CIS115 Week 7 Lab Overview

# Title of Lab: Networking with Python

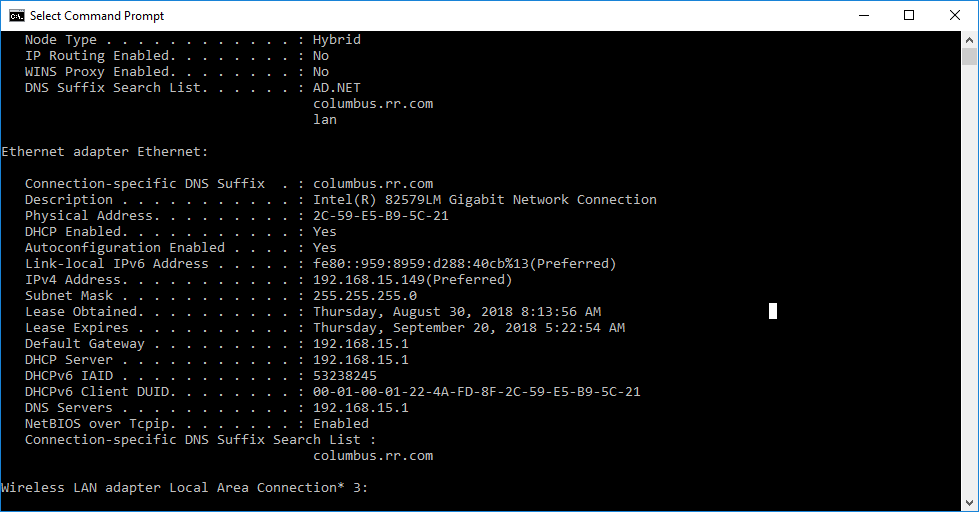
## Deliverables

* A source code Python file.
* A Word document containing both source code and the screen print of the program outputs.

# Lab Steps

## Part 1 – Finding your IP address

We will create a python program to do a port scan. To do this you need to find the ip address of your computer. Open a Command Prompt (Start button -> Windows System-> Command Prompt). At the command prompt type *ipconfig –all*



In the above example the IP address is IPv4 **192.168.15.149**

## Part 2 – Running Your Code

After you have set up your router we will create a python program to do a port scan. Open Idle create a new file. Enter the following python code to create a port scanner. NOTE - do not run the port scanner on any site except your router and your own machine.

|  |
| --- |
| #!/usr/bin/env python  import socket  import subprocess  import sys  from datetime import datetime  # Clear the screen  subprocess.call('clear', shell=True)  # Ask for input  remoteServer = input("Enter a remote host to scan: ")  remoteServerIP = socket.gethostbyname(remoteServer)  # Print a nice banner with information on which host we are about to scan  print ("-" \* 60)  print ("Please wait, scanning remote host", remoteServerIP)  print ("-" \* 60)  # Check what time the scan started  t1 = datetime.now()  # Using the range function to specify ports (here it will scans all ports between 1 and 1024)  # We also put in some error handling for catching errors  try:  for port in range(1,1025):  sock = socket.socket(socket.AF\_INET, socket.SOCK\_STREAM)  result = sock.connect\_ex((remoteServerIP, port))  if result == 0:  print ("Port {}: Open".format(port))  sock.close()  except KeyboardInterrupt:  print ("You pressed Ctrl+C")  sys.exit()  except socket.gaierror:  print ("Hostname could not be resolved. Exiting")  sys.exit()  except socket.error:  print ("Couldn't connect to server")  sys.exit()  # Checking the time again  t2 = datetime.now()  # Calculates the difference of time, to see how long it took to run the script  total = t2 - t1  # Printing the information to screen  print ("Scanning Completed in: ", total) |

Run the above code and enter the IP address of the machine (note the machine above is 192.168.8.113). This will take several minutes - **even up to 10 minutes** so please be patient! You may also try entering in the ip address of your router (shown below)

