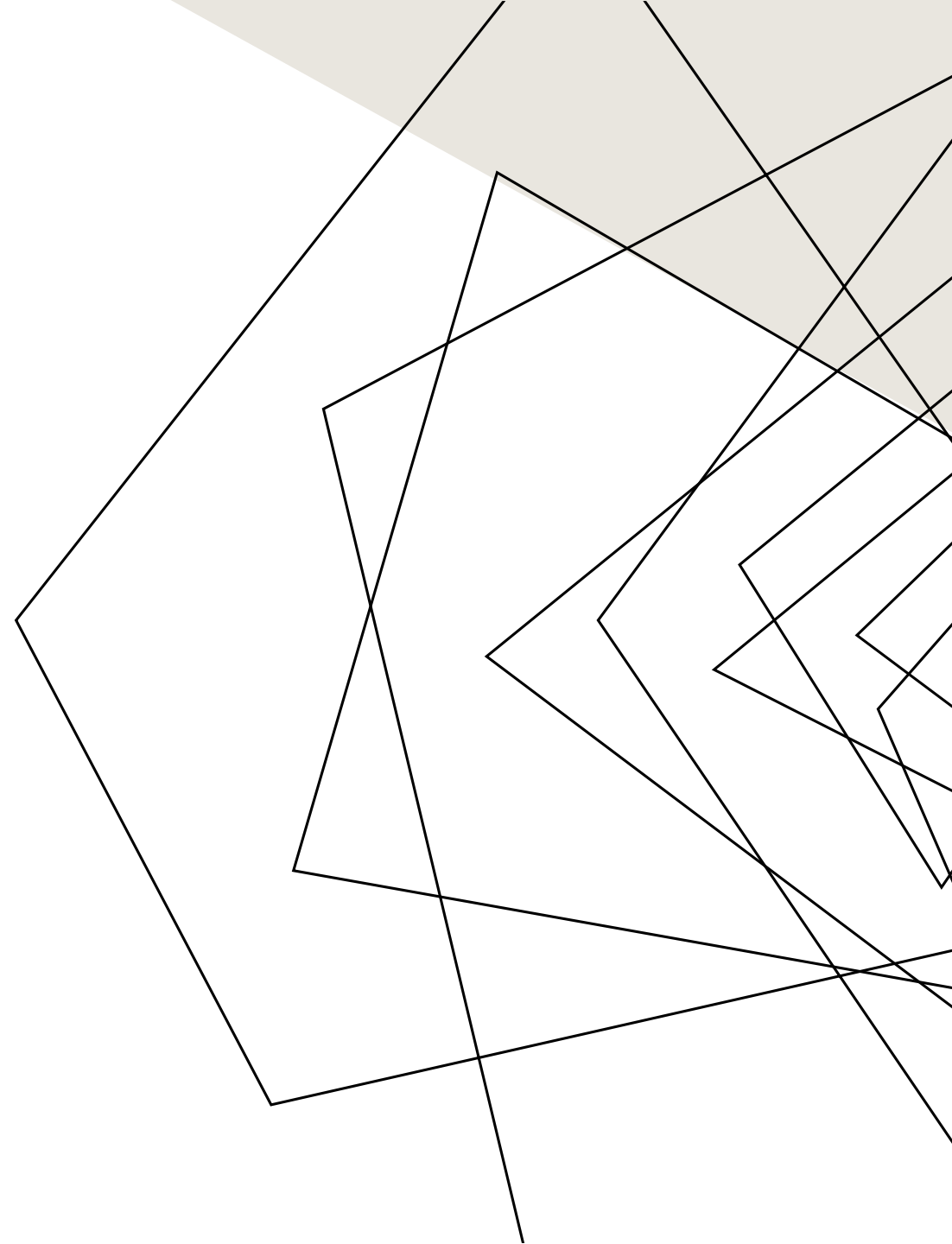


Abstract geometric lines in white on a black background, forming various polygons and intersecting lines.

IT PROJECTS WITH  
CISCO PACKET TRACER  
BY BRYAN ORTEGA IT  
PROJECTS WITH CISCO  
PACKET TRACER BY  
BRYAN ORTEGA

## ABOUT US

I am an entry-level cybersecurity student eager to grow in the IT field., I am committed to expanding my skills and gaining practical experience. My goal is to contribute to the protection of digital assets while continually learning and advancing in the fast-evolving world of cybersecurity. I am Comptia A+ and N+ certified. Currently perusing the sec+ certification. throughout my studies I would like to apply my knowledge into action.



# DHCP SCOPE

- Here I set up a DHCP server using packet tracer.
- I used 2 pcs, 1 switch, 1 router and copper straight through cable.
- First thing I did was go to my router>CLI; created a DHCP pool, created a network for the scope to work in, default router.
- Second, I configured an IP address so the router can communicate with the switch.
- Third, I IPconfig the pc to verify it received the DHCP

The screenshot displays the Cisco Packet Tracer interface. The main workspace shows a network topology with the following components and connections:

- PC-PT PC0** connected to **2960 24TT Switch0** via a copper straight-through cable.
- 2960 24TT Switch0** connected to **ISR4331 DHCP server** via a copper straight-through cable.

Two configuration windows are open:

- PC0 Configuration Window:** Shows the output of the `ipconfig` command. It displays the FastEthernet0 connection details, including the Link-local IPv6 Address (FE80::200:CFF:FEAC:663C), IPv6 Address (FE80::200:CFF:FEAC:663C), IPv4 Address (169.254.102.61), Subnet Mask (255.255.0.0), and Default Gateway (0.0.0.0).
- PC1 Configuration Window:** Shows the output of the `ipconfig` command. It displays the FastEthernet0 connection details, including the Link-local IPv6 Address (FE80::260:2FFF:FEBE:B14E), IPv6 Address (FE80::260:2FFF:FEBE:B14E), IPv4 Address (192.168.0.1), Subnet Mask (255.255.255.0), and Default Gateway (192.168.0.254).

The bottom status bar indicates the simulation is running in **Realtime** mode.

# ICMP

The screenshot displays the Cisco Packet Tracer interface. On the left, a terminal window for PC0 shows the results of a ping command to 192.168.0.51, indicating successful communication with 4 packets sent and received. Below the terminal, a network diagram shows PC0 connected to a Sniffer (Sniffer0), which is connected to a 2960-24TT Switch, which is then connected to PC1. On the right, the Sniffer0 GUI is open, showing the 'GUI' tab. The 'Incoming Packets' section is active, displaying a detailed view of an Ethernet II frame and an ICMP Echo (ping) request. The frame details include: Preamble (101010...), Destination Address (0060.478D.7293), Source Address (855C.B286), Type (0x0800), and Length (0x00000000). The ICMP details show: Version (4), Type (8), Code (0), Checksum (0x0000), Identifier (0x0005), Sequence Number (0x0001), and Source IP (192.168.0.51). The destination IP is 192.168.0.50. The bottom status bar shows the time as 00:07:31 and the temperature as 56°F.

- **Internet Control Message Protocol. Confirms other devices on the network.**
- **Used 2 pcs, 1 switch, 1 sniffer and used the automatically choose connection type feature for cabling.**
- **First gave each PC a IPv4 address.**
- **Second went on the sniffer> GUI>edit filters> Misc and unchecked STP traffic filter.**
- **Third ping one of the pcs, confirmed communication between pcs and checked the ICMP traffic on the sniffer.**

# SNMP PORT 161/162

- Monitors and configures networking devices
- Used 1 pc, 1 sniffer, 1 switch, 1 router and copper straight-through cable.
- First router>CLI> configured some Ip information, then configured SNMP on the router by typing "SNMP-server community", created a password for read only and then created another password for read-write.
- Second went to the sniffer>GUI>edit filters and cleared the STP traffic
- Third configured the IP address on the pc, then click on the desktop, MIB browser > advanced and configured the SNMP information

