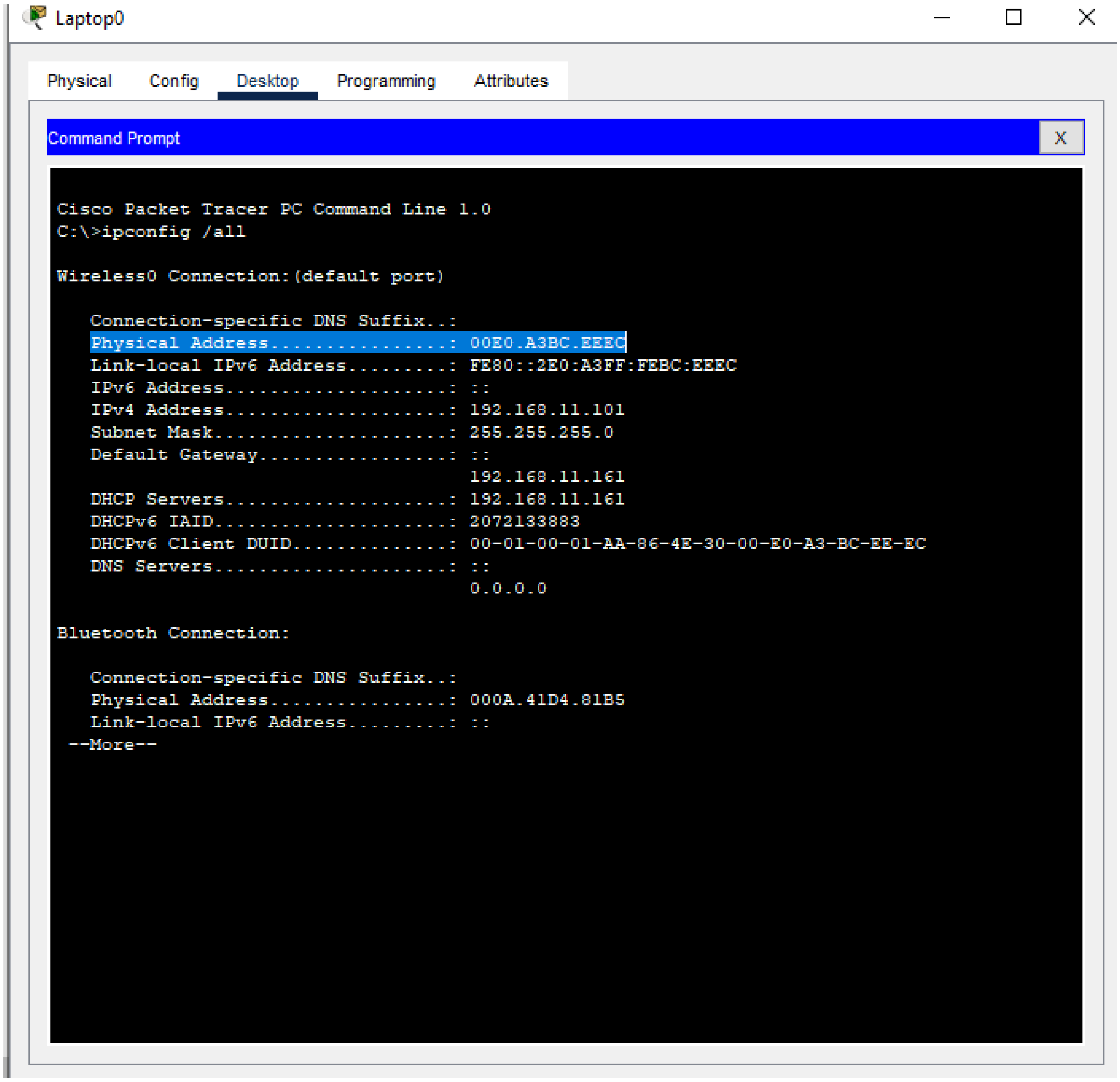
This wireless network has WPA2-Personal enabled. To connect to this network, enter the required passphrase in the appropriate field below. Then click the **Connect** button.

Security: WPA2-Personal — Please select the wireless security method used by your existing wireless network.

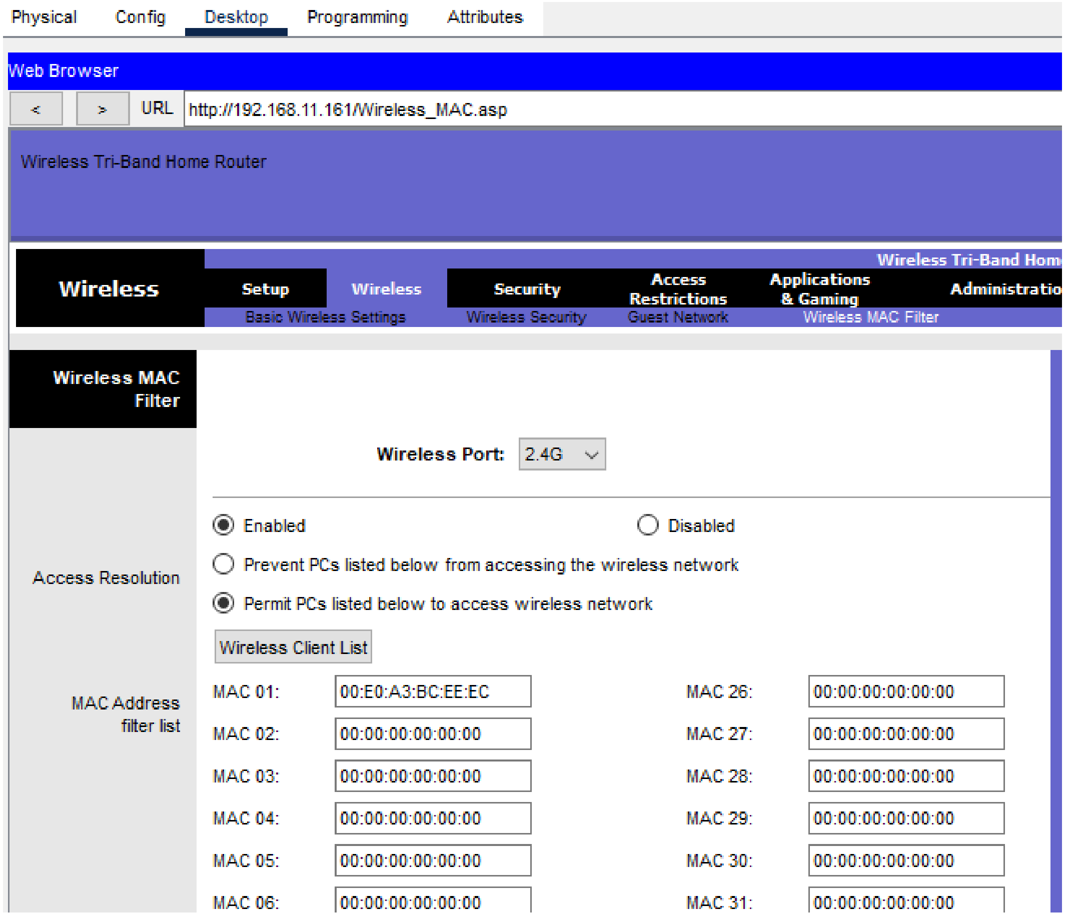
Pre-shared Key: Pa$$word — Please enter a Pre-shared Key that is 8 to 63 characters in length.

Stage 4 — Implement wireless MAC address filtering to further secure the wireless network

In this stage involve implementing MAC address filtering to improve the security of a wireless network. To access the router's admin panel, by opening a web browser and enter the router's IP address [192.168.11.161] and it will show authorization. Log in using the admin username and password.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig /all

Wireless0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address................: 00E0.A3BC.EEEC
   Link-local IPv6 Address.........: FE80::2E0:A3FF:FEBC:EEEC
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.11.101
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     192.168.11.161
   DHCP Servers....................: 192.168.11.161
   DHCPv6 IAID.....................: 2072133883
   DHCPv6 Client DUID..............: 00-01-00-01-AA-86-4E-30-00-E0-A3-BC-EE-EC
   DNS Servers.....................: ::
                                     0.0.0.0

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Physical Address................: 000A.41D4.81B5
   Link-local IPv6 Address.........: ::
 --More--
```



URL http://192.168.11.161/Wireless_MAC.asp

Wireless Tri-Band Home Router

Wireless MAC Filter

Wireless Port: 2.4G

● Enabled ○ Disabled

Access Resolution

○ Prevent PCs listed below from accessing the wireless network

● Permit PCs listed below to access wireless network

Wireless Client List

MAC Address filter list

MAC 01:	00:E0:A3:BC:EE:EC	MAC 26:	00:00:00:00:00:00
MAC 02:	00:00:00:00:00:00	MAC 27:	00:00:00:00:00:00
MAC 03:	00:00:00:00:00:00	MAC 28:	00:00:00:00:00:00
MAC 04:	00:00:00:00:00:00	MAC 29:	00:00:00:00:00:00
MAC 05:	00:00:00:00:00:00	MAC 30:	00:00:00:00:00:00
MAC 06:	00:00:00:00:00:00	MAC 31:	00:00:00:00:00:00

In the Router’s setting, Wireless and look for MAC address filtering and enable MAC filtering. Collect the MAC addresses of approved devices. Open a command prompt and typing ipconfig /all and enter. It shows MAC addresses under physical address. Add MAC addresses to the allow list in the router’s admin panel.

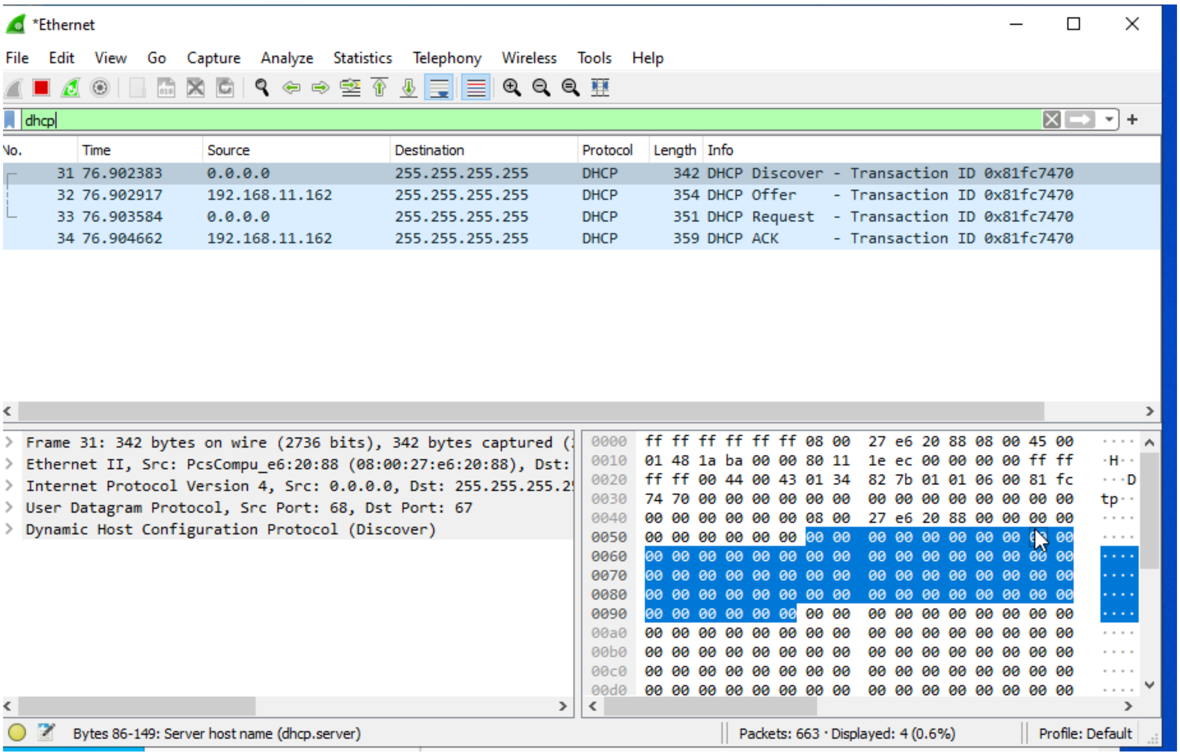
Assessment 4

Assessment Instructions

Capture the transmitted/received data using network sniffer technology

Scenario – You have been asked to prove how DHCP operates and how some protocols can be considered more secure than others.

Stage 1 – Using the network set up in outcome 2, set up your network packet sniffer to capture and understand the DHCP communication process between the DHCP server and a selected Host



```
dhcp
```

```
No.     Time        Source          Destination      Protocol  Length  Info
     31 76.902383   0.0.0.0         255.255.255.255  DHCP         342  DHCP Discover - Transaction ID 0x81fc7470
     32 76.902917   192.168.11.162  255.255.255.255  DHCP         354  DHCP Offer    - Transaction ID 0x81fc7470
     33 76.903584   0.0.0.0         255.255.255.255  DHCP         351  DHCP Request  - Transaction ID 0x81fc7470
     34 76.904662   192.168.11.162  255.255.255.255  DHCP         359  DHCP ACK      - Transaction ID 0x81fc7470
```

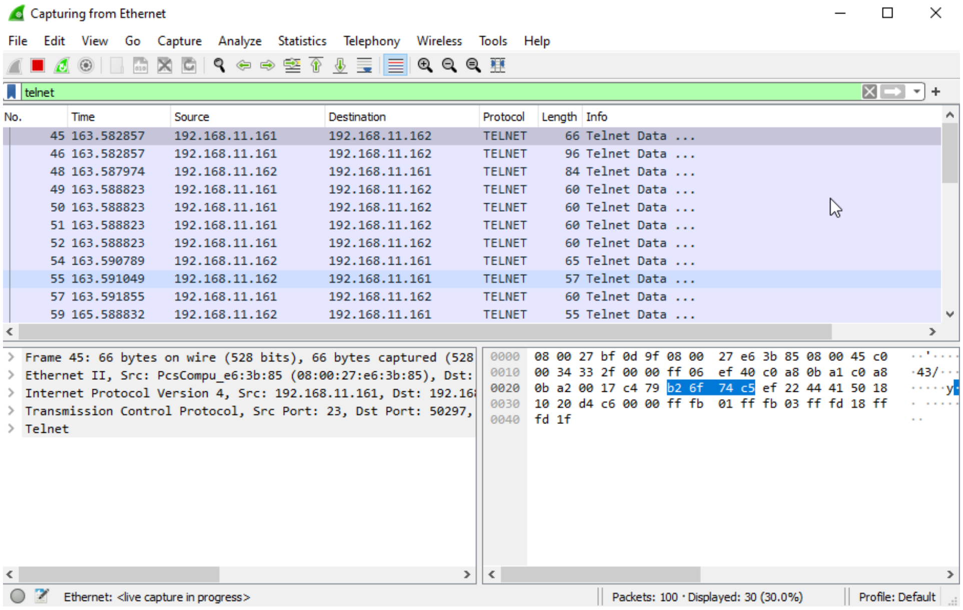
```
> Frame 31: 342 bytes on wire (2736 bits), 342 bytes captured (
> Ethernet II, Src: PcsCompu_e6:20:88 (08:00:27:e6:20:88), Dst:
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.2
> User Datagram Protocol, Src Port: 68, Dst Port: 67
> Dynamic Host Configuration Protocol (Discover)
```

```
0000  ff ff ff ff ff ff 08 00  27 e6 20 88 08 00 45 00   ····
0010  01 48 1a ba 00 00 80 11  1e ec 00 00 00 00 ff ff   ·H··
0020  ff ff 00 44 00 43 01 34  82 7b 01 01 06 00 81 fc   ···D
0030  74 70 00 00 00 00 00 00  00 00 00 00 00 00 00 00   tp··
0040  00 00 00 00 00 00 08 00  27 e6 20 88 00 00 00 00   ····
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ····
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ····
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ····
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ····
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ····
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ····
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ····
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ····
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ····
```

```
Bytes 86-149: Server host name (dhcp.server)    Packets: 663 · Displayed: 4 (0.6%)    Profile: Default
```

Set up a network using DHCP and using a packet sniffer – Wireshark to capture and analysis the data exchanged during DHCP communication between the server and a host.

Stage 2 – You should have been provided a suitable test environment which includes a Telnet and SSH Server. You should also have a login for each of the servers. Your task is to capture the packet data during the login process of each and compare the results from each.



Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

telnet

No.	Time	Source	Destination	Protocol	Length	Info
45	163.582857	192.168.11.161	192.168.11.162	TELNET	66	Telnet Data ...
46	163.582857	192.168.11.161	192.168.11.162	TELNET	96	Telnet Data ...
48	163.587974	192.168.11.162	192.168.11.161	TELNET	84	Telnet Data ...
49	163.588823	192.168.11.161	192.168.11.162	TELNET	60	Telnet Data ...
50	163.588823	192.168.11.161	192.168.11.162	TELNET	60	Telnet Data ...
51	163.588823	192.168.11.161	192.168.11.162	TELNET	60	Telnet Data ...
52	163.588823	192.168.11.161	192.168.11.162	TELNET	60	Telnet Data ...
54	163.590789	192.168.11.162	192.168.11.161	TELNET	65	Telnet Data ...
55	163.591049	192.168.11.162	192.168.11.161	TELNET	57	Telnet Data ...
57	163.591855	192.168.11.161	192.168.11.162	TELNET	60	Telnet Data ...
59	165.588832	192.168.11.162	192.168.11.161	TELNET	55	Telnet Data ...

```
> Frame 45: 66 bytes on wire (528 bits), 66 bytes captured (528
> Ethernet II, Src: PcsCompu_e6:3b:85 (08:00:27:e6:3b:85), Dst:
> Internet Protocol Version 4, Src: 192.168.11.161, Dst: 192.16
> Transmission Control Protocol, Src Port: 23, Dst Port: 50297,
> Telnet
```

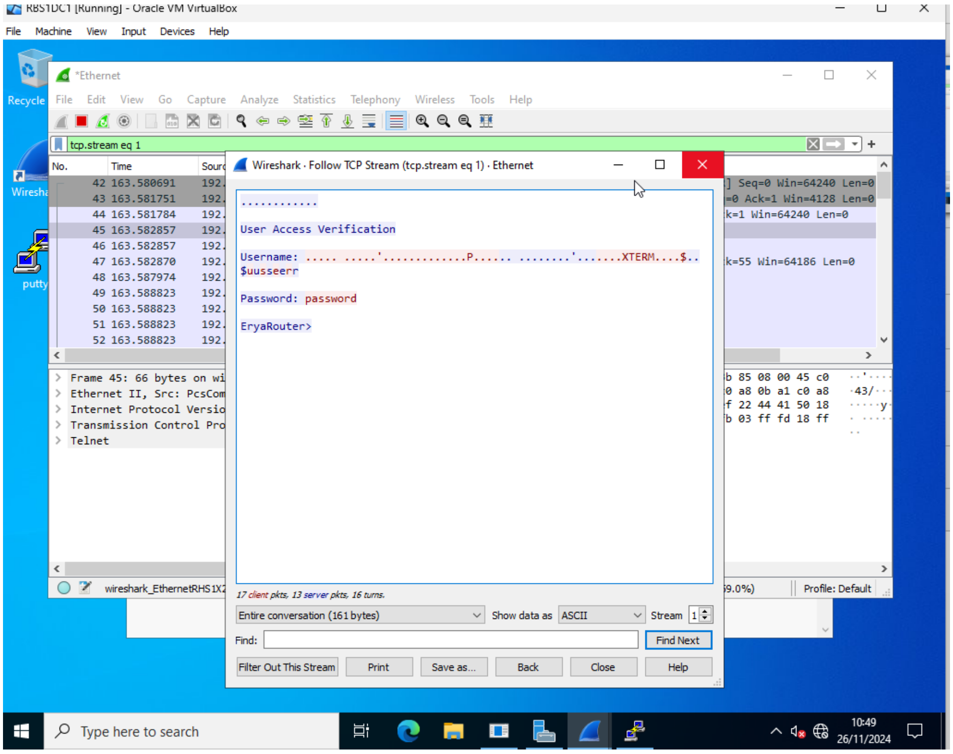
```
0000  08 00 27 bf 0d 9f 08 00  27 e6 3b 85 08 00 45 c0   ··'·····
0010  00 34 33 2f 00 00 ff 06  ef 40 c0 a8 0b a1 c0 a8   ·43/····
0020  0b a2 00 17 c4 79 b2 6f  74 c5 ef 22 44 41 50 18   ·····y
0030  10 20 d4 c6 00 00 ff fb  01 ff fb 03 ff fd 18 ff   · ·····
0040  fd 1f                                              ··
```

Ethernet: <live capture in progress>

Packets: 100 · Displayed: 30 (30.0%)

Profile: Default

This stage is provided with a test environment that includes a Telnet server and SSH server. This goal is to capture packet data during login process by using Wireshark. By using Telnet it should see plain text data, including the username and password are visible in the captured packets.



RHS1DC1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle
Wiresha
putty
*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Type here to search

tcp.stream eq 1

Wireshark · Follow TCP Stream (tcp.stream eq 1) · Ethernet

```
............

User Access Verification

Username: ..... .....'............P...... ........'.......XTERM....$..
$uusseerr

Password: password

EryaRouter>
```

17 client pkts, 13 server pkts, 16 turns.

Entire conversation (161 bytes)

Show data as ASCII

Stream 1

Find:

Find Next

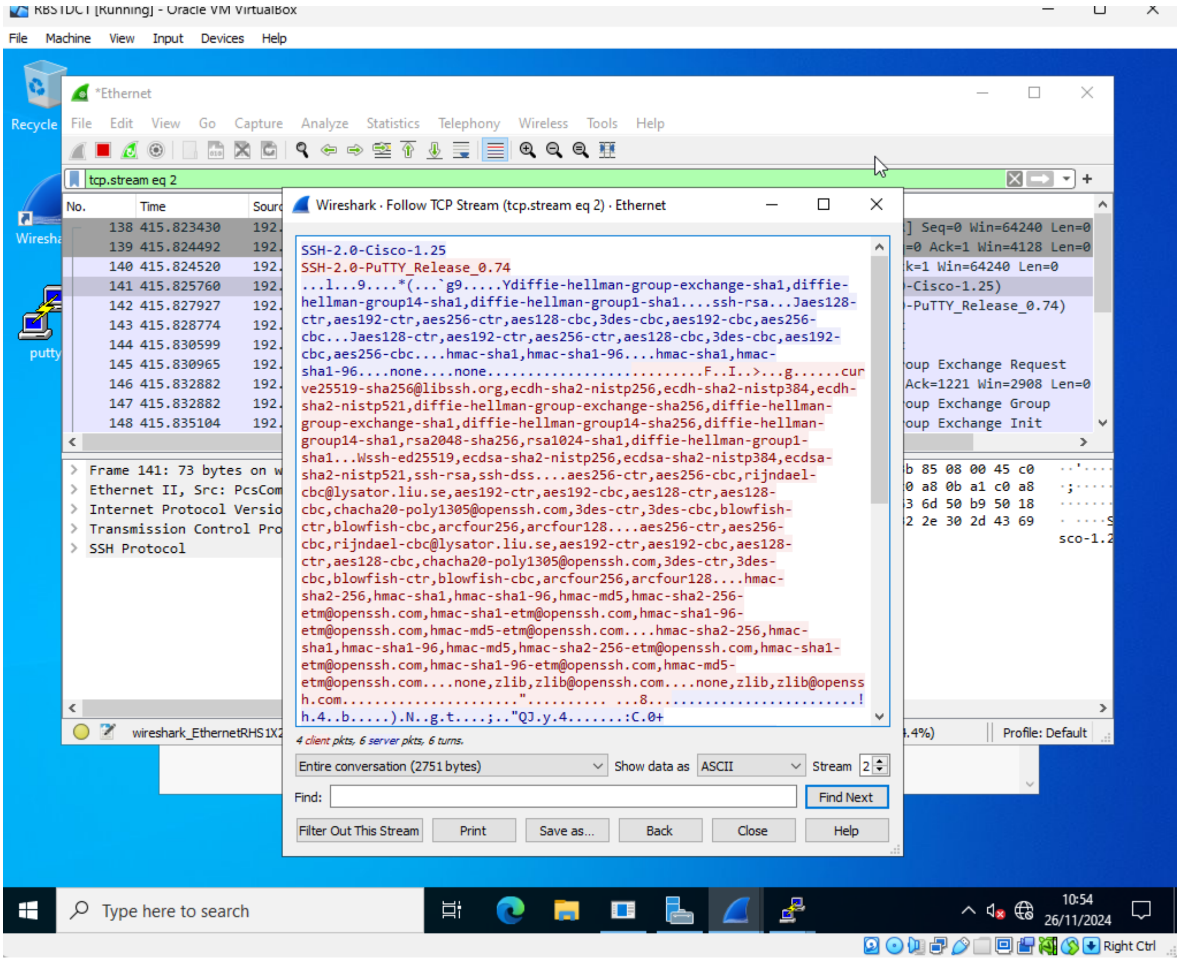
Filter Out This Stream
Print
Save as...
Back
Close
Help

wireshark_EthernetRHS1X2

Profile: Default

10:49
26/11/2024

Capture SSH traffic by using Wireshark while logging into the SSH server. Apply a filter for SSH traffic and observe and save packet capture. SSH analyse the capture packets, and the data should be encrypted and unreadable. The image show PuTTY configured to connect to an SSH server at 192.168.11.161 on port 22 and ensures all traffic is encrypted.



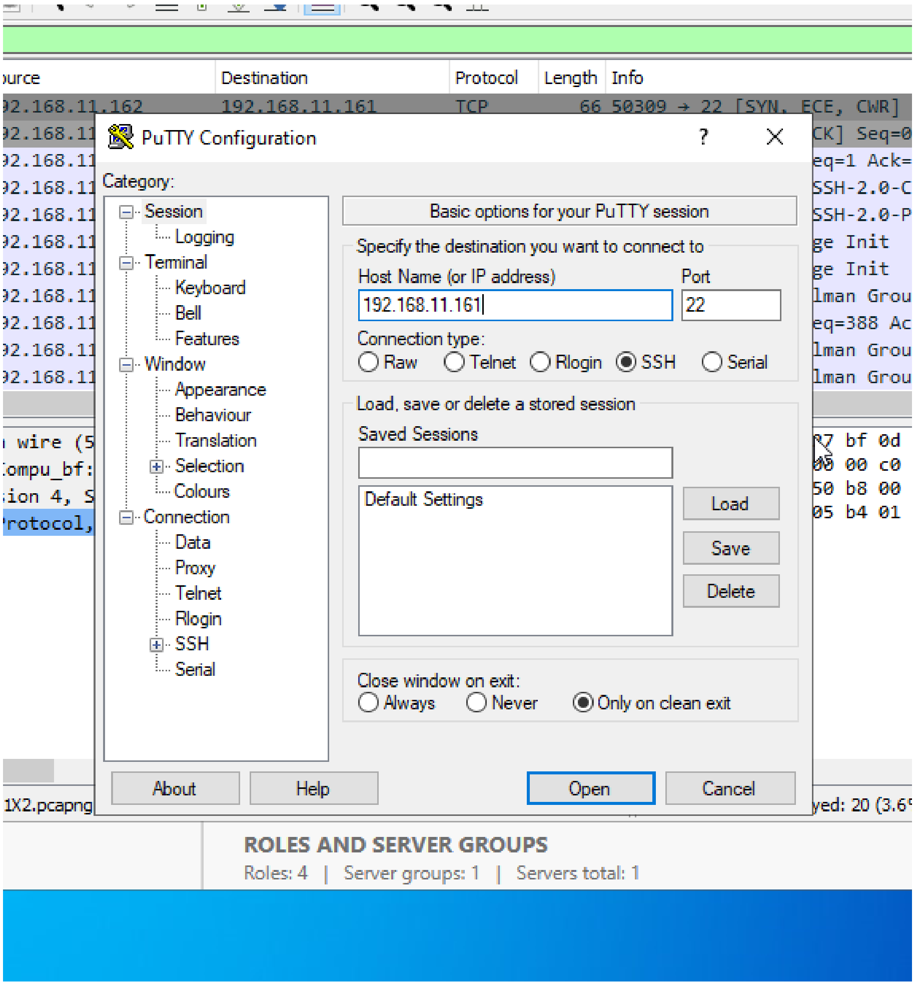
RBSTDCT [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 2
Wireshark · Follow TCP Stream (tcp.stream eq 2) · Ethernet
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help
Type here to search
10:54
26/11/2024
Right Ctrl

```
SSH-2.0-Cisco-1.25
SSH-2.0-PuTTY_Release_0.74
...l...9....*(...`g9.....Ydiffie-hellman-group-exchange-sha1,diffie-
hellman-group14-sha1,diffie-hellman-group1-sha1....ssh-rsa...Jaes128-
ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc,aes192-cbc,aes256-
cbc...Jaes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc,aes192-
cbc,aes256-cbc....hmac-sha1,hmac-sha1-96....hmac-sha1,hmac-
sha1-96....none....none.........................F..I..>...g......cur
ve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-
sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-
group-exchange-sha1,diffie-hellman-group14-sha256,diffie-hellman-
group14-sha1,rsa2048-sha256,rsa1024-sha1,diffie-hellman-group1-
sha1...Wssh-ed25519,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-
sha2-nistp521,ssh-rsa,ssh-dss....aes256-ctr,aes256-cbc,rijndael-
cbc@lysator.liu.se,aes192-ctr,aes192-cbc,aes128-ctr,aes128-
cbc,chacha20-poly1305@openssh.com,3des-ctr,3des-cbc,blowfish-
ctr,blowfish-cbc,arcfour256,arcfour128....aes256-ctr,aes256-
cbc,rijndael-cbc@lysator.liu.se,aes192-ctr,aes192-cbc,aes128-
ctr,aes128-cbc,chacha20-poly1305@openssh.com,3des-ctr,3des-
cbc,blowfish-ctr,blowfish-cbc,arcfour256,arcfour128....hmac-
sha2-256,hmac-sha1,hmac-sha1-96,hmac-md5,hmac-sha2-256-
etm@openssh.com,hmac-sha1-etm@openssh.com,hmac-sha1-96-
etm@openssh.com,hmac-md5-etm@openssh.com....hmac-sha2-256,hmac-
sha1,hmac-sha1-96,hmac-md5,hmac-sha2-256-etm@openssh.com,hmac-sha1-
etm@openssh.com,hmac-sha1-96-etm@openssh.com,hmac-md5-
etm@openssh.com....none,zlib,zlib@openssh.com....none,zlib,zlib@openss
h.com.....................".......... ...8..........................!
h.4..b.....).N..g.t....;.."QJ.y.4.......:C.0+
```

4 client pkts, 6 server pkts, 6 turns.

Entire conversation (2751 bytes) Show data as ASCII Stream 2

Find:



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 192.168.11.161

Port: 22

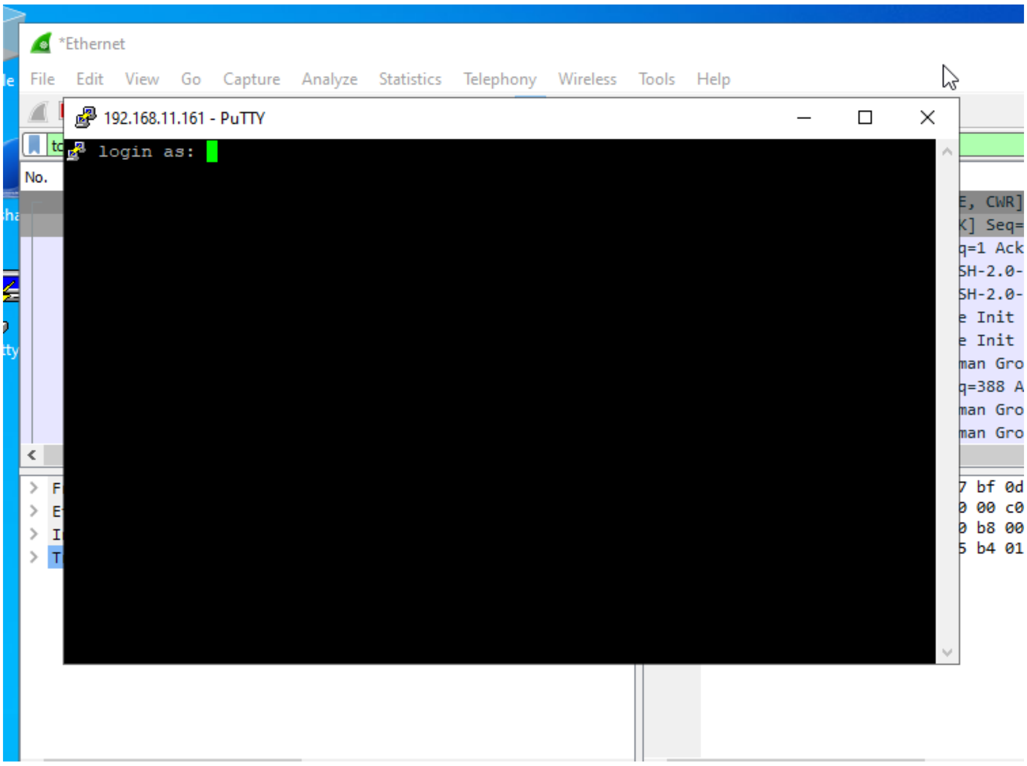
Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions

Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

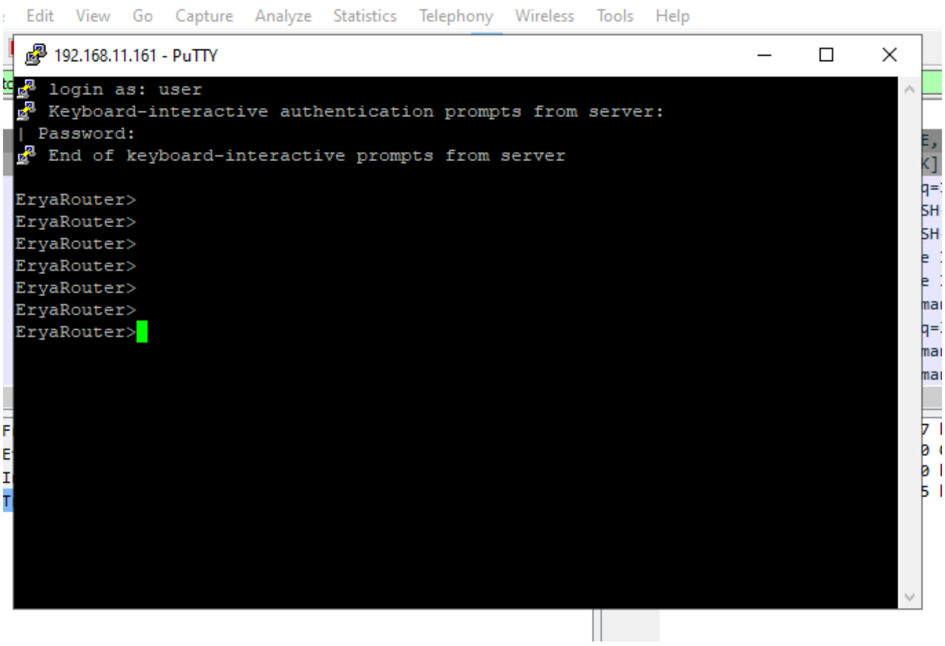


192.168.11.161 - PuTTY

```
login as:
```

Protocol	Encryption	Data Visibility	Security Implications
Telnet	None	Data is visible in plaintext	Vulnerable
SSH	Yes	Data is encrypted and unreadable	Secure against data

In conclusion that Telnet demonstrates how insecure due to the lack of encryption, and it highlight how SSH ensures secure communication through encryption.


Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
192.168.11.161 - PuTTY

```
login as: user
Keyboard-interactive authentication prompts from server:
| Password:
End of keyboard-interactive prompts from server

EryaRouter>
EryaRouter>
EryaRouter>
EryaRouter>
EryaRouter>
EryaRouter>
EryaRouter>
```

Stage 3 – Using the network set up in outcome 3, and using a wireless packet sniffer, capture the wireless data with and without the encryption being applied. Compare the output of each.

the data had been encrypted