Project One - Encrypted Overlay Network

Objective:

Design and Implement an overlay network

- Encrypted
    - Communications
    - System files yes
        - All active just remove when done
- Single network **endpoint**
    - What the clients connect to in order to get information on the network
        - Active clients
        - Store IP:Domain mappings?
- Multiple network **clients/end-systems**
    - Each will have an IP
    - Each will have an Overlay Network Name
    - They need to register with the network before they can send or receive communications over the network
- Connection **Flows**
    - Flow 1: Occurs when new clients are created
        - Register name with the network (controller)
            - Link IP with the name -- store on the network device
    - Flow 2: Occurs every 10 seconds on **each client**
        - Retrieve all active clients on the network from the controller
            - The controller will need a list of all registered and a list of all active end-systems
                - Does this need persistence?
    - Flow 3: Occurs every 15 seconds on **each client**
        - The client establishes a connection with all other **active** clients on the network
            - Sends PING message
            - The recipient responds with PONG

Planning:

Two Files

network.py:

- Authenticated to clients with a certificate
- Authenticate Clients
    - Use a unique token
    - Use Client Certificates
        - How are they shared (pre-shared?)
- Organization
    - Multithreaded process
        - Accept connection pass to handler - handler calls appropriate functions.
    - Functions for each flow (1 and 2)

        - Multiple threads for the functions - so we can manage multiple connections
    - Main Driver for coordination
- How do we handle exiting the program
    - Does the exit need to be controlled
    - Let OS kill orphan processes?
- Flow 1
- Flow 2

client.py:

- Uses certificate to authenticate system running network.py
- Authenticate to network controller
    - Pass Token + Nonce
    - Use Certificate -- Probably this (Generate one for a client IP+Domain if neither is used on the network controller)
- Organization
    - Function for accepting connections (PING PONG flow)
    - Functions for each flow (1, 2, and 3)

Sending and receiving should take part in the same code