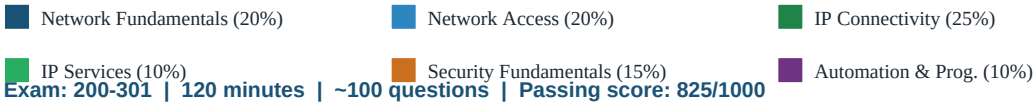
Page 1: CCNA 200-301 Overview & Exam Blueprint

Your roadmap to Cisco Certified Network Associate certification



Exam: 200-301 | 120 minutes | ~100 questions | Passing score: 825/1000

Question types: Multiple choice, drag-and-drop, fill-in, simlets, simulations

No partial credit | Questions can be flagged for review

■ EXAM DOMAINS & WEIGHTS

Domain	%	Key Topics
1. Network Fundamentals	20%	OSI, TCP/IP, Ethernet, IPv4/6, Wireless
2. Network Access	20%	VLANs, Trunking, STP, EtherChannel, Wireless
3. IP Connectivity	25%	Routing, OSPF, Static routes, IPv6
4. IP Services	10%	NAT, DHCP, DNS, NTP, QoS, SNMP
5. Security Fundamentals	15%	ACLs, AAA, VPN, Threat types, Port security
6. Automation & Programmability	10%	REST API, JSON, YANG, Puppet, Chef, Ansible

■ STUDY STRATEGY

- **Week 1-2:** Fundamentals — OSI, TCP/IP, IPv4, subnetting. Master binary math!
- **Week 3-4:** Switching — VLANs, STP, EtherChannel. Build a lab in Packet Tracer.
- **Week 5-6:** Routing — OSPF, static routes, NAT, DHCP, ACLs.
- **Week 7-8:** Security, Wireless, Automation. Practice exams daily.
- **Week 9:** Review weak areas. Take 3+ full practice exams. Aim for 85%+.

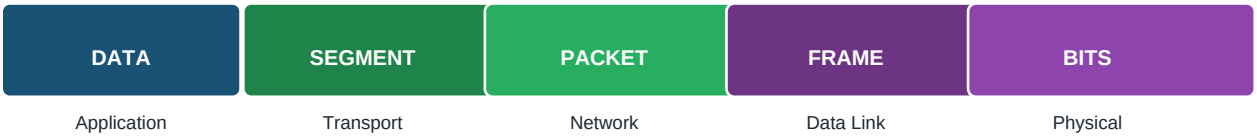
■ EXAM ALERT: Questions include simulations (simlets) — practice CLI commands in Packet Tracer or GNS3!

■ ***MEMORY TRICK:*** *"Never Ask For Small Purple Donuts At All" → Never, Access, For, Small, Purple, Donuts, All = 6 CCNA domains*

Page 2: Network Fundamentals

OSI vs TCP/IP models and the encapsulation process

■ ENCAPSULATION PROCESS



Encapsulation: Data → Segment → Packet → Frame → Bits

■ OSI vs TCP/IP Comparison

OSI Layer	OSI Name	TCP/IP Layer	Protocols/Examples
7	Application	Application	HTTP, HTTPS, FTP, DNS, SMTP, Telnet
6	Presentation	Application	SSL/TLS, ASCII, JPEG, Encryption
5	Session	Application	NetBIOS, RPC, SQL sessions
4	Transport	Transport	TCP (reliable), UDP (fast)
3	Network	Internet	IP, ICMP, OSPF, BGP
2	Data Link	Network Access	Ethernet, Wi-Fi (802.11), ARP
1	Physical	Network Access	Cables, Fiber, Hubs, Repeaters

TCP

- Connection-oriented (3-way handshake)
- Reliable delivery + error recovery
- Flow control (windowing)
- Sequencing & acknowledgments
- Uses: HTTP, FTP, SMTP, SSH

UDP

- Connectionless — no handshake
- Best-effort, no retransmission
- Lower overhead, faster
- No sequencing
- Uses: DNS, DHCP, TFTP, VoIP, Video

■ EXAM ALERT: TCP SYN→SYN-ACK→ACK = 3-way hands

■ MEMORY TRICK: *"Unreliable Delivery Protocol" = UDP*

Page 3: OSI Model Deep Dive

Layer-by-layer breakdown with protocols, PDUs, and devices

L7	Application	HTTP, FTP, DNS, SMTP
L6	Presentation	SSL/TLS, Encryption, Compression
L5	Session	NetBIOS, RPC, PPTP
L4	Transport	TCP, UDP — Segments
L3	Network	IP, ICMP, OSPF — Packets
L2	Data Link	Ethernet, MAC — Frames
L1	Physical	Cables, Hubs, NIC — Bits

■ OSI LAYER REFERENCE TABLE

L#	Name	PDU	Key Protocols	Devices
7	Application	Data	HTTP(80) HTTPS(443) FTP(21) DNS(53)	Hosts, Servers
6	Presentation	Data	SSL/TLS, JPEG, MPEG, ASCII, Encryption	Hosts
5	Session	Data	NetBIOS, RPC, SQL, PPTP	Hosts
4	Transport	Segment	TCP, UDP — Port numbers	Firewalls, L4 LB
3	Network	Packet	IP, ICMP, OSPF, BGP, ARP*	Routers, L3 SW
2	Data Link	Frame	Ethernet, 802.11, PPP, HDLC	Switches, Bridges
1	Physical	Bits	V.35, DSL, 802.3, TIA-568	Hubs, Cables, NIC

■ ***MEMORY TRICK:*** *"All People Seem To Need Data Processing" (L7→L1) or "Please Do Not Throw Sausage Pizza Away" (L1→L7)*

■ COMMON PORT NUMBERS

Protocol	Port	Transport	Protocol	Port	Transport
FTP Data	20	TCP	DNS	53	TCP/UDP
FTP Control	21	TCP	DHCP Server	67	UDP
SSH	22	TCP	DHCP Client	68	UDP
Telnet	23	TCP	HTTP	80	TCP
SMTP	25	TCP	HTTPS	443	TCP
TFTP	69	UDP	SNMP	161	UDP
NTP	123	UDP	Syslog	514	UDP

■ **EXAM ALERT: Know these ports! FTP=20/21, SSH=22, Telnet=23, SMTP=25, DNS=53, HTTP=80, HTTPS=443**

Page 4: Ethernet & MAC Addressing

Frame structure, MAC learning, and switching operation

■ ETHERNET FRAME STRUCTURE

Preamble 7B	SFD 1B	Dst MAC 6B	Src MAC 6B	Type/Len 2B	Data/Payload 46-1500B	FCS 4B

■ MAC ADDRESS STRUCTURE

MAC = 48-bit / 6-byte hexadecimal address burned into NIC (BIA)

Format: **`AA:BB:CC:DD:EE:FF`** or **`AABB.CCDD.EEFF`** (Cisco notation)

OUI (First 3 bytes)	Device ID (Last 3 bytes)
AA:BB:CC	DD:EE:FF
Organizationally Unique ID	Assigned by manufacturer
Identifies vendor (Cisco, Intel…)	Unique per device

■ MAC TABLE LEARNING (CAM TABLE)

1. Frame arrives on port — switch reads SOURCE MAC
2. If source MAC not in CAM table → ADD it (port + VLAN)
3. Check DESTINATION MAC in CAM table:
   • Found → UNICAST forward to that port only
   • Not found → FLOOD to all ports except ingress (unknown unicast)
4. Broadcasts (FF:FF:FF:FF:FF:FF) → always flooded
5. CAM entries age out after 300 seconds (default)

■ EXAM ALERT: "Unknown unicast flooding" ≠ broadcast. Switch floods ONLY when destination MAC is unknown.

```
SW1# show mac address-table
SW1# show mac address-table dynamic
SW1# clear mac address-table dynamic
```

Page 5: IPv4 Addressing

Address classes, private ranges, binary math, and CIDR

■ IPv4 ADDRESS CLASSES

Class	Range	Default Mask	Private Range	Use
A	1.0.0.0–126.x.x.x	255.0.0.0 /8	10.0.0.0/8	Large networks
B	128.0.0.0–191.255.x.x	255.255.0.0 /16	172.16.0.0/12	Medium networks
C	192.0.0.0–223.255.255.x	255.255.255.0 /24	192.168.0.0/16	Small networks
D	224.0.0.0–239.x.x.x	N/A	N/A	Multicast
E	240.0.0.0–255.x.x.x	N/A	N/A	Experimental

Special Addresses: 127.0.0.1 (loopback) | 169.254.x.x (APIPA) | 0.0.0.0 (any)

■ BINARY QUICK REFERENCE

Bit Position	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Value	128	64	32	16	8	4	2	1

Example: `11000000` = 128+64 = **192**

Example: `10101000` = 128+32+8 = **168**

Example: `00001010` = 8+2 = **10**

■ SUBNET MASK → CIDR QUICK REFERENCE

CIDR	Subnet Mask	Hosts	CIDR	Subnet Mask	Hosts
/8	255.0.0.0	16,777,214	/25	255.255.255.128	126
/16	255.255.0.0	65,534	/26	255.255.255.192	62
/24	255.255.255.0	254	/27	255.255.255.224	30
/28	255.255.255.240	14	/29	255.255.255.248	6
/30	255.255.255.252	2	/32	255.255.255.255	1 (host)

■ EXAM ALERT: IPv4 header = 20 bytes minimum. TTL field prevents infinite loops. Default TTL=64 (Linux), 128 (Windows), 255 (Cisco)

Page 6: Subnetting Mastery

CIDR notation, magic numbers, and rapid subnet calculation

■ SUBNETTING VISUAL BREAKDOWN

Example: 192.168.10.0/24

11000000	10101000	00001010	00000000
Net	Net	Net	Host
192	168	10	0

`Subnet Magic Numbers: /25=128  /26=64  /27=32  /28=16  /29=8  /30=4`

Hosts per subnet = 2^(32-prefix) - 2

■ MAGIC NUMBER METHOD

Step 1: Find the interesting octet (where mask is not 255 or 0)
Step 2: Magic Number = 256 – subnet mask octet
Step 3: Multiples of magic number = subnet boundaries
Step 4: Hosts/subnet = 2^(host bits) – 2

```
Example: 192.168.1.0 /26 (mask 255.255.255.192)
Magic = 256 - 192 = 64
Subnets: .0 .64 .128 .192
Range 1: 192.168.1.0 → .63 (usable: .1–.62, BC: .63)
Range 2: 192.168.1.64 → .127 (usable: .65–.126, BC: .127)
Hosts = 2^6 - 2 = 62 per subnet
```

■ SUBNETTING CHEAT TABLE

Prefix	Mask Octet	Magic#	Subnets(/24)	Hosts
/25	128	128	2	126
/26	192	64	4	62
/27	224	32	8	30
/28	240	16	16	14
/29	248	8	32	6
/30	252	4	64	2

■ ***MEMORY TRICK:*** *"128-64-32-16-8-4-2-1" — memorize subnet mask values! Mask values always sum to multiples going right to left.*

■ **EXAM ALERT: VLSM: Variable Length Subnet Masking — use different prefix lengths to conserve addresses. Always subnet from LARGEST to smallest!**

Page 7: IPv6 Addressing

128-bit addressing, types, autoconfiguration, and dual-stack

■ IPv6 ADDRESS STRUCTURE

IPv6 Address: 128-bit, 8 groups of 16 bits (hex)

2001	0DB8	ABCD	0001	0000	0000	0000	0001
Global	Routing	Subnet	Subnet	Interface	Interface	Interface	Interface

Type

Global Unicast	Link-Local	Multicast	Loopback
2000::/3	FE80::/10	FF00::/8	::1/128

SLAAC: Device generates its own address using Router Advertisement (RA)

EUI-64: MAC split + FFFE inserted → 64-bit Interface ID

■ ABBREVIATION RULES

Rule	Example (Full)	Example (Short)
Leading zeros in group can be dropped	2001:0DB8:0000:0001	2001:DB8:0:1
One group of consecutive zeros → ::	2001:DB8:0:0:0:0:0:1	2001:DB8::1
:: can only appear ONCE in address	FE80:0:0:0:0:0:0:1	FE80::1
Loopback: 0:0:0:0:0:0:0:1	All zeros	::1

SLAAC

- Stateless Address Autoconfiguration
- Router sends RA with prefix
- Host generates Interface ID (EUI-64)
- No DHCP server needed
- EUI-64: Split MAC → insert FFFE → flip 7th bit

DHCPv6

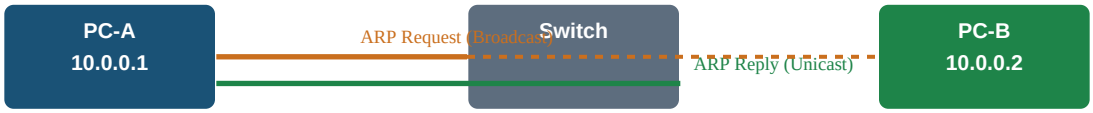
- Stateful: server tracks assignments
- Stateless: router provides prefix, DHCP provides DNS
- M flag in RA = use stateful DHCPv6
- O flag in RA = other info from DHCP
- NDP replaces ARP in IPv6

■ EXAM ALERT: IPv4 vs IPv6: No broadcast in IPv6 (uses multicast). IPv6 header = 40 bytes fixed. No fragmentation at routers.

Page 8: ARP & Neighbor Discovery

Address resolution in IPv4 (ARP) and IPv6 (NDP)

■ ARP PROCESS (IPv4)



1: Who has 10.0.0.2? (ff:ff:ff:ff:ff:ff)

2: I am 10.0.0.2! (unicast back)

3: ARP table updated

■ IPv4 ARP vs IPv6 NDP Comparison

Feature	ARP (IPv4)	NDP (IPv6)
Protocol	Layer 2 (EtherType 0x0806)	ICMPv6 (Layer 3)
Address Resolution	ARP Request/Reply	NS/NA (Neighbor Solicitation/Advertisement)
Router Discovery	Not native (uses ICMP)	Router Solicitation/Advertisement (RS/RA)
Broadcasts	Uses broadcast	Uses multicast (no broadcast in IPv6)
Cache	ARP cache (show arp)	Neighbor cache (show ipv6 neighbors)
Duplicate Detection	Gratuitous ARP	DAD (Duplicate Address Detection)

■■ KEY ARP COMMANDS

```
Router# show arp ! View ARP cache
Router# clear arp-cache ! Clear ARP entries
Router# show ip arp 192.168.1.10 ! Specific entry
Router# debug arp ! Debug ARP (careful!)

! NDP (IPv6) Commands:
Router# show ipv6 neighbors ! IPv6 neighbor cache
Router# clear ipv6 neighbors ! Clear NDP cache
```

■ EXAM ALERT: ARP Spoofing/Poisoning is a common attack — attacker sends fake ARP replies to redirect traffic. DAI (Dynamic ARP Inspection) mitigates this.

■ ***MEMORY TRICK:*** *"ARP = Address Resolution Protocol" — converts IP to MAC. "NDP is ARP on steroids for IPv6" — does ARP + Router Discovery + DAD*

Page 9: Switching Concepts

CAM table, frame forwarding methods, and switch operation

■■ SWITCH OPERATION OVERVIEW

Operation	Description	Example
Learning	Records source MAC + port in CAM table	Frame from PC1 on Gi0/1
Filtering	If src and dst on same port → drop	Hub attached to port
Forwarding	Known dst MAC → send to specific port	Known unicast
Flooding	Unknown dst or broadcast → all ports except ingress	Unknown unicast, BC, MC
Aging	CAM entries removed after timeout (300s default)	Aged-out entries flooded again

■ FRAME FORWARDING METHODS

Method	When Forwarded	Error Check	Latency	Use Case
Store-and-Forward	After full frame received	Yes (FCS)	Higher	Default on modern switches
Cut-Through	After dst MAC read (14B)	No	Lowest	Low-latency environments
Fragment-Free	After first 64 bytes	Partial	Medium	Avoids runts

■ DUPLEX & SPEED

Half Duplex: Cannot send and receive simultaneously → collisions possible → CSMA/CD
Full Duplex: Simultaneous send + receive → no collisions → no CSMA/CD needed
Auto-negotiation: Cisco default — negotiate speed/duplex. Mismatch causes performance issues!
Speed mismatch: Interface goes down. Duplex mismatch: interface up but poor performance.

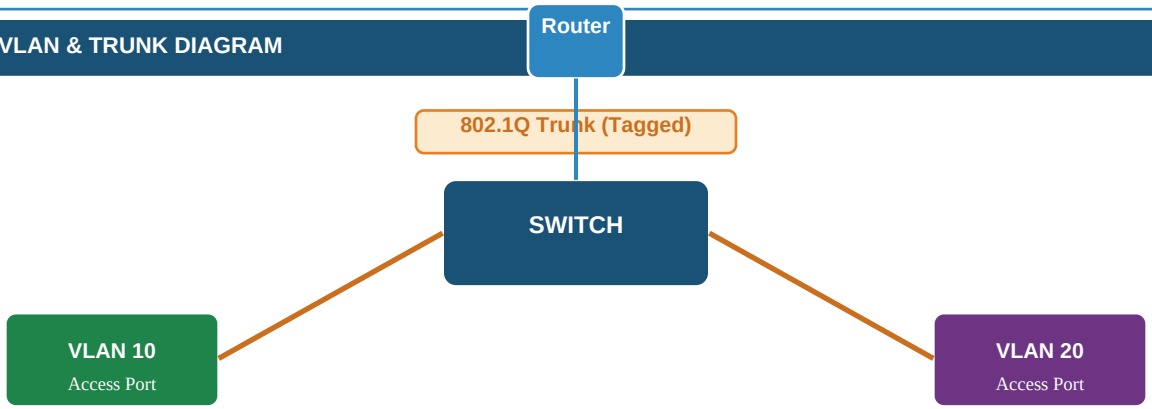
```
SW1(config-if)# duplex full
SW1(config-if)# speed 1000
SW1# show interfaces Gi0/1 ! Check speed, duplex, errors
SW1# show mac address-table ! View CAM table
SW1# show interfaces counters ! View frame/error counters
```

■ EXAM ALERT: Duplex mismatch = late collisions on full-duplex side, excessive collisions on half-duplex side. Check with "show interfaces"

Page 10: VLANs & Trunking

Virtual LANs, 802.1Q tagging, access vs trunk ports

■■ VLAN & TRUNK DIAGRAM



■ ACCESS vs TRUNK PORT COMPARISON

Feature	Access Port	Trunk Port
VLANs	Belongs to ONE VLAN	Carries MULTIPLE VLANs
Tagging	No 802.1Q tag	802.1Q tag on all except native VLAN
Connected to	End devices (PCs, phones)	Switches, routers, servers
Native VLAN	N/A	VLAN 1 (default) — sent untagged
Config cmd	switchport mode access	switchport mode trunk

■■ VLAN CONFIGURATION COMMANDS

```
! Create VLAN and name it
SW1(config)# vlan 10
SW1(config-vlan)# name SALES

! Configure access port
SW1(config-if)# switchport mode access
SW1(config-if)# switchport access vlan 10

! Configure trunk port
SW1(config-if)# switchport mode trunk
SW1(config-if)# switchport trunk encapsulation dot1q
SW1(config-if)# switchport trunk allowed vlan 10,20,30
SW1(config-if)# switchport trunk native vlan 99

! Verify
SW1# show vlan brief
SW1# show interfaces trunk
```

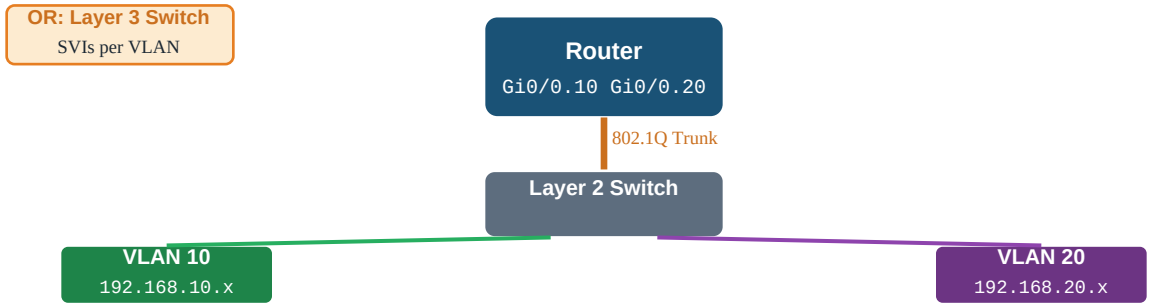
■ **EXAM ALERT: Native VLAN mismatch = CDP warning + security risk (VLAN hopping attack). Always set native VLAN to unused VLAN!**

■ ***MEMORY TRICK:*** *"Access = 1 VLAN, Trunk = Many VLANs" — like a single lane road vs. a highway with multiple lanes*

Page 11: Inter-VLAN Routing

Router-on-a-stick (ROAS) and Layer 3 switch SVIs

■ INTER-VLAN ROUTING DIAGRAM



■ ROAS vs L3 SWITCH COMPARISON

Feature	Router-on-a-Stick (ROAS)	Layer 3 Switch (SVI)
Device needed	Router + Switch	Layer 3 capable switch only
Interface	Sub-interfaces (Gi0/0.10)	SVIs (interface vlan 10)
Performance	Single link bottleneck	Wire-speed switching
Cost	Requires separate router	Single device
Best for	Small networks, SOHO	Enterprise, high traffic

■■ CONFIGURATION COMMANDS

ROAS (Router-on-a-Stick):

```
R1(config)# interface Gi0/0
R1(config-if)# no shutdown
R1(config)# int Gi0/0.10
R1(config-subif)# encapsulation dot1q 10
R1(config-subif)# ip address 192.168.10.1 255.255.
R1(config)# int Gi0/0.20
R1(config-subif)# encapsulation dot1q 20
R1(config-subif)# ip address 192.168.20.1 255.255.
```

Layer 3 Switch SVI:

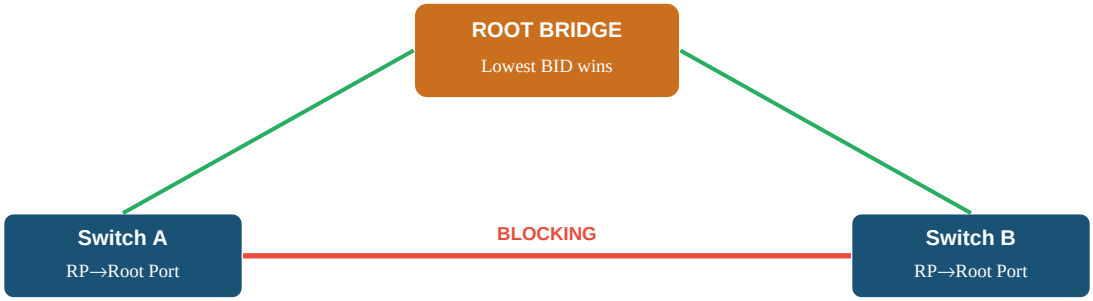
```
SW1(config)# ip routing
SW1(config)# vlan 10
SW1(config)# interface vlan 10
SW1(config-if)# ip address 192.168.10.1
255.255.255.0
SW1(config-if)# no shutdown
SW1(config)# interface vlan 20
SW1(config-if)# ip address 192.168.20.1
255.255.255.0
```

■ EXAM ALERT: For ROAS: trunk port on switch side must be configured with "switchport mode trunk" to match! L3 switch needs "ip routing" command.

Page 12: Spanning Tree Protocol (STP)

Root bridge election, port roles, states, and RSTP

■ STP TOPOLOGY DIAGRAM



BID = Priority (32768) + MAC | Root Port (RP) = Best path to root | Red = Blocking port

PORT ROLES

Root Port (RP): Best path toward root bridge. One per non-root switch.

Designated Port (DP): Best port on each segment toward root. Forwards traffic.

Non-Designated (Blocked): Creates loop — put in blocking state.

ROOT BRIDGE ELECTION

- Lowest Bridge ID (BID) wins
- BID = Priority (2B) + MAC Address (6B)
- Default priority: 32768 (+ VLAN ID in PVST)
- Tie = Lowest MAC wins

PORT STATES (802.1D)

Blocking → Listening → Learning → Forwarding

Blocking (20s) → Listening (15s) → Learning (15s) → Forwarding

Total convergence time: ~50 seconds for 802.1D

RSTP (802.1w) Improvements

- Convergence: ~1-2 seconds (vs 50s STP)
- New port roles: Alternate, Backup

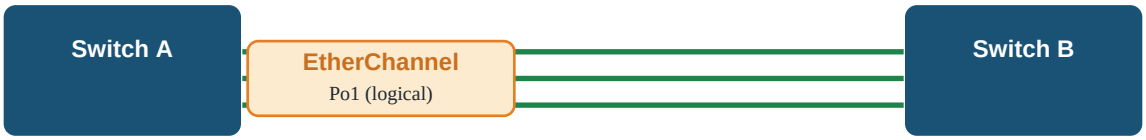
```
SW1(config)# spanning-tree vlan 10 priority 4096 ! Lower = more likely root
SW1(config)# spanning-tree vlan 10 root primary ! Automatically sets priority
SW1(config-if)# spanning-tree portfast ! For access ports only!
SW1(config-if)# spanning-tree bpduguard enable ! Protect portfast ports
SW1# show spanning-tree vlan 10
```

■ EXAM ALERT: PortFast + BPDUGuard = best practice for access ports. BPDUGuard shuts port if BPDU received (prevents loops from unauthorized switches).

Page 13: EtherChannel

Link aggregation, LACP, PAgP, and load balancing

■ ETHERCHANNEL DIAGRAM



`LACP (802.3ad): active/passive | PAgP (Cisco): desirable/auto | Static: on/on`

Load balancing: src-mac, dst-mac, src-dst-ip, src-dst-port

Benefits: Bandwidth aggregation + redundancy

■ LACP vs PAgP vs Static

Feature	LACP (802.3ad)	PAgP (Cisco)	Static (On)
Standard	IEEE 802.3ad	Cisco Proprietary	N/A
Negotiate	Yes	Yes	No
Modes	Active / Passive	Desirable / Auto	On
Active side	Both can be Active	Desirable initiates	Both must be On
Max links	16 (8 active)	8	8

■■ ETHERCHANNEL CONFIGURATION

```
! LACP EtherChannel
SW1(config)# interface range Gi0/1-2
SW1(config-if-range)# channel-group 1 mode active ! LACP active
SW1(config-if-range)# switchport mode trunk

! Configure Port-channel interface
SW1(config)# interface Port-channel 1
SW1(config-if)# switchport mode trunk
SW1(config-if)# switchport trunk allowed vlan 10,20

! Verify
SW1# show etherchannel summary
SW1# show etherchannel port-channel
```

■ EXAM ALERT: All physical ports in EtherChannel must match: speed, duplex, VLAN config, trunking. Mismatch = channel will not form!

■ ***MEMORY TRICK:*** *"LACP = Love All Cisco Products" (vendor-neutral), PAgP = "Pretty Annoying Gets Proprietary" (Cisco only)*

Page 14: Routing Fundamentals

Static vs dynamic routing, administrative distance, routing table

■■ ROUTING TABLE DIAGRAM

Code	Network	AD/Metric	Next Hop	Interface
C	10.0.0.0/24	0/0	Direct	Gi0/0
S	192.168.1.0/24	1/0	10.0.0.1	Gi0/0
O	172.16.0.0/16	110/2	10.0.0.2	Gi0/1
R	0.0.0.0/0	120/1	10.0.0.254	Gi0/0

C=Connected S=Static O=OSPF R=RIP | Longest match wins!

■ ADMINISTRATIVE DISTANCE (AD)

Route Source	AD	Route Source	AD
Connected	0	OSPF	110
Static	1	IS-IS	115
EIGRP Summary	5	RIP	120
External BGP	20	EIGRP External	170
EIGRP Internal	90	Internal BGP	200
IGRP	100	Unknown	255 (unusable)

■■ STATIC ROUTING CONFIGURATION

```
! Standard static route
R1(config)# ip route 192.168.2.0 255.255.255.0 10.0.0.2

! Default route (gateway of last resort)
R1(config)# ip route 0.0.0.0 0.0.0.0 10.0.0.1

! Floating static (backup, higher AD)
R1(config)# ip route 192.168.2.0 255.255.255.0 10.0.0.3 5

! IPv6 static route
R1(config)# ipv6 route 2001:db8:2::/64 2001:db8:1::2

! Verify routing table
R1# show ip route
R1# show ip route static
R1# show ip route 192.168.2.0
```

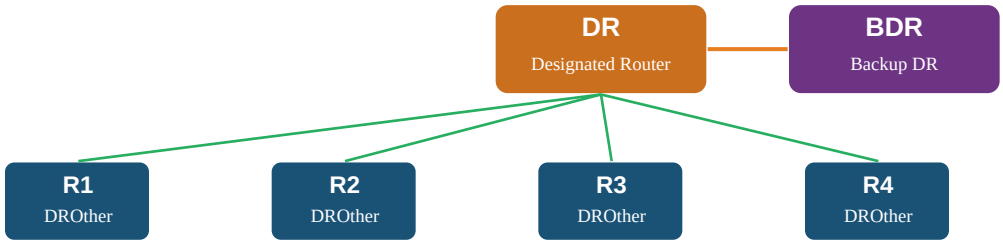
■ EXAM ALERT: Longest prefix match wins when multiple routes match. /32 beats /24 beats /0 (default). AD breaks ties between routing protocols.

■ ***MEMORY TRICK:*** *"C S E O I R E I U" = Connected(0) Static(1) EIGRP(90) OSPF(110) IS-IS(115) RIP(120) EIGRP-ext(170) iBGP(200) Unknown(255)*

Page 15: OSPF — Open Shortest Path First

Link-state routing: neighbor formation, LSAs, DR/BDR, SPF algorithm

■ OSPF NETWORK DIAGRAM




```
OSPF States: Down→Init→2-Way→ExStart→Exchange→Loading→FULL
```

NEIGHBOR STATES

Down → No hellos received

Init → Hello received, not bidirectional

2-Way → Bidirectional, DR/BDR election here

ExStart → Master/slave election, DBD sequence

Exchange → DBDs exchanged

Loading → LSRs/LSUs/LSAcks

Full → ■ Full adjacency established

OSPF HELLO REQUIREMENTS

Neighbors must match:

- Same Area ID
- Same Hello/Dead intervals (10/40s Ethernet)
- Same subnet + mask
- Same authentication
- Same MTU (for full adjacency)
- Stub flag must match

■■ OSPF CONFIGURATION

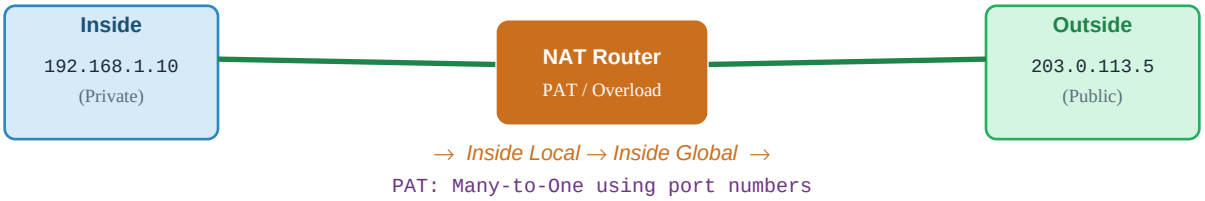
```
R1(config)# router ospf 1
R1(config-router)# router-id 1.1.1.1
R1(config-router)# network 10.0.0.0 0.0.0.255 area 0
R1(config-router)# network 192.168.1.0 0.0.0.255 area 0
R1(config-router)# passive-interface Gi0/2 ! No hellos on this int

! Verification
R1# show ip ospf neighbor
R1# show ip ospf database
R1# show ip route ospf
R1# show ip ospf interface brief
```

■ EXAM ALERT: OSPF uses Dijkstra SPF algorithm. Cost = Reference BW / Interface BW. Default ref BW = 100Mbps. Change with "auto-cost reference-bandwidth 1000" for GigE.

Page 16: IP Services

NAT, NTP, DNS, SNMP, Syslog, QoS, and FHRP

■ NAT DIAGRAM



■ NAT TYPES

Type	Mapping	Use Case	Config
Static NAT	1-to-1 (fixed)	Server with public IP	ip nat inside source static
Dynamic NAT	Pool of public IPs	Multiple users, pool of IPs	ip nat pool + ACL
PAT/Overload	Many-to-1 (port-based)	Internet sharing (most common)	ip nat inside source list overload

```
! PAT Configuration (most common)
R1(config)# access-list 1 permit 192.168.1.0 0.0.0.255
R1(config)# ip nat inside source list 1 interface Gi0/0 overload
R1(config-if)# ip nat inside ! Internal interface
R1(config-if)# ip nat outside ! External interface
R1# show ip nat translations
R1# show ip nat statistics
```

■ NTP | ■ DNS | ■ SNMP | ■ SYSLOG

Service	Port	Purpose	Key Config
NTP	123/UDP	Time synchronization (Stratum 0-15)	ntp server
DNS	53/TCP+UDP	Name → IP resolution	ip domain-lookup, ip name-server
SNMP v2c	161/UDP	Network monitoring	snmp-server community RO
SNMP v3	161/UDP	Secure monitoring (AuthPriv)	snmp-server group/user
Syslog	514/UDP	Log messages (0=Emergency, 7=Debug)	logging host
HSRP	—	First-hop redundancy (virtual gateway)	standby ip

■ EXAM ALERT: SNMP v3 = most secure (authentication + encryption). SNMP v2c = community string only (no encryption). Syslog levels 0-7: Every Awesome Cisco Engineer Can Do It Normally

Page 17: DHCP & DNS Deep Dive

DORA process, relay agents, DNS resolution flow, and split DNS

■ DHCP DORA PROCESS

DORA: Discover → Offer → Request → Acknowledge

Lease includes: IP, Subnet, Gateway, DNS, Lease Time

■■ DHCP CONFIGURATION

```
! DHCP Server Config
R1(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.10
R1(config)# ip dhcp pool VLAN10
R1(dhcp-config)# network 192.168.1.0 255.255.255.0
R1(dhcp-config)# default-router 192.168.1.1
R1(dhcp-config)# dns-server 8.8.8.8 8.8.4.4
R1(dhcp-config)# lease 7 ! 7 days lease time

! DHCP Relay Agent (ip helper-address)
R1(config-if)# ip helper-address 10.0.0.100 ! DHCP server IP

! Verify
R1# show ip dhcp pool
R1# show ip dhcp binding
R1# show ip dhcp conflict
```

■ DNS RESOLUTION FLOW

1. Client checks local DNS cache → Hit? Return IP. Miss? Continue.
2. Query sent to local Recursive Resolver (ISP / configured DNS)
3. Recursive Resolver checks cache → Hit? Return. Miss? Continue.
4. Query Root Name Server (.com? .org? .net?) → Returns TLD server
5. Query TLD Server (.com) → Returns Authoritative NS for domain
6. Query Authoritative Name Server → Returns final IP address
7. Result cached + returned to client (TTL determines cache duration)

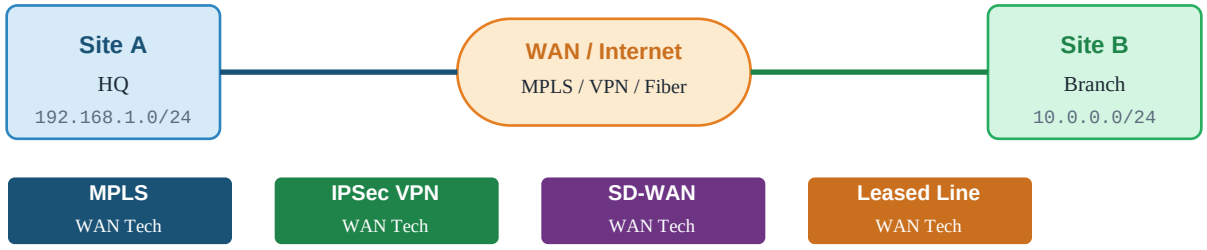
Record Type	Purpose	Example
A	IPv4 address for hostname	cisco.com → 72.163.4.161
AAAA	IPv6 address for hostname	cisco.com → 2001:420::
CNAME	Alias to another name	www → cisco.com
MX	Mail server for domain	cisco.com MX mailhost.cisco.com
PTR	Reverse lookup (IP → name)	161.4.163.72 → cisco.com
NS	Authoritative name servers	cisco.com NS ns1.cisco.com

■ EXAM ALERT: ip helper-address forwards not just DHCP (UDP 67/68) but also: TFTP(69), DNS(53), NTP(123), NetBIOS(137,138), TACACS(49)

Page 18: WAN Technologies

MPLS, VPNs, broadband, SD-WAN, and WAN connectivity options

■ WAN TOPOLOGY DIAGRAM



■ WAN TECHNOLOGIES COMPARISON

Technology	Type	Speed	Key Feature
Leased Line (T1/E1)	Dedicated	1.5/2 Mbps	Always-on, expensive, guaranteed BW
MPLS	Provider managed	Variable	Traffic engineering, QoS labels, VPNs
IPSec VPN	Encrypted tunnel	Varies	Secure tunnel over public internet
GRE Tunnel	Encapsulation	Varies	Tunnels non-IP traffic, no encryption
DMVPN	Dynamic VPN	Varies	Hub-and-spoke + dynamic spoke-to-spoke
SD-WAN	Software-defined	Variable	Centralized control, path selection, cloud
Broadband (DSL/Cable)	Shared/asymmetric	10-1000 Mbps	Low cost, asymmetric, not guaranteed
Metro Ethernet	Ethernet WAN	10 Mbps+	Ethernet interface, provider backbone

■ VPN TYPES

Site-to-Site VPN:

- Router-to-router encrypted tunnel
- Always-on connection
- IPSec: AH (integrity) or ESP (encrypt+auth)
- IKE Phase 1: ISAKMP SA (key exchange)
- IKE Phase 2: IPSec SA (data)

Remote Access VPN:

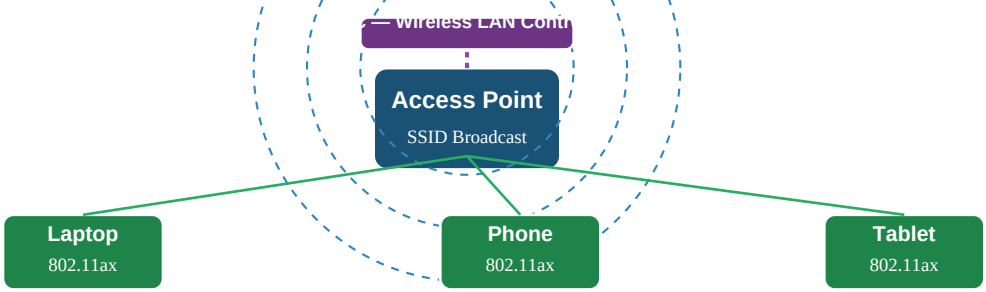
- Client-to-site (individual users)
- Cisco AnyConnect (SSL/TLS)
- Full tunnel vs split tunnel
- Authentication: AAA, MFA
- SSL VPN = web browser based

■ EXAM ALERT: MPLS uses labels (not IP addresses) for forwarding. PE routers add/remove labels. CE routers connect to PE. LSP = Label Switched Path.

Page 19: Wireless Networking

WLAN architecture, 802.11 standards, channels, and security

■ WIRELESS ARCHITECTURE DIAGRAM



■ 802.11 STANDARDS

Standard	Freq Band	Max Speed	Range	Also Called
802.11a	5 GHz	54 Mbps	Short	Wi-Fi 1 (legacy)
802.11b	2.4 GHz	11 Mbps	Long	Wi-Fi 2 (legacy)
802.11g	2.4 GHz	54 Mbps	Medium	Wi-Fi 3
802.11n	2.4/5 GHz	600 Mbps	Good	Wi-Fi 4 (MIMO)
802.11ac	5 GHz	3.5 Gbps	Medium	Wi-Fi 5 (MU-MIMO)
802.11ax	2.4/5/6 GHz	9.6 Gbps	Best	Wi-Fi 6/6E (OFDMA)

■ WIRELESS SECURITY

Security	Auth	Encryption	Status
WEP	Open/Shared	RC4 (40/128-bit)	■ Deprecated — BROKEN
WPA	PSK/802.1X	TKIP	■ Deprecated
WPA2	PSK/802.1X	AES-CCMP	■ Acceptable
WPA3	SAE/802.1X	AES-GCMP-256	■ Recommended
802.1X/EAP	RADIUS server	Various	■ Enterprise standard

2.4 GHz non-overlapping channels: 1, 6, 11

5 GHz: Many non-overlapping channels (36, 40, 44, 48…)

Autonomous AP: Self-configured, no controller

Lightweight AP (LWAP): Managed by WLC. Uses CAPWAP tunnels (UDP 5246/5247)

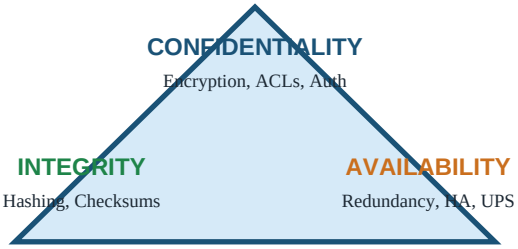
■ EXAM ALERT: WPA2-Personal = PSK (pre-shared key). WPA2-Enterprise = 802.1X with RADIUS. Always choose WPA3 or WPA2 AES for exam questions.

■ ***MEMORY TRICK:*** *"1-6-11 the magic three" — only non-overlapping 2.4 GHz channels*

Page 20: Network Security Fundamentals

CIA triad, threat types, attack vectors, and defense strategies

■■ CIA TRIAD



CIA Triad — Foundation of Network Security

■■ COMMON THREAT TYPES

Threat	Description	Mitigation
Phishing	Deceptive emails to steal credentials	User training, email filtering
DoS/DDoS	Flood target to deny service	Rate limiting, ACLs, ISP filtering
MITM	Intercept/alter communication	Encryption, PKI, HTTPS
ARP Spoofing	Fake ARP replies to redirect traffic	DAI (Dynamic ARP Inspection)
VLAN Hopping	Access unauthorized VLANs	Disable DTP, set native VLAN
Brute Force	Try all password combinations	Account lockout, strong passwords
SQL Injection	Malicious DB queries via input	Input validation, WAF
Ransomware	Encrypt files, demand ransom	Backups, patching, AV
Social Engineering	Manipulate users psychologically	Security awareness training

■ SECURITY CONCEPTS

AAA Framework:

- **Authentication:** Who are you? (username/pw, cert)
- **Authorization:** What can you do? (permissions)
- **Accounting:** What did you do? (logs)

AAA Protocols:

- RADIUS: UDP 1812/1813, encrypts password only
- TACACS+: TCP 49, encrypts ENTIRE payload, Cisco

Cryptography Basics:

- Symmetric: Same key encrypt/decrypt (AES)
- Asymmetric: Public/private key pair (RSA)
- Hashing: One-way, integrity (SHA-256, MD5)
- PKI: Certificate Authority signs certs

Firewall Types:

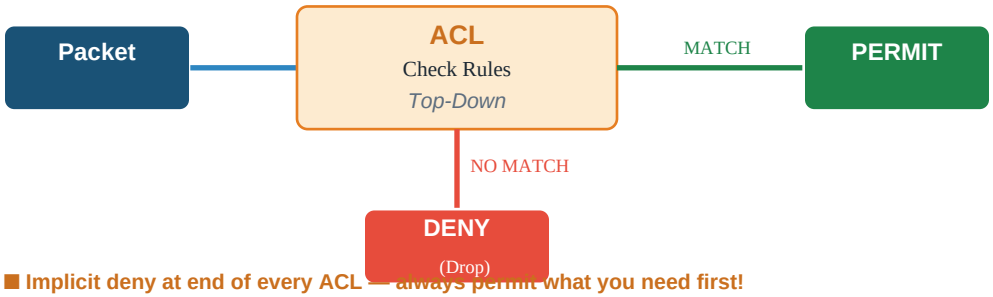
- Stateless: ACL-based, packet by packet

■ EXAM ALERT: RADIUS combines authentication + authorization in single response. TACACS+ separates A, A, and A. TACACS+ preferred for device admin (more granular).

Page 21: Access Control Lists (ACLs)

Standard vs extended ACLs, rule processing, and placement

■ ACL PROCESSING DIAGRAM



■ **Implicit deny at end of every ACL — always permit what you need first!**

■ STANDARD vs EXTENDED ACLs

Feature	Standard ACL	Extended ACL
Number range	1-99, 1300-1999	100-199, 2000-2699
Filters on	Source IP only	Src IP, Dst IP, Protocol, Port
Placement	Close to DESTINATION	Close to SOURCE
Named	Yes (ip access-list standard)	Yes (ip access-list extended)
Granularity	Low (coarse filtering)	High (very specific)

■■ ACL CONFIGURATION

```
! Standard ACL — permit specific host
R1(config)# access-list 10 permit 192.168.1.0 0.0.0.255
R1(config)# access-list 10 deny any ! (implicit anyway)

! Extended ACL — permit web traffic only
R1(config)# access-list 110 permit tcp 10.0.0.0 0.0.0.255 any eq 80
R1(config)# access-list 110 permit tcp 10.0.0.0 0.0.0.255 any eq 443
R1(config)# access-list 110 deny ip any any log

! Apply to interface
R1(config-if)# ip access-group 10 in ! Inbound filtering
R1(config-if)# ip access-group 110 out ! Outbound filtering

! Named ACL (preferred)
R1(config)# ip access-list extended BLOCK_TELNET
R1(config-ext-nacl)# deny tcp any any eq 23
R1(config-ext-nacl)# permit ip any any

R1# show access-lists
R1# show ip interface Gi0/0 ! Shows applied ACLs
```

■ **EXAM ALERT: Wildcard mask = inverse of subnet mask. 255.255.255.0 → wildcard 0.0.0.255. "any" = 0.0.0.0 255.255.255.255. "host" = 0.0.0.0**

■ ***MEMORY TRICK:*** *"Standard ACLs go near destination (S=Source only), Extended go near source (E=Everything checked)"*

Page 22: Device Hardening & Port Security

SSH, password protection, banners, port security, and 802.1X

■ PORT SECURITY DIAGRAM

`Max MACs: default=1 | Sticky learning: auto-adds to running config`

Recovery: no shutdown | errdisable recovery cause psecure-violation

■■ DEVICE HARDENING COMMANDS

```
! Enable SSH (disable Telnet)
R1(config)# hostname R1
R1(config)# ip domain-name cisco.com
R1(config)# crypto key generate rsa modulus 2048
R1(config)# ip ssh version 2
R1(config)# line vty 0 4
R1(config-line)# transport input ssh
R1(config-line)# login local

! Password protection
R1(config)# enable secret Cisco123! ! Hashed (MD5)
R1(config)# service password-encryption ! Weak but encrypts type 7
R1(config)# username admin secret Cisco123!

! Banners
R1(config)# banner motd # AUTHORIZED USERS ONLY #

! Exec timeout
R1(config-line)# exec-timeout 10 0 ! 10 min idle timeout

! Port Security on switchport
SW1(config-if)# switchport mode access
SW1(config-if)# switchport port-security
SW1(config-if)# switchport port-security maximum 2
SW1(config-if)# switchport port-security mac-address sticky
SW1(config-if)# switchport port-security violation restrict

SW1# show port-security interface Gi0/1
```

■ HARDENING CHECKLIST

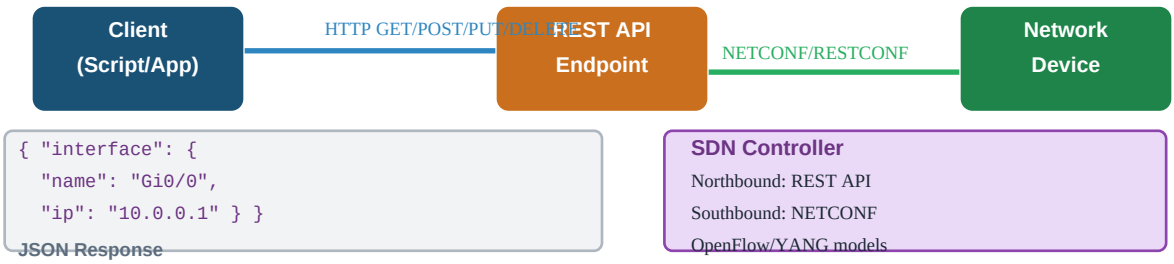
- ■ Change default passwords — never leave factory defaults
- ■ Use SSH v2 — disable Telnet (clear text)
- ■ Enable "enable secret" — never use "enable password"
- ■ Configure login banners — legal notification required
- ■ Disable unused interfaces — shutdown unused ports
- ■ Enable port security — prevent MAC flooding attacks
- ■ Use SNMPv3 — disable v1/v2c on production networks
- ■ Configure exec-timeout — prevent unattended sessions
- ■ Use AAA with RADIUS/TACACS+ — centralized auth

■ EXAM ALERT: "enable secret" uses MD5 hash. "enable password" is clear text. "service password-encryption" uses Type 7 (reversible). Always use "secret" commands!

Page 23: Network Automation & APIs

REST APIs, JSON, YANG, SDN, and configuration management tools

■ AUTOMATION ARCHITECTURE DIAGRAM



■ AUTOMATION TOOLS COMPARISON

Tool	Type	Language	Agent?	Use Case
Ansible	Agentless	YAML Playbooks	No	Push-based, simple automation
Puppet	Agent-based	Puppet DSL/Ruby	Yes	Declarative, pull-based
Chef	Agent-based	Ruby (Recipes)	Yes	Infrastructure as code
Python/Netmiko	Script	Python	No	Custom automation, SSH/API
Terraform	Infrastructure	HCL	No	Cloud/infra provisioning

■ REST API METHODS

HTTP Method	CRUD Operation	Action	Idempotent?
GET	Read	Retrieve resource/data	Yes
POST	Create	Create new resource	No
PUT	Update	Replace entire resource	Yes
PATCH	Update	Partial update	No
DELETE	Delete	Remove resource	Yes

```
# JSON Example (Router Interface Data):
{
"ietf-interfaces:interface": {
"name": "GigabitEthernet0/0",
"type": "ianaift:ethernetCsmacd",
"enabled": true,
"ietf-ip:ipv4": {
"address": [{"ip": "10.0.0.1", "prefix-length": 24}]
}
}
}
```

■ **EXAM ALERT: Data formats: JSON = JavaScript Object Notation (human-readable, key-value). XML = eXtensible Markup Language (verbose). YAML = YAML Ain't Markup Language (Ansible uses this).**

■ ***MEMORY TRICK:*** *"GET just reads, POST creates new, PUT replaces all, PATCH changes part, DELETE removes" = REST in one sentence*

Page 24: Troubleshooting Methodology

Structured troubleshooting, layered approach, and common issues

■ 7-STEP TROUBLESHOOTING PROCESS

1. IDENTIFY	2. ESTABLISH	3. TEST	4. PLAN	5. IMPLEMENT	6. VERIFY	7. DOCUMENT
Define the problem	Theory of probable cause	Test the theory	Establish action plan	Implement / escalate	Verify full functionality	Document findings

OSI Layered Approach:

Bottom-Up: L1 (cables?) → L2 (MAC/switch?) → L3 (IP/route?) → L4 (port?) → L7 (app?)

Top-Down: Start at application layer and work down. Divide-and-Conquer: Start at L3.

`Key commands: ping, traceroute, show ip interface brief, show ip route, debug ip icmp`

■ COMMON ISSUES BY LAYER

OSI Layer	Common Problem	Diagnostic Command
L1 Physical	Cable unplugged, NIC failure, duplex mismatch	show interfaces (check line/protocol)
L2 Data Link	MAC conflict, STP loop, VLAN mismatch	show mac-address-table, show spanning-tree
L3 Network	Routing loop, missing route, wrong mask	show ip route, ping, traceroute
L4 Transport	Port blocked, ACL denying, NAT issue	show ip nat translations, show access-lists
L7 Application	DNS failure, service down, wrong URL	nslookup, telnet

■■ KEY TROUBLESHOOTING COMMANDS

```
! Connectivity tests
R1# ping 8.8.8.8 ! Basic connectivity
R1# ping 8.8.8.8 source Gi0/0 ! Ping with specific source
R1# traceroute 8.8.8.8 ! Path discovery
R1# ping 8.8.8.8 repeat 100 ! Extended ping

! Interface troubleshooting
R1# show interfaces Gi0/0 ! Full interface stats
R1# show ip interface brief ! Quick status view
R1# show interfaces Gi0/0 counters ! Error counters

! Routing troubleshooting
R1# show ip route ! Full routing table
R1# show ip route 192.168.1.0 ! Specific route lookup
R1# show ip protocols ! Active routing protocols

! CDP / LLDP neighbor discovery
R1# show cdp neighbors ! Layer 2 neighbors
R1# show cdp neighbors detail ! Full neighbor info (IP etc)
R1# show lldp neighbors ! LLDP neighbors
```

■ EXAM ALERT: "show interfaces" output: "up/up" = good | "down/down" = L1 problem | "up/down" = L2 problem | "admin down/down" = manual shutdown

Page 25: CLI Commands Master Cheat Sheet

Essential Cisco IOS commands organized by category

■ MUST-KNOW SHOW COMMANDS

Command	Output
show ip interface brief	IP, status of all interfaces (quick overview)
show interfaces Gi0/0	Full stats, errors, MAC, duplex, speed
show ip route	Full routing table with codes and metrics
show running-config	Current active configuration
show startup-config	Saved configuration (NVRAM)
show version	IOS version, uptime, hardware info, license
show vlan brief	VLAN list with ports assigned
show interfaces trunk	Trunk ports and allowed VLANs
show spanning-tree	STP topology, root bridge, port roles/states
show mac address-table	CAM table (MAC → port mapping)
show ip ospf neighbor	OSPF neighbor states and adjacencies
show ip nat translations	Active NAT/PAT translations
show access-lists	ACL rules with match counters
show cdp neighbors detail	Neighbor device info (model, IP, IOS)
show etherchannel summary	EtherChannel status and bundled ports

■ CONFIGURATION COMMANDS BY CATEGORY

Routing & IP:

```
R1(config)# ip route 0.0.0.0 0.0.0.0
R1(config)# router ospf 1
R1(config-router)# network area 0
R1(config-if)# ip address
R1(config-if)# no shutdown
R1(config-if)# ip helper-address
```

ACLs:

```
R1(config)# access-list 1 permit
R1(config)# ip access-list extended BLOCK
R1(config-ext-nacl)# permit tcp any any eq 443
R1(config-ext-nacl)# deny ip any any log
R1(config-if)# ip access-group 110 in
R1# show access-lists
```

VLANs & Trunking:

```
SW1(config)# vlan 10
SW1(config-vlan)# name SALES
SW1(config-if)# switchport mode access
SW1(config-if)# switchport access vlan 10
SW1(config-if)# switchport mode trunk
SW1(config-if)# switchport trunk native vlan 99
```

STP & EtherChannel:

```
SW1(config)# spanning-tree vlan 1 root primary
SW1(config-if)# spanning-tree portfast
SW1(config-if)# spanning-tree bpduguard enable
SW1(config-if)# channel-group 1 mode active
SW1(config)# int Port-channel 1
SW1# show spanning-tree vlan 10
```

Security & Passwords:

```
R1(config)# enable secret
R1(config)# username admin secret
R1(config)# line vty 0 4
R1(config-line)# transport input ssh
R1(config-line)# login local
R1(config-line)# exec-timeout 10 0
```

NAT & DHCP:

```
R1(config)# ip dhcp pool LAN
R1(dhcp-config)# network 192.168.1.0 /24
R1(dhcp-config)# default-router 192.168.1.1
R1(config)# access-list 1 permit 192.168.1.0 0.0.0.255
R1(config)# ip nat inside source list 1
interface Gi0/0 overload
```

■ **EXAM ALERT: CTRL+Z = exit to privileged mode | CTRL+C = abort | Tab = autocomplete | ? = help | "do" prefix runs EXEC cmd from config mode**

■ ***MEMORY TRICK:*** *"show run" saves your day — always verify configuration after changes. "copy run start" saves it permanently!*