**1. ccna\_troubleshooting1.pkt**

**Objective:** Practice Layer 2/3 troubleshooting  
**Steps:**

* Verify VLAN configuration on switches (show vlan brief)
* Check IP settings on PCs (ipconfig) and pings
* Use show ip interface brief on routers to confirm interface status
* Trace packets using **Simulation Mode** and identify drops or misroutes
* Document issues and solutions

**🔹 2. CUSTOM1.pkt**

**Objective:** Custom topologies, likely with mix of routing and switching  
**Steps:**

* Open topology and map the architecture manually
* Identify all devices and their assigned roles (Router/Switch/PC/Firewall)
* Verify addressing schema and use ping, traceroute
* Simulate a security event (e.g., route manipulation, ARP poisoning if enabled)
* Create a change log for configuration edits

**🔹 3. EIGRP Troubleshooting.pkt**

**Objective:** Troubleshoot EIGRP configuration and adjacency issues  
**Steps:**

* Use show ip protocols, show ip route, and show ip eigrp neighbors
* Verify autonomous system (AS) numbers match on all routers
* Confirm correct network statements are configured
* Check passive interfaces and ACLs blocking EIGRP traffic

**🔹 4. EIGRP Troubleshooting Complete.pkt**

**Objective:** Review a completed and functional EIGRP setup  
**Steps:**

* Use show run and show ip route to understand routing logic
* Compare with the broken version (EIGRP Troubleshooting.pkt)
* Practice failure injection (shutdown interfaces) and observe recovery
* Use as baseline for your own troubleshooting documentation

**🔹 5. ICND1 RIP.pkt**

**Objective:** RIP Version 1/2 basics  
**Steps:**

* Use show ip protocols and debug ip rip
* Check if only classful networks are used (RIPv1 limitation)
* Verify no auto-summary is set if subnets used
* Practice adding/removing network statements

**🔹 6. ICND2 EIGRP.pkt**

**Objective:** EIGRP in a more complex (ICND2-level) network  
**Steps:**

* Validate all interfaces with show ip interface brief
* Ensure correct AS number and wildcard masks
* Confirm routing table convergence
* Induce link failures and measure route failover time

**🔹 7. ICND2 OSPF.pkt**

**Objective:** OSPF single-area configuration and behavior  
**Steps:**

* Use show ip ospf neighbor, show ip route ospf
* Check router IDs and OSPF process IDs
* Observe DR/BDR election with show ip ospf interface
* Simulate neighbor loss and review hello/dead timers

**🔹 8. Multi-area OSPF.pkt**

**Objective:** Multi-area OSPF topology (stub, backbone, transit)  
**Steps:**

* Use show ip ospf database
* Understand ABR (Area Border Router) roles
* Validate area types and inter-area routes
* Create a diagram to visualize LSAs and areas

**🔹 9. Multi-area OSPF Complete.pkt**

**Objective:** Verified working multi-area OSPF  
**Steps:**

* Use as a reference to debug your own setups
* Compare configurations against the incomplete file
* Perform routing path analysis with traceroute
* Test end-to-end connectivity from hosts in different areas

**🔹 10. LAB.pkt**

**Objective:** General lab – likely integrated concepts  
**Steps:**

* Review all IP assignments and subnetting
* Test full L2 and L3 reachability
* Use the lab to design a security ACL (standard/extended)
* Add a new VLAN and verify inter-VLAN routing

**Filename: OSPF Troubleshooting.pkt**

**Objective:** Diagnose and resolve issues in a single-area or multi-area OSPF network.  
**Guideline:**

* Use show ip ospf neighbor to identify missing adjacencies.
* Validate IP addressing and subnet mask consistency across connected interfaces.
* Check for passive-interface errors and ensure correct area IDs.
* Cyber focus: Simulate misconfigurations as an example of misrouting or routing black holes.

**🔹 Filename: PhasedISPMigration.pkt**

**Objective:** Observe and manage a transition between ISPs with minimal downtime.  
**Guideline:**

* Identify primary vs backup ISP routing paths (likely static or default routes).
* Simulate an ISP outage and verify failover behavior.
* Use show ip route to examine how default routes change.
* Cyber focus: Discuss security risks during migrations, such as DNS poisoning or BGP hijacks (conceptually).

**🔹 Filename: PPP Troubleshooting.pkt**

**Objective:** Troubleshoot a Point-to-Point Protocol (PPP) WAN link.  
**Guideline:**

* Use show interface and debug ppp negotiation to inspect link authentication.
* Check for incorrect CHAP/PAP credentials or encapsulation mismatches.
* Verify clock rates and serial port status (up/up).
* Cyber focus: Highlight weak authentication risks in legacy WAN links.

**🔹 Filename: Router on a stick.pkt**

**Objective:** Enable inter-VLAN routing using a single physical interface.  
**Guideline:**

* Use show vlan brief on the switch and verify trunk port configuration.
* On router: ensure sub-interfaces (e.g., Gig0/0.10) are configured with encapsulation dot1q.
* Ping across VLANs to confirm connectivity.
* Cyber focus: Discuss VLAN hopping attacks and mitigation (e.g., disabling unused ports, no auto trunking).

**🔹 Filename: Scenario 1.pkt**

**Objective:** Practice comprehensive network configuration and troubleshooting.  
**Guideline:**

* Analyze topology: identify roles of routers, switches, and hosts.
* Verify IP schema, routing protocols, and VLAN configuration.
* Trace traffic path and diagnose any failed pings.
* Cyber focus: Introduce ACLs or firewall concepts to restrict or monitor traffic.

**🔹 Filename: Simple\_Frame\_Relay.pkt**

**Objective:** Understand basic Frame Relay concepts and configuration.  
**Guideline:**

* Use show frame-relay map and show frame-relay pvc to validate setup.
* Check DLCI values and encapsulation.
* Use serial interfaces and sub-interfaces appropriately (multipoint vs point-to-point).
* Cyber focus: Compare legacy WAN tech to MPLS/SD-WAN and their security implications.

**🔹 Filename: SOHO.pkt**

**Objective:** Configure a Small Office/Home Office network with basic routing and security.  
**Guideline:**

* Assign IP addresses and test DHCP/DNS functionality.
* Configure NAT/PAT for internet access simulation.
* Implement basic firewall rules or ACLs on the edge device.
* Cyber focus: Emphasize endpoint protection, guest Wi-Fi isolation, and default password risks.

**🔹 Filename: STP.pkt**

**Objective:** Observe Spanning Tree Protocol in action to prevent Layer 2 loops.  
**Guideline:**

* Use show spanning-tree to view root bridge and port states.
* Identify blocked ports and verify STP convergence.
* Cyber focus: Discuss BPDU Guard, Root Guard, and STP manipulation attacks (e.g., rogue root bridge).

**🔹 Filename: STP2.pkt**

**Objective:** Advanced STP topology with potential for load balancing or tuning.  
**Guideline:**

* Observe STP behavior across redundant links.
* Change bridge priorities to manipulate root bridge election.
* Cyber focus: Simulate a Layer 2 DoS by flooding BPDUs (conceptually).

**🔹 Filename: STP Load Balancing.pkt**

**Objective:** Implement load balancing by tuning STP priorities and port costs.  
**Guideline:**

* Change root bridge per VLAN (PVST+ likely in use).
* Use show spanning-tree vlan X to confirm desired topology.
* Cyber focus: Secure STP setup and avoid attacker-controlled root bridge manipulation.

**Filename: STP3.pkt**

**Objective:** Understand advanced STP behavior in redundant topologies.  
**Guideline:**

* Use show spanning-tree to analyze root bridge elections.
* Identify blocked, designated, and root ports in the STP topology.
* Modify bridge priority or port cost to control path selection.
* **Cyber focus:** Discuss STP-based attacks (e.g., rogue root bridge) and introduce security features like BPDU Guard and Root Guard.

**🔹 Filename: SVI.pkt**

**Objective:** Configure and test **Switch Virtual Interfaces (SVIs)** for VLAN intercommunication.  
**Guideline:**

* Use show vlan brief to confirm VLANs are created and assigned.
* On multilayer switch, configure SVIs using interface vlan X and assign IP addresses.
* Test inter-VLAN routing between PCs in different VLANs.
* **Cyber focus:** Teach the importance of VLAN segmentation for security and simulate ACLs to restrict VLAN-to-VLAN communication.

**🔹 Filename: TASK05.pkt**

**Objective:** Likely an assignment task covering a mix of routing, switching, or addressing.  
**Guideline:**

* Inspect IP assignments and interface status using show ip int brief.
* Verify connectivity using ping and traceroute.
* Check routing table with show ip route (RIP, EIGRP, OSPF depending on setup).
* **Cyber focus:** Ask students to harden the network by applying basic ACLs and disabling unused ports.

**🔹 Filename: VLANs---SpanningTreeProtocol.pkt**

**Objective:** Integrate VLAN segmentation with STP redundancy handling.  
**Guideline:**

* Create and assign VLANs to switchports using switchport access vlan X.
* Verify trunk ports and configure them if missing (switchport mode trunk).
* Use show spanning-tree vlan X to observe per-VLAN STP behavior (PVST+).
* **Cyber focus:** Educate students about VLAN hopping risks and best practices to mitigate them (e.g., disabling DTP, setting native VLAN to unused ID).