

CLI MASTER & NETWORK ENGINEERING GUIDE

ULTIMATE CISCO CHEATSHEET++

2026

1 Ultimate Cisco CLI Master Cheatsheet & Network Engineering Guide

Ultimate Cisco CLI Master Cheatsheet & Network Engineering Guide covering IOS commands, routing, switching, OSPF, BGP, VLANs, and real-world troubleshooting.

> ⚠ Warning
>
> Production networks require careful planning and change management.

2 Device Fundamentals

2.1 Device Initialization

```
! Complete factory reset (Nuke everything)
Router# delete nvram:startup-config
Router# delete flash:vlan.dat
Router# erase nvram:
Router# erase flash:
Router# write erase
Router# reload

! Partial reset (keep IOS)
Router# write erase
Router# delete vlan.dat
Router# reload
```

> ☠ Danger Zone
>
> These commands will completely wipe your device. Always have backups!

2.2 Boot Process & ROMMON

```
! Interrupt boot process (during first 60 seconds)
! Press Ctrl+Break or send break signal

! ROMMON Commands:
rommon 1 > confreg 0x2142      ! Bypass startup config
rommon 2 > reset               ! Reboot
rommon 3 > dir flash:          ! List files
rommon 4 > boot flash:c2900-universalk9-mz.SPA.157-3.M.bin
rommon 5 > tftpdnld            ! TFTP download
```

2.3 Password Recovery Procedures

For Routers (ISR G2/ASR):

1. Connect console cable

2. Power cycle, break to ROMMON
3. `confreg 0x2142`
4. `reset`
5. Skip initial config
6. `enable`
7. `copy startup-config running-config`
8. Change passwords
9. `config-register 0x2102`
10. `copy running-config startup-config`
11. `reload`

For Switches (Catalyst):

1. Power off
2. Hold Mode button while powering on
3. Release when LED changes
4. `flash_init`
5. `load_helper`
6. `rename flash:config.text flash:config.text.old`
7. `boot`
8. `enable`
9. `rename flash:config.text.old flash:config.text`
10. `copy flash:config.text system:running-config`
11. Change passwords
12. `copy running-config startup-config`

2.4 Hardware Inventory

```
! Show hardware details
Router# show inventory
Router# show diag
Router# show environment
Router# show module
Router# show idprom backplane

! Cisco 2960X/3650/3850 Stack Commands
Switch# show switch
Switch# show switch detail
Switch# show switch neighbors
Switch# switch 1 provision ws-c3650-24ps
Switch# switch 1 priority 15
Switch# switch 2 renumber 3
Switch# switch 1 reload
```

2.5 IOS Image Management

```
! Verify current IOS
Router# show version
Router# show boot
Router# show flash:
Router# dir flash:

! Upgrade IOS via TFTP
Router# copy tftp://192.168.1.10/c2900-universalk9-mz.SPA.157-3.M
    .bin flash:
Router# boot system flash:c2900-universalk9-mz.SPA.157-3.M.bin
Router# copy running-config startup-config
Router# reload

! Bundle/Install Mode (Cat3K/4K)
Switch# archive download-sw /force-reload /overwrite tftp
    ://192.168.1.10/cat3k_caa-universalk9.16.12.04.SPA.bin

! Install Mode (IOS XE)
Router# request platform software package install switch all file
     tftp://192.168.1.10/asr1000-universalk9.17.03.03.SPA.pkg
```

3 IOS Navigation & Basics

3.1 Command Line Fundamentals

```
! Command Abbreviation (up to unique characters)
Router# conf t          ! configure terminal
Router# sh run          ! show running-config
```

```
Router# sh ip int br  ! show ip interface brief
Router# wr            ! write memory (copy run start)

! Command History & Editing
Ctrl+A              ! Move to beginning of line
Ctrl+E              ! Move to end of line
Ctrl+W              ! Delete previous word
Esc+B               ! Move back one word
Esc+F               ! Move forward one word
Ctrl+R              ! Redisplay line
Ctrl+U              ! Delete entire line
Ctrl+Y              ! Paste deleted text
Tab                 ! Auto-complete

! Search in Long Outputs
Router# show running-config | include ospf
Router# show running-config | section router
Router# show running-config | exclude !
Router# show running-config | begin interface
Router# show running-config | count ospf
```

3.2 Context-Sensitive Help

```
Router# ?                    ! Show available commands
Router# show ?               ! Show available show commands
Router# configure ?          ! Show configuration options
Router# interface gigabitEthernet 0/0/0 ?
Router# show ip route <Tab> ! Auto-complete

! Partial Command Completion
Router# sh ip ro<Tab>       ! Completes to "show ip route"
```

3.3 User Privilege Levels

```
! Configure privilege levels
Router(config)# privilege exec level 5 configure terminal
Router(config)# privilege exec level 5 show running-config
Router(config)# privilege interface level 5 shutdown
Router(config)# username admin privilege 5 secret P@ssw0rd

! View privilege levels
Router# show privilege
Router# show privilege all

! Enable secret levels
Router(config)# enable secret level 5 SuperSecret123
Router# enable 5
```

3.4 Command Aliases

```
! Create custom command aliases
Router(config)# alias exec srs show running-config | section
Router(config)# alias exec shbr show ip interface brief
Router(config)# alias exec routes show ip route
Router(config)# alias exec neighbors show cdp neighbors detail
Router(config)# alias configure config t

! Persistent aliases
Router(config)# alias exec backup copy running-config tftp
   ://192.168.1.10/
Router# backup R1-config.txt
```

3.5 Command Scripting with TCL

```
! TCL Shell Access
Router# tclsh
Router(tcl)# puts [exec "show version"]
Router(tcl)# foreach i {1 2 3 4 5} { puts "Interface Gi0/$i" }
Router(tcl)# exit

! One-liner TCL commands
Router# tclsh puts [exec "show ip interface brief"]
```

4 File System Operations

4.1 File System Navigation

```
! Explore file system
Router# pwd                     ! Present working directory
Router# dir                     ! List files
Router# dir flash:              ! List flash contents
Router# dir nvram:              ! List NVRAM contents
Router# dir usbflash0:          ! USB flash (if available)
Router# dir sdflash:            ! SD card (ASR/ISR)
Router# dir bootflash:          ! Boot flash
Router# dir system:             ! System files

! File Operations
Router# copy source-url destination-url
Router# copy running-config flash:backup-config
Router# copy flash:config.text tftp://192.168.1.10/
Router# delete flash:old-config.text
Router# erase flash:            ! Format flash (DANGER!)
Router# mkdir flash:backups
Router# rmdir flash:backups
```

4.2 Configuration Management

```
! Configuration Archive
Router# archive
Router(config-archive)# path flash:backups/$h-config
Router(config-archive)# maximum 10
Router(config-archive)# time-period 1440
Router(config-archive)# write-memory

! View archive
Router# show archive
Router# configure replace flash:backups/R1-config-1

! Rollback Configuration
Router# configure replace flash:backup-config 10
Router# configure revert now
Router# configure confirm

! Configuration Checkpoints (IOS XE)
Router# checkpoint database
Router# show checkpoint database
Router# rollback checkpoint checkpoint_name
```

4.3 Secure Copy (SCP) Operations

```
! Configure SCP server
Router(config)# ip scp server enable
Router(config)# username admin secret admin123
Router(config)# ip ssh version 2

! Copy via SCP
Router# copy running-config scp://admin@192.168.1.10/backups/R1-
    config
Router# copy scp://admin@192.168.1.10/configs/new-config running-
    config

! SCP from Linux to Router
# scp R1-config admin@10.0.0.1:flash:
```

4.4 USB Operations

```
! Check USB status
Router# show usb
Router# dir usbflash0:

! Copy to/from USB
Router# copy running-config usbflash0:/backup-config
Router# copy usbflash0:/new-ios.bin flash:

```

```
! Boot from USB
Router(config)# boot system usbflash0:c2900-universalk9-mz.SPA
   .157-3.M.bin
```

4.5 Automated Backups

```
! EEM Script for Auto-Backup
Router(config)# event manager applet AUTO-BACKUP
Router(config-applet)# event timer cron cron-entry "0 2 * * *"
Router(config-applet)# action 1.0 cli command "enable"
Router(config-applet)# action 2.0 cli command "copy running-
   config tftp://192.168.1.10/backups/$_device_name-
   $_event_pub_time"
Router(config-applet)# action 3.0 syslog msg "Backup completed
   successfully"
```

5 Licensing Management

5.1 License Types & Models

```
! Show license information
Router# show license
Router# show license feature
Router# show license udi
Router# show license right-to-use
Router# show license tech-support

! Smart Licensing (IOS XE)
Router# show license status
Router# show license authorization
Router# license smart register idtoken XXXX-XXXX-XXXX-XXXX
Router# license smart reservation request local
Router# license smart reservation install file flash:reservation.
   lic

! Traditional Licensing (Permanent/Evaluation)
Router# show license all
Router# license install flash:license.lic
Router# license boot level ipbasek9
Router# reload
```

5.2 License Operations

```
! Save License to File
Router# license save flash:all_licenses.lic

! Export/Import License
```

```
Router# license export flash:license_pa.lic
Router# license import flash:new_license.lic

! Evaluation License
Router# license accept end user agreement
Router# license boot level securityk9
Router# reload

! Check License Compliance
Router# show license violation
```

5.3 Right-to-Use (RTU) Licensing

```
! RTU License Management
Router# license right-to-use activate ipservices
Router# license right-to-use deactivate ipservices
Router# show license right-to-use
Router# license right-to-use perpetual ipservices accept
```

5.4 DNA Center Licensing

```
! DNA Center Integration
Router# license smart register idtoken XXXX-XXXX-XXXX-XXXX
Router# license smart reservation request id DNA-CENTER-ID
Router# license smart authorization request
Router# license smart reservation install
```

6 Device Management

6.1 System Configuration

```
! Basic Device Setup
Router(config)# hostname R1-CORE
Router(config)# no ip domain-lookup
Router(config)# ip domain-name company.com
Router(config)# service password-encryption
Router(config)# service timestamps debug datetime msec localtime
   show-timezone
Router(config)# service timestamps log datetime msec localtime
   show-timezone
Router(config)# logging buffered 16384 debugging
Router(config)# logging console critical
Router(config)# logging monitor debugging
Router(config)# logging host 192.168.100.10
Router(config)# logging source-interface Loopback0

! Banner Configuration
```

```
Router(config)# banner motd ^
**********************************************************************
*           AUTHORIZED ACCESS ONLY                                   *
*  This system is the property of Company Inc.                       *
*  Unauthorized access is prohibited and will be prosecuted.         *
**********************************************************************
^
Router(config)# banner login ^
Please enter your credentials to access this device.
Contact Network Operations for assistance.
^
Router(config)# banner exec ^
Welcome to R1-CORE. You are logged in as $username.
Current time: $_timenow
^
```

6.2 NTP Configuration

```
! NTP Server Configuration
Router(config)# ntp server 0.pool.ntp.org prefer
Router(config)# ntp server 1.pool.ntp.org
Router(config)# ntp server 2.pool.ntp.org
Router(config)# ntp server 192.168.100.10

! NTP Authentication
Router(config)# ntp authenticate
Router(config)# ntp authentication-key 1 md5 NTP-KEY-123
Router(config)# ntp trusted-key 1
Router(config)# ntp server 0.pool.ntp.org key 1

! NTP Master/Peer
Router(config)# ntp master 3
Router(config)# ntp peer 192.168.1.2
Router(config)# ntp update-calendar

! NTP Access Control
Router(config)# ntp access-group peer 10
Router(config)# ntp access-group serve-only 20
Router(config)# ntp access-group serve 30
Router(config)# ntp access-group query-only 40

! Verification
Router# show ntp associations
Router# show ntp status
Router# show ntp clock
Router# show clock detail
```

6.3 DNS Configuration

```
! DNS Server Configuration
Router(config)# ip name-server 8.8.8.8
Router(config)# ip name-server 8.8.4.4
Router(config)# ip name-server 192.168.100.10
Router(config)# ip domain-name company.com
Router(config)# ip domain-list branch.company.com
Router(config)# ip domain-list partner.com
Router(config)# ip domain lookup source-interface Loopback0

! DNS Host Entries
Router(config)# ip host router1.company.com 192.168.1.1
Router(config)# ip host switch1 10.0.0.1 10.0.0.2
Router(config)# ip host ftp-server 192.168.100.10

! DNS Caching
Router(config)# ip dns server
Router(config)# ip dns cache
Router(config)# ip dns spoofing 192.168.1.1

! Verification
Router# show hosts
Router# nslookup router1.company.com
Router# ping router1.company.com
```

6.4 Syslog Configuration

```
! Syslog Server Setup
Router(config)# logging on
Router(config)# logging host 192.168.100.10
Router(config)# logging host 192.168.100.11
Router(config)# logging trap debugging
Router(config)# logging facility local7
Router(config)# logging source-interface Loopback0
Router(config)# logging origin-id hostname
Router(config)# logging sequence-numbers
Router(config)# logging discriminator OSPF msg-body includes "
    OSPF"

! Local Logging
Router(config)# logging buffered 16384 informational
Router(config)# logging console warnings
Router(config)# logging monitor debugging
Router(config)# logging persistent url flash:logs size 4096
Router(config)# logging history debugging

! Logging Filters
Router(config)# logging filter OSPF ROUTER-ID 1.1.1.1
Router(config)# logging filter BGP neighbor 192.168.1.2

```

```
! Verification
Router# show logging
Router# show logging history
Router# show logging filter
```

6.5 SNMP Configuration

```
! SNMPv2c Configuration
Router(config)# snmp-server community RO-COMMUNITY RO 10
Router(config)# snmp-server community RW-COMMUNITY RW 20
Router(config)# snmp-server host 192.168.100.10 version 2c RO-
   COMMUNITY
Router(config)# snmp-server enable traps
Router(config)# snmp-server trap-source Loopback0
Router(config)# snmp-server queue-length 100
Router(config)# snmp-server location "Data Center Rack A1"
Router(config)# snmp-server contact "Network Operations
   noc@company.com"
Router(config)# snmp-server chassis-id R1-CORE-ASR1001

! SNMPv3 Configuration (Secure)
Router(config)# snmp-server group ADMIN v3 priv read ALL write
   ALL
Router(config)# snmp-server user admin1 ADMIN v3 auth sha
   AuthPass123 priv aes 128 PrivPass123
Router(config)# snmp-server host 192.168.100.10 version 3 priv
   admin1
Router(config)# snmp-server enable traps snmp authentication
   linkdown linkup coldstart warmstart
Router(config)# snmp-server enable traps config
Router(config)# snmp-server enable traps entity
Router(config)# snmp-server enable traps cpu threshold
Router(config)# snmp-server enable traps memory threshold
Router(config)# snmp-server enable traps ospf
Router(config)# snmp-server enable traps bgp

! SNMP Views
Router(config)# snmp-server view ALL iso included
Router(config)# snmp-server view RESTRICTED system included
Router(config)# snmp-server view RESTRICTED interfaces excluded

! Verification
Router# show snmp
Router# show snmp user
Router# show snmp group
Router# show snmp host
```

7 Security Fundamentals

7.1 Password Management

```
! Password Configuration
Router(config)# enable secret SuperSecret123!
Router(config)# enable algorithm-type scrypt secret
   EvenMoreSecret456!
Router(config)# username admin privilege 15 secret P@ssw0rd123!
Router(config)# username operator privilege 5 secret 0p3rator!
Router(config)# service password-encryption
Router(config)# security passwords min-length 10
Router(config)# login block-for 300 attempts 3 within 60
Router(config)# login delay 2
Router(config)# login on-failure log
Router(config)# login on-success log

! Line Password Configuration
Router(config-line)# password Cons0leP@ss
Router(config-line)# login local
Router(config-line)# exec-timeout 5 0
Router(config-line)# absolute-timeout 30
Router(config-line)# session-timeout 30
Router(config-line)# logout-warning 5

! Password Recovery Prevention
Router(config)# no service password-recovery
Router(config)# enable secret recovery SecretRecovery789!
```

7.2 SSH Hardening

```
! SSH Configuration
Router(config)# ip ssh version 2
Router(config)# ip ssh time-out 60
Router(config)# ip ssh authentication-retries 2
Router(config)# ip ssh maxstartups 3
Router(config)# ip ssh logging events
Router(config)# ip ssh server algorithm mac hmac-sha2-256 hmac-
   sha2-512
Router(config)# ip ssh server algorithm encryption aes128-ctr
   aes192-ctr aes256-ctr
Router(config)# ip ssh server algorithm hostkey rsa-sha2-256 rsa-
   sha2-512
Router(config)# ip ssh server disable-deprecated-version 1.99
Router(config)# ip ssh server max-sessions-per-connection 10

! SSH Key-Based Authentication
Router(config)# crypto key generate rsa modulus 4096
Router(config)# crypto key generate dsa modulus 2048
```

```
Router(config)# crypto key generate ecdsa curve 256
Router(config)# ip ssh pubkey-chain
Router(config-ssh-pubkey)# username admin
Router(config-ssh-pubkey)# key-hash ssh-rsa AAAA...==
Router(config-ssh-pubkey)# exit

! SSH Source Interface
Router(config)# ip ssh source-interface Loopback0
Router(config)# ip ssh vrf MGMT

! Verification
Router# show ip ssh
Router# show ssh
Router# show crypto key mypubkey rsa
```

7.3 TCP/UDP Small Services

```
! Disable Unnecessary Services
Router(config)# no service tcp-small-servers
Router(config)# no service udp-small-servers
Router(config)# no service finger
Router(config)# no ip bootp server
Router(config)# no ip http server
Router(config)# no ip http secure-server
Router(config)# no ip source-route
Router(config)# no ip gratuitous-arps
Router(config)# no cdp run          ! Disable globally
Router(config)# no lldp run         ! Disable globally
Router(config)# no ip proxy-arp
Router(config)# no ip unreachables
Router(config)# no ip redirects
Router(config)# no ip mask-reply

! Per-Interface Services
Router(config-if)# no cdp enable
Router(config-if)# no lldp transmit
Router(config-if)# no lldp receive
Router(config-if)# no ip directed-broadcast
Router(config-if)# no ip unreachables
Router(config-if)# no ip proxy-arp
```

7.4 Control Plane Policing (CoPP)

```
! CoPP Configuration
Router(config)# class-map match-any COPP-CRITICAL
Router(config-cmap)# match access-group 110
Router(config-cmap)# exit

Router(config)# class-map match-any COPP-IMPORTANT
```

```
Router(config-cmap)# match access-group 120
Router(config-cmap)# exit

Router(config)# policy-map COPP-POLICY
Router(config-pmap)# class COPP-CRITICAL
Router(config-pmap-c)# police 8000 conform-action transmit exceed
   -action drop
Router(config-pmap-c)# exit
Router(config-pmap)# class COPP-IMPORTANT
Router(config-pmap-c)# police 40000 conform-action transmit
   exceed-action drop
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default
Router(config-pmap-c)# police 10000 conform-action transmit
   exceed-action drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit

Router(config)# control-plane
Router(config-cp)# service-policy input COPP-POLICY
Router(config-cp)# exit

! ACLs for CoPP
Router(config)# access-list 110 permit tcp any any eq 22
Router(config)# access-list 110 permit tcp any any eq 23
Router(config)# access-list 120 permit ospf any any
Router(config)# access-list 120 permit eigrp any any
Router(config)# access-list 120 permit pim any any
```

8 AAA & Access Control

8.1 AAA Basics

```
! Enable AAA
Router(config)# aaa new-model
Router(config)# aaa authentication login default local
Router(config)# aaa authentication enable default enable
Router(config)# aaa authorization exec default local
Router(config)# aaa accounting exec default start-stop group
   radius

! Local User Database
Router(config)# username admin privilege 15 algorithm-type scrypt
    secret AdminPass123!
Router(config)# username operator privilege 5 secret Op3rator!
Router(config)# username guest privilege 1 secret GuestAccess!

! Enable Password
Router(config)# enable secret level 15 SuperSecret!
```

```
Router(config)# enable secret level 5 OperatorPass
```

8.2 RADIUS Configuration

```
! RADIUS Server Configuration
Router(config)# radius server ISE-PRIMARY
Router(config-radius-server)# address ipv4 192.168.100.10 auth-port 1812 acct-port 1813
Router(config-radius-server)# key RadiusKey123!
Router(config-radius-server)# retransmit 3
Router(config-radius-server)# timeout 5
Router(config-radius-server)# exit

Router(config)# radius server ISE-SECONDARY
Router(config-radius-server)# address ipv4 192.168.100.11 auth-port 1812 acct-port 1813
Router(config-radius-server)# key RadiusKey456!
Router(config-radius-server)# exit

! RADIUS Server Group
Router(config)# aaa group server radius ISE-GROUP
Router(config-sg-radius)# server name ISE-PRIMARY
Router(config-sg-radius)# server name ISE-SECONDARY
Router(config-sg-radius)# exit

! AAA with RADIUS
Router(config)# aaa authentication login default group ISE-GROUP local
Router(config)# aaa authentication enable default group ISE-GROUP enable
Router(config)# aaa authorization exec default group ISE-GROUP local
Router(config)# aaa accounting exec default start-stop group ISE-GROUP
Router(config)# aaa accounting network default start-stop group ISE-GROUP
```

8.3 TACACS+ Configuration

```
! TACACS+ Server Configuration
Router(config)# tacacs server TACACS-PRIMARY
Router(config-server-tacacs)# address ipv4 192.168.100.20
Router(config-server-tacacs)# key TacacsKey123!
Router(config-server-tacacs)# single-connection
Router(config-server-tacacs)# timeout 10
Router(config-server-tacacs)# exit

! TACACS+ Server Group
Router(config)# aaa group server tacacs+ TACACS-GROUP
```

```
Router(config-sg-tacacs)# server name TACACS-PRIMARY
Router(config-sg-tacacs)# exit

! AAA with TACACS+
Router(config)# aaa authentication login default group TACACS-
   GROUP local
Router(config)# aaa authentication enable default group TACACS-
   GROUP enable
Router(config)# aaa authorization commands 15 default group
   TACACS-GROUP local
Router(config)# aaa authorization config-commands
Router(config)# aaa authorization exec default group TACACS-GROUP
    local
Router(config)# aaa accounting commands 15 default start-stop
   group TACACS-GROUP
Router(config)# aaa accounting exec default start-stop group
   TACACS-GROUP
```

8.4 Command Authorization

```
! Command Authorization Levels
Router(config)# privilege exec level 5 show running-config
Router(config)# privilege exec level 5 show interfaces
Router(config)# privilege exec level 10 configure terminal
Router(config)# privilege exec level 15 reload
Router(config)# privilege interface level 5 shutdown
Router(config)# privilege interface level 10 ip address

! Command Sets
Router(config)# parser view ROOT
Router(config-view)# secret RootView123!
Router(config-view)# commands exec include all show
Router(config-view)# commands exec include configure
Router(config-view)# commands exec include reload
Router(config-view)# exit

Router(config)# parser view OPERATOR
Router(config-view)# secret OperatorView456!
Router(config-view)# commands exec include show
Router(config-view)# commands exec exclude show running-config
Router(config-view)# commands exec include ping
Router(config-view)# commands exec include traceroute
Router(config-view)# exit
```

8.5 Downloadable ACLs

```
! RADIUS with Downloadable ACLs
Router(config)# ip access-list extended DYNACL-WEBSERVER
Router(config-ext-nacl)# permit tcp any host 192.168.1.10 eq 80
```

```
Router(config-ext-nacl)# permit tcp any host 192.168.1.10 eq 443
Router(config-ext-nacl)# deny ip any any
Router(config-ext-nacl)# exit

! AAA Attribute for ACL
Router(config)# aaa authorization network default group ISE-GROUP
```

9 Management Protocols

9.1 HTTP/HTTPS Management

```
! HTTP Server Configuration
Router(config)# ip http server
Router(config)# ip http port 8080
Router(config)# ip http authentication local
Router(config)# ip http access-class 10
Router(config)# ip http secure-server
Router(config)# ip http secure-port 443
Router(config)# ip http secure-ciphersuite aes256-cbc-sha1
Router(config)# ip http timeout-policy idle 60 life 86400
   requests 100

! ACL for HTTP Access
Router(config)# access-list 10 permit 192.168.100.0 0.0.0.255
Router(config)# access-list 10 deny any

! Verification
Router# show ip http server status
Router# show ip http secure-server status
```

9.2 Netconf/RESTCONF

```
! NETCONF Configuration
Router(config)# netconf-yang
Router(config)# netconf-yang feature candidate-datastore
Router(config)# netconf-yang feature notify
Router(config)# netconf-yang feature url
Router(config)# netconf-yang ssh port 830

! RESTCONF Configuration
Router(config)# restconf
Router(config)# ip http secure-server
Router(config)# restconf data-entries 10000

! Verification
Router# show netconf-yang sessions
Router# show restconf
```

9.3 gRPC/Telemetry

```
! gRPC Configuration
Router(config)# grpc
Router(config-grpc)# port 57400
Router(config-grpc)# no-tls
Router(config-grpc)# address-family ipv4
Router(config-grpc)# max-request-total 64
Router(config-grpc)# max-request-per-user 16

! Telemetry Configuration
Router(config)# telemetry ietf subscription 101
Router(config-telemetry)# encoding encode-kvgpb
Router(config-telemetry)# filter xpath /interfaces/interface/
   statistics
Router(config-telemetry)# source-address 192.168.1.1
Router(config-telemetry)# stream yang-push
Router(config-telemetry)# update-policy periodic 500
Router(config-telemetry)# receiver ip address 192.168.100.30 5432
    protocol grpc-tcp
```

9.4 NETCONF/YANG Models

```
! YANG Models
Router# show platform software yang-management process
Router# show yang-operational memory
Router# show yang schema

! Install YANG Models
Router# copy tftp://192.168.1.10/ietf-interfaces@2014-05-08.yang
   flash:
Router# install add file flash:ietf-interfaces@2014-05-08.yang
   activate

! NETCONF Operations
# From Linux with netconf-client
# netconf-console --host 10.0.0.1 --port 830 --user admin --
   password pass --get-config
```

10 Ethernet Switching

10.1 MAC Address Table

```
! MAC Address Operations
Switch# show mac address-table
Switch# show mac address-table dynamic
Switch# show mac address-table aging-time
Switch# show mac address-table count
```

```
Switch# show mac address-table interface gigabitEthernet 1/0/1
Switch# show mac address-table vlan 10
Switch# show mac address-table address 0050.7966.6800

! MAC Table Configuration
Switch(config)# mac address-table aging-time 300
Switch(config)# mac address-table learning vlan 10
Switch(config)# no mac address-table learning vlan 20
Switch(config)# mac address-table static 0050.7966.6800 vlan 10
   interface gi1/0/1
Switch(config)# mac address-table notification change
Switch(config)# mac address-table limit maximum 1000 vlan 10

! Clear MAC Table
Switch# clear mac address-table dynamic
Switch# clear mac address-table dynamic interface gi1/0/1
Switch# clear mac address-table dynamic vlan 10
Switch# clear mac address-table dynamic address 0050.7966.6800
```

10.2 Port Configuration

```
! Basic Port Configuration
Switch(config)# interface gigabitEthernet 1/0/1
Switch(config-if)# description "Connected to Server01"
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# switchport voice vlan 20
Switch(config-if)# spanning-tree portfast
Switch(config-if)# spanning-tree bpduguard enable
Switch(config-if)# no shutdown
Switch(config-if)# exit

! Speed/Duplex Configuration
Switch(config-if)# speed 1000
Switch(config-if)# duplex full
Switch(config-if)# negotiation auto
Switch(config-if)# mtu 9216        ! Jumbo frames

! Error Disable Recovery
Switch(config)# errdisable recovery cause psecure-violation
Switch(config)# errdisable recovery cause bpduguard
Switch(config)# errdisable recovery interval 30
Switch(config)# errdisable detect cause all

! Interface Templates
Switch(config)# template USER-PORT
Switch(config-template)# switchport mode access
Switch(config-template)# switchport access vlan 10
Switch(config-template)# spanning-tree portfast
Switch(config-template)# spanning-tree bpduguard enable
```

```
Switch(config-template)# storm-control broadcast level 10.00
Switch(config-template)# service-policy input AUTOQOS-VOIP
Switch(config-template)# exit

Switch(config)# interface range gi1/0/1 - 24
Switch(config-if-range)# source template USER-PORT
```

10.3 CDP/LLDP

```
! CDP Configuration
Switch(config)# cdp run
Switch(config)# cdp timer 60
Switch(config)# cdp holdtime 180
Switch(config)# cdp advertise-v2
Switch(config-if)# cdp enable
Switch(config-if)# no cdp enable

! LLDP Configuration
Switch(config)# lldp run
Switch(config)# lldp timer 30
Switch(config)# lldp holdtime 120
Switch(config)# lldp reinit 2
Switch(config-if)# lldp transmit
Switch(config-if)# lldp receive
Switch(config-if)# lldp med

! Verification
Switch# show cdp neighbors
Switch# show cdp neighbors detail
Switch# show cdp traffic
Switch# show lldp neighbors
Switch# show lldp neighbors detail
Switch# show lldp traffic
Switch# show lldp interface gi1/0/1
```

10.4 UDLD & Loop Guard

```
! UDLD Configuration
Switch(config)# udld enable
Switch(config)# udld aggressive
Switch(config-if)# udld port aggressive
Switch(config-if)# udld disable

! Loop Guard
Switch(config)# spanning-tree loopguard default
Switch(config-if)# spanning-tree guard loop
Switch(config-if)# spanning-tree guard root

! Verification
```

```
Switch# show udld neighbors
Switch# show udld gi1/0/1
Switch# show spanning-tree inconsistentports
```

11 VLANs & Trunking

11.1 VLAN Configuration

```
! VLAN Creation
Switch(config)# vlan 10
Switch(config-vlan)# name SALES
Switch(config-vlan)# state active
Switch(config-vlan)# exit

Switch(config)# vlan 20
Switch(config-vlan)# name ENGINEERING
Switch(config-vlan)# exit

Switch(config)# vlan 99
Switch(config-vlan)# name MANAGEMENT
Switch(config-vlan)# exit

! VLAN Range
Switch(config)# vlan 100-200
Switch(config-vlan)# name USER-VLANS
Switch(config-vlan)# exit

! Extended VLANs (1006-4094)
Switch(config)# vlan 2000
Switch(config-vlan)# name EXTENDED-VLAN
Switch(config-vlan)# exit

! Private VLANs
Switch(config)# vlan 500
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# private-vlan association 501-502
Switch(config-vlan)# exit

Switch(config)# vlan 501
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# exit

Switch(config)# vlan 502
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# exit
```

11.2 VLAN Trunking

```
! Trunk Configuration
Switch(config)# interface gigabitEthernet 1/0/24
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport trunk native vlan 99
Switch(config-if)# switchport trunk allowed vlan 10,20,30,99
Switch(config-if)# switchport trunk allowed vlan add 40-50
Switch(config-if)# switchport trunk allowed vlan remove 30
Switch(config-if)# switchport trunk pruning vlan 2-1001
Switch(config-if)# switchport nonegotiate
Switch(config-if)# spanning-tree guard root
Switch(config-if)# exit

! Dynamic Trunking
Switch(config-if)# switchport mode dynamic desirable
Switch(config-if)# switchport mode dynamic auto

! VLAN Translation
Switch(config-if)# switchport vlan mapping 10 110
Switch(config-if)# switchport vlan mapping 20 120

! Verification
Switch# show interfaces trunk
Switch# show interfaces gi1/0/24 switchport
Switch# show interfaces gi1/0/24 trunk
Switch# show vlan
Switch# show vlan id 10
Switch# show vlan name SALES
```

11.3 VTP Configuration

```
! VTP Setup
Switch(config)# vtp domain COMPANY
Switch(config)# vtp mode server
Switch(config)# vtp password VTP-Pass123!
Switch(config)# vtp version 2
Switch(config)# vtp pruning
Switch(config)# vtp interface Loopback0

! VTP Client
Switch(config)# vtp mode client
Switch(config)# vtp transparent

! Verification
Switch# show vtp status
Switch# show vtp password
Switch# show vtp counters
Switch# show vlan brief
```

11.4 Voice VLAN

```
! Voice VLAN Configuration
Switch(config)# interface gigabitEthernet 1/0/10
Switch(config-if)# switchport voice vlan 110
Switch(config-if)# switchport priority extend cos 0
Switch(config-if)# auto qos voip trust
Switch(config-if)# mls qos trust cos
Switch(config-if)# spanning-tree portfast
Switch(config-if)# spanning-tree bpduguard enable

! LLDP-MED for Voice
Switch(config)# lldp run
Switch(config-if)# lldp med
Switch(config-if)# lldp med-tlv-select inventory-management
   network-policy
```

11.5 VLAN ACLs (VACLs)

```
! VLAN Access Maps
Switch(config)# vlan access-map BLOCK-SERVER 10
Switch(config-access-map)# match ip address SERVER-ACL
Switch(config-access-map)# action drop
Switch(config-access-map)# exit

Switch(config)# vlan access-map BLOCK-SERVER 20
Switch(config-access-map)# action forward
Switch(config-access-map)# exit

Switch(config)# vlan filter BLOCK-SERVER vlan-list 10

! VLAN-based ACL
Switch(config)# ip access-list extended SERVER-ACL
Switch(config-ext-nacl)# deny tcp any host 192.168.10.10 eq 3389
Switch(config-ext-nacl)# permit ip any any
```

12 Spanning Tree Protocol

12.1 STP Basics

```
! STP Mode Selection
Switch(config)# spanning-tree mode rapid-pvst
Switch(config)# spanning-tree mode mst
Switch(config)# spanning-tree mode pvst

! Bridge Priority
Switch(config)# spanning-tree vlan 1,10,20,30 priority 4096
Switch(config)# spanning-tree vlan 40-50 priority 8192
```

```
! Root Guard
Switch(config)# spanning-tree portfast bpduguard default
Switch(config-if)# spanning-tree guard root
Switch(config-if)# spanning-tree bpdufilter enable
Switch(config-if)# spanning-tree bpduguard enable

! Verification
Switch# show spanning-tree
Switch# show spanning-tree vlan 10
Switch# show spanning-tree interface gi1/0/1
Switch# show spanning-tree detail
Switch# show spanning-tree inconsistentports
Switch# show spanning-tree mst configuration
```

12.2 MST Configuration

```
! MST Setup
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# name REGION1
Switch(config-mst)# revision 1
Switch(config-mst)# instance 1 vlan 10,20,30
Switch(config-mst)# instance 2 vlan 40,50,60
Switch(config-mst)# exit

! MST Instance Parameters
Switch(config)# spanning-tree mst 1 priority 4096
Switch(config)# spanning-tree mst 2 priority 8192
Switch(config)# spanning-tree mst 0-2 hello-time 2
Switch(config)# spanning-tree mst 0-2 forward-time 15
Switch(config)# spanning-tree mst 0-2 max-age 20

! Verification
Switch# show spanning-tree mst
Switch# show spanning-tree mst configuration
Switch# show spanning-tree mst 1
Switch# show spanning-tree mst interface gi1/0/1
```

12.3 STP Timers & Optimization

```
! STP Timers
Switch(config)# spanning-tree vlan 1 hello-time 2
Switch(config)# spanning-tree vlan 1 forward-time 15
Switch(config)# spanning-tree vlan 1 max-age 20
Switch(config)# spanning-tree transmit hold-count 6

! PortFast & BPDU Guard
Switch(config)# spanning-tree portfast default
Switch(config)# spanning-tree portfast bpduguard default
```

```
Switch(config-if)# spanning-tree portfast
Switch(config-if)# spanning-tree portfast trunk

! UplinkFast & BackboneFast
Switch(config)# spanning-tree uplinkfast
Switch(config)# spanning-tree backbonefast

! STP Loop Guard
Switch(config)# spanning-tree loopguard default
Switch(config-if)# spanning-tree guard loop
```

12.4 STP Security Features

```
! BPDU Guard
Switch(config)# spanning-tree portfast bpduguard default
Switch(config)# errdisable recovery cause bpduguard
Switch(config)# errdisable recovery interval 30

! BPDU Filter
Switch(config)# spanning-tree portfast bpdufilter default
Switch(config-if)# spanning-tree bpdufilter enable

! Root Guard
Switch(config-if)# spanning-tree guard root

! TC Guard
Switch(config)# spanning-tree tc-guard
Switch(config)# spanning-tree tc-filter

! Verification
Switch# show spanning-tree summary
Switch# show spanning-tree detail
Switch# debug spanning-tree events
```

13 EtherChannel & LACP

13.1 EtherChannel Configuration

```
! LACP Configuration (Recommended)
Switch(config)# interface range gigabitEthernet 1/0/1-2
Switch(config-if-range)# channel-group 1 mode active
Switch(config-if-range)# channel-protocol lacp
Switch(config-if-range)# lacp port-priority 1000
Switch(config-if-range)# lacp rate fast
Switch(config-if-range)# exit

! PAgP Configuration
Switch(config-if-range)# channel-group 1 mode desirable
```

```
Switch(config-if-range)# channel-protocol pagp
Switch(config-if-range)# pagp port-priority 1000

! Static EtherChannel
Switch(config-if-range)# channel-group 1 mode on

! Port-Channel Interface
Switch(config)# interface port-channel 1
Switch(config-if)# description "Uplink to Core"
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk native vlan 99
Switch(config-if)# switchport trunk allowed vlan 10,20,30,99
Switch(config-if)# lacp system-priority 1000
Switch(config-if)# lacp system-id 0050.7966.6800
Switch(config-if)# exit
```

13.2 Load Balancing

```
! EtherChannel Load Balancing
Switch(config)# port-channel load-balance src-dst-ip
Switch(config)# port-channel load-balance src-dst-mac
Switch(config)# port-channel load-balance src-dst-port
Switch(config)# port-channel load-balance src-ip
Switch(config)# port-channel load-balance dst-ip
Switch(config)# port-channel load-balance src-mac
Switch(config)# port-channel load-balance dst-mac

! Per-VLAN Load Balancing
Switch(config)# vlan 10
Switch(config-vlan)# lacp load-balancing src-dst-ip
Switch(config-vlan)# exit

! Verification
Switch# show etherchannel summary
Switch# show etherchannel port-channel
Switch# show etherchannel load-balance
Switch# show lacp neighbor
Switch# show lacp internal
Switch# show lacp counters
Switch# show pagp neighbor
Switch# show pagp internal
```

13.3 Advanced EtherChannel

```
! Cross-Stack EtherChannel (StackWise)
Switch(config)# interface port-channel 10
Switch(config-if)# stack-port 1/1-1/2
Switch(config-if)# switchport mode trunk
Switch(config-if)# exit
```

```
! VSS EtherChannel
Switch(config)# interface port-channel 100
Switch(config-if)# vss-port-channel
Switch(config-if)# switchport mode trunk
Switch(config-if)# exit

! Minimum Links
Switch(config-if)# lacp min-links 2
Switch(config)# port-channel min-links 2

! Maximum Links
Switch(config-if)# lacp max-bundle 8

! Graceful Shutdown
Switch(config-if)# lacp graceful-convergence
```

13.4 Troubleshooting EtherChannel

```
! Common Issues & Fixes
Switch# show etherchannel detail
Switch# show etherchannel inconsistency
Switch# debug etherchannel
Switch# debug lacp
Switch# debug pagp

! Clear EtherChannel
Switch# clear lacp counters
Switch# clear pagp counters
Switch(config)# default interface port-channel 1

! Manual Intervention
Switch(config)# interface gi1/0/1
Switch(config-if)# shutdown
Switch(config-if)# no channel-group
Switch(config-if)# no shutdown
Switch(config-if)# channel-group 1 mode active
```

14 IP Addressing & Services

14.1 IP Address Configuration

```
! Basic IP Addressing
Router(config)# interface gigabitEthernet 0/0
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# ip address 10.0.0.1 255.255.255.0 secondary
Router(config-if)# ip directed-broadcast
Router(config-if)# ip unreachables
```

```
Router(config-if)# ip redirects
Router(config-if)# ip proxy-arp
Router(config-if)# no shutdown

! Loopback Interfaces
Router(config)# interface loopback 0
Router(config-if)# ip address 1.1.1.1 255.255.255.255
Router(config-if)# description "Router ID and Management"
Router(config-if)# ip ospf network point-to-point

! VLSM Subnetting
Router(config-if)# ip address 172.16.1.1 255.255.255.192
Router(config-if)# ip address 10.1.1.1 255.255.255.224
Router(config-if)# ip address 192.168.1.129 255.255.255.240

! IPv6 Addressing
Router(config-if)# ipv6 enable
Router(config-if)# ipv6 address 2001:db8::1/64
Router(config-if)# ipv6 address fe80::1 link-local
Router(config-if)# ipv6 address autoconfig
```

14.2 DHCP Services

```
! DHCP Server Configuration
Router(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.10
Router(config)# ip dhcp excluded-address 192.168.1
Router(config)# ip dhcp excluded-address 192.168.1.254
Router(config)# ip dhcp pool LAN-POOL
Router(dhcp-config)# network 192.168.1.0 255.255.255.0
Router(dhcp-config)# default-router 192.168.1.1
Router(dhcp-config)# dns-server 8.8.8.8 8.8.4.4
Router(dhcp-config)# domain-name company.com
Router(dhcp-config)# lease 8
Router(dhcp-config)# option 150 ip 192.168.1.10  ! TFTP for VoIP
Router(dhcp-config)# client-identifier 0100.5056.c000.08
Router(dhcp-config)# host 192.168.1.100 255.255.255.0
Router(dhcp-config)# exit

! DHCP Relay
Router(config-if)# ip helper-address 192.168.100.10
Router(config-if)# ip forward-protocol udp 67
Router(config-if)# ip forward-protocol udp 68

! DHCP Options
Router(config)# ip dhcp ping timeout 100
Router(config)# ip dhcp ping packets 2
Router(config)# ip dhcp conflict logging
Router(config)# ip dhcp snooping
```

14.3 DHCP Snooping

```
! DHCP Snooping Configuration
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10,20,30
Switch(config)# ip dhcp snooping information option
Switch(config)# ip dhcp snooping limit rate 100
Switch(config)# ip dhcp snooping verify mac-address
Switch(config)# ip dhcp snooping database flash:dhcp-snooping.db
Switch(config)# ip dhcp snooping database write-delay 300

! Trusted/Untrusted Ports
Switch(config-if)# ip dhcp snooping trust
Switch(config-if)# ip dhcp snooping limit rate 50
Switch(config-if)# ip dhcp snooping vlan 10 information option

! Verification
Switch# show ip dhcp snooping
Switch# show ip dhcp snooping binding
Switch# show ip dhcp snooping statistics
Switch# debug ip dhcp snooping
```

14.4 ARP Configuration

```
! ARP Settings
Router(config)# arp timeout 300
Router(config)# arp 192.168.1.100 0050.7966.6800 arpa
Router(config)# arp proxy disable
Router(config)# arp gratuitous ignore

! Proxy ARP
Router(config-if)# ip proxy-arp
Router(config-if)# no ip proxy-arp

! ARP Inspection (DAI)
Switch(config)# ip arp inspection vlan 10,20
Switch(config)# ip arp inspection validate src-mac dst-mac ip
Switch(config)# ip arp inspection log-buffer entries 32
Switch(config)# ip arp inspection log-buffer logs 1024 interval
   10
Switch(config-if)# ip arp inspection trust
Switch(config-if)# ip arp inspection limit rate 100
```

15 Static Routing

15.1 Basic Static Routes

```
! Standard Static Routes
Router(config)# ip route 192.168.2.0 255.255.255.0 10.0.0.2
Router(config)# ip route 192.168.3.0 255.255.255.0
   GigabitEthernet0/1 10.0.0.3
Router(config)# ip route 192.168.4.0 255.255.255.0 10.0.0.4 50

! Default Route
Router(config)# ip route 0.0.0.0 0.0.0.0 203.0.113.1
Router(config)# ip route 0.0.0.0 0.0.0.0 Dialer1

! Summary Routes
Router(config)# ip route 172.16.0.0 255.255.0.0 10.0.0.1
Router(config)# ip route 10.0.0.0 255.255.0.0 Null0

! Floating Static Routes
Router(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.1
Router(config)# ip route 0.0.0.0 0.0.0.0 192.168.2.1 250
```

15.2 Static Route Tracking

```
! IP SLA Tracking
Router(config)# ip sla 1
Router(config-ip-sla)# icmp-echo 8.8.8.8 source-interface
   GigabitEthernet0/0
Router(config-ip-sla)# timeout 1000
Router(config-ip-sla)# frequency 5
Router(config-ip-sla)# exit

Router(config)# ip sla schedule 1 life forever start-time now

Router(config)# track 10 ip sla 1 reachability
Router(config-track)# delay down 10 up 5

Router(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.1 track 10
Router(config)# ip route 0.0.0.0 0.0.0.0 192.168.2.1 250
```

15.3 Policy-Based Routing

```
! PBR Configuration
Router(config)# access-list 100 permit tcp any any eq 80
Router(config)# access-list 100 permit tcp any any eq 443

Router(config)# route-map PBR-OUTBOUND permit 10
Router(config-route-map)# match ip address 100
Router(config-route-map)# set ip next-hop 192.168.1.10
Router(config-route-map)# set interface Null0
Router(config-route-map)# set ip dscp af41
Router(config-route-map)# set ip precedence flash
```

```
Router(config-route-map)# exit

Router(config)# interface GigabitEthernet0/0
Router(config-if)# ip policy route-map PBR-OUTBOUND

! Global PBR
Router(config)# ip local policy route-map PBR-OUTBOUND
```

15.4 VRF-Aware Static Routing

```
! VRF Static Routes
Router(config)# ip route vrf CUSTOMER-A 192.168.1.0 255.255.255.0
    10.0.0.2
Router(config)# ip route vrf CUSTOMER-B 172.16.0.0 255.255.0.0
   GigabitEthernet0/1.100

! VRF Leaking
Router(config)# ip route vrf CUSTOMER-A 0.0.0.0 0.0.0.0
   GigabitEthernet0/0 global
Router(config)# ip route 10.0.0.0 255.255.255.0 GigabitEthernet0
   /0 vrf CUSTOMER-A
```

16 OSPF

16.1 OSPF Basics

```
! OSPF Process Configuration
Router(config)# router ospf 100
Router(config-router)# router-id 1.1.1.1
Router(config-router)# auto-cost reference-bandwidth 1000
Router(config-router)# timers throttle spf 10 100 5000
Router(config-router)# timers throttle lsa all 10 100 5000
Router(config-router)# timers lsa arrival 1000
Router(config-router)# max-lsa 12000
Router(config-router)# log-adjacency-changes detail
Router(config-router)# passive-interface default
Router(config-router)# no passive-interface GigabitEthernet0/0
Router(config-router)# network 10.0.0.0 0.255.255.255 area 0
Router(config-router)# network 192.168.1.0 0.0.0.255 area 0
Router(config-router)# exit

! Interface Configuration
Router(config-if)# ip ospf 100 area 0
Router(config-if)# ip ospf hello-interval 10
Router(config-if)# ip ospf dead-interval 40
Router(config-if)# ip ospf priority 100
Router(config-if)# ip ospf cost 10
Router(config-if)# ip ospf network point-to-point
```

```
Router(config-if)# ip ospf mtu-ignore
Router(config-if)# ip ospf authentication message-digest
Router(config-if)# ip ospf message-digest-key 1 md5 OSPF-KEY
```

16.2 OSPF Area Types

```
! Multi-Area OSPF
Router(config-router)# router ospf 100
Router(config-router)# area 1 stub
Router(config-router)# area 1 default-cost 100
Router(config-router)# area 2 stub no-summary
Router(config-router)# area 3 nssa
Router(config-router)# area 3 nssa default-information-originate
Router(config-router)# area 3 nssa no-redistribution
Router(config-router)# area 4 nssa no-summary
Router(config-router)# area 10 virtual-link 2.2.2.2
Router(config-router)# area 10 authentication message-digest

! Summarization
Router(config-router)# area 1 range 10.1.0.0 255.255.0.0
Router(config-router)# area 1 range 10.2.0.0 255.255.0.0
   advertise
Router(config-router)# area 1 range 10.3.0.0 255.255.0.0 not-
   advertise
Router(config-router)# summary-address 192.168.0.0 255.255.0.0
```

16.3 OSPF Authentication

```
! OSPF Authentication
! Plain Text
Router(config-if)# ip ospf authentication
Router(config-if)# ip ospf authentication-key OSPF-PASS

! MD5 Authentication
Router(config-if)# ip ospf authentication message-digest
Router(config-if)# ip ospf message-digest-key 1 md5 OSPF-MD5-KEY

! Key Chain Authentication
Router(config)# key chain OSPF-KEYS
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string OSPF-KEY-1
Router(config-keychain-key)# cryptographic-algorithm md5
Router(config-keychain-key)# accept-lifetime 00:00:00 Jan 1 2024
   infinite
Router(config-keychain-key)# send-lifetime 00:00:00 Jan 1 2024
   infinite

Router(config-if)# ip ospf authentication key-chain OSPF-KEYS
```

16.4 OSPF Advanced Features

```
! OSPF Graceful Restart
Router(config)# router ospf 100
Router(config-router)# nsf cisco helper
Router(config-router)# nsf ietf helper
Router(config-router)# nsf ietf helper strict-lsa-checking

! OSPF Filtering
Router(config-router)# distribute-list 10 in
Router(config-router)# distribute-list 20 out
Router(config-router)# area 1 filter-list prefix FILTER-1 in
Router(config-router)# area 1 filter-list prefix FILTER-2 out

! OSPF Cost Manipulation
Router(config-if)# ip ospf cost 100
Router(config-if)# bandwidth 10000
Router(config)# auto-cost reference-bandwidth 10000

! OSPF Database Control
Router(config-router)# max-lsa 50000 warning-only
Router(config-router)# max-metric router-lsa on-startup 300
```

16.5 OSPF Verification

```
! OSPF Show Commands
Router# show ip ospf
Router# show ip ospf neighbor
Router# show ip ospf neighbor detail
Router# show ip ospf interface
Router# show ip ospf interface brief
Router# show ip ospf database
Router# show ip ospf database router
Router# show ip ospf database network
Router# show ip ospf database summary
Router# show ip ospf database asbr-summary
Router# show ip ospf database external
Router# show ip ospf database nssa-external
Router# show ip ospf border-routers
Router# show ip ospf virtual-links
Router# show ip ospf request-list
Router# show ip ospf retransmission-list
Router# show ip ospf events
Router# show ip ospf statistics
Router# show ip route ospf
```

16.6 OSPF Troubleshooting

```
! OSPF Debug Commands
Router# debug ip ospf adj
Router# debug ip ospf events
Router# debug ip ospf flood
Router# debug ip ospf lsa-generation
Router# debug ip ospf packet
Router# debug ip ospf retransmission
Router# debug ip ospf spf
Router# debug ip ospf hello
Router# debug ip ospf mpls traffic-eng

! OSPF Clear Commands
Router# clear ip ospf process
Router# clear ip ospf counters
Router# clear ip ospf redistribution
```

17 EIGRP

17.1 EIGRP Basics

```
! EIGRP Configuration
Router(config)# router eigrp 100
Router(config-router)# eigrp router-id 1.1.1.1
Router(config-router)# network 10.0.0.0 0.255.255.255
Router(config-router)# network 192.168.1.0
Router(config-router)# no auto-summary
Router(config-router)# metric weights 0 1 0 1 0 0
Router(config-router)# maximum-paths 4
Router(config-router)# variance 2
Router(config-router)# traffic-share balanced
Router(config-router)# timers active-time 3
Router(config-router)# log-neighbor-changes
Router(config-router)# exit

! Interface Configuration
Router(config-if)# ip bandwidth-percent eigrp 100 50
Router(config-if)# ip hello-interval eigrp 100 5
Router(config-if)# ip hold-time eigrp 100 15
Router(config-if)# ip summary-address eigrp 100 10.1.0.0
   255.255.0.0
Router(config-if)# ip authentication mode eigrp 100 md5
Router(config-if)# ip authentication key-chain eigrp 100 EIGRP-
   KEYS
```

17.2 EIGRP Named Mode

```
! EIGRP Named Mode Configuration
```

```
Router(config)# router eigrp COMPANY
Router(config-router)# address-family ipv4 unicast autonomous-
   system 100
Router(config-router-af)# topology base
Router(config-router-af-topology)# exit-af-topology
Router(config-router-af)# network 10.0.0.0 0.255.255.255
Router(config-router-af)# network 192.168.1.0 0.0.0.255
Router(config-router-af)# af-interface GigabitEthernet0/0
Router(config-router-af-interface)# hello-interval 5
Router(config-router-af-interface)# hold-time 15
Router(config-router-af-interface)# authentication mode md5
Router(config-router-af-interface)# authentication key-chain
   EIGRP-KEYS
Router(config-router-af-interface)# exit-af-interface
Router(config-router-af)# topology base
Router(config-router-af-topology)# variance 2
Router(config-router-af-topology)# maximum-paths 4
Router(config-router-af-topology)# exit-af-topology
Router(config-router-af)# exit-address-family
```

17.3 EIGRP Authentication

```
! EIGRP Authentication with Key Chain
Router(config)# key chain EIGRP-KEYS
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string EIGRP-KEY-1
Router(config-keychain-key)# accept-lifetime 00:00:00 Jan 1 2024
   infinite
Router(config-keychain-key)# send-lifetime 00:00:00 Jan 1 2024
   infinite

! Interface Configuration
Router(config-if)# ip authentication mode eigrp 100 md5
Router(config-if)# ip authentication key-chain eigrp 100 EIGRP-
   KEYS

! Named Mode Authentication
Router(config-router-af-interface)# authentication mode md5
Router(config-router-af-interface)# authentication key-chain
   EIGRP-KEYS
```

17.4 EIGRP Stub Routing

```
! EIGRP Stub Configuration
Router(config-router)# eigrp stub
Router(config-router)# eigrp stub connected
Router(config-router)# eigrp stub static
Router(config-router)# eigrp stub summary
Router(config-router)# eigrp stub redistributed
```

```
Router(config-router)# eigrp stub receive-only

! Named Mode Stub
Router(config-router-af)# eigrp stub-site
Router(config-router-af)# eigrp stub connected summary leak-map
   LEAK
```

17.5 EIGRP Route Filtering

```
! Route Filtering
Router(config-router)# distribute-list 10 in
Router(config-router)# distribute-list 20 out
Router(config-router)# distribute-list gateway GW-FILTER in
Router(config-router)# distribute-list prefix PREFIX-FILTER out

! Prefix Lists
Router(config)# ip prefix-list EIGRP-OUT seq 10 permit
   10.1.0.0/16
Router(config)# ip prefix-list EIGRP-OUT seq 20 deny 0.0.0.0/0 le
    32

! Route Maps
Router(config)# route-map EIGRP-FILTER permit 10
Router(config-route-map)# match ip address prefix-list ALLOWED
Router(config-route-map)# exit
```

17.6 EIGRP Verification

```
! EIGRP Show Commands
Router# show ip eigrp neighbors
Router# show ip eigrp neighbors detail
Router# show ip eigrp topology
Router# show ip eigrp topology all-links
Router# show ip eigrp topology 10.1.1.0/24
Router# show ip eigrp interfaces
Router# show ip eigrp interfaces detail
Router# show ip eigrp traffic
Router# show ip eigrp accounting
Router# show ip eigrp events
Router# show ip eigrp plugins
Router# show ip route eigrp
Router# show ip protocols

! EIGRP Debug Commands
Router# debug eigrp packets
Router# debug eigrp neighbors
Router# debug eigrp fsm
Router# debug eigrp notifications
```

18 BGP

18.1 BGP Basics

```
! BGP Configuration
Router(config)# router bgp 65001
Router(config-router)# bgp router-id 1.1.1.1
Router(config-router)# bgp log-neighbor-changes
Router(config-router)# bgp bestpath as-path multipath-relax
Router(config-router)# bgp bestpath compare-routerid
Router(config-router)# bgp bestpath med missing-as-worst
Router(config-router)# bgp bestpath med confed
Router(config-router)# neighbor 192.168.1.2 remote-as 65002
Router(config-router)# neighbor 192.168.1.2 description "EBGP to
   ISP"
Router(config-router)# neighbor 192.168.1.2 update-source
   Loopback0
Router(config-router)# neighbor 192.168.1.2 ebgp-multihop 255
Router(config-router)# neighbor 192.168.1.2 password BGP-PASS
Router(config-router)# neighbor 192.168.1.2 timers 10 30
Router(config-router)# neighbor 192.168.1.2 advertisement-
   interval 5
Router(config-router)# network 10.0.0.0 mask 255.255.255.0
Router(config-router)# network 192.168.0.0
Router(config-router)# maximum-paths 4
Router(config-router)# maximum-paths ibgp 4
Router(config-router)# exit
```

18.2 iBGP Configuration

```
! iBGP Full Mesh
Router(config)# router bgp 65001
Router(config-router)# neighbor 10.0.0.2 remote-as 65001
Router(config-router)# neighbor 10.0.0.2 update-source Loopback0
Router(config-router)# neighbor 10.0.0.2 next-hop-self
Router(config-router)# neighbor 10.0.0.3 remote-as 65001
Router(config-router)# neighbor 10.0.0.3 update-source Loopback0
Router(config-router)# neighbor 10.0.0.3 next-hop-self

! Route Reflector
Router(config-router)# neighbor 10.0.0.4 remote-as 65001
Router(config-router)# neighbor 10.0.0.4 route-reflector-client
Router(config-router)# neighbor 10.0.0.5 remote-as 65001
Router(config-router)# neighbor 10.0.0.5 route-reflector-client

! Confederation
Router(config-router)# bgp confederation identifier 65000
Router(config-router)# bgp confederation peers 65002 65003
```

18.3 BGP Route Filtering

```
! Prefix Lists
Router(config)# ip prefix-list CUSTOMER-ROUTES seq 10 permit
   192.168.0.0/16 le 24
Router(config)# ip prefix-list CUSTOMER-ROUTES seq 20 deny
   0.0.0.0/0 le 32

! AS Path Access Lists
Router(config)# ip as-path access-list 10 permit ^65001_
Router(config)# ip as-path access-list 10 permit ^65002$
Router(config)# ip as-path access-list 20 deny _65003_

! Route Maps
Router(config)# route-map BGP-IN permit 10
Router(config-route-map)# match ip address prefix-list CUSTOMER-
   ROUTES
Router(config-route-map)# match as-path 10
Router(config-route-map)# set local-preference 200
Router(config-route-map)# set community 65001:100
Router(config-route-map)# exit

! Apply Route Maps
Router(config-router)# neighbor 192.168.1.2 route-map BGP-IN in
Router(config-router)# neighbor 192.168.1.2 route-map BGP-OUT out
Router(config-router)# neighbor 192.168.1.2 prefix-list CUSTOMER-
   OUT out
Router(config-router)# neighbor 192.168.1.2 filter-list 10 in
```

18.4 BGP Communities

```
! Community Configuration
Router(config)# ip bgp-community new-format
Router(config)# route-map SET-COMMUNITY permit 10
Router(config-route-map)# set community 65001:100 65001:200
   additive
Router(config-route-map)# set community no-export
Router(config-route-map)# set community no-advertise
Router(config-route-map)# set community internet
Router(config-route-map)# set community local-as
Router(config-route-map)# exit

! Community Lists
Router(config)# ip community-list standard NO-EXPORT permit no-
   export
Router(config)# ip community-list expanded CUSTOMER permit
   65001:100 65001:200
Router(config)# ip community-list expanded CUSTOMER permit
   65001:300

```

```
! Match Communities
Router(config-route-map)# match community CUSTOMER
```

18.5 BGP Route Manipulation

```
! Path Selection Manipulation
! 1. Weight (Cisco proprietary, local to router)
Router(config-router)# neighbor 192.168.1.2 weight 200

! 2. Local Preference (within AS)
Router(config-route-map)# set local-preference 150

! 3. AS Path Prepending
Router(config-route-map)# set as-path prepend 65001 65001 65001

! 4. MED (between ASes)
Router(config-route-map)# set metric 100

! 5. Origin Code
Router(config-route-map)# set origin igp
Router(config-route-map)# set origin egp
Router(config-route-map)# set origin incomplete
```

18.6 BGP Verification

```
! BGP Show Commands
Router# show ip bgp
Router# show ip bgp summary
Router# show ip bgp neighbors
Router# show ip bgp neighbors 192.168.1.2
Router# show ip bgp neighbors 192.168.1.2 advertised-routes
Router# show ip bgp neighbors 192.168.1.2 received-routes
Router# show ip bgp neighbors 192.168.1.2 routes
Router# show ip bgp community
Router# show ip bgp community 65001:100
Router# show ip bgp dampened-paths
Router# show ip bgp flap-statistics
Router# show ip bgp regexp ^65001
Router# show ip bgp ipv4 unicast
Router# show ip bgp vpnv4 vrf CUSTOMER
Router# show bgp all summary
Router# show bgp l2vpn evpn

! BGP Debug Commands
Router# debug ip bgp
Router# debug ip bgp updates
Router# debug ip bgp keepalives
Router# debug ip bgp dampening
Router# debug ip bgp events
```

```
Router# debug ip bgp filters
```

19 Access Control Lists

19.1 Standard ACLs

```
! Standard Numbered ACLs (1-99, 1300-1999)
Router(config)# access-list 10 permit 192.168.1.0 0.0.0.255
Router(config)# access-list 10 permit 10.0.0.0 0.255.255.255
Router(config)# access-list 10 deny any log

! Standard Named ACLs
Router(config)# ip access-list standard MANAGEMENT
Router(config-std-nacl)# permit 192.168.100.0 0.0.0.255
Router(config-std-nacl)# permit 10.0.0.0 0.255.255.255
Router(config-std-nacl)# deny any log
Router(config-std-nacl)# exit

! Apply to Interface
Router(config-if)# ip access-group 10 in
Router(config-if)# ip access-group MANAGEMENT out
```

19.2 Extended ACLs

```
! Extended Numbered ACLs (100-199, 2000-2699)
Router(config)# access-list 100 permit tcp 192.168.1.0 0.0.0.255
   any eq 80
Router(config)# access-list 100 permit tcp 192.168.1.0 0.0.0.255
   any eq 443
Router(config)# access-list 100 permit udp 192.168.1.0 0.0.0.255
   any eq 53
Router(config)# access-list 100 permit icmp 192.168.1.0 0.0.0.255
    any echo
Router(config)# access-list 100 permit icmp 192.168.1.0 0.0.0.255
    any echo-reply
Router(config)# access-list 100 deny ip any any log

! Extended Named ACLs
Router(config)# ip access-list extended INTERNET-ACCESS
Router(config-ext-nacl)# permit tcp 192.168.1.0 0.0.0.255 any eq
   www
Router(config-ext-nacl)# permit tcp 192.168.1.0 0.0.0.255 any eq
   443
Router(config-ext-nacl)# permit udp 192.168.1.0 0.0.0.255 any eq
   domain
Router(config-ext-nacl)# permit icmp 192.168.1.0 0.0.0.255 any
Router(config-ext-nacl)# deny ip any any log-input
Router(config-ext-nacl)# exit
```

```
17
18 ! Apply to Interface
19 Router(config-if)# ip access-group INTERNET-ACCESS out
```

19.3 Advanced ACL Features

```
1  ! Time-Based ACLs
2  Router(config)# time-range WORK-HOURS
3  Router(config-time-range)# periodic weekdays 9:00 to 17:00
4  Router(config-time-range)# absolute start 00:00 1 Jan 2024 end
       23:59 31 Dec 2024
5
6  Router(config)# ip access-list extended WORK-ACL
7  Router(config-ext-nacl)# permit tcp any any eq 80 time-range WORK
       -HOURS
8  Router(config-ext-nacl)# deny ip any any
9  Router(config-ext-nacl)# exit
10
11 ! Reflexive ACLs
12 Router(config)# ip access-list extended OUTBOUND
13 Router(config-ext-nacl)# permit tcp any any reflect TCP-TRAFFIC
14 Router(config-ext-nacl)# permit udp any any reflect UDP-TRAFFIC
15 Router(config-ext-nacl)# permit icmp any any reflect ICMP-TRAFFIC
16 Router(config-ext-nacl)# exit
17
18 Router(config)# ip access-list extended INBOUND
19 Router(config-ext-nacl)# evaluate TCP-TRAFFIC
20 Router(config-ext-nacl)# evaluate UDP-TRAFFIC
21 Router(config-ext-nacl)# evaluate ICMP-TRAFFIC
22 Router(config-ext-nacl)# deny ip any any log
23 Router(config-ext-nacl)# exit
24
25 ! Dynamic/Lock-and-Key ACLs
26 Router(config)# username remote-user password RemotePass123
27 Router(config)# access-list 110 dynamic REMOTE-ACCESS timeout 120
       permit ip any any
28 Router(config)# line vty 0 4
29 Router(config-line)# login local
30 Router(config-line)# autocommand access-enable host timeout 10
```

19.4 ACL Optimization & Management

```
1  ! ACL Sequence Numbers
2  Router(config)# ip access-list extended OPTIMIZED-ACL
3  Router(config-ext-nacl)# 10 permit tcp any any eq 80
4  Router(config-ext-nacl)# 20 permit tcp any any eq 443
5  Router(config-ext-nacl)# 30 deny tcp any any eq 3389
6  Router(config-ext-nacl)# 40 permit ip any any
7  Router(config-ext-nacl)# exit
```

```
! Insert/Delete/Resequence
Router(config-ext-nacl)# 15 permit tcp any any eq 22
Router(config-ext-nacl)# no 20
Router(config-ext-nacl)# resequence 10 10 10

! ACL Logging
Router(config-ext-nacl)# permit tcp any any eq 80 log
Router(config-ext-nacl)# permit tcp any any eq 80 log-input
Router(config-ext-nacl)# deny ip any any log

! ACL Statistics
Router# show access-lists
Router# show access-lists INTERNET-ACCESS
Router# show ip access-list
Router# clear access-list counters
Router# clear access-list counters INTERNET-ACCESS
```

19.5 Infrastructure ACLs (iACLs)

```
! iACL for Infrastructure Protection
Router(config)# ip access-list extended INFRASTRUCTURE-ACL
! Permit BGP
Router(config-ext-nacl)# permit tcp host 192.168.1.2 eq bgp host
   192.168.1.1
Router(config-ext-nacl)# permit tcp host 192.168.1.2 host
   192.168.1.1 eq bgp
! Permit OSPF
Router(config-ext-nacl)# permit ospf any any
! Permit EIGRP
Router(config-ext-nacl)# permit eigrp any any
! Permit ICMP for Management
Router(config-ext-nacl)# permit icmp 192.168.100.0 0.0.0.255 any
   echo
Router(config-ext-nacl)# permit icmp 192.168.100.0 0.0.0.255 any
   echo-reply
Router(config-ext-nacl)# permit icmp 192.168.100.0 0.0.0.255 any
   ttl-exceeded
Router(config-ext-nacl)# permit icmp 192.168.100.0 0.0.0.255 any
   unreachable
! Permit SSH/HTTPS for Management
Router(config-ext-nacl)# permit tcp 192.168.100.0 0.0.0.255 any
   eq 22
Router(config-ext-nacl)# permit tcp 192.168.100.0 0.0.0.255 any
   eq 443
! Permit NTP
Router(config-ext-nacl)# permit udp 192.168.100.0 0.0.0.255 any
   eq 123
! Permit Syslog
```

```
Router(config-ext-nacl)# permit udp 192.168.100.0 0.0.0.255 any
   eq 514
! Deny and Log Everything Else
Router(config-ext-nacl)# deny ip any any log-input
Router(config-ext-nacl)# exit

! Apply iACL
Router(config-if)# ip access-group INFRASTRUCTURE-ACL in
```

20 Zone-Based Firewall

20.1 ZBFW Configuration

```
! Zone Configuration
Router(config)# zone security INSIDE
Router(config-sec-zone)# description "Trusted Internal Network"
Router(config-sec-zone)# exit

Router(config)# zone security OUTSIDE
Router(config-sec-zone)# description "Untrusted External Network"
Router(config-sec-zone)# exit

Router(config)# zone security DMZ
Router(config-sec-zone)# description "Demilitarized Zone"
Router(config-sec-zone)# exit

! Assign Interfaces to Zones
Router(config)# interface GigabitEthernet0/0
Router(config-if)# zone-member security INSIDE
Router(config-if)# exit

Router(config)# interface GigabitEthernet0/1
Router(config-if)# zone-member security OUTSIDE
Router(config-if)# exit

Router(config)# interface GigabitEthernet0/2
Router(config-if)# zone-member security DMZ
Router(config-if)# exit
```

20.2 Class Maps & Policy Maps

```
! Class Maps for Traffic Classification
Router(config)# class-map type inspect match-any INSIDE-OUTSIDE-
   CMAP
Router(config-cmap)# match protocol http
Router(config-cmap)# match protocol https
Router(config-cmap)# match protocol dns
Router(config-cmap)# match protocol icmp
```

```
Router(config-cmap)# exit

Router(config)# class-map type inspect match-any OUTSIDE-DMZ-CMAP
Router(config-cmap)# match protocol tcp
Router(config-cmap)# match access-group name DMZ-SERVERS
Router(config-cmap)# exit

! Policy Maps for Actions
Router(config)# policy-map type inspect INSIDE-OUTSIDE-PMAP
Router(config-pmap)# class type inspect INSIDE-OUTSIDE-CMAP
Router(config-pmap-c)# inspect
Router(config-pmap-c)# pass
Router(config-pmap-c)# drop log
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default
Router(config-pmap-c)# drop log
Router(config-pmap-c)# exit
Router(config-pmap)# exit

Router(config)# policy-map type inspect OUTSIDE-DMZ-PMAP
Router(config-pmap)# class type inspect OUTSIDE-DMZ-CMAP
Router(config-pmap-c)# inspect
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default
Router(config-pmap-c)# drop log
Router(config-pmap-c)# exit
Router(config-pmap)# exit
```

20.3 Zone Pairs & Service Policies

```
! Zone Pairs
Router(config)# zone-pair security INSIDE-TO-OUTSIDE source
   INSIDE destination OUTSIDE
Router(config-sec-zone-pair)# description "Internal to External
   Traffic"
Router(config-sec-zone-pair)# service-policy type inspect INSIDE-
   OUTSIDE-PMAP
Router(config-sec-zone-pair)# exit

Router(config)# zone-pair security OUTSIDE-TO-DMZ source OUTSIDE
   destination DMZ
Router(config-sec-zone-pair)# description "External to DMZ
   Traffic"
Router(config-sec-zone-pair)# service-policy type inspect OUTSIDE
   -DMZ-PMAP
Router(config-sec-zone-pair)# exit

Router(config)# zone-pair security DMZ-TO-OUTSIDE source DMZ
   destination OUTSIDE
```

```
Router(config-sec-zone-pair)# description "DMZ to External Traffic"
Router(config-sec-zone-pair)# service-policy type inspect DMZ-OUTSIDE-PMAP
Router(config-sec-zone-pair)# exit

! Default Deny (Self Zone)
Router(config)# zone-pair security SELF-TO-ANY source self destination any
Router(config-sec-zone-pair)# service-policy type inspect SELF-PMAP
Router(config-sec-zone-pair)# exit

Router(config)# zone-pair security ANY-TO-SELF source any destination self
Router(config-sec-zone-pair)# service-policy type inspect SELF-PMAP
Router(config-sec-zone-pair)# exit
```

20.4 ZBFW Parameters & Tuning

```
! Timeouts and Thresholds
Router(config)# parameter-map type inspect global
Router(config-profile)# alert on
Router(config-profile)# audit-trail on
Router(config-profile)# session total 200000
Router(config-profile)# tcp synwait-time 30
Router(config-profile)# tcp finwait-time 5
Router(config-profile)# tcp idle-time 3600
Router(config-profile)# udp idle-time 30
Router(config-profile)# dns-timeout 5
Router(config-profile)# max-incomplete high 800
Router(config-profile)# max-incomplete low 400
Router(config-profile)# one-minute high 800
Router(config-profile)# one-minute low 400
Router(config-profile)# tcp max-incomplete host 50 block-time 0
Router(config-profile)# exit

! Protocol-specific Parameters
Router(config)# parameter-map type inspect http
Router(config-profile)# protocol-violation action drop-connection log
Router(config-profile)# body-match-max-size 1024
Router(config-profile)# request-method rfc get head post put delete options trace connect
Router(config-profile)# exit
```

20.5 ZBFW Verification

```
! ZBFW Show Commands
Router# show zone security
Router# show zone-pair security
Router# show policy-map type inspect zone-pair sessions
Router# show policy-map type inspect zone-pair stats
Router# show policy-map type inspect zone-pair INSIDE-TO-OUTSIDE
Router# show zone-pair security INSIDE-TO-OUTSIDE
Router# show policy-map type inspect all
Router# show class-map type inspect
Router# show parameter-map type inspect
Router# show policy-firewall stats

! ZBFW Debug Commands
Router# debug policy-firewall
Router# debug policy-firewall events
Router# debug policy-firewall protocol
Router# debug zone-pair
Router# debug zone security

! Clear Commands
Router# clear policy-firewall stats
Router# clear policy-firewall sessions
Router# clear zone-pair counter
```

21 IPSec VPN

21.1 Site-to-Site IPSec VPN

```
! Phase 1: IKE Policy
Router(config)# crypto isakmp policy 10
Router(config-isakmp)# encryption aes 256
Router(config-isakmp)# hash sha256
Router(config-isakmp)# authentication pre-share
Router(config-isakmp)# group 14
Router(config-isakmp)# lifetime 86400
Router(config-isakmp)# exit

Router(config)# crypto isakmp key VPN-KEY-123 address 203.0.113.2
Router(config)# crypto isakmp keepalive 10 periodic

! Phase 2: IPSec Transform Set
Router(config)# crypto ipsec transform-set TS-ESP-AES256-SHA256
   esp-aes 256 esp-sha256-hmac
Router(config-crypto-trans)# mode tunnel
Router(config-crypto-trans)# exit

Router(config)# crypto ipsec transform-set TS-ESP-AES128-SHA esp-
   aes esp-sha-hmac
Router(config-crypto-trans)# mode tunnel
```

```
Router(config-crypto-trans)# exit

! IPSec Profile (New Style)
Router(config)# crypto ipsec profile IPSEC-PROFILE
Router(config-ipsec-profile)# set transform-set TS-ESP-AES256-
   SHA256
Router(config-ipsec-profile)# set pfs group14
Router(config-ipsec-profile)# set security-association lifetime
   seconds 28800
Router(config-ipsec-profile)# set security-association lifetime
   kilobytes 4608000
Router(config-ipsec-profile)# exit
```

21.2 Crypto Map Configuration

```
! Crypto Map (Traditional)
Router(config)# crypto map CRYPTO-MAP 10 ipsec-isakmp
Router(config-crypto-map)# description "VPN to Branch Office"
Router(config-crypto-map)# set peer 203.0.113.2
Router(config-crypto-map)# set transform-set TS-ESP-AES256-SHA256
Router(config-crypto-map)# set pfs group14
Router(config-crypto-map)# match address VPN-INTERESTING-TRAFFIC
Router(config-crypto-map)# set security-association lifetime
   seconds 28800
Router(config-crypto-map)# set security-association lifetime
   kilobytes 4608000
Router(config-crypto-map)# exit

! Interesting Traffic ACL
Router(config)# ip access-list extended VPN-INTERESTING-TRAFFIC
Router(config-ext-nacl)# permit ip 192.168.1.0 0.0.0.255
   192.168.2.0 0.0.0.255
Router(config-ext-nacl)# permit ip 192.168.1.0 0.0.0.255
   192.168.3.0 0.0.0.255
Router(config-ext-nacl)# exit

! Apply Crypto Map to Interface
Router(config)# interface GigabitEthernet0/0
Router(config-if)# crypto map CRYPTO-MAP
Router(config-if)# exit
```

21.3 VTI (Virtual Tunnel Interface)

```
! VTI Configuration
Router(config)# interface Tunnel0
Router(config-if)# description "VTI to Branch Office"
Router(config-if)# ip address 10.255.255.1 255.255.255.252
Router(config-if)# tunnel source GigabitEthernet0/0
Router(config-if)# tunnel destination 203.0.113.2
```

```
Router(config-if)# tunnel mode ipsec ipv4
Router(config-if)# tunnel protection ipsec profile IPSEC-PROFILE
Router(config-if)# exit

! Static Route over VTI
Router(config)# ip route 192.168.2.0 255.255.255.0 Tunnel0
Router(config)# ip route 192.168.3.0 255.255.255.0 Tunnel0
```

21.4 DMVPN Configuration

```
! DMVPN Phase 3
Router(config)# interface Tunnel100
Router(config-if)# description "DMVPN Hub"
Router(config-if)# ip address 10.255.255.1 255.255.255.0
Router(config-if)# ip mtu 1400
Router(config-if)# ip nhrp authentication DMVPN-KEY
Router(config-if)# ip nhrp map multicast dynamic
Router(config-if)# ip nhrp network-id 100
Router(config-if)# ip nhrp redirect
Router(config-if)# ip tcp adjust-mss 1360
Router(config-if)# tunnel source GigabitEthernet0/0
Router(config-if)# tunnel mode gre multipoint
Router(config-if)# tunnel key 100
Router(config-if)# tunnel protection ipsec profile IPSEC-PROFILE
Router(config-if)# exit

! DMVPN Spoke
Router(config)# interface Tunnel100
Router(config-if)# description "DMVPN Spoke"
Router(config-if)# ip address 10.255.255.2 255.255.255.0
Router(config-if)# ip mtu 1400
Router(config-if)# ip nhrp authentication DMVPN-KEY
Router(config-if)# ip nhrp map 10.255.255.1 203.0.113.1
Router(config-if)# ip nhrp map multicast 203.0.113.1
Router(config-if)# ip nhrp network-id 100
Router(config-if)# ip nhrp nhs 10.255.255.1
Router(config-if)# ip nhrp registration timeout 300
Router(config-if)# ip nhrp shortcut
Router(config-if)# ip tcp adjust-mss 1360
Router(config-if)# tunnel source GigabitEthernet0/0
Router(config-if)# tunnel mode gre multipoint
Router(config-if)# tunnel key 100
Router(config-if)# tunnel protection ipsec profile IPSEC-PROFILE
Router(config-if)# exit
```

21.5 GETVPN Configuration

```
! GETVPN Key Server
Router(config)# crypto gdoi group GETVPN-GROUP
```

```
Router(config-gdoi-group)# identity number 100
Router(config-gdoi-group)# server local
Router(config-gdoi-group-server)# rekey lifetime seconds 86400
Router(config-gdoi-group-server)# rekey retransmit 10 number 3
Router(config-gdoi-group-server)# rekey authentication mypubkey
   rsa GETVPN-KEYS
Router(config-gdoi-group-server)# rekey transport unicast
Router(config-gdoi-group-server)# sa ipsec 1
Router(config-gdoi-group-server-sa)# profile IPSEC-PROFILE
Router(config-gdoi-group-server-sa)# match address ipv4 GETVPN-
   ACL
Router(config-gdoi-group-server-sa)# replay counter window-size
   64
Router(config-gdoi-group-server-sa)# exit
Router(config-gdoi-group-server)# address ipv4 192.168.100.10
Router(config-gdoi-group-server)# exit
Router(config-gdoi-group)# exit

! GETVPN Group Member
Router(config)# crypto gdoi group GETVPN-GROUP
Router(config-gdoi-group)# identity number 100
Router(config-gdoi-group)# server address ipv4 192.168.100.10
Router(config-gdoi-group)# exit

Router(config)# interface Tunnel0
Router(config-if)# tunnel mode ipsec ipv4
Router(config-if)# tunnel protection gdoi profile GETVPN-GROUP
```

21.6 IPSec Verification

```
! IPSec Show Commands
Router# show crypto isakmp sa
Router# show crypto isakmp peers
Router# show crypto ipsec sa
Router# show crypto ipsec sa detail
Router# show crypto ipsec sa interface GigabitEthernet0/0
Router# show crypto session
Router# show crypto session detail
Router# show crypto engine connections active
Router# show crypto map
Router# show crypto map interface GigabitEthernet0/0
Router# show crypto gdoi
Router# show crypto gdoi ks
Router# show crypto gdoi gm
Router# show dmvpn
Router# show dmvpn detail
Router# show nhrp
Router# show nhrp traffic

! IPSec Debug Commands
```

```
Router# debug crypto isakmp
Router# debug crypto ipsec
Router# debug crypto engine
Router# debug crypto gdoi
Router# debug nhrp
Router# debug tunnel

! Clear Commands
Router# clear crypto isakmp
Router# clear crypto sa
Router# clear crypto session
Router# clear crypto gdoi
```

22 VoIP Configuration

22.1 VoIP Basics

```
! DHCP for VoIP Phones
Router(config)# ip dhcp pool VOICE-POOL
Router(dhcp-config)# network 10.10.0.0 255.255.255.0
Router(dhcp-config)# default-router 10.10.0.1
Router(dhcp-config)# option 150 ip 10.0.0.10  ! Call Manager
Router(dhcp-config)# option 66 ip 10.0.0.10   ! TFTP Server
Router(dhcp-config)# lease 8
Router(dhcp-config)# exit

! Voice VLAN Configuration
Switch(config)# vlan 110
Switch(config-vlan)# name VOICE
Switch(config-vlan)# exit

Switch(config)# interface gigabitEthernet 1/0/1
Switch(config-if)# switchport voice vlan 110
Switch(config-if)# switchport priority extend cos 0
Switch(config-if)# auto qos voip trust
Switch(config-if)# spanning-tree portfast
Switch(config-if)# spanning-tree bpduguard enable
```

22.2 Call Manager Express

```
! CME Basic Configuration
Router(config)# telephony-service
Router(config-telephony)# max-ephones 24
Router(config-telephony)# max-dn 48
Router(config-telephony)# ip source-address 10.0.0.1 port 2000
Router(config-telephony)# auto assign 1 to 24
Router(config-telephony)# system message "Company Phone System"
Router(config-telephony)# voicemail 5000
```

```
Router(config-telephony)# max-conferences 8 gain -6
Router(config-telephony)# transfer-system full-consult
Router(config-telephony)# exit

! Ephone Configuration
Router(config)# ephone-dn 1 dual-line
Router(config-ephone-dn)# number 1001
Router(config-ephone-dn)# name "John Doe"
Router(config-ephone-dn)# exit

Router(config)# ephone 1
Router(config-ephone)# device-security-mode
Router(config-ephone)# mac-address 0050.7966.6800
Router(config-ephone)# type 7960
Router(config-ephone)# button 1:1
Router(config-ephone)# exit
```

22.3 Dial Peers

```
! POTS Dial Peers
Router(config)# dial-peer voice 1 pots
Router(config-dial-peer)# destination-pattern 9T
Router(config-dial-peer)# port 0/0/0:23
Router(config-dial-peer)# forward-digits all
Router(config-dial-peer)# exit

! VoIP Dial Peers
Router(config)# dial-peer voice 100 voip
Router(config-dial-peer)# destination-pattern 2...
Router(config-dial-peer)# session target ipv4:10.0.0.2
Router(config-dial-peer)# codec g711ulaw
Router(config-dial-peer)# dtmf-relay h245-alphanumeric
Router(config-dial-peer)# fax rate disable
Router(config-dial-peer)# exit

! SIP Trunk Configuration
Router(config)# voice service voip
Router(config-voi-serv)# allow-connections sip to sip
Router(config-voi-serv)# sip
Router(config-voi-serv-sip)# bind control source-interface
   Loopback0
Router(config-voi-serv-sip)# bind media source-interface
   Loopback0
Router(config-voi-serv-sip)# registrar server expires max 3600
   min 3600
Router(config-voi-serv-sip)# exit
```

23 QoS Implementation

23.1 QoS Classification & Marking

```
! Class Maps
Router(config)# class-map match-any VOICE
Router(config-cmap)# match dscp ef
Router(config-cmap)# match ip rtp 16384 16383
Router(config-cmap)# exit

Router(config)# class-map match-any VIDEO
Router(config-cmap)# match dscp af41 af42 af43
Router(config-cmap)# match ip precedence 4
Router(config-cmap)# exit

Router(config)# class-map match-any CALL-SIGNALING
Router(config-cmap)# match dscp cs3
Router(config-cmap)# match dscp af31
Router(config-cmap)# exit

Router(config)# class-map match-any INTERACTIVE-VIDEO
Router(config-cmap)# match dscp af21 af22 af23
Router(config-cmap)# exit

Router(config)# class-map match-any NETWORK-CONTROL
Router(config-cmap)# match dscp cs6
Router(config-cmap)# exit

Router(config)# class-map match-any BULK-DATA
Router(config-cmap)# match dscp af11 af12 af13
Router(config-cmap)# exit

Router(config)# class-map match-any SCAVENGER
Router(config-cmap)# match dscp cs1
Router(config-cmap)# exit
```

23.2 Policy Maps

```
! LLQ for Voice and Video
Router(config)# policy-map WAN-EDGE-POLICY
Router(config-pmap)# class VOICE
Router(config-pmap-c)# priority percent 10
Router(config-pmap-c)# exit
Router(config-pmap)# class VIDEO
Router(config-pmap-c)# priority percent 23
Router(config-pmap-c)# exit
Router(config-pmap)# class CALL-SIGNALING
Router(config-pmap-c)# bandwidth percent 5
Router(config-pmap-c)# exit
```

```
Router(config-pmap)# class INTERACTIVE-VIDEO
Router(config-pmap-c)# bandwidth percent 10
Router(config-pmap-c)# random-detect
Router(config-pmap-c)# exit
Router(config-pmap)# class NETWORK-CONTROL
Router(config-pmap-c)# bandwidth percent 5
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default
Router(config-pmap-c)# bandwidth remaining percent 25
Router(config-pmap-c)# random-detect
Router(config-pmap-c)# exit
Router(config-pmap)# exit
```

23.3 AutoQoS

```
! AutoQoS VoIP
Router(config)# interface GigabitEthernet0/0
Router(config-if)# auto qos voip trust
Router(config-if)# service-policy output AUTOQOS-POLICY
Router(config-if)# exit

! AutoQoS for Enterprise
Router(config-if)# auto qos trust dscp
Router(config-if)# auto discovery qos

! Verification
Router# show auto qos
Router# show auto discovery qos
Router# show policy-map interface GigabitEthernet0/0
```

23.4 QoS Verification

```
! QoS Show Commands
Router# show policy-map
Router# show policy-map interface
Router# show policy-map interface GigabitEthernet0/0 input
Router# show policy-map interface GigabitEthernet0/0 output
Router# show class-map
Router# show mls qos
Router# show mls qos interface
Router# show mls qos maps
Router# show mls qos statistics
Router# show mls qos queueing
Router# show queueing interface GigabitEthernet0/0

! QoS Debug Commands
Router# debug qos
Router# debug policy-firewall
Router# debug nbar
```

24 Wireless Networking

24.1 WLC Configuration

```
! WLC Basic Setup
WLC(config)# config interface create MANAGEMENT 99 192.168.99.10
   255.255.255.0 192.168.99.1
WLC(config)# config interface create GUEST 100 192.168.100.10
   255.255.255.0 192.168.100.1
WLC(config)# config interface create CORPORATE 10 192.168.10.10
   255.255.255.0 192.168.10.1

! Management User
WLC(config)# config mgmtuser add admin AdminPass123! read-write
WLC(config)# config mgmtuser add operator Oper@tor123 read-only

! WLAN Configuration
WLC(config)# config wlan create 1 CORPORATE-WIFI
WLC(config-wlan)# config wlan ssid 1 CORPORATE-WIFI
WLC(config-wlan)# config wlan interface 1 CORPORATE
WLC(config-wlan)# config wlan security wpa akm psk set-key ascii
   WiF1-Passw0rd 1
WLC(config-wlan)# config wlan security wpa akm psk enable 1
WLC(config-wlan)# config wlan enable 1
WLC(config-wlan)# exit

! Guest WLAN
WLC(config)# config wlan create 2 GUEST-WIFI
WLC(config-wlan)# config wlan ssid 2 GUEST-WIFI
WLC(config-wlan)# config wlan interface 2 GUEST
WLC(config-wlan)# config wlan security web-auth enable 2
WLC(config-wlan)# config wlan security web-auth parameter-map
   GUEST-PARAMS 2
WLC(config-wlan)# config wlan enable 2
WLC(config-wlan)# exit
```

24.2 AP Management

```
! AP Configuration
WLC(config)# config ap mode local AP01
WLC(config)# config ap primary-base WLC01 AP01 192.168.99.10
WLC(config)# config ap country US AP01
WLC(config)# config ap group-name FLOOR1 AP01
WLC(config)# config ap name AP01 0050.7966.6800
WLC(config)# config ap tx-power 1 AP01
WLC(config)# config ap led-state enable AP01

! AP Groups
WLC(config)# config wlan apgroup add-profile AP-GROUP
```

```
WLC(config)# config wlan apgroup add-profile AP-GROUP-FLOOR1
WLC(config-apgroup)# config wlan apgroup interface-mapping add AP-GROUP-FLOOR1 1 CORPORATE
WLC(config-apgroup)# config wlan apgroup interface-mapping add AP-GROUP-FLOOR1 2 GUEST
WLC(config-apgroup)# config ap group-name AP-GROUP-FLOOR1 AP01
```

24.3 Wireless Security

```
! WPA2-Enterprise
WLC(config)# config wlan security wpa akm 802.1x enable 1
WLC(config)# config wlan security wpa wpa2 enable 1
WLC(config)# config wlan security dot1x authentication-server 1 192.168.100.20
WLC(config)# config wlan security dot1x accounting-server 1 192.168.100.20

! WPA3 Configuration
WLC(config)# config wlan security wpa akm sae enable 1
WLC(config)# config wlan security wpa wpa3 enable 1
WLC(config)# config wlan security wpa akm sae psk set-key ascii WPA3-Passw0rd 1

! MAC Filtering
WLC(config)# config macfilter add 0050.7966.6800 "CEO iPhone"
WLC(config)# config wlan macfilter 1 enable
```

24.4 Wireless Troubleshooting

```
! WLC Show Commands
WLC# show ap summary
WLC# show ap config general AP01
WLC# show wlan summary
WLC# show wlan 1
WLC# show client summary
WLC# show client detail 0050.7966.6800
WLC# show interface summary
WLC# show interface detail MANAGEMENT
WLC# show mobility summary
WLC# show mobility anchor
WLC# show radius summary
WLC# show mesh summary
WLC# show cdp neighbors
WLC# show log

! Debug Commands
WLC# debug client 0050.7966.6800
WLC# debug dot1x events enable
WLC# debug wps events enable
```

```
WLC# debug mobility handoff enable
WLC# debug aaa events enable
```

25 Data Center Technologies

25.1 Nexus Switching

```
! Nexus Basic Configuration
Nexus(config)# feature interface-vlan
Nexus(config)# feature lacp
Nexus(config)# feature vpc
Nexus(config)# feature ospf
Nexus(config)# feature bgp
Nexus(config)# feature ssh

! VPC Configuration
Nexus(config)# vpc domain 1
Nexus(config-vpc-domain)# peer-keepalive destination 10.0.0.2
   source 10.0.0.1
Nexus(config-vpc-domain)# peer-gateway
Nexus(config-vpc-domain)# auto-recovery
Nexus(config-vpc-domain)# ip arp synchronize
Nexus(config-vpc-domain)# delay restore 300
Nexus(config-vpc-domain)# exit

Nexus(config)# interface port-channel 10
Nexus(config-if)# vpc 10
Nexus(config-if)# switchport mode trunk
Nexus(config-if)# switchport trunk allowed vlan 10,20,30
Nexus(config-if)# spanning-tree port type network
Nexus(config-if)# exit
```

25.2 FCoE Configuration

```
! FCoE Setup
Nexus(config)# feature fcoe
Nexus(config)# vsan database
Nexus(config-vsan-db)# vsan 100
Nexus(config-vsan-db)# exit

Nexus(config)# interface fc1/1
Nexus(config-if)# switchport mode f
Nexus(config-if)# switchport trunk allowed vsan 100
Nexus(config-if)# no shutdown
Nexus(config-if)# exit

Nexus(config)# fcoe vsan 100
```

26.2 MPLS L3VPN

```
! VRF Configuration
Router(config)# ip vrf CUSTOMER-A
Router(config-vrf)# rd 65001:100
Router(config-vrf)# route-target export 65001:100
Router(config-vrf)# route-target import 65001:100
Router(config-vrf)# exit

! VRF Interface
Router(config)# interface GigabitEthernet0/0.100
Router(config-if)# encapsulation dot1Q 100
Router(config-if)# ip vrf forwarding CUSTOMER-A
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# exit

! MP-BGP for VPNv4
Router(config)# router bgp 65001
Router(config-router)# neighbor 2.2.2.2 remote-as 65001
Router(config-router)# neighbor 2.2.2.2 update-source Loopback0
Router(config-router)# address-family vpnv4
Router(config-router-af)# neighbor 2.2.2.2 activate
Router(config-router-af)# neighbor 2.2.2.2 send-community
   extended
Router(config-router-af)# exit-address-family
Router(config-router)# address-family ipv4 vrf CUSTOMER-A
Router(config-router-af)# redistribute connected
Router(config-router-af)# redistribute static
Router(config-router-af)# exit-address-family
```

27 Systematic Troubleshooting

27.1 OSI Model Troubleshooting

```
! Layer 1 - Physical
Router# show interfaces status
Router# show interfaces description
Router# show controllers
Router# show environment
Router# show power
Router# show module

! Layer 2 - Data Link
Router# show interfaces
Router# show interfaces trunk
Router# show spanning-tree
Router# show vlan
Router# show mac address-table
Router# show cdp neighbors
```

```
Router# show lldp neighbors

! Layer 3 - Network
Router# show ip interface brief
Router# show ip route
Router# show ip protocols
Router# show ip ospf neighbor
Router# show ip eigrp neighbors
Router# show ip bgp summary
Router# show arp

! Layer 4 - Transport
Router# show tcp brief
Router# show tcp statistics
Router# show udp

! Layer 7 - Application
Router# show logging
Router# show processes cpu
Router# show memory
Router# show buffers
```

27.2 Troubleshooting Methodology

```
! 1. Define the Problem
! 2. Gather Information
Router# show tech-support
Router# show logging
Router# show clock
Router# show version

! 3. Analyze Information
Router# show processes cpu sorted
Router# show memory
Router# show interfaces counters errors
Router# show buffers

! 4. Eliminate Possibilities
Router# traceroute 8.8.8.8
Router# ping 8.8.8.8
Router# pathping 8.8.8.8

! 5. Propose Hypothesis
! 6. Test Hypothesis
Router# debug ip packet
Router# debug ip ospf events
Router# debug ip eigrp
Router# debug ip bgp updates

! 7. Solve the Problem
```

```
Router# reload
Router# clear ip route *
Router# clear arp
Router# clear mac address-table

! 8. Document Solution
Router# show running-config
Router# copy running-config startup-config
```

27.3 Common Troubleshooting Commands

```
! Connectivity Testing
Router# ping 8.8.8.8
Router# ping 8.8.8.8 source Loopback0
Router# ping 8.8.8.8 size 1500 df-bit
Router# ping ipv6 2001:db8::1
Router# traceroute 8.8.8.8
Router# traceroute ipv6 2001:db8::1
Router# pathping 8.8.8.8

! Packet Capture
Router# monitor capture CAP interface GigabitEthernet0/0 both
Router# monitor capture CAP match ipv4 any any
Router# monitor capture CAP start
! ... wait for traffic ...
Router# monitor capture CAP stop
Router# monitor capture CAP export flash:capture.pcap

! Performance Monitoring
Router# show processes cpu history
Router# show processes cpu sorted
Router# show processes memory
Router# show memory statistics
Router# show interfaces statistics
Router# show platform cpu packet statistics
Router# show platform hardware qfp active statistics drop
```

27.4 Debug Commands

```
! Selective Debugging
Router# debug ip packet detail  ! CAUTION: Very verbose!
Router# debug condition interface GigabitEthernet0/0
Router# debug condition ip 192.168.1.1
Router# debug ip ospf hello
Router# debug ip eigrp packets
Router# debug ip bgp updates
Router# debug ppp negotiation
Router# debug isdn q921
Router# debug dialer
```

```
Router# debug frame-relay lmi

! Control Debug Output
Router# terminal monitor
Router# terminal no monitor
Router# undebug all
Router# no debug all
Router# debug sanity  ! Check debug impact

! Log Debug to Buffer
Router# logging buffered 100000 debugging
Router# show logging
```

28 Best Practices

28.1 Configuration Management

```
! Configuration Archive Best Practices
Router(config)# archive
Router(config-archive)# path flash:archive-$h
Router(config-archive)# write-memory
Router(config-archive)# time-period 1440
Router(config-archive)# maximum 14
Router(config-archive)# exit

! Automated Backups
Router(config)# kron policy-list BACKUP
Router(config-kron-policy)# cli write memory
Router(config-kron-policy)# cli copy running-config tftp
   ://192.168.100.10/backups/$h-config
Router(config-kron-policy)# exit

Router(config)# kron occurrence DAILY-BACKUP at 2:00 recurring
Router(config-kron-occurrence)# policy-list BACKUP
Router(config-kron-occurrence)# exit
```

28.2 Security Hardening

```
! Security Checklist
! 1. Disable Unused Services
no service pad
no ip source-route
no ip bootp server
no service tcp-small-servers
no service udp-small-servers
no ip http server
no ip http secure-server
no cdp run
```

```
no lldp run

! 2. Enable Password Encryption
service password-encryption
enable secret [strong-password]
security passwords min-length 12

! 3. Configure AAA
aaa new-model
aaa authentication login default local
aaa authorization exec default local
username admin privilege 15 secret [hash]

! 4. Enable SSH
ip domain-name company.com
crypto key generate rsa modulus 2048
ip ssh version 2
ip ssh time-out 60
ip ssh authentication-retries 2

! 5. Configure Logging
logging host 192.168.100.10
logging trap debugging
logging source-interface Loopback0

! 6. Implement ACLs
! 7. Enable NTP
! 8. Regular Updates
```

28.3 Performance Optimization

```
! CPU Optimization
Router(config)# process cpu threshold type total rising 80
   interval 5 falling 70 interval 5
Router(config)# ip cef
Router(config)# mls cef

! Memory Optimization
Router(config)# memory reserve critical 4096
Router(config)# buffers small permanent 100
Router(config)# buffers middle permanent 100
Router(config)# buffers big permanent 100

! Interface Optimization
Router(config-if)# no ip route-cache cef
Router(config-if)# ip tcp adjust-mss 1360
Router(config-if)# ip mtu 1500
Router(config-if)# keepalive 10

! Routing Optimization
```

```
Router(config-router)# timers basic 5 15 5 40
Router(config-router)# maximum-paths 4
Router(config-router)# traffic-share balanced
```

28.4 Documentation Standards

```
! Configuration Header
!
! Device: R1-CORE
! Location: Data Center Rack A1
! Purpose: Core Router for Company Network
! Contact: Network Operations (noc@company.com)
! Last Modified: 2024-01-01 by John Doe
! Change Ticket: NET-2024-001
!
! Interface Descriptions
interface GigabitEthernet0/0
 description Uplink to ISP1 - Circuit ID: ISP-001
interface GigabitEthernet0/1
 description Uplink to ISP2 - Circuit ID: ISP-002
interface Loopback0
 description Router ID and Management
!
! VLAN Documentation
vlan 10
 name SALES
 description Sales Department VLAN
!
! ACL Documentation
ip access-list extended INTERNET-ACCESS
 remark Allow HTTP/HTTPS from Internal Network
 remark Allow DNS queries
 remark Deny and log all other traffic
!
! Routing Documentation
router ospf 100
 ! Area 0 - Backbone Area
 ! Area 1 - Branch Offices (Stub)
 ! Area 2 - Data Center (NSSA)
!
! BGP Documentation
router bgp 65001
 ! eBGP with ISP1 (AS 65002)
 ! eBGP with ISP2 (AS 65003)
 ! iBGP with Internal Routers
!
```

29 Common Issues & Fixes

29.1 Interface Issues

```
! Interface Won't Come Up
! 1. Check Physical Connection
Router# show interfaces gigabitEthernet 0/0
! Look for: administratively down, line protocol down

! 2. Enable Interface
Router(config)# interface gigabitEthernet 0/0
Router(config-if)# no shutdown

! 3. Check Speed/Duplex
Router# show interfaces gigabitEthernet 0/0 status
Router(config-if)# speed 1000
Router(config-if)# duplex full
Router(config-if)# negotiation auto

! 4. Check VLAN Configuration
Router# show interfaces gigabitEthernet 0/0 switchport
Router(config-if)# switchport mode access
Router(config-if)# switchport access vlan 10

! 5. Check Errors
Router# show interfaces gigabitEthernet 0/0 counters errors
Router# clear counters gigabitEthernet 0/0
```

29.2 Routing Issues

```
! OSPF Neighbor Not Forming
! 1. Check Connectivity
Router# ping <neighbor-ip>

! 2. Check OSPF Parameters
Router# show ip ospf interface gigabitEthernet 0/0
! Verify: Area, Hello/Dead Timers, Authentication

! 3. Check Network Type
Router# show ip ospf interface gigabitEthernet 0/0
Router(config-if)# ip ospf network point-to-point

! 4. Check ACLs/Firewall
Router# show ip access-lists
Router# show zone-pair security

! 5. Debug OSPF
Router# debug ip ospf adj
Router# debug ip ospf hello
```

```
! BGP Peer Not Coming Up
! 1. Check TCP Connectivity
Router# telnet <peer-ip> 179

! 2. Check BGP Parameters
Router# show ip bgp neighbors
! Verify: AS Number, Authentication, Timers

! 3. Check Route to Peer
Router# show ip route <peer-ip>
Router(config)# ip route <peer-ip> 255.255.255.255 <next-hop>

! 4. Debug BGP
Router# debug ip bgp
Router# debug ip tcp transactions
```

29.3 VPN Issues

```
! IPSec VPN Not Establishing
! 1. Check Connectivity
Router# ping <peer-ip>

! 2. Check IKE Policy
Router# show crypto isakmp policy
! Verify: Encryption, Hash, DH Group, Lifetime

! 3. Check Transform Sets
Router# show crypto ipsec transform-set
! Verify: Encryption, Hash, Mode

! 4. Check Interesting Traffic
Router# show crypto map
Router# show access-lists

! 5. Check NAT/Traversal
Router(config-if)# ip nat inside
Router(config-if)# ip nat outside
Router# debug crypto isakmp
Router# debug crypto ipsec
```

29.4 Switching Issues

```
! VLAN Issues
! 1. Check VLAN Configuration
Switch# show vlan brief
Switch# show vlan id 10

! 2. Check Trunk Configuration
```

```
Switch# show interfaces trunk
Switch# show interfaces gigabitEthernet 1/0/24 switchport

! 3. Check STP
Switch# show spanning-tree vlan 10
Switch# show spanning-tree inconsistentports

! 4. Check VTP
Switch# show vtp status
Switch# show vtp password

! EtherChannel Issues
! 1. Check Channel Group
Switch# show etherchannel summary
Switch# show etherchannel port-channel

! 2. Check Protocol
Switch# show lacp neighbor
Switch# show pagp neighbor

! 3. Check Configuration Consistency
Switch# show running-config interface port-channel 1
Switch# show running-config interface gigabitEthernet 1/0/1
Switch# show running-config interface gigabitEthernet 1/0/2
```

29.5 Performance Issues

```
! High CPU Utilization
! 1. Identify Process
Router# show processes cpu sorted
Router# show processes cpu history

! 2. Check for Broadcast Storms
Router# show interfaces counters broadcast
Switch# show storm-control

! 3. Check for Loops
Router# show spanning-tree
Switch# show spanning-tree inconsistentports

! 4. Check Routing Protocols
Router# show ip ospf neighbor
Router# show ip bgp summary
Router# debug ip routing

! High Memory Usage
Router# show memory
Router# show memory statistics
Router# show buffers
Router# show processes memory
```