Architecture

Implementing Cisco SD-WAN Solutions (ENSDWI)

KNOWLEDGE CHEATSHEET

FABRIC RESPONSIBILITIES

- **vManage** — Manage
- **vBond** — Orchestrate
- **vSmart** — Control
- **WAN Edge** — Forward

01 Architecture 20%

Planes and component roles

- **vManage** provides centralized configuration, templates, inventory, software management and monitoring. **vSmart** distributes overlay reachability, security key information and policy through OMP.
- **vBond** authenticates initial participants, discovers translated addresses and introduces WAN Edges to controllers. Its orchestration role does not include forwarding user traffic.
- **WAN Edge** routers forward traffic, establish data tunnels and run service-side routing protocols. BFD measures tunnel health directly between edges.
- **Management**, **control**, **orchestration** and **data** are separate planes. Hosting controllers in a cloud does not centralize the branch-to-branch data path.
- Cisco Catalyst SD-WAN terminology uses **Manager**, **Controller** and **Validator** for vManage, vSmart and vBond respectively. Recognize both naming conventions.

Underlay, overlay and segmentation

- The **underlay** supplies IP reachability over Internet, MPLS or cellular networks. The **overlay** supplies secure logical connectivity independent of provider routing.
- **VPN 0** contains transport connectivity and controller reachability. **VPN 512** serves out-of-band management. **Service VPNs** isolate application routing and traffic.
- A **system IP** is a stable logical router identifier, independent of interface addressing. A **site ID** groups routers at one site; an **organization name** identifies the fabric.
- **OMP** runs inside secure DTLS/TLS control connections between WAN Edges and vSmart. Edge-to-edge **IPsec** tunnels carry user traffic; controllers are not data-plane transit nodes.
- **DTLS** uses UDP; **TLS** uses TCP. Permit actual control ports and configured offsets through firewalls. Successful ICMP reachability alone does not prove control connectivity.

TLOC identity and connectivity

- A **TLOC** is identified by **system IP, color and encapsulation**. It is an overlay next hop representing a transport attachment, not a service prefix.
- **TLOC routes** carry reachability attributes including public/private address and port information. **Preference** and **weight** influence path selection and traffic distribution.

Architecture / Controllers

Implementing Cisco SD-WAN Solutions (ENSDWI)

KNOWLEDGE CHEATSHEET

FABRIC RESPONSIBILITIES

- **vManage** — Manage
- **vBond** — Orchestrate
- **vSmart** — Control
- **WAN Edge** — Forward

- **Colors** label transports for tunnel formation and policy. Public colors support translated address use; private colors normally use private transport addressing.
- The tunnel-interface **restrict** option limits peering to the same color. Without restriction, reachable compatible TLOCs of different colors can form tunnels.
- With two usable TLOCs at each of two remote sites, unrestricted full-mesh connectivity permits **2 × 2 = 4** tunnel pairs between them. Policy and reachability can reduce that set.
- A private transport can need a public address for controller access while using private addresses for data tunnels. Evaluate **control reachability** separately from **data reachability**.

Platforms, topology and resilience

- **IOS XE SD-WAN** runs on supported ISR, ASR and Catalyst edge platforms; **vEdge** uses a different software family. Match features, memory and images to the exact platform.
- **Virtual WAN Edges** extend the overlay into hypervisors and public clouds. Cisco UCS and ENCS supply compute; NFVIS hosts supported virtual network functions.
- A default **full mesh** permits direct intersite tunnels. **Hub-and-spoke**, regional hubs and partial meshes use centralized policy to control advertised routes and TLOCs.
- **Multi-Region Fabric** separates access regions from a core region through border routers. A middle-mile provider connects regions; regional topology and end-to-end SLA design remain explicit decisions.
- Loss of **vManage** affects management and telemetry, while existing forwarding can continue. Loss of **vSmart** removes fresh control updates; cached state may sustain forwarding during graceful restart.
- Redundant controllers, transport links and WAN Edges protect different failure domains. Controller redundancy does not replace LAN gateway or data-tunnel redundancy.

02 Controller Deployment 15%

Controller hosting and bring-up

- For **on-premises controllers**, provision supported compute, storage and interfaces, then own backups and disaster recovery. Cloud hosting simplifies infrastructure deployment but still requires sound connectivity design.
- **OVA** is associated with VMware deployment; **QCOW2** with KVM. Initial deployment packages and software upgrade images serve different purposes and are not interchangeable.
- Configure unique **system IPs**, consistent organization identity, transport addressing, routes, DNS and NTP. Transport interfaces need reachability to the controller endpoints.

Controllers

Implementing Cisco SD-WAN Solutions (ENSDWI)

KNOWLEDGE CHEATSHEET

CONTROLLER READINESS

Underlay Reachability → **Trust** Certificates → **Identity** Authorization → **Control** Sessions

- Expose **vBond** through a reachable public address when Internet-based onboarding requires it. A DNS name resolving to multiple orchestrators supports redundant discovery.
- A **vManage cluster** scales management services and resilience. Plan application, configuration, messaging and database roles together; a VM snapshot alone is not a complete cluster recovery design.

Certificates and authorization

- Fabric authentication checks **certificate trust**, **organization identity** and the authorized device identity. Install the correct root chain and synchronize the WAN Edge authorization list.
- Controllers require signed **identity certificates**. Generate a CSR, obtain the certificate from the selected CA and install it with the appropriate trust chain.
- A **web-server certificate** secures browser access to vManage. It is distinct from the controller certificate used for fabric authentication.
- Hardware **SUDI** supplies a manufacturer-installed identity on supported IOS XE platforms. Register the correct hardware identity; inventory UDI and secure identity records can differ.
- Load the WAN Edge list through **Smart Account/PnP synchronization** or a signed authorized-list upload, then distribute it to controllers. Having a certificate alone does not authorize every device.
- **Valid**, **staging** and **invalid** are authorization states. Staging supports control connectivity before data-plane participation; invalidation prevents normal admission.
- **OpenSSL genrsa** creates a private key; **req -x509** creates a self-signed certificate. Keep private keys protected and distribute the public root certificate to trust participants.

Control connection troubleshooting

- Work from **underlay reachability** to DNS, ports/NAT, time, certificates and authorization. Check both directions through intervening firewalls before changing overlay policy.
- Use **show control local-properties**, **show control connections** and connection history on vEdge; IOS XE uses corresponding **show sdwan control** commands.
- **show certificate installed** exposes certificate details. Verify issuer, validity period and trust chain; correct clock synchronization is necessary for validity checks.
- **CTORGNMMIS** indicates organization-name mismatch. **DCONFAIL** identifies DTLS connection failure and requires reachability and handshake investigation rather than an assumed certificate diagnosis.

Controllers / WAN Edges

Implementing Cisco SD-WAN Solutions (ENSDWI)

KNOWLEDGE CHEATSHEET

EDGE DEPLOYMENT

Bootstrap Discover → **Authenticate** Join → **Configure** Templates → **Forward** OMP + BFD

- A **connect** state is an attempt in progress; **up** indicates an established session. A system-IP change can require session reestablishment and consistency checks across management records.
- **vdaemon** handles secure control connectivity. Event traces and control history help distinguish transport, authentication and process failures.

03 Router Deployment 20%

Onboarding and reusable configuration

- **ZTP/PnP** needs bootstrap connectivity, an address/default route, DNS and access to the discovery service. The redirect supplies organization and orchestrator information.
- After discovery, the edge authenticates to **vBond**, learns controller endpoints, establishes secure control connections and receives configuration from **vManage** using NETCONF.
- For virtual edges, use the assigned **chassis identity** and **activation token**. The vEdge Cloud activation command follows **request vedge-cloud activate chassis-number … token …** syntax.
- **Feature templates** describe individual functions; a **device template** combines them for a platform. Use global values for shared settings and device variables for unique addressing.
- A localized policy is associated with the **device template**; interface settings reference its ACL or QoS objects. Preview the generated configuration before attaching or updating devices.
- **Configuration groups** provide reusable configuration through feature profiles and parcels. Device tags can select subsets for association and deployment. Avoid competing configuration ownership.

OMP route types and path selection

- **OMP prefix routes (vRoutes)** advertise service-network prefixes and their VPN, originator, origin and TLOC next hops. **TLOC routes** describe transports; **service routes** advertise inserted services.
- An OMP prefix needs a **resolvable TLOC** and a usable data path for forwarding. A received route is not automatically installed or reachable.
- **OMP preference** favors higher values. Other selection factors include route validity, local administrative distance, origin type, origin metric and TLOC preference; compare attributes in their proper selection stage.
- **send-path-limit** controls advertised paths per prefix; **ecmp-limit** controls installed equal-cost paths. **send-backup-paths** lets vSmart advertise additional non-best alternatives.
- Controller-to-controller advertisements have a separate **controller-send-path-limit** setting. Raising one path limit does not automatically raise every advertisement or forwarding limit.
- Use **show omp peers**, **show omp routes**, **show omp tlocs** and **show omp services** on vEdge; use the **show sdwan omp** equivalents on IOS XE.

WAN Edges

Implementing Cisco SD-WAN Solutions (ENSDWI)

KNOWLEDGE CHEATSHEET

EDGE DEPLOYMENT

Bootstrap Discover → **Authenticate** Join → **Configure** Templates → **Forward** OMP + BFD

Routing integration and convergence

- Advertise required **connected**, **static** and supported routing-protocol routes into OMP. Redistribution from OMP into BGP, OSPF or EIGRP on the LAN is a separate configuration.
- **Administrative distance** compares route sources locally; a routing protocol's metric compares its own paths. OMP policy preference and BGP local preference are different attributes.
- **Overlay AS** supports BGP loop prevention when routes traverse OMP and return through another site. Use a consistent design across interconnected data centers; preserve AS paths when required.
- Use **BGP communities** and route policies to classify or filter exported prefixes. **no-export** restricts advertisement beyond the applicable AS boundary.
- OSPF **max-metric router-LSA** can make an edge a less preferred transit exit. **NSSA** allows redistributed external routes as Type 7 LSAs; default origination is a separate choice.
- **OMP hold time** detects missing peers; the **advertisement interval** controls update pacing. **Graceful restart** retains stale routing information temporarily after control loss.
- The **EOR timer** bounds restart synchronization while waiting for end-of-RIB information. Coordinate graceful-restart retention with IPsec key lifetime; cached routes cannot repair a failed data tunnel.

Local redundancy and tunnel health

- **TLOC extension** lets one edge use its neighbor's transport through a local interconnect. Configure the transport-owning side to extend the WAN interface and the receiving side as a tunnel attachment.
- The extension needs transport routing and adequate **MTU** for its encapsulation. Supported GRE-based extension enables designs beyond a directly connected Layer 2 handoff.
- **VRRP** supplies a shared LAN gateway. Higher priority normally wins; track overlay or relevant prefix reachability so a router with a failed WAN does not remain the active gateway.
- **BFD** tests edge-to-edge tunnel liveness and gathers loss, latency and jitter. Its hello interval and multiplier govern failure detection; application-route sampling governs SLA statistics.
- Use **show bfd sessions** for tunnel peers and **show bfd tloc-summary-list** for TLOC summaries on vEdge. Check local/remote color, session state and failure history.
- **vBond STUN** discovers translated IP addresses and ports. NAT type and mapping behavior affect direct tunnels; some symmetric-NAT combinations prevent successful hole punching.

WAN Edges / Policies

Implementing Cisco SD-WAN Solutions (ENSDWI)

KNOWLEDGE CHEATSHEET

POLICY DECISIONS

- **Control** — Routes & TLOCs
- **Data** — Packets
- **App route** — SLA paths
- **Local** — ACL & QoS

Multicast and cloud connectivity

- Hosts use **IGMP membership reports** to request multicast reception. **PIM** handles multicast routing on relevant service-side interfaces; OMP distributes overlay multicast control information.
- An overlay **replicator** receives traffic and creates copies for receivers. Multicast autodiscovery advertises replicator availability through vSmart; vSmart does not replicate user packets.
- Configure source, receiver and replicator roles for the required **service VPN**. A replicator with no local multicast hosts does not need LAN membership configuration merely to replicate overlay traffic.
- **Cloud OnRamp for IaaS** extends the overlay through cloud WAN Edges and transit networking. Prepare cloud permissions, supported marketplace images, templates, subnets and routing.
- **Cloud OnRamp for Multicloud** automates cloud gateway and cloud-network integration. AWS transit gateways, Azure VNet connectivity and Google Cloud connectivity have provider-specific designs.
- **Cloud OnRamp for Colocation** places shared security and optimization services in regional facilities. Service chains steer traffic through VNFs instead of deploying every service at every branch.

04 Policies 20%

Policy types and application direction

- **Centralized control policy** filters or changes OMP routes and TLOCs on vSmart. **Centralized data policy** matches packets and is enforced by WAN Edges.
- **Localized control policy** uses routing policies for local protocol behavior. **Localized data policy** provides interface ACLs, classification, marking, policing and QoS treatment.
- Build **groups of interest** first: sites, VPNs, prefixes, data prefixes, applications, colors, TLOCs and SLA classes as needed. Then define ordered match/action sequences and apply them.
- Sequences run from **lowest to highest number**, stopping at the first match. Deliberately configure the **default action** so unmatched traffic or routes receive the intended treatment.
- Control-policy **in** evaluates advertisements arriving at vSmart from listed sites; **out** evaluates advertisements sent toward listed sites. Direction is relative to vSmart.
- Data-policy **from-service** handles traffic entering from the LAN; **from-tunnel** handles traffic arriving from the overlay. Match the service VPN and apply to the intended site set.
- Use **show policy from-vsmart** on vEdge to inspect received policy. Verify counters and actual forwarding as well as successful policy activation.

Policies

Implementing Cisco SD-WAN Solutions (ENSDWI)

KNOWLEDGE CHEATSHEET

POLICY DECISIONS

- **Control** — Routes & TLOCs
- **Data** — Packets
- **App route** — SLA paths
- **Local** — ACL & QoS

Topology control and service insertion

- For **hub-and-spoke**, advertise hub TLOCs and appropriate routes to spokes while suppressing direct spoke connectivity. Hiding prefixes alone does not necessarily remove spoke-to-spoke tunnels.
- To change paths seen by selected spokes, apply an **outbound control policy** toward those spokes. Match a specific **originator** when the requirement targets one router rather than all future routers at a site.
- **Route preference** can favor a data center or transport for matching prefixes. Preserve a reachable backup unless the design explicitly requires traffic to stop when the preferred path fails.
- For **service insertion**, the edge attached to the firewall advertises the service in the relevant VPN. A control or data policy steers the selected traffic toward that service.
- Keep the **service next hop**, VPN, return path and firewall state consistent. Scope department-specific inspection with VPN, prefix or application matches instead of redirecting all traffic.
- **On-demand tunnels** initially use a hub path, then establish direct spoke tunnels when needed. Spoke enablement, traffic-engineering service and backup-TLOC policy must work together; idle timers remove unused tunnels.

Application-aware routing and SaaS

- **Application-aware routing** matches applications or traffic classes to an **SLA class** containing loss, latency and jitter thresholds. All configured SLA conditions must be satisfied.
- **preferred-color** selects the desired compliant transport. Define alternate compliant paths and backup behavior explicitly; preference alone is not a guarantee that traffic can never use another color.
- **Strict** SLA behavior can drop traffic when no eligible path satisfies the policy. Non-strict fallback and backup-SLA options serve continuity requirements; inspect the complete policy before predicting a path.
- BFD **poll interval** and the application-route averaging **multiplier** affect the observation window. A shorter window reacts faster but can follow transient variation.
- **Cloud OnRamp for SaaS** compares candidate Internet exits using measured application quality. A **client site** may use its own DIA or an overlay path to a **gateway site**.
- A **vQoE score** summarizes application experience. Service-VPN DNS, usable Internet exits and NAT must support probing and application identification; BFD tunnel health alone does not measure the whole SaaS path.

Policies / Security & QoS

Implementing Cisco SD-WAN Solutions (ENSDWI)

KNOWLEDGE CHEATSHEET

POLICY DECISIONS

- **Control** — Routes & TLOCs
- **Data** — Packets
- **App route** — SLA paths
- **Local** — ACL & QoS

DIA, route leaking and overlapping addresses

- **Direct Internet access (DIA)** sends selected service-VPN traffic through a local transport exit. Configure NAT on the Internet-facing **VPN 0** interface and a valid Internet route.
- A service-VPN default route into **VPN 0** enables route-based DIA. A centralized data policy can instead select applications, sources or destinations for **nat use-vpn 0** treatment.
- Order **private-destination exceptions** before a broad DIA match so internal traffic follows the overlay. Match a specific transport when egress source address or jurisdiction matters.
- **NAT fallback** permits normal route lookup when the intended DIA action is unavailable. Choose fallback according to availability requirements; verify translation and return traffic.
- **VPN membership policy** controls route distribution for VPN participation. **Route leaking** deliberately imports selected prefixes between VPNs and requires return reachability plus appropriate security policy.
- For shared DNS, DHCP or application services, define the **VPN lists** and **prefix lists** before the leaking policy. Use NAT or address redesign when overlapping prefixes must communicate.

05 Security and Quality of Service 15%

Secure fabric and application firewall

- **Certificates** authenticate fabric participants; **IPsec** protects data traffic. Modern supported data-plane suites include **AES-256-GCM** for encryption and integrity; GRE alone does not encrypt payloads.
- vSmart distributes **key information** through the secure control plane. Rekeying refreshes security associations; design key retention alongside graceful restart and supported pairwise-key behavior.
- **Zone-based firewall** groups interfaces or VPNs into source and destination zones. A directional **zone pair** selects the policy for traffic crossing that boundary.
- **Inspect** creates state for permitted flows and corresponding return traffic; **pass** permits without equivalent stateful inspection; **drop** rejects. Application awareness enables Layer 7 matching.
- A VPN belongs to a single firewall zone in the VPN-based model. Route leaking provides reachability; firewall policy separately determines which inter-VPN traffic is allowed.
- Integrated security support depends on **edge platform**, memory, software and licenses. Do not assume IOS XE threat-defense features are available on every vEdge or virtual router.

Security & QoS

Implementing Cisco SD-WAN Solutions (ENSDWI)

KNOWLEDGE CHEATSHEET

TRAFFIC TREATMENT

Classify Match → **Protect** Inspect → **Schedule** Queue → **Optimize** Deliver

Umbrella and integrated threat defense

- **Umbrella DNS security** evaluates DNS queries against domain intelligence. Configure registration credentials and attach the security policy; use **local-domain bypass** for internal namespaces.
- The **intelligent proxy** can inspect selected suspicious destinations instead of treating every domain identically. DNS filtering, URL filtering and full web inspection enforce at different stages.
- **Secure Internet Gateway (SIG)** sends traffic to cloud security over supported tunnels, commonly IPsec. Routing or data policy selects traffic; endpoint trackers support tunnel failover.
- **Snort IPS** detects network threats using signatures. Connectivity, Balanced and Security rule sets trade permissiveness against protection; select the appropriate inspection policy.
- **AMP** evaluates file reputation and disposition using hashes; **Threat Grid** supplies sandbox analysis. **Secure Endpoint** protects endpoints and files on hosts beyond the router's inspection path.
- A **TLS proxy** establishes separate client-side and server-side sessions to inspect eligible encrypted traffic. Trusted signing certificates and decryption policy are prerequisites; UTD evaluates the TLS ClientHello.
- **TrustSec** classifies identities into 16-bit **SGTs** and enforces group policy. **Inline tagging** carries tags with packets; **SXP** exchanges IP-to-SGT bindings. Check FIPS and platform compatibility.

QoS classification and scheduling

- Classify traffic on **ingress**, assign a **forwarding class**, map it to a queue and apply the **QoS map** on the appropriate egress interface. Marking alone does not allocate bandwidth.
- In the classic vEdge eight-queue model, **queue 0** provides low-latency priority service, commonly for voice. Other queues use weighted scheduling; protect control and BFD traffic from starvation.
- **LLQ** prioritizes delay-sensitive traffic; **WRR** shares service by weight. **WRED** drops probabilistically before a queue fills, using configured drop profiles.
- **DSCP rewrite** changes packet markings. **Packet loss priority** affects drop treatment during congestion; it is distinct from selecting a forwarding queue.
- A **policer** meters traffic with rate and burst limits and can drop excess packets. A **shaper** buffers traffic to smooth the output rate to the contracted circuit bandwidth.
- Check **units** before entering values: shaping fields may use Kbps, policer rates may use bps and bursts may use bytes. Convert explicitly: **1 byte = 8 bits**.
- **Adaptive QoS** adjusts shaping to available WAN capacity using configured bounds and measurements. Cloud-edge scheduling options such as **cloud-qos** depend on platform and interface direction.

Security & QoS / Operations

Implementing Cisco SD-WAN Solutions (ENSDWI)

KNOWLEDGE CHEATSHEET

OPERATE THE FABRIC

- **Events** — Conditions
- **Audit** — Changes
- **Telemetry** — Trends
- **API** — Automation

WAN optimization and loss mitigation

- **TCP optimization** proxies supported TCP flows and improves behavior across high-latency or lossy WAN paths. **SACK** identifies received segments so retransmission can target missing data.
- **Data redundancy elimination (DRE)** reduces repeated data transmission between optimization peers. Preserve **flow symmetry** and verify TCP-optimization and platform prerequisites.
- **Forward error correction (FEC)** adds recovery information to tolerate packet loss. **Packet duplication** sends copies over multiple paths and removes duplicates at the receiver, trading bandwidth for resilience.
- An **AppNav Controller** intercepts and distributes eligible flows to optimization service nodes. AppNav steers traffic; WAAS service nodes perform the acceleration.

06 Management and Operations 10%

Monitoring and operational evidence

- Devices send **events** to vManage; **alarms** correlate operational conditions that need attention. **Audit logs** record administrative actions such as configuration changes and software operations.
- Use **real-time monitoring** for current OMP routes, TLOCs, services, BFD and interface state. Historical statistics show trends; simulate flows and tunnel-health tools explain forwarding decisions.
- **vAnalytics** analyzes application usage and experience plus tunnel loss, latency and jitter. **DPI** identifies applications; **cflowd/flow telemetry** records traffic visibility for analysis.
- **SNMPv3** separates authentication from privacy: SHA/MD5-family choices authenticate, while AES-family choices encrypt supported sessions. Prefer secure algorithms supported by the device and operating mode.
- Use remote **syslog**, consistent NTP and deliberate local-disk logging settings. Syslog **alert** is severity 1; dashboard alarm labels such as Major describe a different classification system.
- Restrict in-band management with **allow-service**, ACLs and AAA. Prefer SSH and narrowly permitted services over broad access on transport interfaces; VPN 512 supports out-of-band access.

Software and access lifecycle

- The vManage **software repository** stores images locally or references remote servers. Ensure the selected management/transport path can reach the image source before scheduling downloads.
- Follow the target release's supported **upgrade path** and compatibility matrix. The usual controller sequence is **vManage → vBond → vSmart → WAN Edges**, with staged edge upgrades.
- **Upload**, **install**, **activate/reboot** and **set default** are distinct operations. Verify platform image type, free storage, post-upgrade control sessions and rollback readiness.

Operations

Implementing Cisco SD-WAN Solutions (ENSDWI)

KNOWLEDGE CHEATSHEET

OPERATE THE FABRIC

- **Events** — Conditions
- **Audit** — Changes
- **Telemetry** — Trends
- **API** — Automation

- An image referenced by a **service chain** or active software state can have deletion dependencies. Remove dependencies and retain a usable recovery image before repository cleanup.
- Use **RBAC**, user groups and supported VPN/segment scoping for least-privilege administration. Tenant separation requires deliberate controller, identity and configuration boundaries.

REST API automation

- vManage exposes authenticated **HTTPS REST APIs** under **/dataservice**. Automate inventory, monitoring and supported configuration workflows with the caller's assigned permissions.
- **GET** retrieves, **POST** creates or initiates actions, **PUT** updates and **DELETE** removes supported resources. **JSON** uses objects, arrays and scalar values; these are data types, not HTTP methods.
- Maintain the authentication **session cookie** and required **CSRF token**. Handle expiry and reuse sessions instead of creating a new login for every request.
- A successful action submission can return an **action ID** before work finishes. Poll task status and inspect per-device results before treating template attachment or upgrades as complete.
- Distinguish **real-time device queries** from **aggregated historical statistics**. Check the installed API schema for endpoint names, required parameters and supported operations.