Cheat Sheet for comprehensive Cisco Certified Network Associate (CCNA) - Cyber Ops

Network Fundamentals

- **OSI Model**
  - **Layer 7: Application** - HTTP, FTP, DNS
  - **Layer 6: Presentation** - SSL/TLS, JPEG, MPEG
  - **Layer 5: Session** - NetBIOS, PPTP
  - **Layer 4: Transport** - TCP, UDP
  - **Layer 3: Network** - IP, ICMP, OSPF
  - **Layer 2: Data Link** - Ethernet, MAC, ARP
  - **Layer 1: Physical** - Cables, Hubs, Switches
- **TCP/IP Model**
  - **Application** - HTTP, FTP, DNS
  - **Transport** - TCP, UDP
  - **Internet** - IP, ICMP
  - **Network Access** - Ethernet, MAC, ARP

IP Addressing and Subnetting

- **IPv4 Addressing**
  - **Format**: `xxx.xxx.xxx.xxx`
  - **Classes**:
    - **A**: 1.0.0.0 - 126.255.255.255
    - **B**: 128.0.0.0 - 191.255.255.255
    - **C**: 192.0.0.0 - 223.255.255.255
    - **D**: 224.0.0.0 - 239.255.255.255 (Multicast)
    - **E**: 240.0.0.0 - 255.255.255.255 (Reserved)

- **Subnetting**
  - **CIDR Notation**: `/24` = 255.255.255.0
  - **Subnet Mask**: 255.255.255.0
  - **Subnet Calculation**:
    - **Formula**: 2^n (n = number of bits borrowed)
    - **Example**: `/26` = 2^2 = 4 subnets
- **Private IP Ranges**
  - **Class A**: 10.0.0.0 - 10.255.255.255
  - **Class B**: 172.16.0.0 - 172.31.255.255
  - **Class C**: 192.168.0.0 - 192.168.255.255

Routing and Switching

- **Routing Protocols**
  - **Static Routing**
    - **Command**: `ip route <destination> <subnet mask> <next hop>`
    - **Example**: `ip route 192.168.2.0 255.255.255.0 192.168.1.1`
  - **Dynamic Routing**
    - **RIP**: `router rip`, `network <network>`
    - **OSPF**: `router ospf <process-id>`, `network <network> <wildcard mask> area <area-id>`
    - **EIGRP**: `router eigrp <as-number>`, `network <network>`
- **Switching**
  - **VLANs**
    - **Create VLAN**: `vlan <vlan-id>`, `name <vlan-name>`
    - **Assign Port to VLAN**: `interface <interface>`, `switchport mode access`, `switchport access vlan <vlan-id>`
  - **Trunking**:

- **Command**: `switchport mode trunk`

- **Allowed VLANs**: `switchport trunk allowed vlan <vlan-list>`

Network Security

- **Access Control Lists (ACLs)**

- **Standard ACL**: `access-list <acl-number> {permit|deny} <source>`

- **Extended ACL**: `access-list <acl-number> {permit|deny} <protocol> <source> <destination> <optional-port>`

- **Apply ACL**: `ip access-group <acl-number> {in|out}`

- **Firewalls**

- **Zone-Based Policy Firewall (ZBF)**

- **Create Zone**: `zone security <zone-name>`

- **Assign Interface**: `interface <interface>`, `zone-member security <zone-name>`

- **Policy**: `policy-map type inspect <policy-name>`, `class <class-name>`, `inspect`

- **VPNs**

- **Site-to-Site VPN**

- **IPSec**: `crypto isakmp policy <priority>`, `crypto ipsec transform-set <name> <transforms>`

- **Tunnel Interface**: `interface Tunnel <number>`, `ip address <ip> <mask>`, `tunnel source <source>`, `tunnel destination <destination>`

Network Management

- **SNMP**

- **Configure**: `snmp-server community <community-string> {ro|rw}`

- **Traps**: `snmp-server enable traps`

- **Syslog**

- **Configure**: `logging <ip-address>`

- **Severity Levels**: `logging trap <level>`

- **NTP**

- **Configure**: `ntp server <ip-address>`
- **Authentication**: `ntp authenticate`, `ntp authentication-key <key-id> md5 <key>`

Troubleshooting

- **Ping**: `ping <ip-address>`
- **Traceroute**: `traceroute <ip-address>`
- **Show Commands**
  - **Interfaces**: `show ip interface brief`
  - **Routing Table**: `show ip route`
  - **ARP Table**: `show ip arp`
  - **ACLs**: `show access-lists`
  - **VLANs**: `show vlan brief`

Cybersecurity Operations

- **Intrusion Detection/Prevention Systems (IDS/IPS)**
  - **Configure**: `ip inspect name <name> <protocol>`
  - **Apply**: `interface <interface>`, `ip inspect <name> in`
- **Logging and Monitoring**
  - **Syslog**: `logging <ip-address>`
  - **NetFlow**: `ip flow-export version 5`, `ip flow-export destination <ip> <port>`
- **Incident Response**
  - **Identify**: Use `show` commands to gather evidence.
  - **Contain**: Apply ACLs or firewall rules to isolate affected areas.
  - **Eradicate**: Remove malicious code or configurations.
  - **Recover**: Restore from backups and reconfigure security settings.
  - **Lessons Learned**: Document the incident and improve security policies.

Tips and Tricks

- **Save Configuration**: `write memory` or `copy running-config startup-config`

- **Backup Configuration**: `copy running-config tftp://<ip-address>/<filename>`
- **Restore Configuration**: `copy tftp://<ip-address>/<filename> running-config`
- **Clear Configuration**: `erase startup-config`, `reload`
- **Debugging**: `debug <feature>`, `undebug all`

Examples

- **Static Route Example**:

```
ip route 192.168.2.0 255.255.255.0 192.168.1.1
```

- **VLAN Configuration Example**:

```
vlan 10
 name Sales
interface GigabitEthernet0/1
 switchport mode access
 switchport access vlan 10
```

- **ACL Example**:

```
access-list 1 permit 192.168.1.0 0.0.0.255
interface GigabitEthernet0/1
 ip access-group 1 in
```

This cheat sheet provides a comprehensive overview of essential concepts, commands, and tips for the CCNA Cyber Ops certification. Use it as a quick reference guide during your studies and practical exercises.

By Ahmed Baheeg Khorshid

ver 1.0