Enterprise Network Device Configuration Cheat Sheet

> **Purpose**: This document is a real-world, enterprise-grade reference for initial switch configuration, hardening, and verification. It is written to be stored in GitHub and used as a repeatable baseline for production or lab environments.

---

1. Access & Privilege Control

Enter Privileged and Global Configuration Modes

```
enable
configure terminal
```

Set Device Hostname

```
hostname SW-ACCESS-01
```

Disable DNS Lookup (Prevents CLI Hang on Typos)

```
no ip domain-lookup
```

---

2. Console Line Hardening

Configure Console Timeout & Logging

```
line console 0
exec-timeout 5 0
logging synchronous
```

Why this matters: - Prevents unattended sessions - Improves usability during troubleshooting

---

3. Authentication & Credential Security

Enable Password Encryption (Required Baseline)

```
service password-encryption
```

Reality check: - This is **not strong encryption** (Type 7) - It **prevents shoulder-surfing and config leaks** - Mandatory minimum in enterprise baselines

Enable Encrypted Privileged Mode Access

```
enable secret cisco
```

Create Local Admin User (Privileged)

```
username admin privilege 15 secret cisco123
```

Enterprise Note: - Replace weak secrets immediately - Use TACACS+/RADIUS in production environments

---

4. SSH Configuration (Secure Remote Access)

Enforce Strong SSH Parameters

```
ip ssh time-out 60
ip ssh authentication-retries 3
```

Why this matters: - Limits brute-force attempts - Reduces attack surface

Define Domain Name (Required for RSA Keys)

```
ip domain-name corp.local
```

Generate RSA Keys

```
crypto key generate rsa
```

Enforce Secure SSH Version

```
ip ssh version 2
```

Configure VTY Lines for SSH Only

```
line vty 0 15
login local
transport input ssh
```

Security Standard: - Telnet is disabled - SSH v2 only

---

5. Legal & Security Banner

Message of the Day (MOTD)

```
banner motd #
UNAUTHORIZED ACCESS IS PROHIBITED
#
```

Why this matters: - Legal protection - Compliance requirement (DoD, HIPAA, SOX, PCI-DSS)

---

6. Interface Hardening (Access Switch Best Practice)

Disable Unused Services (Global Hardening)

```
no ip http server
no ip http secure-server
```

Why this matters: - Removes unnecessary management services - Reduces exploitable attack surface

Shutdown Unused Access Ports

```
interface range fa0/2-24
shutdown
switchport mode access
switchport nonegotiate
```

Reserved / Special Interface Configuration

```
interface fa0/1
description ACCESS_PORT_RESERVED
```

Security Impact: - Prevents rogue device access - Disables DTP negotiation

---

7. Verification & Audit Commands

Review Line Configuration

```
show run | section line
```

Verify SSH Status

```
show ip ssh
```

View Active Users

```
show users
```

---

8. Enterprise Hardening Checklist

- [ ] Hostname set correctly
- [ ] DNS lookup disabled
- [ ] Console timeout enforced
- [ ] Encrypted enable secret configured
- [ ] Local admin account created
- [ ] SSH v2 enabled
- [ ] Telnet disabled
- [ ] MOTD banner configured
- [ ] Unused ports shutdown
- [ ] Interface descriptions applied

---

9. Version Control Best Practices (GitHub)

Recommended Repo Structure:

```
network-baselines/
├── switches/
│   └── access-switch-baseline.md
├── routers/
├── firewalls/
└── README.md
```

Rules: - Never store real passwords - Use variables or placeholders - Treat configs as infrastructure-as-code

---

10. Final Reality Check

This baseline is **minimum acceptable** for enterprise access switches.

If you deploy less than this: - You are insecure - You are non-compliant - You are one mistake away from an incident

Raise the standard or expect failure.