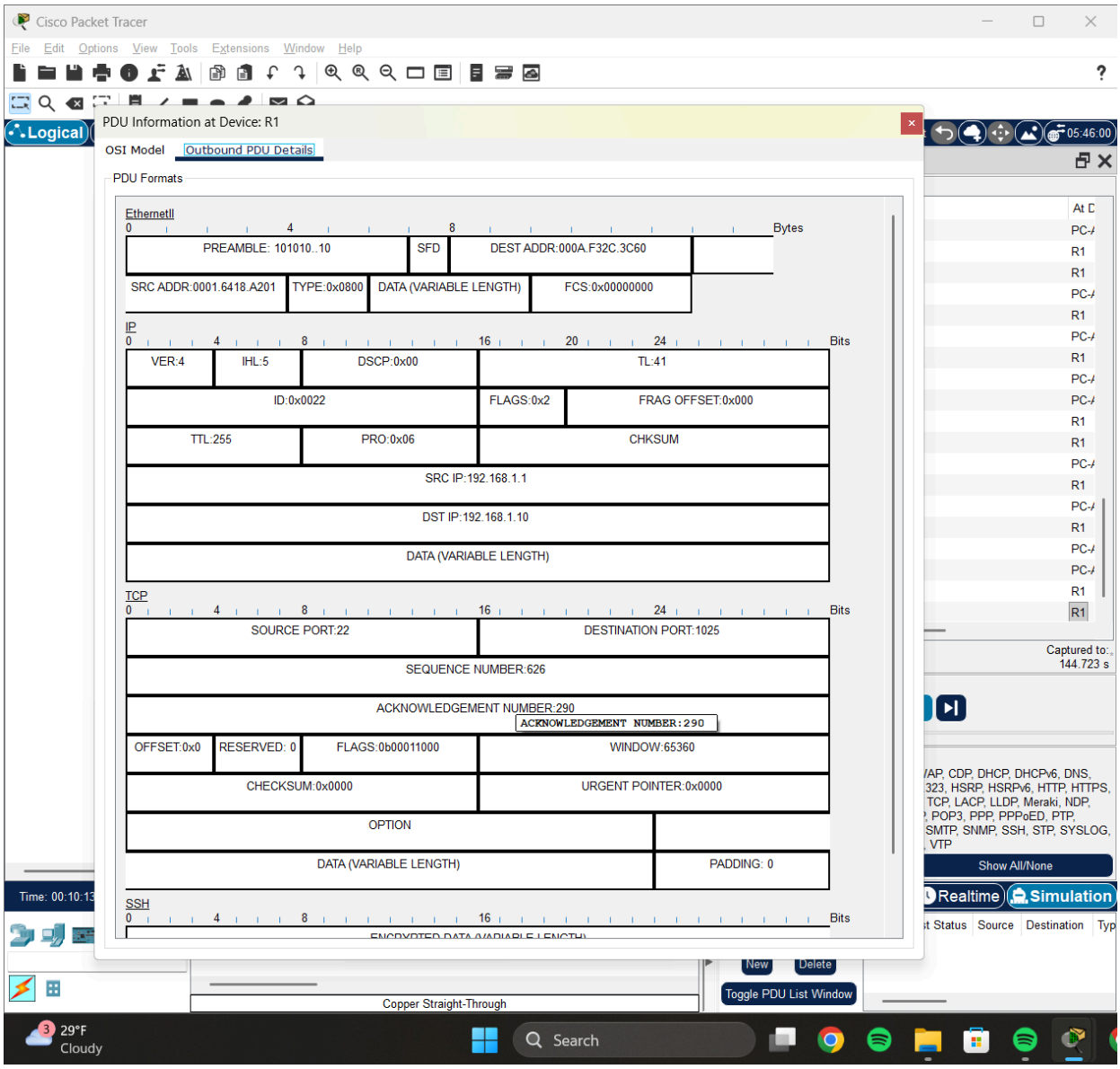
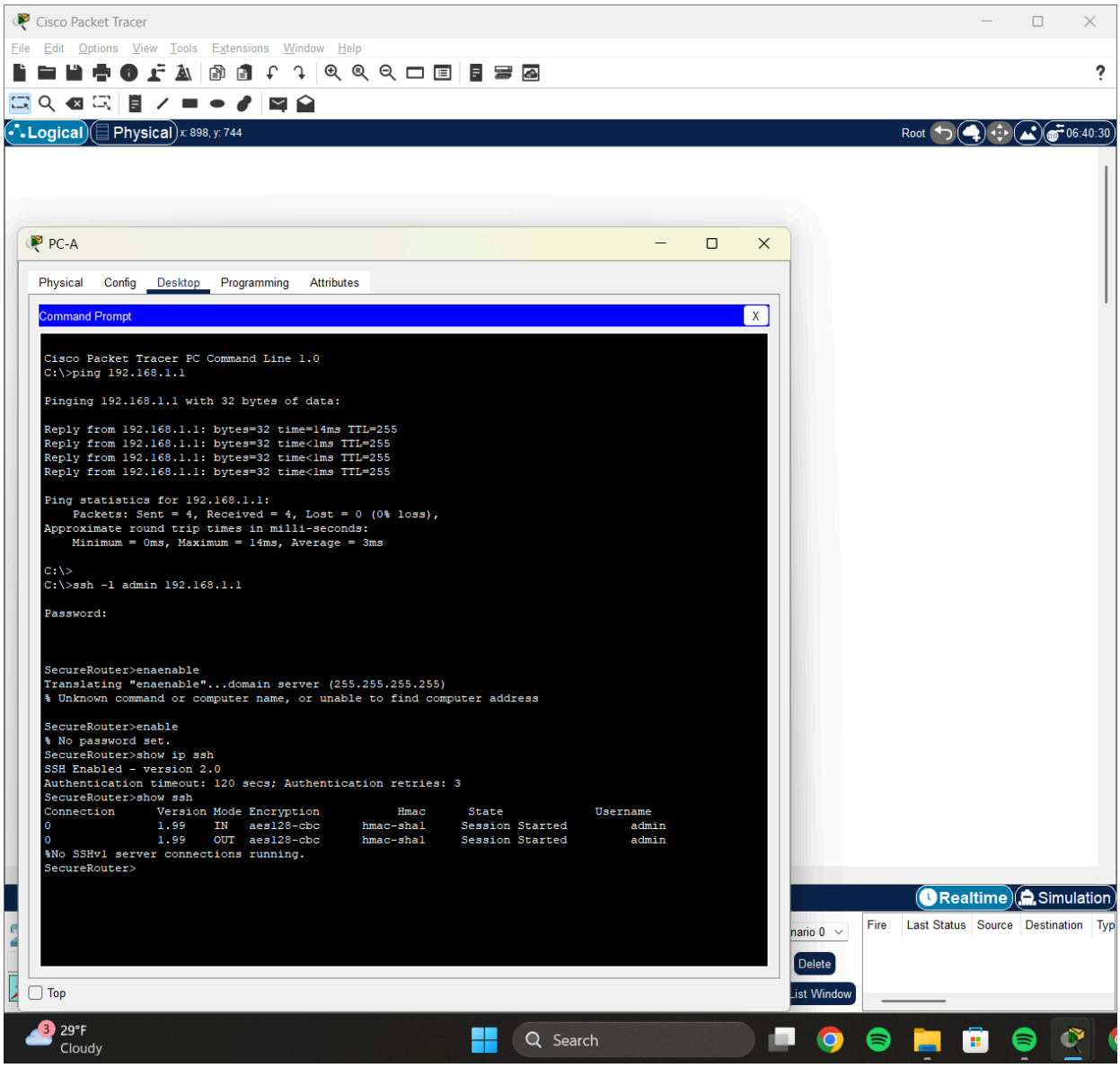
This lab demonstrates secure remote access using SSH instead of clear-text protocols. I configured R1 to use SSH v2, generated RSA keys, and created a local admin account. Using PC-A, I established an SSH session and verified encrypted packets in Packet Tracer's Simulation Mode. The router's `show ip ssh` and `show ssh` outputs confirmed the secure session, and no cleartext connections (like Telnet) were allowed. This meets the requirements for encrypted communication and session integrity.

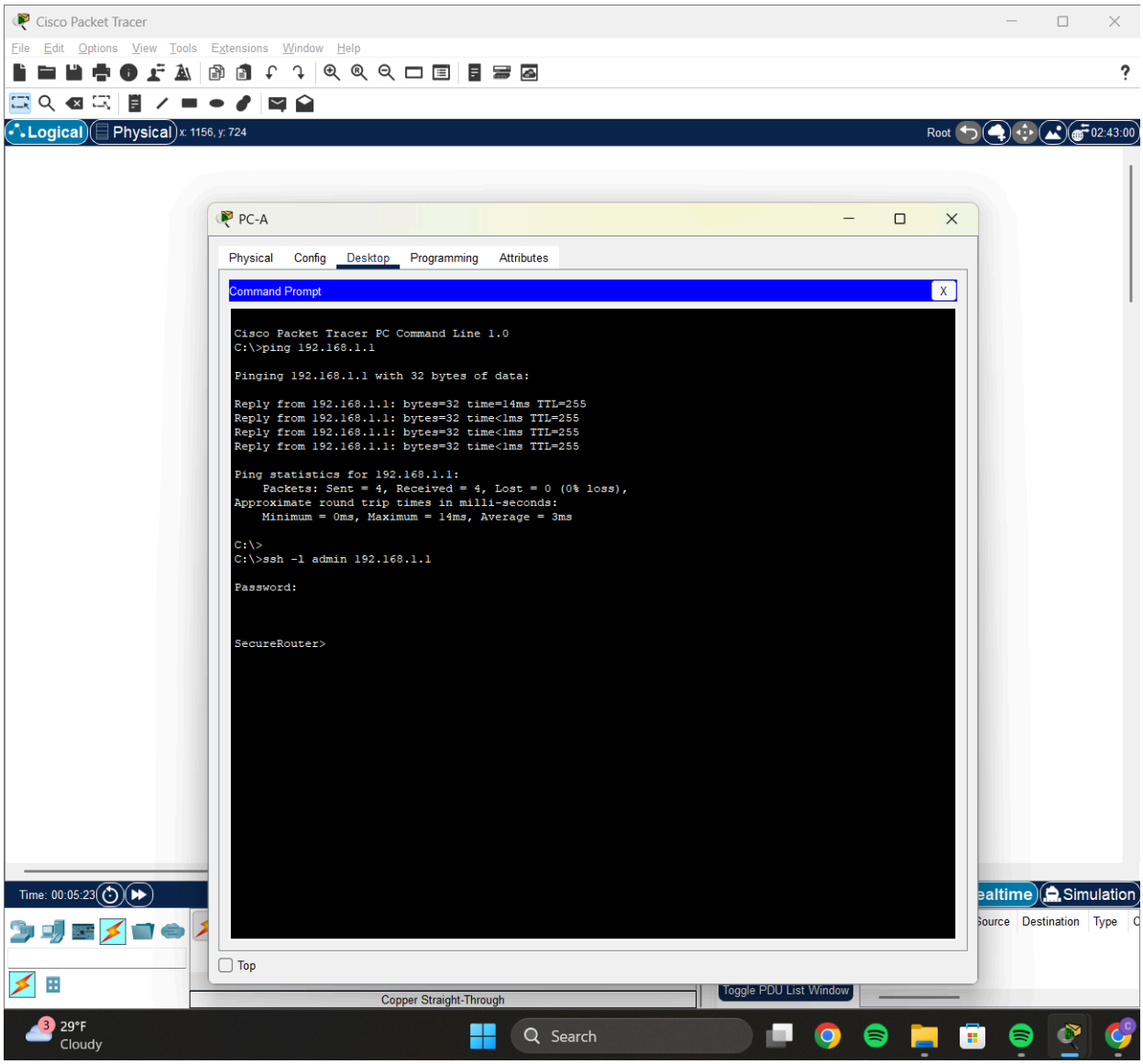
Encrypted SSH, TCP port 22 no clear text



SSH Commands Output, Version 2



Verified SSH Tunnel.


Cisco Packet Tracer
File Edit Options View Tools Extensions Window Help
Logical Physical x: 1156, y: 724
Root 02:43:00
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=14ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Ping statistics for 192.168.1.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 14ms, Average = 3ms
C:\>
C:\>ssh -l admin 192.168.1.1
Password:
SecureRouter>
Top
Time: 00:05:23
Simulation
Source Destination Type
Copper Straight-Through
Toggle PDU List Window
29°F
Cloudy
Search