Edge Foundations

Implementing Cisco Collaboration Cloud and Edge Solutions

KNOWLEDGE CHEATSHEET

FINDING A WORKING MEDIA PATH

ICE Gather candidates → **STUN** Check connectivity → **Direct** Use viable path → **TURN** Relay if needed

01 Collaboration edge foundations

NAT, signaling and media

- **NAT** changes packet addresses and ports, while SIP/SDP can still advertise private addresses inside the payload. Successful signaling alone does not prove that bidirectional media can flow.
- In **SDP**, the **c= connection line** identifies a media connection address; **m=** describes media type, port and formats; **b=** carries bandwidth information. Static NAT handling must advertise reachable media addresses.
- A **SIP ALG** attempts to inspect and rewrite signaling. Encrypted signaling prevents payload inspection; unwanted inspection can also corrupt traversal behavior. Use the intended Expressway traversal design and firewall policy.

ICE, STUN and TURN

- **ICE** gathers candidate media addresses, performs connectivity checks and selects a working candidate pair. Host, server-reflexive and relay candidates represent different possible paths.
- **STUN** discovers a NAT-mapped address and supports connectivity checks. **TURN** allocates a relay when a usable direct path cannot be established; restrictive NAT or firewall behavior can make relaying necessary.
- **Media optimization** can send media directly between compatible endpoints while signaling remains anchored through call control. ICE does not replace MRA registration, QoS or packet-loss recovery.
- For intermittent **one-way audio**, compare advertised candidates with actual packet flows. Check UDP reachability, NAT mappings, STUN/TURN access and relay fallback in both directions.

Expressway-C and Expressway-E

- **Expressway-C** connects to internal collaboration services; **Expressway-E** provides the external edge in the DMZ. Internal endpoints can remain registered to Unified CM while Expressway handles external access.
- The **traversal client on C** initiates the connection to the **traversal server on E**. Keepalives maintain the path so E can pass incoming requests over an established connection.
- **B2B calling** connects organizations using SIP or H.323 addressing. **MRA** proxies supported remote clients to enterprise UC services. MRA uses a dedicated **Unified Communications traversal zone**.
- Traversal carries signaling and multiplexed media across the firewall boundary. Separate signaling reachability from RTP/RTCP reachability when diagnosing a call.

Edge Foundations / Expressway

Implementing Cisco Collaboration Cloud and Edge Solutions

KNOWLEDGE CHEATSHEET

FINDING A WORKING MEDIA PATH

ICE Gather candidates → **STUN** Check connectivity → **Direct** Use viable path → **TURN** Relay if needed

Protocol and address interworking

- **SIP/H.323 interworking** translates supported call signaling between protocols. It differs from **transcoding**, which changes the media codec; endpoints still need compatible media capabilities.
- **Registered only** limits SIP/H.323 gateway behavior to calls involving a locally registered endpoint. **On** permits supported interworking even when neither endpoint is locally registered.
- **DTMF interworking** bridges supported RTP telephone events and H.245 user-input indications. Match the relay method across each call leg; signaling translation does not make every DTMF method interoperable.
- **IPv4/IPv6 interworking** requires a suitable dual-stack design. Configure addresses, DNS and firewall reachability for each family; two NICs and dual-stack operation are separate concepts.

Media encryption policy

- **TLS** protects signaling; **SRTP** protects media. Evaluate encryption on each call leg rather than assuming that encrypted signaling guarantees encrypted media.
- **Auto** applies no specific Expressway media encryption policy and follows endpoint requests. **Best effort** attempts encryption and permits unencrypted fallback.
- **Force encrypted** requires encrypted media and rejects an incompatible unencrypted leg. **Force unencrypted** requires clear media and may fail when the peer insists on encryption.
- Zone and subzone media policy applies to the associated **SIP call leg**. Expressway can invoke its **B2BUA** to enforce the policy; this is distinct from configuring a codec or a cipher name.

02 Expressway configuration and operations

Zones and call-routing paths

- A **neighbor zone** connects a known peer such as Unified CM, another Expressway or Cisco Meeting Server. A **DNS zone** discovers remote destinations from the called domain.
- A **traversal zone** crosses the firewall boundary. Match client/server roles, transport, ports and authentication on both sides; configuring a zone does not automatically create every required route.
- A typical **B2B path** is Unified CM SIP trunk to Expressway-C, traversal to Expressway-E, then a DNS-zone search toward the remote organization. Inbound routing follows explicit rules toward internal destinations.
- The **local zone** covers local routing resources; the **default zone** handles otherwise unclassified requests. Use source-zone distinctions to separate trusted internal calls from internet-originated calls.

Expressway

Implementing Cisco Collaboration Cloud and Edge Solutions

KNOWLEDGE CHEATSHEET

EXPRESSWAY ROUTING DECISIONS

Alias Normalize → **Policy** Authorize → **Search** Select zone → **Peer** Connect

Transforms, search rules and regex

- **Pre-search transforms** normalize the called alias before route searching. **Search rules** select target zones and can constrain source, protocol, pattern and authentication requirements.
- Transforms rewrite addresses; they do not change codecs. Normalize optional URI ports or alternate domains before a later suffix or regex match that expects a canonical address.
- For **regular expressions**, use **^** and **$** to anchor a complete match, **\d** for a digit, **{4}** for four repetitions, **\.** for a literal dot and parentheses for capture groups. **\1** reuses the first captured group.
- Process rules by configured **priority**; lower numeric values run first. Check **continue/stop on match** behavior and avoid broad patterns that shadow more specific destinations.
- For **IP dialing**, distinguish local unregistered IP destinations from internet IP calls. Keep internal routing indirect through the edge where required; restrict direct external IP routing deliberately.

DNS records and service selection

- **A/AAAA records** map hostnames to addresses. **SRV records** advertise a service target, port, priority and weight. Lower SRV priority is preferred; weight distributes selection among equal-priority targets.
- For **B2B SIP**, recognize **_sips._tcp** for TLS, **_sip._tcp** for TCP and **_sip._udp** for UDP. **_h323ls._udp** advertises the H.323 location service.
- **URI dialing** uses the destination domain for DNS discovery. Verify the resolver selected by Expressway, including any domain-specific DNS configuration, then resolve both the SRV target and its address.
- Use **FQDNs** that resolve from the calling system and match certificate identities. A failed neighbor zone can be a DNS or TLS problem even when the search rule is correct.

DMZ interfaces and static NAT

- **Single-NIC with static NAT** advertises Expressway-E's public NAT address. Expressway-C must be able to reach that advertised address; the firewall may need NAT reflection or an equivalent supported path.
- **Dual-NIC Expressway-E** separates internal and external DMZ paths. Place the default route toward the external network and add specific internal routes through the internal interface as needed.
- Configure **static NAT** on the appropriate Expressway-E interface to match the firewall translation. Check return-path routing and avoid overlapping subnets or unintended asymmetric paths.
- Opening one signaling port does not establish a complete deployment. Permit the required **client, traversal and media flows**, with the correct direction, source, destination and address translation.

Expressway

Implementing Cisco Collaboration Cloud and Edge Solutions

KNOWLEDGE CHEATSHEET

EXPRESSWAY ROUTING DECISIONS

Alias Normalize → **Policy** Authorize → **Search** Select zone → **Peer** Connect

Subzones, links, pipes and QoS

- **Subzones** group endpoints for bandwidth control. **Links** connect subzones and zones; **pipes** impose bandwidth restrictions on traffic using those links.
- A link can have multiple applicable bandwidth constraints; the **most restrictive available limit** governs admission. Confirm the required links exist before diagnosing a missing traversal path as a codec problem.
- **Call admission control** limits admitted demand. **QoS** classifies, marks, queues and shapes packets during congestion. Pipes alone do not prioritize packets on a saturated WAN.
- Apply QoS across endpoints, Expressway, switches and routers. Common enterprise markings include **EF 46** for voice and **AF41 34** for interactive video; verify the actual service policy and preserved markings.

Call policy and toll-fraud prevention

- **Call Policy** can allow, reject or redirect calls. Expressway supports local **CPL**, a policy service, or disabled policy; route selection and authorization serve different purposes.
- Restrict internet-originated calls to approved **domains and extension ranges**. Anchor regex patterns so a valid internal prefix cannot also match a longer PSTN destination.
- Require appropriate **authentication** before exposing PSTN routes. Do not treat arbitrary default-zone internet traffic as authenticated or infer trust solely from a caller-supplied URI.
- Use **Unified CM partitions and calling search spaces** to constrain the Expressway trunk as well. Trace source zone, normalized destination and matched policy when investigating toll fraud.

Licensing, backups and diagnostics

- Distinguish **system entitlement**, enabled features and concurrent session capacity. Traditional **release keys** enable a software release; **option keys** enable features. Smart Licensing uses entitlement registration and consumption reporting.
- **Rich Media Sessions**, traversal, advanced networking and TURN capacity refer to different licensing concerns. Match the installed licensing model and actual call type; MRA and B2B have different consumption rules.
- Back up **configuration and security material** securely and retain the encryption password. A backup is not a live-call checkpoint or an archive of all logs and call history.
- Restore to the **matching software release** and follow the cluster procedure using each peer's own backup. Preserve peer identity and certificates; plan backups explicitly rather than assuming an automatic schedule exists.
- Use **alarms**, diagnostic logging, search history and client problem reports together. For missing inbound B2B calls, first establish whether requests reach Expressway-E, then follow the call toward C and Unified CM.

Mobile & Remote Access

Implementing Cisco Collaboration Cloud and Edge Solutions

KNOWLEDGE CHEATSHEET

REMOTE ACCESS DEPENDENCIES

- **DNS** — Discover edge
- **TLS** — Establish trust
- **UC traversal** — Reach services
- **Provisioning** — Register client

03 Mobile and Remote Access

Discovery and UC prerequisites

- Publish **_collab-edge._tls.example.com** in external DNS for the user's discovery domain. Its target is an Expressway-E FQDN, normally on **TCP 8443**, with a publicly reachable address record.
- Internal Jabber discovery uses **_cisco-uds._tcp** toward Unified CM, normally on **TCP 8443**. Keep internal UC discovery records in the internal DNS view so remote clients select MRA correctly.
- Enable the appropriate **UC domains** on Expressway-C and discover the **Unified CM and IM and Presence nodes** needed by the deployment. Use suitable AXL permissions and verify service availability.
- Provision the user, associated devices, service profile and required UC services. Distinguish failure to discover services from failed credentials, failed XMPP binding or failed SIP registration.

Certificate identity and trust

- Validate the **trust chain**, expiry, intended usage and peer name. Install required root and intermediate CAs, keep **NTP** correct and use a server identity that matches the configured FQDN.
- The **Expressway-E certificate** includes the MRA discovery/registration domains. The **Expressway-C certificate** includes the secure phone security profile names for certificate-based secure registrations and its cluster name when clustered.
- Both Expressways require the appropriate **client-authentication certificate usage** for mutual TLS. For federated group chat, include the applicable chat-node aliases; use the CSR fields for the enabled features.
- A **private CA** can work where clients trust it; public trust is preferable at the external edge and required by clients whose trust stores cannot accept the private CA. Jabber trust does not imply phone trust.
- A CSR binds names to a public key; the signed certificate must match its **private key**. Use an appropriate RSA key size, commonly **2048 bits**, and a certificate template with the required server/client authentication usages.

Mobile & Remote Access

Implementing Cisco Collaboration Cloud and Edge Solutions

KNOWLEDGE CHEATSHEET

REMOTE ACCESS DEPENDENCIES

- **DNS** — Discover edge
- **TLS** — Establish trust
- **UC traversal** — Reach services
- **Provisioning** — Register client

UC traversal and secure call control

- Establish **mutual certificate trust** before enabling TLS verification on the UC traversal pair. A reachable peer can still fail because of an untrusted chain or a mismatched TLS verify subject name.
- When clustered, verify the expected **Expressway-C cluster identity** on E and ensure it is present in C's certificate. Peer addresses must resolve and match the identity verified on the receiving leg.
- For a secure **Unified CM SIP trunk**, Expressway trust belongs in **CallManager-trust**. **Tomcat** certificates secure HTTPS services; **CallManager** certificates secure SIP service identity.
- When B2B and MRA coexist, use a dedicated **Unified CM SIP trunk listening port** that avoids MRA line-registration ports. OAuth-enabled SIP lines can introduce additional port conflicts; trace the actual transport and listener.
- Do not disable certificate verification to conceal a trust failure. Correct the peer name, CA chain, certificate usage or certificate associated with the service.

Firewall flows and HTTP allow lists

- Recognize common MRA paths: **TCP 8443** for external discovery/HTTPS, **TCP 5061** for external secure SIP, **TCP 5222** for external XMPP, and **TCP 2222** from C to E for the SSH tunnel carrying proxied HTTP traffic.
- Traversal signaling commonly uses **TCP 7001**, and the C-to-E XMPP path commonly uses **TCP 7400**. Confirm the configured service ports and media ranges rather than applying one port list to every deployment.
- The **HTTP allow list on Expressway-C** controls proxied access to internal web resources. Add photo, update and other required servers using the correct scheme, host, port, path and supported method.
- Automatically generated inbound rules cover discovered UC services; **editable inbound rules** cover additional resources. Advanced file transfer may need access to all relevant IM and Presence nodes.
- Validate imported **CSV allow-list rules** against the expected columns and supported methods. Test the exact URL that the client requests instead of granting unrestricted access to an internal web server.

Mobile & Remote Access / Hybrid Services

Implementing Cisco Collaboration Cloud and Edge Solutions

KNOWLEDGE CHEATSHEET

REMOTE ACCESS DEPENDENCIES

- **DNS** — Discover edge
- **TLS** — Establish trust
- **UC traversal** — Reach services
- **Provisioning** — Register client

Authentication and failure isolation

- **SAML SSO** and **OAuth with refresh** address different functions: federated authentication and token-based authorization. Align Expressway authorization settings with the capabilities enabled on Unified CM.
- If **TCP SYNs receive no response**, inspect DNS targets, NAT and firewall paths first. A certificate problem occurs after TCP connectivity; a refused connection can indicate a closed port or inactive listener.
- For **TLS negotiation failure**, compare configured peer names with certificate SANs and inspect CA chains. For traversal **user not found**, verify the configured traversal credentials and the authentication database on E.
- For **HTTP 429**, review authentication rate controls and expected device demand. For XMPP failures, verify the XCP service, listening ports, IM and Presence health and intercluster synchronization.
- For **activation-code onboarding**, check supported phone firmware, the UC onboarding configuration, code validity and external discovery/connectivity. Enterprise MRA onboarding and cloud MPP registration use different provisioning paths.

04 Webex hybrid services and devices

Cloud, hybrid and connector roles

- **Control Hub** manages the Webex organization, users, services and devices. A hybrid deployment connects cloud capabilities to selected on-premises services while preserving their responsibilities.
- An **Expressway-C connector host** runs supported hybrid connectors and registers to the cloud. This is a separate role from Expressway-E's external traversal function.
- In a **Jabber hybrid deployment**, cloud messaging can coexist with **Unified CM calling** and separate voicemail or meeting services. Identify the provider of each service rather than assuming all functions moved to the cloud.
- **Jabber Team Messaging Mode** requires aligned identities in Unified CM and Webex. In **Webex Messenger** deployments, cloud accounts and policies govern IM/presence; phone and voicemail services need their own integrations.

Hybrid Services

Implementing Cisco Collaboration Cloud and Edge Solutions

KNOWLEDGE CHEATSHEET

HYBRID SERVICE RESPONSIBILITIES

- **Directory** — Identities
- **Calendar** — Meeting join
- **Video Mesh** — Local media
- **Edge & CCUC** — Cloud visibility

Messaging interoperability

- The **Hybrid Message Service model** uses an Expressway-C Message Connector between Webex messaging and on-premises IM and Presence. It is distinct from client registration through MRA.
- AXL access needs an enabled service, reachable publisher, trusted certificate and a dedicated **application account with Standard AXL API Access**. Avoid reusing the main administrator account for connector access.
- For multiple IM and Presence clusters, maintain **Intercluster Sync Agent** operation. **Resource groups** associate users with appropriate connector resources for geographic placement and availability.
- A **grayed contact** or unavailable presence is a user/service state signal. Check identity mapping, activity and presence connectivity before assuming that calling or the underlying IP network has failed.

Directory synchronization and domains

- **Directory Connector** runs on a supported Windows host and synchronizes on-premises **Active Directory** into Webex. Set the synchronization scope using selected containers and LDAP filters.
- Map names, email identity, **SIP addresses** and account-disabled state deliberately. A **dry run** previews changes; verify deletion impact before applying a changed filter or attribute mapping.
- After initial synchronization, check **incremental sync** scheduling, service health and logs for missing new users. Synchronization creates identities; licensing separately enables services.
- **Entra ID SCIM provisioning** synchronizes cloud identities directly. Verify assignment scope, provisioning logs, endpoint/token and attribute mappings; enabling SSO alone does not provision users.
- **Domain verification** proves ownership through DNS. **Domain claiming** associates the domain with the organization and controls where accounts are created. Directory room-resource SIP attributes can make on-premises rooms discoverable.

Hybrid Calendar and meeting join

- **Hybrid Calendar** reads supported calendar events to supply meeting details, scheduling integration and **one button to push (OBTP)**. **@webex** can request Webex meeting information in supported invitations.
- For **Microsoft 365** or **Google Workspace**, configure the respective cloud calendar integration, authorize the required application access and enable the intended users. Directory synchronization alone does not grant calendar access.

Hybrid Services

Implementing Cisco Collaboration Cloud and Edge Solutions

KNOWLEDGE CHEATSHEET

HYBRID SERVICE RESPONSIBILITIES

- **Directory** — Identities
- **Calendar** — Meeting join
- **Video Mesh** — Local media
- **Edge & CCUC** — Cloud visibility

- On-premises **Exchange** integration uses the supported Calendar Connector architecture. Choose the connector model from the mailbox platform rather than assuming every calendar needs Expressway.
- Use **bulk user updates** for existing users and appropriate **automatic license assignment templates** for future users. Verify mailbox identity, room/workspace configuration and service entitlement when OBTP is missing.

Video Mesh signaling and media

- **Video Mesh** hosts eligible meeting media on enterprise nodes, with cloud resources providing overflow and connections to other participants. It reduces some cloud media traffic without replacing Webex cloud control.
- **Cloud-registered clients** signal to Webex; **on-premises SIP endpoints** use Unified CM or Expressway call control, which routes their calls toward the configured Video Mesh resources.
- Clients use **STUN reachability and round-trip measurements** in media-cluster selection. Available on-premises resources, capacity and policy influence placement; geographic proximity alone does not determine the selected node.
- Nodes can form **cascades** to join meeting participants across nodes and the cloud. Spare capacity on another eligible node can serve additional participants; maintenance and capacity affect admission.
- Plan cloud signaling over **HTTPS**, media reachability, node-to-node paths and supported proxy behavior separately. A signaling proxy does not automatically proxy real-time UDP media.
- For **HD video**, verify the organization's video settings, supported endpoint resolution, available bandwidth and node capacity. Raising a resolution setting cannot repair congestion or packet loss.

Device linking and cloud visibility

- **Webex Edge for Devices** links supported on-premises registered devices to cloud management and features while retaining on-premises registration. Device linking is distinct from full cloud registration.
- Use **Device Connector** for supported device-linking workflows. Enable the required endpoint configuration control so Control Hub can manage supported settings instead of having Unified CM overwrite them.
- **Cloud-Connected UC** supplies cloud analytics, inventory and troubleshooting for on-premises UC. Its agent and service modules connect UC nodes to Control Hub; it does not relocate Unified CM call control.
- **RoomOS macros** automate device actions and workflows. Manage macro availability, configuration and software through supported device tools, and test how custom automation interacts with normal controls.

Cloud Calling & Management

Implementing Cisco Collaboration Cloud and Edge Solutions

KNOWLEDGE CHEATSHEET

CLOUD CALLING OPERATIONS

Identity Provision → **Calling** Route → **Security** Govern → **Telemetry** Diagnose

05 Cloud calling, security and management

SSO, claims and administrator roles

- **SAML SSO** federates Webex authentication to an IdP such as ADFS. Exchange **service-provider and IdP metadata**, configure the trust and claims, then test authentication before enabling the organization-wide change.
- Match the asserted identity to the Webex user. In **ADFS**, claim rules can map an email LDAP attribute to the expected **uid** claim; configure the NameID format required by the integration.
- Enforce **MFA** through the chosen identity provider or supported account policy. SSO authenticates users; it does not replace provisioning, service licenses or administrator authorization.
- Use **least-privilege roles and scopes** for user, device, calling and compliance administration. Organization-wide scope does not grant functions absent from the assigned role.

Calling coexistence and migration

- For a phased **Unified CM to Webex Calling migration**, inventory users, numbers, dial plans, devices and supported firmware. Validate feature compatibility and service assignments before moving a pilot group.
- A **local gateway** connects Webex Calling to supported on-premises PBX or PSTN resources. In Control Hub, **trunks** represent connections, **route groups** provide route choices and **dial plans** map patterns to routes.
- Preserve extension dialing with explicit **on-premises routing patterns** and normalize external numbers to **+E.164** where required. Coordinate cloud rules with Unified CM translations and route patterns to prevent loops.
- Before migrating a phone, provision its **Calling license, location and number/extension**. Check device eligibility, conversion entitlement and **Enterprise versus MPP firmware**; conversion alone does not complete cloud provisioning.
- Use supported **migration tools** to assess and transfer eligible configuration, then verify inbound, outbound, emergency and internal calling. Cloud-Connected UC visibility and phone migration are separate functions.

Cloud Calling & Management

Implementing Cisco Collaboration Cloud and Edge Solutions

KNOWLEDGE CHEATSHEET

CLOUD CALLING OPERATIONS

Identity Provision → **Calling** Route → **Security** Govern → **Telemetry** Diagnose

Local gateway and survivability

- For a secure **CUBE local gateway**, configure the applicable registration-based or certificate-based trunk, trusted CA chain, valid gateway identity, TLS signaling and compatible media security.
- **SIPS URI formatting** and **TLS transport** are separate settings: **url sips** affects URI/service discovery behavior, while **session transport tcp tls** selects transport. Check both against the gateway design.
- A **404 Not Found** after a request reaches the gateway suggests an unresolved destination or route. Inspect dial-peer matching and number normalization; a registered trunk can still have an incomplete dial plan.
- **Site Survivability** lets supported endpoints use a local survivability gateway during loss of cloud connectivity. It needs prior endpoint/gateway provisioning and a usable local calling or PSTN path.
- The gateway's **webex-sgw mode** and registration status identify survivability operation. Verify supported endpoint registrations and local call completion during a controlled outage; cloud-only features may be unavailable.

Calling features and shared workspaces

- For **auto attendants**, configure business/holiday schedules, language, menus and no-input handling. A menu timeout controls lack of caller input; ringing/no-answer treatment is a separate call-flow stage.
- For **call queues and operating modes**, check the active mode, schedule type, priority, time zone and manual overrides. A correctly defined schedule may not be the mode currently controlling calls.
- For **translation patterns**, verify scope, matching and replacement before routing. Location-specific behavior can explain why a short code works in one office but fails in another.
- **Call intercept** can reject calls even when a device is registered and its number is assigned. Check service features and policies before changing media or network settings for a rejected call.
- **Hot desking** gives supported shared workspace phones temporary user personalization. Configure the workspace/device capability and eligible users; shared lines and call park solve different needs.

Cloud Calling & Management

Implementing Cisco Collaboration Cloud and Edge Solutions

KNOWLEDGE CHEATSHEET

CLOUD CALLING OPERATIONS

Identity Provision → **Calling** Route → **Security** Govern → **Telemetry** Diagnose

Encryption, compliance and external access

- Distinguish **transport encryption**, service encryption at rest and **end-to-end encryption**. Eligibility and feature support depend on the meeting or messaging mode; one security toggle does not enforce every requirement.
- The **identity service** handles authentication and tokens; the **key management service** handles content keys; content services store encrypted content. Key custody and content storage are separate responsibilities.
- **Hybrid Data Security** places supported Webex content key services on premises. Configure HDS nodes, certificates, database access, network/proxy connectivity and redundancy using the supported setup tooling.
- **eDiscovery, retention, legal hold and DLP** govern supported content through compliance roles and integrations. HDS is not a blanket mechanism for every meeting type or a substitute for device-access policy.
- For **external communication restrictions**, check allowed domains, exempt groups and existing memberships. Do not assume a new policy removes external participants already in spaces; review and remediate existing access explicitly.

Control Hub troubleshooting and quality

- Use **Control Hub troubleshooting** for participant-level meeting and call details, and **analytics** for trends. Search by meeting or user identity and align the date, time zone and available retention window.
- For **one-way audio**, check mute, selected microphone, permissions and actual outbound media, then inspect firewall behavior and loss. Successful call setup and device registration do not prove healthy audio.
- Compare **loss, jitter, latency and bandwidth** by participant, direction and region. A shared regional impairment suggests a common network path; a single participant may indicate a local device or access link.
- During WAN congestion, validate **DSCP classification**, low-latency voice queues and video bandwidth allocation. Shape traffic to the real bottleneck and confirm packet counters; prioritization cannot create bandwidth.
- For a failed **cloud activation**, verify code validity, firmware, DNS, time and required service URLs/ports. General internet ping reachability does not establish access to Webex provisioning services.

Cloud Calling & Management

Implementing Cisco Collaboration Cloud and Edge Solutions

KNOWLEDGE CHEATSHEET

CLOUD CALLING OPERATIONS

Identity Provision → **Calling** Route → **Security** Govern → **Telemetry** Diagnose

APIs, applications and meeting controls

- Use **Messaging APIs** to create messages, **People APIs** for profiles and **Meetings APIs** for supported meeting workflows. The messaging create operation is **POST /v1/messages** on the Webex APIs service.
- Use supported **webhooks** for event notifications and APIs for follow-up actions. Separate meeting lifecycle events from Calling records and compliance events; choose permissions and resources for each requirement.
- The **Webex Developer portal** supports integrations and bots; **App Hub** helps users discover apps; **Control Hub** governs organizational services and device administration. Use scoped OAuth access and secure token storage.
- **Meeting sharing privileges** control who may present content, while site or organization policy sets defaults and limits. Host controls, authenticated participation and managed-device requirements need their own configuration.
- The **AI Assistant** can generate supported meeting summaries, key points and action items. Check entitlement and organizational settings; AI summaries, translation and noise removal are distinct features.