- Filename: eccouncil-ceh31250-v11-8-5-1-sniffing-defenses.md
- Show Name: CEHv11 (312-50)
- Topic Name: Network and Perimeter Hacking: Sniffing
- Episode Name: Sniffing Defenses
  ==========

Sniffing Defenses

Objectives:

- List and detail common defensive tactics and tools used to detect and prevent common sniffing attacks

---

- Sniffing Defenses?
  - Encryption
  - Physical security (no attaching hardware sniffers)
  - Static ARP and/or IP
  - Use IPv6
  - IDS to detect sniffing
  - Promiscuous mode scanner
- Switch based attacks
  - Defenses?
    - Switch Port Security (`port-security`)
    - DHCP Snooping and Binding Tables
      - Records info on untrusted devices (MAC,VLAN,IP,Lease Time, etc)
        - Works like a firewall between trusted and un-trusted devices
    - Port-based NAC
    - Dynamic ARP Inspection
    - Disable Trunk auto-negotiation
      - For both access ports and trunk ports
    - Don't use the Default VLAN (double-tagging)
    - Change Native VLANs to unused ID (double-tagging)
    - Force Native VLAN tagging (double-tagging)
    - STP Attacks
      - BPDU Guard (disables unauthorized ports after sending BPDUs)
      - Root Guard (ensures status of the current Root-Bridge)
- DNS Defenses
  - DNSSEC
  - Block outbound traffic from UDP 53
  - Restrict external DNS queries
    - DNS Sinkhole
  - Encryption of DNS traffic