Network Services Cheat Sheet for Cisco Beginners

This is a generic cheat sheet and not for a specific use case.

Syslog Configuration

What is Syslog?

Syslog sends log messages to a central server for monitoring, troubleshooting, and compliance. Messages include system events, errors, and status updates.

Basic Syslog Configuration

```
Router(config)# logging [syslog-server-ip]
Router(config)# logging trap [severity-level]
```

Example

```
Router(config)# logging 192.168.1.100
Router(config)# logging trap informational
```

Syslog Severity Levels

- **0 - Emergency**: System unusable
- **1 - Alert**: Immediate action needed
- **2 - Critical**: Critical conditions
- **3 - Error**: Error conditions
- **4 - Warning**: Warning conditions
- **5 - Notice**: Normal but significant
- **6 - Informational**: Informational messages
- **7 - Debug**: Debug messages

Additional Syslog Commands

```
Router(config)# logging source-interface gigabit0/0
Router(config)# logging facility local0
Router(config)# service timestamps log datetime
```

SNMPv2 Configuration

What is SNMPv2?

Simple Network Management Protocol v2 (SNMPv2) allows network management systems to monitor and manage network devices using community strings for authentication.

Basic SNMPv2 Configuration

```
Router(config)# snmp-server community [string] [ro|rw]
Router(config)# snmp-server location [text]
Router(config)# snmp-server contact [text]
```

Example

```
Router(config)# snmp-server community public ro
Router(config)# snmp-server community private rw
Router(config)# snmp-server location "Data Center A"
Router(config)# snmp-server contact "admin@company.com"
```

SNMP Access Control

```
Router(config)# snmp-server community [string] [ro|rw] [acl-number]
```

Example with ACL

```
Router(config)# access-list 50 permit 192.168.1.0 0.0.0.255
Router(config)# snmp-server community public ro 50
```

Enable SNMP Traps

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host [management-station-ip] [community]
```

Example

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host 192.168.1.200 public
```

Netflow Configuration

What is Netflow?

Netflow collects and exports IP traffic flow information for network monitoring, analysis, and troubleshooting. It tracks who, what, when, where, and how traffic flows.

Basic Netflow Configuration

```
Router(config-if)# ip flow ingress
Router(config-if)# ip flow egress
```

Configure Netflow Export

```
Router(config)# ip flow-export destination [collector-ip] [port]
Router(config)# ip flow-export source [interface]
Router(config)# ip flow-export version [version-number]
```

Example

```
! Enable flow on interfaces
interface gigabit0/0
 ip flow ingress
 ip flow egress

! Configure export
ip flow-export destination 192.168.1.150 9996
ip flow-export source gigabit0/1
ip flow-export version 5
```

Netflow Cache Settings

```
Router(config)# ip flow-cache timeout active [minutes]
Router(config)# ip flow-cache timeout inactive [seconds]
```

Example

```
Router(config)# ip flow-cache timeout active 30
Router(config)# ip flow-cache timeout inactive 15
```

Essential Show Commands

Syslog Show Commands

```
Router# show logging
Router# show logging history
```

SNMPv2 Show Commands

```
Router# show snmp
Router# show snmp community
Router# show snmp host
```

Netflow Show Commands

```
Router# show ip flow interface
Router# show ip flow export
Router# show ip cache flow
```

Security Considerations

Syslog Security

- Use dedicated management network
- Secure syslog server access
- Consider encrypted transport

SNMP Security

- Change default community strings
- Use access lists to restrict access
- Avoid "public" and "private" strings

Netflow Security

- Secure collector communication
- Limit export to trusted servers
- Monitor for performance impact

Key Points

- **Syslog**: Centralized logging for monitoring and troubleshooting
- **SNMPv2**: Network monitoring with community string authentication
- **Netflow**: Traffic flow analysis and network visibility
- **All services** can impact router performance
- **Security** is important - change defaults and use access lists

---

Remember: These services consume router resources - monitor performance and implement security best practices!