Packet Capture Checklist

The packets in this checklist can all be generated using just RouterOS. If you don't have any MikroTik routers handy, you can create Cloud Hosted Routers (MikroTik routers in a virtual environment) for free. Turn collecting packet captures into a game. Encourage your co-workers and friends to do it with you. Practice building up mock networks to gain the opportunity to collect the packet capture. You will learn more in a year of looking at the packets than you would with a year of classroom instruction. If you can build up all of these scenarios and collect the packet capture, whether you feel confident or not, then you have some very respectable network administration skills. Most net admins could not sit down and complete this checklist… will you be able to?

Layer 2 Captures

- ☐ 60GHz Management Frames
- ☐ ARP (Address Resolution Protocol)
- ☐ BGP VPLS (Border Gateway Protocol Virtual Private LAN Service)
- ☐ Bonding
- ☐ CAPsMAN
- ☐ DHCP (Dynamic Host Configuration Protocol)
- ☐ DHCP Relay Messages
- ☐ Loop Protect Messages
- ☐ MAC-Telnet
- ☐ MESH
- ☐ MPLS (Multiprotocol Label Switching)
- ☐ MSTP (Multiple Spanning Tree Protocol)
- ☐ Nstreme
- ☐ Nstreme Dual
- ☐ NV2
- ☐ PPPoE (Point-to-Point Protocol over Ethernet)
- ☐ RoMON (Router Management Overlay Network)
- ☐ RSTP (Rapid Spanning Tree Protocol)
- ☐ STP (Spanning Tree Protocol)
- ☐ TE (Traffic Engineering)
- ☐ VLAN (Virtual LAN)
- ☐ VLAN (Q in Q)
- ☐ VPLS (Virtual Private LAN Service)
- ☐ VRRP (Virtual Router Redundancy Protocol)
- ☐ VXLAN (Virtual Extensible LAN)
- ☐ WDS (Wireless Distribution System)
- ☐ Wireless Management Frames
- ☐ WOL (Wake-on-LAN)

Layer 3 Captures

- ☐ Bandwidth Test
- ☐ BGP (Border Gateway Protocol)
- ☐ EOIP Tunnel (Ethernet Over IP)
- ☐ Flood Ping
- ☐ GRE Tunnel (Generic Routing Encapsulation)
- ☐ IP Tunnel
- ☐ IPSEC (IP Security)
- ☐ L2TP (Layer Two Tunneling Protocol)
- ☐ L2TPv3
- ☐ LDP (Label Distribution Protocol)
- ☐ Masquerade
- ☐ OSPF (Open Shortest Path First)
- ☐ OVPN (Open Virtual Private Network)
- ☐ Ping Speed
- ☐ PPTP (Point-to-Point Tunneling Protocol)
- ☐ RADIUS Messages (Remote Authentication Dial-In User Service)
- ☐ RIP (Routing Information Protocol)
- ☐ SSTP (Secure Socket Tunneling Protocol)
- ☐ Traceroute
- ☐ Winbox
- ☐ WireGuard

Common Protocol Captures

- ☐ CDP (Cisco Discovery Protocol)
- ☐ E-mail
- ☐ FTP (File Transfer Protocol)
- ☐ ICMP (Internet Control Message Protocol)
- ☐ IPv4 Options
- ☐ MNDP (MikroTik Neighbor Discovery protocol)
- ☐ NTP (Network Time Protocol)
- ☐ SNMP (Simple Network Management Protocol)
- ☐ SNTP (Simple Network Time Protocol)
- ☐ SSH (Secure Shell Protocol)
- ☐ TCP (Transmission Control Protocol)
- ☐ Telnet
- ☐ TFTP (Trivial File Transfer Protocol)
- ☐ TOS/ DSCP (Type of Service/ Differentiated Services Code Point)
- ☐ Traffic Flow/ Net Flow
- ☐ UDP (User Datagram Protocol)
- ☐ Web