

IT 資格道場

CCNP ENCOR 350-401 学 習用テキスト

予備知識ゼロから合格ラインへ —— 読んで理解する1冊目

無料サンプル(第1章まで)

Cisco CCNP Enterprise ENCOR 350-401 v1.2 Exam Topics(Cisco 公式 PDF・2026-10-13 取得)準拠
2026年10月版

ご利用にあたって

- このテキストは「IT資格道場」(www.shikaku-doujou.com)の購入者限定テキストのうち、学習用テキストの第1章までを収録した**無料サンプル**です。どなたでもご覧いただけます。
- 無料サンプルも著作物です。転載・改変しての再配布・二次販売はできません。
- AI モデルの学習データとしてのご利用(学習目的の入力・データセット化を含む)はできません。
- 製品版(学習用テキスト・頻出度別ノート・暗記用ノートの3点)は、ご購入者を識別できる透かし入りのPDFとして提供されます。
- 本PDFはスマートフォン・タブレットでの閲覧に合わせたA5版面・文字サイズで組版しています。

目次

試験の概要 [intro]

第1章 アーキテクチャ [1.1.a/1.1.b/1.2.a/1.2.b/1.3.a/1.3.b/1.4]

階層型設計:2層・3層・コラプストコア [1.1.a]

ファブリック設計:スパインリーフ [1.1.a]

オンプレミスとクラウド:IaaS/PaaS/SaaS とパブリック/プライベート/ハイブリッド [1.1.a]

冗長化の考え方:機器・リンク・電源 [1.1.b]

SSO・NSF・NSR:スーパーバイザ冗長 [1.1.b]

StackWise・VSS:スタックと仮想シャーシ [1.1.b]

FHRP:HSRP・VRRP・GLBP [1.1.b]

Catalyst SD-WAN の構成要素:Manager・Controller・Validator・WAN Edge [1.2.a]

コントロールプレーンとデータプレーン:OMP・TLOC・IPsec・BFD [1.2.a]

カラー、制御ポリシーとデータポリシー、REST API [1.2.a]

SD-WAN の利点と制約 [1.2.b]

SD-Access の構成:コントロールプレーンノード・ボーダー・エッジ・ファブリック WLC
[1.3.a]

SD-Access のプレーン:LISP・VXLAN・CTS/SGT [1.3.a]

従来キャンパスとの相互接続:ボーダーノードとフュージョンルータ [1.3.b]

QoS の分類とマーキング:DSCP・CoS・信頼境界 [1.4]

MQC の設定の読み取り:class-map・policy-map・service-policy [1.4]

ポリシングとシェーピング,LLQ・CBWFQ・WRED [1.4]

サンプルはここまでです

試験の概要 [intro]

ENCOR(試験コード 350-401)は、CCNP Enterprise と CCIE Enterprise の認定に共通する試験で、企業ネットワークの中核の技術を扱います。試験時間は 120 分です。出題範囲は v1.2 の 6 分野できていて、この教材の第 1 章から第 6 章は、分野の順を入れ替えていません。問題数と合格点は、Cisco の公式の範囲に記載がありません。

章	分野(v1.2)	配点
第 1 章	アーキテクチャ (Architecture)	15%
第 2 章	仮想化(Virtualization)	10%
第 3 章	インフラストラクチャ (Infrastructure)	30%
第 4 章	ネットワークアシュアランス (Network Assurance)	10%
第 5 章	セキュリティ(Security)	20%
第 6 章	自動化と AI(Automation and Artificial Intelligence)	15%

見出しの末尾の [1.1.a] は、v1.2 の細目の番号です。受験料や試験日程は、申し込みの前に Cisco 公式サイトで最新情報をご確認ください。

第1章 アーキテクチャ

[1.1.a/1.1.b/1.2.a/1.2.b/1.3.a/1.3.b/1.4]

この章は、企業ネットワークの土台の作り方を扱う。順に、キャンパスの層構造、冗長化、SD-WAN、SD-Access、QoS を読む。

設計の問いは「どの機器にどの役割を置くか」で決まる。設定の問いは「出力のどの行が原因か」で決まる。この 2 つを手で言えるようになるのが、この章の目標です。

階層型設計:2 層・3 層・コラプストコア [1.1.a]

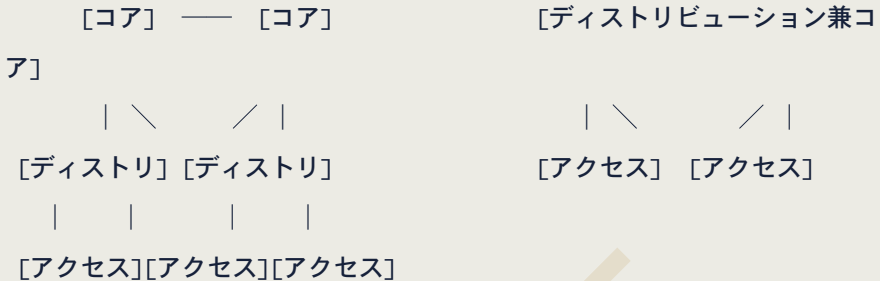
キャンパス LAN は、役割の違う層を積んで作ります。基本は 3 層。端末に近い側から、アクセス層・ディストリビューション層・コア層と呼びます。

層	役割	置くもの
アクセス層	端末の収容	PoE、ポートセキュリティ、QoS の信頼境界
ディストリビューション層	アクセスの集約と、サービスへの入口	経路集約、ポリシー、FHRP
コア層	ディストリビューション同士の高速な転送	転送だけ。ポリシーは置かない

Cisco の設計ガイドは、アクセスを「端末と利用者がネットワークへ直接入る層」、ディストリビューションを「アクセスを集約しサービスへつなぐ層」と書いています。コアは「大規模な LAN でディストリビューション同士をつなぐ層」です[1-1]。コアが止まると全体に響く。だからコアには、速く運ぶ以外の仕事を載せません。

3 層

2 層(コラプストコア)



2 層は、ディストリビューションとコアを 1 つの層に畳んだ設計です。この畳んだ層を**コラプストコア**と呼びます。建物が 1 つのキャンパスや、小さな拠点で使う。ネットワークが大きくなると、WAN との境界やインターネットへの出口が増えます。それらをアクセス側のディストリビューションから切り離したくなったとき、専用のコアを足した 3 層へ移ります。つまり 3 層は、規模が大きくなったときの形だ。

試験では、機能をどの層に置くかが問われます。アクセス層に置くのは、PoE、ポートセキュリティ、QoS の信頼境界です。ディストリビューション層に置くのは、経路集約、アクセスリスト、FHRP のゲートウェイです。コア層は転送だけを担当する。「コアにアクセスリストを置く」という選択肢は誤りです。

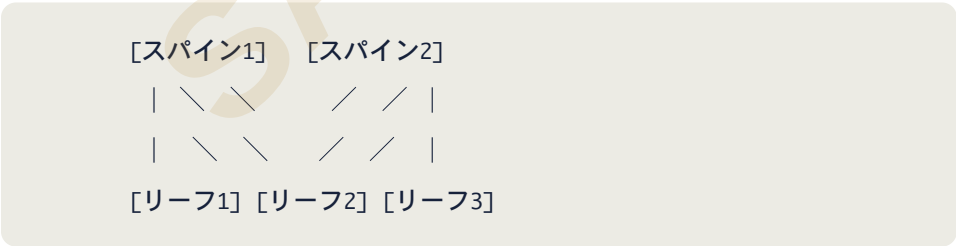
STP のブロックを減らす設計もある。アクセスとディストリビューションの間を L3 にする**ルーテッドアクセス**です。L3 の境界がアクセススイッチまで下がるので、その間のスパンニングツリーのループが無くなります。収束はルーティングプロトコルが担います。代わりに、VLAN は 1 つの配線室の中に閉じ、別の階へ同じ VLAN を延ばせません。

比較	L2 アクセス	ルーテッドアクセス
L2/L3 の境界	ディストリビューション	アクセス
ループの抑止	STP がブロックする	複数の経路をルーティングが使い分ける
ゲートウェイの冗長	FHRP が要る	アクセス自身がゲートウェイ
VLAN の広がり	複数の配線室へ延ばせる	1 つの配線室だけ

もう 1 つ、**モジュール化**があります。建物やブロックごとに同じ形の部品で組むと、障害の影響が他へ広がりません。増設も切り分けも、部品の単位で済みます。

ファブリック設計:スパインリーフ [1.1.a]

データセンターで使う**スパインリーフ**は、階層型と形が違います。リーフが端末やサーバを収容し、スパインがリーフ同士をつなぎます。



決まりは 3 つです。

- リーフは全てのスパインに接続する。
- リーフ同士は直接つながらない。
- スパイン同士も直接つながらない。

この結果、どのリーフ間でも通信は「リーフ → スパイン → リーフ」の 2 ホップになります。スパインの本数だけ等コスト(ECMP)の経路が並ぶので、どのリーフ間も同じ遅延で、負荷も分かれます。

拡張は横に広がります。容量が足りなければスパインを足し、ポートが足りなければリーフを足す。3 層のように、上位の機器を大きな機種へ入れ替える必要はありません。スパインとリーフの間を L3 で組み、その上にオーバーレイを重ねたものが、ファブリックです。SD-Access のファブリックは 1.3.a で読みます。

オンプレミスとクラウド: IaaS/PaaS/SaaS とパブリック/プライベート/ハイブリッド [1.1.a]

クラウドの分類は NIST SP 800-145 が決めたものを、試験もそのまま使います [^t1-2]。定義は「5 つの特徴・3 つのサービスモデル・4 つの配置モデル」です。

5 つの特徴は次のとおり。

- オンデマンド・セルフサービス
- 幅広いネットワークアクセス
- リソースの共用
- スピーディな拡張性
- サービスが計測可能

サービスモデルは、利用者が管理する範囲で分けます。

モデル	事業者が提供する範囲	利用者が管理する範囲	例
IaaS	サーバ・ストレージ・ネットワークの基盤	OS、ミドルウェア、アプリ、データ	仮想マシンを借りる

モデル	事業者が提供する 範囲	利用者が管理する 範囲	例
PaaS	基盤と実行環境	アプリとデータ	アプリを置くだけで 動く環境
SaaS	アプリまで	利用者の設定とデ ータ	Web 上のメール・グ ループウェア

利用者の管理範囲は IaaS が最も広く、PaaS、SaaS の順に狭くなる。「OS のパッチは誰が当てるか」と聞かれたら、IaaS は利用者、PaaS と SaaS は事業者です。

配置モデルは 4 つです。**パブリック**は、不特定の利用者が共用する事業者の基盤です。**プライベート**は 1 つの組織だけが使う基盤で、自社のデータセンターに置いても、事業者に預けてもかまいません。**コミュニティ**は、共通の目的を持つ複数の組織が共有します。**ハイブリッド**は、パブリックとプライベートなど 2 つ以上を組み合わせた形です。

オンプレミスとの違いは、遅延と費用の出方に出る。クラウドはインターネットか WAN をはさむので、遅延が増え、回線の状態にも左右されます。初期費用、設置場所、拡張の速さはクラウドが有利です。拠点からクラウドへの出口をどこに置くかは、設計の論点になる。これを 1.2 の SD-WAN が解きます。

冗長化の考え方:機器・リンク・電源 [1.1.b]

高可用性は、単一障害点を 1 つずつ潰して作ります。冗長にする対象は、層ごとに違う。

対象	冗長的手段
機器	スーパーバイザの 2 枚挿し、電源とファンの冗長
リンク	EtherChannel、複数の経路
ゲートウェイ	FHRP(HSRP・VRRP・GLBP)
経路	ルーティングの等コスト経路

電源は 2 系統から給電を受け、1 台が落ちても動き続けるように組みます。リンクは 1 本の太い線よりも、複数の線を束ね、片方が切れても残りで続ける形にします。冗長化は、切り替わる速さと、切り替わるときに途切れる通信の量で評価する。以降の節は、この途切れを縮める技法です。

SSO・NSF・NSR:スーパーバイザ冗長 [1.1.b]

スーパーバイザを 2 枚持つ機種では、片方(アクティブ)が壊れると、もう片方(スタンバイ)へ切り替えます。切り替わり方を決めるものが冗長モードだ。

RPR(Route Processor Redundancy)は、スタンバイの OS だけ先に起動しておく方式です。切り替わる時、スタンバイは起動時の設定を読み直し、カードを再起動します。起動時の設定は同期されますが、動作中の状態は同期されません。そのぶん復旧に時間がかかる。

SSO(Stateful Switchover)は、アクティブの設定と状態をスタンバイへ同期し続ける方式です。最初に全体を一括で同期し、その後は変化のたびに差分を同期します[^t1-3]。スタンバイは状態をすでに持っているので、切り替わっても L2 の転送を止めません。

```
Switch(config)# redundancy
Switch(config-red)# mode sso
```

設定は上の 2 行です。SSO の前提は、2 枚のスーパーバイザが同じ IOS XE の版を動かしていることです。版が違うと、設定が sso でも SSO では動きません。

NSF(Nonstop Forwarding)は、切り替えの間もデータの転送を続ける仕組みです。転送は、切り替え前から持っている古い転送情報(FIB)で続けます。その裏で、ルーティングプロトコルが経路を作り直す。ルーティングプロトコルが動いているのはアクティブだけで、スタンバイでは動いていません。切り替えのあとは、隣のルータに状態を送り直してもらいます。この隣の協力の仕組みを**グレースフルリスタート**と呼びます。

NSF の用語は 2 つあります。

- **NSF 対応(capable)**: NSF を設定した機器。隣の NSF 対応か NSF 認識の機器から、経路情報を作り直せる。
- **NSF 認識(aware)**: NSF に対応したソフトウェアを動かしている機器。自分は切り替えませんが、隣の切り替えを手伝える。

BGP の NSF では、隣がすべて NSF 認識で、BGP のグレースフルリスタートが設定されている必要があります。BGP は、セッションを張る OPEN メッセージの中で「グレースフルリスタートに対応している」と宣言し合います。両者が宣言を交換していないセッションは、グレースフルリスタートの対象になりません。NSF は SSO の上に載る機能なので、先に SSO を設定します。

NSR(Nonstop Routing)は、ルーティングプロトコルの状態そのものをスタンバイへ同期する方式です。隣の協力が要らないので、隣が NSF 認識でなくて

も使える。NSF と NSR の違いは「隣に助けてもらうか、自分で状態を持つか」の 1 点です。

技法	何を守るか	隣の協力
SSO	設定と状態を同期し、L2 の転送を止めない	要らない
NSF	切り替え中のデータ転送。経路は隣に再送してもらう	要る(NSF 認識)
NSR	ルーティングの状態をスタンバイが持つ	要らない

確認は `show redundancy states` で行います。

```
Switch# show redundancy states
my state = 13 -ACTIVE
peer state = 8  -STANDBY HOT
Mode = Duplex
Unit = Primary
Redundancy Mode (Operational) = sso
Redundancy Mode (Configured)  = sso
Redundancy State                = sso
```

読む順番は決まっている。まず `peer state` が `STANDBY HOT` かどうかを見る。`STANDBY HOT` は、スタンバイが同期を終え、いつでも引き継げる状態を指します。次に `Operational` と `Configured` を比べる。設定が `sso` でも、2 枚の版が違えば `Operational` は `sso` になりません。この出力が示すのは、設定ではなく実際に動いているモードです[^t1-3]。

切り替えを試すときは `redundancy force-switchover` を使います。`reload` は SSO の機能ではなく、機器全体を再起動して転送を止めてしまう。

障害の種類と、効く技法の対応も覚えます。試験は「この障害に効くのはどれか」の形で問います。

障害	効く技法
スーパーバイザの故障	SSO(状態の同期)と NSF/NSR(経路の維持)
筐体 1 台の故障	StackWise、StackWise Virtual、VSS
端末のゲートウェイ機器の故障	FHRP(HSRP・VRRP・GLBP)
リンク 1 本の断線	EtherChannel、複数の経路
電源の故障	電源の冗長

「ゲートウェイの故障に SSO が効く」は誤りです。SSO はスーパーバイザ 2 枚の間の話で、ルータ 2 台の間の話ではありません。2 台のルータで守るなら FHRP です。

StackWise・VSS:スタックと仮想シャーシ [1.1.b]

スタンバイを別の筐体にする方法が、スタックと仮想シャーシです。複数のスイッチを 1 台の論理スイッチとして扱います。

StackWise(スタック)は、Catalyst 9200・9300 のスタックケーブルで、最大 8 台を輪にしてつなぐ方式です。起動後の 120 秒の間に、アクティブとスタンバイが選ばれる。優先度が高いほうが先で、同じなら起動にかかる時間が短いほう、それも同じなら MAC アドレスが小さいほうです(今のアクティブがあれば、それがそのまま残ります)。優先度は手で設定します。変えた値はすぐ記録

されますが、今のアクティブは替わらず、アクティブかスタックが再起動したときの選出に効きます。

StackWise Virtual(SVL)は、Catalyst 9000 の 2 台を 1 台の論理スイッチにします[1-4]。2 台をつなぐ線を **StackWise Virtual Link(SVL)** と呼び、制御と転送の通信を全部運びます。アクティブが L2/L3 の制御と管理を担当し、スタンバイは同期されたホットスタンバイです。転送は両方の機器が、自分のポートで行います。周りのスイッチから見ると 1 台のブリッジなので、アクセスから 2 台へのアップリンクを、ループ無しで張れます。

```
Switch(config)# stackwise-virtual
Switch(config-stackwise-virtual)# domain 1
Switch(config)# interface TenGigabitEthernet1/0/1
Switch(config-if)# stackwise-virtual link 1
Switch(config)# interface TenGigabitEthernet1/0/40
Switch(config-if)# stackwise-virtual dual-active-detection
```

条件は次のとおり。

- 2 台は同じ機種で、同じ版・同じライセンス・同じ SDM テンプレートにする。
- SVL のポートは、同じ速さにそろえる。
- VLAN 4094 は機器間の制御に使われるので、ネットワークのどこにも作らない。
- SVL のポートと DAD のポートは、別にする。

DAD(Dual-Active Detection)は、SVL が切れたときの事故を防ぎます。SVL が切れると、スタンバイは「アクティブが壊れた」と見なして自分がアクティブ

になる。同じ IP と同じ設定のアクティブが、2 台並んでしまいます。DAD は SVL とは別の経路で、互いの生死を見ます。方式は 2 つある。**ファストハロー** は、専用の直結リンクで状態を交換する。**ePAgP** は、2 台にまたがる EtherChannel の PAgP メッセージにアクティブの ID を載せ、変化から検知します。二重のアクティブを検知すると、元のアクティブ側がリカバリモードに入り、SVL と管理用のインタフェース以外を止めて待機します。SVL が直ると、その機器は再起動してスタンバイに戻ります[^t1-4]。

```
Switch# show stackwise-virtual link
```

Switch	SVL	Ports	Link-Status	Protocol-Status
1	1	TenGigabitEthernet1/0/1	U	R
2	1	TenGigabitEthernet2/0/1	U	R


```
Switch# show stackwise-virtual dual-active-detection
```

In dual-active recovery mode: No

Switch	Dad port	Status
1	TenGigabitEthernet1/0/40	up
2	TenGigabitEthernet2/0/40	up

(出力は一部を省略している。) Link-Status の U は up、Protocol-Status の R は ready を表します。2 台とも U と R なら、SVL は正常です。DAD の Status が up なら、バックアップの見張りも生きている。

VSS(Virtual Switching System) は、StackWise Virtual より前の方式で、Catalyst 6500・4500 の 2 台を 1 台にします。線は VSL と呼ぶ。switch virtual domain でドメインを作り、機器に 1 か 2 の番号を与えます。確認には show switch virtual と show switch virtual link を使う。考え方は StackWise Virtual と同じで、名前と対象機種だけが違います。

方式	つなぐ線	台数	対象
StackWise	スタックケーブル (輪)	最大 8 台	Catalyst 9200・ 9300
StackWise Virtual	SVL	2 台	Catalyst 9000
VSS	VSL	2 台	Catalyst 6500・ 4500

FHRP:HSRP・VRRP・GLBP [1.1.b]

スイッチを 1 台に見せる方法とは別に、端末のデフォルトゲートウェイを冗長にする方法があります。端末のゲートウェイには IP アドレスを 1 つしか書けません。そこで複数のルータが、1 つの**仮想 IP** を共有します。これが **FHRP**(First Hop Redundancy Protocol)で、種類は 3 つです。

項目	HSRP	VRRP	GLBP
規格	Cisco 独自	標準(RFC 5798)	Cisco 独自
役割名	アクティブ・スタンバイ	マスター・バックアップ	AVG(代表)・AVF
優先度の既定	100	100	100
横取り(preempt)の既定	無効	有効	フォワーダは有効、AVG は無効
通信	224.0.0.2(v1)・ 224.0.0.102(v2)	224.0.0.18(IP プロトコル 112)	224.0.0.102
仮想 MAC	0000.0C07.ACxx(v1)・ 0000.0C9F.Fxxx(v2)	0000.5E00.01xx	1 グループに最大 4 つ

項目	HSRP	VRRP	GLBP
負荷分散	グループを分けて手動	グループを分けて手動	1グループの中で自動

HSRP の既定の hello は 3 秒、hold は 10 秒です[^t3-25]。グループ番号は、バージョン 1 が 0 から 255、バージョン 2 が 0 から 4095 です[^t1-5]。優先度が高いルータがアクティブになり、同じなら IP アドレスが大きいほうが選ばれます。**横取りは既定で無効**です。優先度の高いルータが復旧しても、`standby preempt` が無ければアクティブを取り返しません。

```
Switch(config)# interface vlan 10
Switch(config-if)# ip address 10.1.10.2 255.255.255.0
Switch(config-if)# standby 10 ip 10.1.10.1
Switch(config-if)# standby 10 priority 110
Switch(config-if)# standby 10 preempt
Switch(config-if)# standby 10 track 1 decrement 20
```

最後の `track` は、追跡対象(たとえば上流のリンク)が落ちたとき、優先度を `decrement` の値だけ下げます。書かなければ下げ幅は 10 です。上の例で上流が落ちると、優先度は 110 から 90 になる。相手の優先度が 100 のままなら、相手が上回ります。役割が動くのは、上回った相手に `preempt` が設定されている場合です。相手に `preempt` が無ければ、こちらの優先度が下がってもアクティブは動きません。

```
Switch# show standby brief
```

```
          P indicates configured to preempt.
```

```
          |
```

Interface	Grp	Pri	P	State	Active	Standby	Virtual IP
Vl10	10	110	P	Active	local	10.1.10.3	10.1.10.1

読み方は次の順です。P が付いていれば、横取りが設定されている。State は自機の役割で、Active の列が local なら自機がアクティブ。Standby の列が unknown なら、相手がまだ見つかっていません。

HSRP の状態は、Initial → Learn → Listen → Speak → Standby → Active の 6 つです。メッセージは Hello・Coupe・Resign の 3 種類で、Coupe は横取りでアクティブを奪うとき、Resign はアクティブを手放すときに出る。

VRRP は標準規格で、マスターは優先度で決まります。**横取りが既定で有効**です。仮想 IP を自分の実アドレスとして持つ機器(アドレスオーナー)の優先度は 255 で、必ずマスターになります。広告の間隔は既定で 1 秒です[^t1-6]。優先度 0 の広告は「マスターが VRRP をやめる」という意味で、バックアップは待たずに引き継ぎます。HSRP との違いは、横取りの既定が逆な点です。

GLBP は、負荷分散までやる Cisco 独自の方式です。AVG が ARP 要求に対して、**AVF ごとに異なる仮想 MAC** を返します[^t1-7]。端末ごとに別のルータへ送られるので、1 つの仮想 IP のまま複数のルータが転送します。hello は 3 秒ごとに 224.0.0.102 へ出ます。

```
Switch(config-if)# glbp 10 ip 10.1.10.1
Switch(config-if)# glbp 10 priority 110
Switch(config-if)# glbp 10 preempt
Switch(config-if)# glbp 10 load-balancing round-robin
```

SSO と FHRP は組み合わせて使えます。SSO の機器では、HSRP の状態もスタンバイのスーパーバイザへ同期されます(SSO 対応の HSRP)。既定で有効で、切り替えでもアクティブの役割を手放しません。GLBP も同じく既定で有効です。ただし GLBP では、Enhanced Object Tracking が SSO に対応していないため、SSO モードでは併用できません。

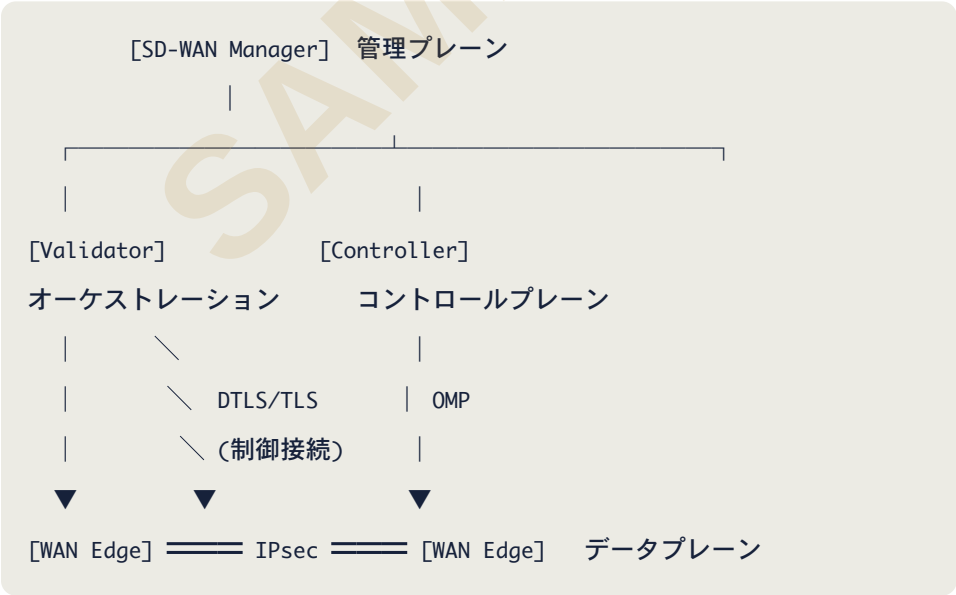
Catalyst SD-WAN の構成要素: Manager・Controller・Validator・WAN Edge [1.2.a]

Cisco Catalyst SD-WAN は、拠点間の WAN を中央から管理する仕組みです。機器は 4 種類あり、役割はプレーンで分かります。旧名も試験に出るので、組で覚えます[^t1-8]。

現在の名前	旧名	プレーン	役割
SD-WAN Manager	vManage	管理	GUI、テンプレート、ポリシーの作成、監視、REST API
SD-WAN Controller	vSmart	コントロール	OMP で WAN Edge へ経路・TLOC・ポリシーを配る

現在の名前	旧名	プレーン	役割
SD-WAN Validator	vBond	オーケストレーション	最初の認証、コントローラの場所の通知、NAT 越えの手助け
WAN Edge	vEdge・cEdge	データ	拠点間の IPsec トンネルでユーザのデータを運ぶ

Controller は経路の表を持って配るだけで、ユーザのデータは通りません。ユーザのデータが通るのは、WAN Edge どうしのトンネルだけです。Validator は WAN Edge が最初に会う相手で、パブリック IP アドレスを持つ必要があります。WAN Edge はハードウェアでも仮想でもかまいません。vEdge は旧 Viptela の OS で動く機器、cEdge は IOS XE で動く機器を指します。



WAN Edge が参加するときの流れは、決まった順です。

- 1. 最初に Validator へつなぎ、認証を受ける。
- 2. Validator から、Manager と Controller の場所を教わる。
- 3. Manager と Controller のそれぞれへ、常時の制御接続を張る。
- 4. 制御接続が張れたら、Validator との接続は切れる。

制御接続は DTLS(既定)または TLS で張ります。状態は次の出力で見る。

```
Edge1# show sdwan control connections
```

PEER TYPE	PEER PROT	SYSTEM IP	SITE ID	PEER PRIVATE IP	PEER PRIVATE PORT	LOCAL COLOR
vsmart	dtls	10.1.1.3	100	203.0.113.13	12346	mpls
up						
vsmart	dtls	10.1.1.3	100	203.0.113.13	12346	biz-internet
up						
vmanage	dtls	10.1.1.1	100	203.0.113.11	12346	mpls
up						
vbond	dtls	0.0.0.0	0	203.0.113.12	12346	mpls
tear_down						

最後の `vbond` の行は、`SYSTEM IP` が `0.0.0.0` と表示されます。Cisco の出力例でも、Validator の行はこの値です[^t1-9]。Controller と Manager が `up` になれば、Validator との接続は切れて当然。この行が `tear_down` でも異常ではありません。

見るべき異常は、Controller の行が `connect` や `challenge` で止まっている場合です。`connect` の履歴に DTLS ハンドシェイクの失敗(DCONFIL)が並んで

いれば、証明書か到達性に問題があります。`tear_down` の履歴に DISTLOC が
出ていれば、TLOC が無効になっています[^t1-9]。

`vsmart` の行は、制御に使うカラーごとに 1 本ずつ張られます。`vmanage` への
接続は、制御に使えるインタフェースが複数あっても 1 つのカラーにしか張ら
れません。表示される Validator のポートは 12346 です。NAT を越えると、外
から見るポート番号が別の値に変わる場合もある。

コントロールプレーンとデータプレーン:OMP・TLOC・IPsec・BFD [1.2.a]

OMP(Overlay Management Protocol)は、SD-WAN の経路制御プロトコル
です。BGP に似ていて、WAN Edge と Controller の間の DTLS か TLS の制御
接続の中を走ります。運ぶ経路は 3 種類です。

- **OMP ルート**: 拠点の中(サービス側)のプレフィックス
- **TLOC ルート**: トランスポートの出入口
- **サービスルート**: ファイアウォールなどのサービスが居る場所

TLOC(Transport Location)は、WAN Edge が WAN の回線につながる点で
す。次の 3 つ組で表します。

要素	意味
システム IP	機器の ID。ルータ ID のように使い、到達で きる必要はない
カラー	回線の種類の名前(mpls、biz-internet、lte など)
カプセル化	IPsec か GRE

同じ拠点に回線が 2 本あれば、TLOC は 2 つです。WAN Edge は自分の TLOC を OMP で Controller へ知らせ、Controller が他の拠点へ配ります。カプセル化が違うと、トンネルは張れません。GRE 同士か IPsec 同士である必要があります。

データプレーンは、WAN Edge どうしが直接張る IPsec トンネルです。トンネルの 1 本ずつに **BFD** が流れます。BFD はトンネルの生死を見るだけでなく、損失・遅延・ジッタも測ります。アプリ認識ルーティングは、この測定値を使う。BFD の hello は既定で 1 秒ごとに送られます。測定値は既定で 10 分ごとの区間(ポーリング間隔)で平均を取り、直近の 6 区間、つまり 1 時間分で SLA を判定します[^t1-10]。

Edge1# show sdwan bfd sessions

SYSTEM IP	SITE ID	STATE	SOURCE TLOC	COLOR	REMOTE TLOC	COLOR	ENCAP	UPTIME
10.1.1.21	200	up	mpls		mpls		ipsec	1:04:12
10.1.1.21	200	up	biz-internet		biz-internet		ipsec	1:04:12
10.1.1.22	300	down	mpls		mpls		ipsec	0:00:00

(列は一部を省略している。)読み取れるのは次の状態です。拠点 200 とは、回線 2 本のどちらでもトンネルが張れている。拠点 300 とは、mpls のトンネルが **down** になっている。制御接続が **up** なのにデータが通らない、という症状は、BFD セッションの **down** で見分けます。制御接続の出力が **up** でも、BFD が **down** ならデータは流れません。

VPN(セグメント) は SD-WAN 独自の呼び名で、実体は VRF です。番号に意味がある。

VPN	用途
VPN 0	トランスポート(WAN 側のインタフェースと制御接続)
VPN 512	管理(帯域外の管理。オーバーレイには広告しない)
それ以外	サービス側の VPN(拠点内のユーザ)

VPN 0 は WAN 側のインタフェースを置く予約済みの VPN で、アドレスは DHCP か固定で与えます。サービス側の VPN は、エンドツーエンドで業務を分けるセグメンテーションに使います。OMP が VPN ごとに経路を運びます。

カラー、制御ポリシーとデータポリシー、REST API [1.2.a]

カラー には、public と private の区別がある。mpls・metro-ethernet・private1 ～ private6 は private です。それ以外 (biz-internet、public-internet、lte、default など)は public。この区別は、トンネルがどのアドレスで張られるかを決めます。TLOC には private と public の 2 つのアドレスがあり、public のカラーが片側にあれば、双方が public のアドレス(NAT の外側)を使います。

既定のオーバーレイは、カラーに関係なくフルメッシュです。`restrict` を付けると、同じカラーの TLOC とだけトンネルを張る。MPLS のような閉じた網は、インターネット側と到達性が無いので、`restrict` を付けるのが定番です。

WAN Edge の WAN 側の設定は、VPN 0 のインタフェースに `tunnel-interface` を置いて、カプセル化とカラーを決めます。次は Viptela 形式の CLI

の例です。

```
system
  host-name Edge1
  system-ip 10.1.1.11
  site-id 100
  organization-name EXAMPLE
  vbond 203.0.113.12
!
vpn 0
  interface ge0/0
    ip address 203.0.113.21/24
  tunnel-interface
    encapsulation ipsec
    color biz-internet
    allow-service all
  no shutdown
```

`system-ip` が機器の ID、`site-id` が拠点の番号、`vbond` が最初に会う Validator の場所です。同じ組織の機器は、同じ `organization-name` を持つ。`color` と `encapsulation` が、TLOC の残り 2 要素に当たります。この設定の TLOC は {10.1.1.11, biz-internet, ipsec} です。

Edge1# show sdwan omp routes

VPN	PREFIX	FROM PEER	PATH ID	LABEL	STATUS	TLOC IP	COLOR
ENCAP							
1	10.20.0.0/16	10.1.1.3	1	1002	C,I,R	10.1.1.21	mpls
ipsec							
1	10.20.0.0/16	10.1.1.3	2	1002	C,I,R	10.1.1.21	biz-
internet ipsec							
1	10.30.0.0/16	10.1.1.3	1	1002	Inv,U	10.1.1.22	mpls
ipsec							

(列は一部を省略している。)各行は、VPN 1 の経路と、その行き先の TLOC を示します。FROM PEER は経路をしてくれた相手で、遠くの拠点ではなく Controller の 10.1.1.3 です。STATUS の C は選ばれた(chosen)、I は installed、R は解決済み(resolved)を表します。Inv と U が付く行は、行き先の TLOC に到達できず(invalid、unresolved)、使われません。その場合は、BFD が down か、TLOC への到達性が無いことを疑います。

ポリシーは、まず作る場所で分ける。**集中ポリシー**は Manager で作り、Controller が配ります。**ローカルポリシー**は機器に直接設定し、アクセスリストや QoS を扱います。集中ポリシーは、さらに 2 種類に分かれる。

集中ポリシー	実行する場所	扱うもの
制御ポリシー	Controller	トポロジ(フルメッシュ、ハブアンドスポーク)、OMP 経路の操作
データポリシー	WAN Edge のデータプレーン	トラフィックの振り分け、DIA、アプリ認識ルーティング

ハブアンドスポークは、拠点が学ぶ TLOC をハブの TLOC だけに絞る制御ポリシーで作ります。ハブを現用と待機の 2 台にするときは、2 台を 1 つの TLOC リストに入れ、現用に高い `preference` を与える。

アプリ認識ルーティングは、集中データポリシーの一種です。Controller に設定して、各機器へ配ります[[^t1-10](#)]。流れは次のとおり。

1. **SLA クラス**を作る。損失・遅延・ジッタの上限を決める(遅延とジッタは 1~1000 ms、損失は 1~100%)。
2. BFD の測定値が SLA クラスを満たすトンネルを、そのアプリの転送に使う。
3. 満たさなくなったら、満たすほかのトンネルへアプリを載せ替える。

SD-WAN Manager は **REST API** を持っています。GUI でできる操作を、プログラムから実行できます。認証は次の順です[[^t1-11](#)]。

1. `POST /j_security_check` に `j_username` と `j_password` を送る。成功すると `JSESSIONID` クッキーが返る。
2. `GET /dataservice/client/token` で XSRF トークンを取る。
3. 以降の要求に `JSESSIONID` クッキーを付ける。POST には `X-XSRF-TOKEN` ヘッダも付ける。

API の入口は `https://(Manager のアドレス)/dataservice/(エンドポイント)` の形です。セッションは 24 時間で切れ、30 分操作しなくても切れる。GET は取得で、クッキーだけで通る。POST と PUT と DELETE は、クッキーと XSRF トークンの両方を付けます。ログインに失敗すると、エラーコードではなく HTML のログインページが返ります。ここが落とし穴だ。

制御接続とデータ接続の症状から、原因の場所を決める問いもあります。

見えている状態	読み取ること
Validator の行だけ <code>tear_down</code>	異常ではない。Controller と Manager が <code>up</code> なら参加は済んでいる
Controller の行が <code>connect</code> のまま、 DCONFALL が並ぶ	DTLS ハンドシェイクの失敗。証明書が到達性を疑う
制御接続はすべて <code>up</code> 、BFD セッションが <code>down</code>	データプレーンの問題。トランスポートの到達性か、カプセル化の不一致を疑う
OMP の経路が <code>Inv,U</code>	行き先の TLOC に到達できない。BFD か到達性を疑う
経路が来ない、Controller の行が無い	制御プレーン側の問題。Validator に着いて以降の手順を追う

Manager は、設定をテンプレートで配ります。機能ごとの設定(フィーチャーテンプレート)を組み合わせ、機器ごとのテンプレートを作り、機器に付けます。同じ値を何台にも配れるので、拠点を増やしても人手の設定が増えません。

SD-WAN の利点と制約 [1.2.b]

利点は 5 つです。

利点	中身
トランスポート非依存	MPLS・インターネット・LTE を混ぜて使える
アプリ認識ルーティング	SLA を満たす回線へアプリを載せ替える
一元のポリシー	Manager で 1 回作り、全拠点へ配る
ゼロタッチ(PnP/ZTP)	新しい機器は Validator に自分でつなぎ、設定を Manager から受け取る。現地での CLI 作業が要らない

利点	中身
セグメンテーション	サービス側の VPN(VRF)で、拠点を超えて業務を分ける

従来の WAN は、拠点ごとに CLI で設定していました。通信はデータセンターへ集めてから外へ出し(バックホール)、回線ごとに経路を制御します。SD-WAN は、拠点から直接インターネットへ出る **DIA**(Direct Internet Access)と、中央管理に置き換えます。クラウドの SaaS や IaaS への出口は、**Cloud OnRamp** が最適な経路を選びます。

制約は 4 つです。

- 制御の前提: Edge から Controller・Manager・Validator に到達できる必要がある。置き場所はオンプレミスでも、Cisco がホストするクラウドでもよいが、どちらでも到達性が前提になる。
- 帯域のオーバーヘッド: IPsec と制御の通信の分だけ、帯域と MTU を使う。トンネルの分、MTU は小さくなる。
- ライセンス: 機器とライセンスの対応が要る。
- 運用: Manager を中心にした管理になる。拠点の機器を CLI で個別に変えると、テンプレートとの食い違いが出る。

試験では、利点と制約を混ぜた選択肢が出ます。「バックホールの削減」「ゼロタッチ」「アプリ認識」は利点。「MTU の減少」「コントローラへの到達性」は制約です。

SD-Access の構成:コントロールプレーンノード・ボーダー・エッジ・ファブリック WLC [1.3.a]

Cisco SD-Access は、キャンパスの有線を中心にした**ファブリック**です。物理の IP ネットワーク(アンダーレイ)の上に、論理のネットワーク(オーバーレイ)を重ねる。従来のキャンパスは、VLAN と ACL を拠点ごとに人手で作る。SD-Access は、Catalyst Center が VN と SGT を自動で配ります。

構成は、4 つのプレーンで分けて覚えます。

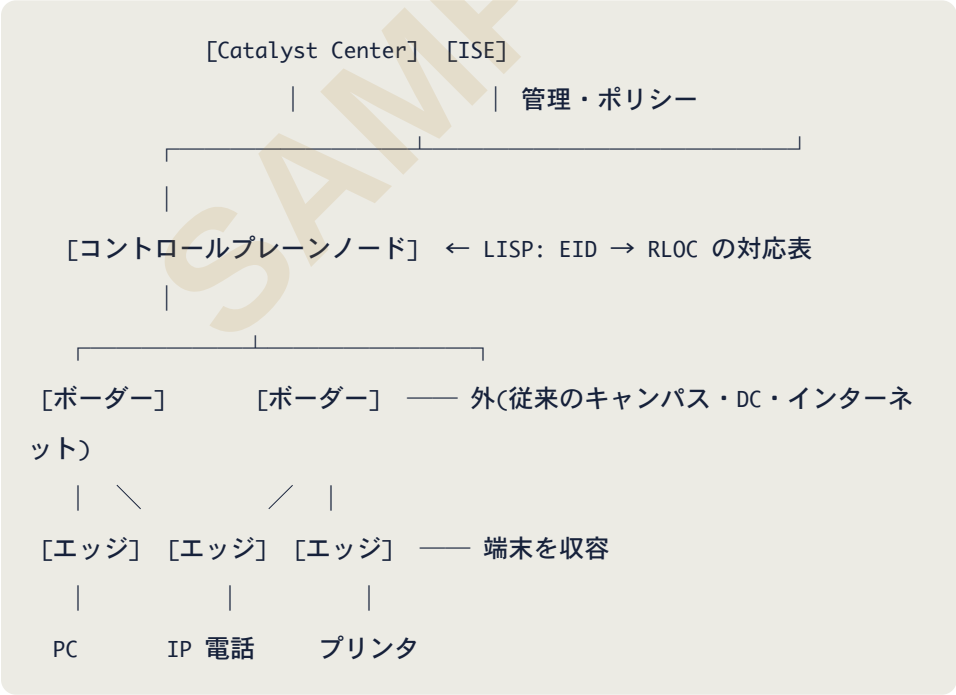
プレーン	担当	中身
コントロール	LISP	端末の位置の登録と問い合わせ
データ	VXLAN	カプセル化して運ぶ
ポリシー	TrustSec(SGT)	グループ単位の許可と拒否
管理	Catalyst Center と ISE	設計・自動配布・認証

ファブリックの機器は、役割で呼び分けます[^t1-12]。

ノード	役割
コントロールプレーンノード	LISP の Map-Server/Map-Resolver(登録を受ける役と、問い合わせに答える役)を 1 台で兼ねる。端末(EID)とエッジ(RLOC)の対応表を持つ
エッジノード	端末を收容し、VXLAN でカプセル化・解除する。端末を検知したらコントロールプレーンノードへ登録する。従来のアクセススイッチに当たる

ノード	役割
ボーダーノード	ファブリックと外(従来のネットワーク・データセンター・インターネット)の出入口
拡張ノード	ファブリックの外の小型スイッチをL2でエッジに足す。IoT やオフィス以外のスペース向け
ファブリック WLC	無線の端末もファブリックの VXLAN に載せる

ファブリック WLC は、無線の設計が v1.2 の範囲から外れた今も、構成要素の名前として出ます。「無線の端末をファブリックに載せるための WLC」と覚えれば足ります。



LISP は「誰がどこに居るか」を分けて管理します。端末の IP アドレスが **EID**(端末の ID)で、その端末を収容するエッジの IP アドレスが**RLOC**(位置)です[^t1-13]。端末が接続すると、エッジが EID をコントロールプレーンノードに登録します(Map-Register)。

別のエッジの下にいる端末へ送るときは、送信側のエッジがコントロールプレーンノードに RLOC を問い合わせます(Map-Request と Map-Reply)。答えの RLOC を宛先に、VXLAN で運ぶ。対応が見つからない宛先は、外部ボーダーが既定の出口として受けます。端末が別のエッジへ移ると、新しい登録で RLOC が更新されます。

データプレーンは、VXLAN の**グループポリシー拡張**(VXLAN-GPO)です。VXLAN は、元のフレームを UDP でくるむ方式で、24 ビットの VNI で仮想ネットワークを区別します。宛先の UDP ポートは 4789 です[^t1-14]。GPO では、ヘッダにグループを示す 16 ビットの **SGT** も入ります。ヘッダの中に SGT を運ぶので、アドレスが変わってもグループは追従する。

アンダーレイは IP ネットワークで、LAN 自動化を使うと IS-IS で組まれます。オーバーレイは、その上の VXLAN です。

エニーキャストゲートウェイは、同じサブネットを持つ全エッジが、同じゲートウェイの IP と MAC を持つ仕組みです。端末がエッジの間を移動しても、ゲートウェイは変わりません。通信が切れないので、HSRP のような FHRP は要りません。

分け方は 2 段です。**仮想ネットワーク(VN)** は VRF で、大きく業務を分けます(マクロセグメンテーション)。1 つの VN の中を **SGT** でさらに細かく分けます(マイクロセグメンテーション)。ポリシーは、送信元のグループと宛先のグループの組み合わせごとの、許可と拒否です。ISE が決めて配る。

送信元 \ 宛先	社員(SGT 10)	サーバ(SGT 20)	ゲスト(SGT 30)
社員(SGT 10)	許可	許可	拒否
ゲスト(SGT 30)	拒否	拒否	許可

行列で書くので、IP アドレスが変わっても、場所が変わっても、規則は書き直さなくて済む。

役割の取り違えは、試験の定番です。次の対応を取り違えないようにします。

取り違えやすい組	正しい対応
LISP と VXLAN	LISP は位置の対応表(コントロール)、VXLAN はカプセル化(データ)
EID と RLOC	EID は端末のアドレス、RLOC はその端末を収容するエッジのアドレス
VN と SGT	VN は VRF による大きな分離、SGT は VN 中のグループ分け
エッジとボーダー	エッジは端末の収容、ボーダーは外との出入口
コントロールプレーンノードとボーダー	前者は対応表を持つ。後者は外へ出る経路を持つ

SD-Access のアンダーレイは、物理の IP ネットワークです。オーバーレイの VXLAN は、そのアンダーレイの IP の上を走ります。アンダーレイが壊れれば、オーバーレイも通りません。

SD-Access のプレーン:LISP・VXLAN・CTS/SGT [1.3.a]

3つのプレーンの関係を、1通の通信で追う。社員のPC(SGT 10)が、別のエッジの下にあるサーバ(SGT 20)へ送る場面です。

1. 送信側のエッジが、コントロールプレーンノードに宛先の RLOC を聞く(LISP)。
2. エッジが元のフレームを VXLAN でくるむ。ヘッダに VNI と送信元の SGT 10 を入れる(VXLAN)。
3. 受信側のエッジが、くるみを外す。送信元 SGT 10 と宛先 SGT 20 の組み合わせで、許可か拒否かを判定する(CTS)。

ポリシーを強制するのは、宛先に近い側のエッジです。判定に使う表は、ISE が配る。この動作が、グループ単位の制御を IP アドレスから切り離しています。

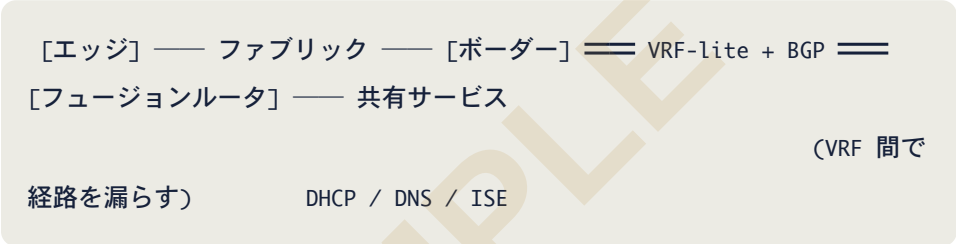
従来キャンパスとの相互接続:ボーダーノードとフュージョンルータ [1.3.b]

ファブリックの外の世界との接続は、ボーダーノードが担当します。種類は 3 つある。

種類	担当
内部ボーダー	社内の既知の経路(データセンターなど)をファブリックへ登録する
外部ボーダー	既定の出口(インターネットなど)。対応が無い宛先を引き受ける
両方(内部と外部、anywhere)	両方を兼ねる

外部ボーダーは、ファブリックの「最後の頼みのゲートウェイ」です。内部ボーダーは、既知のサブネットをコントロールプレーンへ登録します[^t1-12]。

ボーダーの外では、VRF ごとの経路を共有サービスの側へ漏らす必要があります。DHCP・DNS・ISE・Catalyst Center のようなサーバは、すべての VN が使う。そこで、ボーダーの外に共有の VRF を作ってサーバを置き、**フュージョンルータ**が VRF 間で経路を漏らします。ボーダーとフュージョンルータの間は、VRF-lite と BGP で経路を受け渡します。



フュージョンルータで見落とししやすいのは、**SGT がヘッダから落ちる**点です。ボーダーの外の IP ネットワークは、SGT を運びません。外でもグループの制御を続けるなら、次のどちらかで渡します。

- **SXP**: 別のプロトコルで、IP アドレスと SGT の対応(バインディング)を交換する。
- **インラインタギング**: パケットの Cisco メタデータのフィールドに、SGT を直接入れる[^t1-12]。

ファブリックどうしを結ぶ**トランジット**にも、2 種類あります。

トランジット	動き	SGT
IP トランジット(IP ベース)	VRF-lite と BGP で外へ出る。ふつうの IP の網を使う	落ちる。SXP などで渡す
SD-Access トランジット	拠点間も VXLAN で運ぶ	保たれる

L2 ボーダーは、従来の VLAN とファブリックの L2 を、同じサブネットでつなぎます。同じサブネットの端末が、従来のスイッチとファブリックに分かれて居られるので、段階的に移行できます。

移行の型も 2 つある。新しいファブリックを横に作る並行の移行と、既存の機器を段階的に置き換える移行(インクリメンタル)です。

QoS の分類とマーキング:DSCP・CoS・信頼境界 [1.4]

QoS は、混んだ回線で「どの通信を先に送り、どれを後回しにするか」を決める仕組みです。仕事は 3 段階に分かれる。パケットの種類を見分ける(分類)。見分けた結果をパケットに書く(マーキング)。書かれた印に従って扱いを変える(ポリシング・シェーピング・キューイング)。この節は前半の 2 段階です。

マーキングの置き場所は、2 つあります。

場所	印	幅	運ばれる範囲
L3(IP ヘッダ)	DSCP	6 ビット(0～63)	エンドツーエンド
L2(802.1Q タグ)	CoS(PCP)	3 ビット(0～7)	トランクの中だけ

CoS は 802.1Q のタグの中にあるので、タグの無いアクセスポートや、ルータを越えた先には運ばれません。DSCP は IP ヘッダにあるので、ルータを越えても残ります。IP ヘッダの ToS バイトのうち、上位 6 ビットが DSCP です[¹t1-15]。ToS バイトの値は DSCP の 4 倍なので、DSCP 46 は ToS の 184(16 進で 0xB8)になります。

DSCP の上位 3 ビットは、旧来の **IP Precedence** と同じ位置です。下位 3 ビットが 000 の DSCP を**クラスセクタ**(CS)と呼び、CS3 は Precedence 3、CS6 は Precedence 6 に当たります。

代表的な DSCP を次の表に示す。

PHB	DSCP	主な用途
EF	46	音声
AF41	34	対話型のビデオ
AF31	26	重要な業務アプリ
CS3	24	呼制御(シグナリング)
AF21	18	業務データ
AF11	10	大量データの転送
CS6	48	ルーティングプロトコルなどの網制御
BE(既定)	0	優先しない通信

EF(Expedited Forwarding)は、低遅延・低損失・低ジッタで運ぶための扱いです。推奨のコードポイントは 101110、つまり 46 です[^t1-16]。

AF(Assured Forwarding)は、クラスが 4 つ、破棄の優先度が 3 つで、12 通りあります。AFxy と書き、x がクラス(1～4)、y が破棄の優先度(1～3)です[^t1-17]。DSCP の値は $8x + 2y$ で求めます。AF41 は $8 \times 4 + 2 \times 1 = 34$ 、AF43 は $8 \times 4 + 2 \times 3 = 38$ 、AF21 は $8 \times 2 + 2 \times 1 = 18$ です。

y が大きいほど、輻輳時に先に捨てられます。 AF43 は AF41 より先に捨てられ、AF11 は AF13 より後に捨てられる。クラスの数字が大きいほど優先されるわけではありません。クラスどうしの順位は、運用側がキューへの割り当てで決めます。

信頼境界は、端末が付けたマーキングを信じる境界です。利用者のつなぐ PC は、自由に DSCP 46 を付けられます。全部を信じると、誰でも最優先の通信を

送れてしまう。そこで境界の手前のアクセスポートでは、端末の印を信じずに書き換えるか、0に戻します。IP電話は信頼できる端末なので、電話を認識したときだけ信頼します。

```
Switch(config)# interface GigabitEthernet1/0/5  
Switch(config-if)# trust device cisco-phone
```

`trust device cisco-phone` は、Cisco の IP 電話を CDP で見つけたときだけ、電話の付けた印を信じる設定です。種類の一致しない機器がつながると、CoS と DSCP は 0 にされます[^t1-18]。信頼境界は、できるだけ端末に近い、アクセス層に置きます。

信頼しないポートでは、受けた通信を分類して、スイッチが印を付け直します。

```
ip access-list extended VOICE-ACL
  permit udp any any range 16384 32767
!
class-map match-all VOICE
  match access-group name VOICE-ACL
!
policy-map MARK-IN
  class VOICE
    set dscp ef
  class class-default
    set dscp default
!
interface GigabitEthernet1/0/10
  service-policy input MARK-IN
```

読み方は、まず ACL で UDP 16384～32767 を音声と見なして **VOICE** に分類し、入力方向で DSCP を EF(46)に付けています。それ以外は class-default に入り、DSCP 0 に戻される。端末が自分で付けた印は、このポートでは効きません。

MQC の設定の読み取り: class-map・policy-map・service-policy [1.4]

QoS の設定は、MQC(Modular QoS CLI)という 3 段の形で書きます[^t1-19]。

段	コマンド	役割
1. 分類	<code>class-map</code>	どの通信かを決める
2. 動作	<code>policy-map</code>	クラスごとの動作(帯域・優先・ポリシング・シェーピング)を決める
3. 適用	<code>service-policy</code> <code>input/output</code>	インタフェースに付ける

class-map には、規則が 3 つあります。

- `match-all` が既定。何も書かなければ、全ての条件に一致した通信だけが対象になる。
- `match-any` は、条件のどれか 1 つに一致すれば対象になる。
- どのクラスにも当たらない通信は、**class-default** に入る。

class-default を設定しなければ、その通信は QoS の機能を受けません。FIFO のキューで先着順に送られ、あふれると捨てられます。1 つのパケットが入るクラスは、1 つだけです。複数のクラスに当たるときは、policy-map の中で先に書いたクラスが選ばれる。1 つのインタフェースには、入力に 1 つ、出力に 1 つまで policy を付けられます。入力方向ではキューイングが使えず、ポリシングとマーキングが使える。

次の設定を読む。

```
class-map match-all VOICE
  match dscp ef
class-map match-any SIGNALING
  match dscp cs3
  match dscp af31
class-map match-all BULK
  match dscp af11
  match protocol ftp
!
policy-map WAN-OUT
  class VOICE
    priority percent 20
  class SIGNALING
    bandwidth percent 10
  class BULK
    bandwidth percent 5
  class class-default
    fair-queue
!
interface GigabitEthernet0/0/1
  service-policy output WAN-OUT
```

原因を見抜く問いが、ここによく出ます。BULK は match-all なので、「DSCP が AF11 **かつ** プロトコルが FTP」の通信だけが入ります。DSCP が AF11 でも、FTP 以外の通信は BULK に入りません。class-default へ流れます。

AF11 の全部を BULK に入りたいなら、`match protocol ftp` を消すか、`match-any` に変える。ただし `match-any` にすると、DSCP が何でも FTP は BULK に入ります。AND と OR は、クラスの前頭の `match-all` か `match-any` で決まります。`SIGNALING` は `match-any` なので、CS3 か AF31 のどちらかなら入ります。

```
Router# show policy-map interface GigabitEthernet0/0/1 output
GigabitEthernet0/0/1
Service-policy output: WAN-OUT
  Class-map: VOICE (match-all)
    48210 packets, 9642000 bytes
    5 minute offered rate 98000 bps, drop rate 0000 bps
    Match: dscp ef (46)
    Priority: 20% (200000 kbps), burst bytes 5000000, b/w exceed
drops: 0
  Class-map: BULK (match-all)
    0 packets, 0 bytes
    5 minute offered rate 0000 bps, drop rate 0000 bps
    Match: dscp af11 (10)
    Match: protocol ftp
  Class-map: class-default (match-any)
    9981234 packets, 8123456789 bytes
    5 minute offered rate 8420000 bps, drop rate 1750000 bps
    Match: any
```

この出力から読めるのは 3 つです。VOICE は offered rate が 98 kbps で drop が 0 だから、優先の帯域内で問題なく送られている。BULK は 0 packets で、1 本も一致していません。`match-all` の条件が厳しすぎる印です。

class-default の drop rate は 1.75 Mbps で、BULK に入れなかった大量の通信が class-default で捨てられていると読みます。

ポリシングとシェーピング、LLQ・CBWFQ・WRED [1.4]

速度を制限する手段は、2 つあります。

	ポリシング(police)	シェーピング(shape)
超えた分	捨てる、または印を付け替える	バッファに溜めて遅らせる
バッファ	持たない	持つ
方向	入力でも出力でも使える	出力だけ
遅延	増えない	増える

ポリシングは、トークンバケットで速度を測ります。トークンの補充速度が **CIR**(契約した速度)で、バケットの深さが**バースト**(Bc)です[^t1-20]。パケットが来て、トークンが足りれば通す。足りなければ超過として扱います。シェーピングは、足りないパケットを捨てずに待たせる点が違います。

超過の扱いは、3 つに分けられます。単一レートの色マーカースrTCM)では、CIR のほかに CBS(許す通常のバースト)と EBS(許す超過バースト)を決めます[^t1-21]。

色	動作の名前	条件
緑	conform	CBS の範囲に収まる
黄	exceed	CBS を超えるが EBS には収まる
赤	violate	CBS も EBS も超える

```
policy-map LIMIT-GUEST
class GUEST
  police cir 10000000 bc 312500 be 312500
    conform-action transmit
    exceed-action set-dscp-transmit af11
    violate-action drop
!
interface GigabitEthernet1/0/10
  service-policy input LIMIT-GUEST
```

この設定は、ゲストの通信を 10 Mbps に制限します。10 Mbps の範囲は送る。少し超えた分は AF11 に付け替えて送り、大きく超えた分は捨てる。入力方向で使っているので、キューではなくポリシングです。

```
Switch# show policy-map interface GigabitEthernet1/0/10 input
Service-policy input: LIMIT-GUEST
Class-map: GUEST (match-any)
  police:
    cir 10000000 bps, bc 312500 bytes, be 312500 bytes
    conformed 2345 packets, 3100000 bytes; actions: transmit
    exceeded 80 packets, 110000 bytes; actions: set-dscp-transmit
af11
    violated 12 packets, 18000 bytes; actions: drop
```

捨てられているのは、`violated` の行だけです。`exceeded` の行は捨てられておらず、DSCP を付け替えて通っている。「超過の 80 個が捨てられた」と読むのは誤りです。

シェーピングは、出力で使います。WAN の契約帯域が物理の速度より小さいときに、契約の速度に合わせて送り出す。物理が 1 Gbps で契約が 100 Mbps の回線で、物理の速度のまま送ると、事業者側で捨てられます。

```
policy-map CHILD
  class VOICE
    priority percent 20
  class class-default
    bandwidth remaining percent 80
!
policy-map PARENT
  class class-default
    shape average 100000000
    service-policy CHILD
!
interface GigabitEthernet0/0/1
  service-policy output PARENT
```

親が全体を 100 Mbps に整形し、子がその中の優先順位を決めます。子のクラスへは、シェーピング後の帯域を基準に割り振られます。

キューイングには、2 つの帯域の指定があります。

- **bandwidth (CBWFQ)**: クラスに最低限の帯域を保証する。上限ではなく、回線に空きがあるときは保証を超えて使える。
- **priority (LLQ)**: 厳密な優先キューで、先に送る。音声のような遅延に弱い通信向け。帯域を保証すると同時に、上限にもなる。輻輳したときは、設定した帯域を超えた分が捨てられる。

優先キューに上限が無いと、他のクラスが送れなくなります。だから `priority` は上限も兼ねる。LLQ は CBWFQ に優先キューを足したもので、音声は `priority`、そのほかの業務は `bandwidth` で割り振るのが標準の形です。

WRED は、キューが埋まる前から、確率的にパケットを捨てる仕組みです。満杯になってから一斉に捨てる方式(テールドロップ)は、複数の TCP が同時に速度を下げ、同時に戻す「グローバル同期」を起こす。WRED は、破棄の優先度が高いパケット(AFx3 など)から先に、少しずつ捨てます。TCP が個別に速度を下げるので、同期が起きません。UDP の音声のように、捨てられても速度を下げない通信が入る優先キューには、使いません。

道具の選び方は、解きたい問題で決まる。

解きたい問題	使う道具
音声の遅延とジッタを抑える	<code>priority</code> (LLQ)
業務ごとに最低限の帯域を守る	<code>bandwidth</code> (CBWFQ)
契約帯域を超えて送らない	<code>shape</code> (出力)
受け側で上限を課す、印を付け替える	<code>police</code> (入力でも出力でも)
TCP のグローバル同期を防ぐ	WRED
端末が付けた印を信じない	信頼境界での再マーキング

「シェーピングで入力方向の帯域を制限する」は誤りです。シェーピングは出力だけで使います。入力側で上限を課すなら、ポリシングです。

QoS の設定を読む問題では、次の順に確かめると原因が決まります。

1. 方向(input か output)を見る。入力ではキューイングが使えない。

2. `match-all` と `match-any` が、意図どおりの AND と OR になっているのを見る。
 3. どのクラスにも当たらない通信が、`class-default` に入っているのを見る。
 4. `show policy-map interface` の `drop rate` が出ているクラスを見る。
 5. 超過の動作が、捨てるのか、付け替えるのかを見る。
-

■ サンプルはここまでです

続き(第2章～巻末)は、CCNP ENCOR 問題集のご購入で、頻出度別ノート・暗記用ノートと合わせて3点すべてダウンロードできます。

CCNP ENCOR 350-401 学習用テキスト(無料サンプル)

版

2026年10月版(Cisco CCNP Enterprise ENCOR 350-401 v1.2 Exam Topics(Cisco 公式 PDF・2026-10-13 取得)準拠)

発行

IT資格道場(<https://www.shikaku-doujou.com>)

お問い合わせ

info@shikaku-doujou.com

Cisco、CCNP、CCIE および Cisco IOS は、Cisco Systems, Inc. またはその関連会社の米国およびその他の国における商標または登録商標です。記載されているその他の会社名・製品名・サービス名は、各社の商標または登録商標です。

本教材は公式の出題範囲(350-401 v1.2)の内容を基に作成したもので、Cisco との提携・承認関係はありません。

本文・図表・設問はすべてオリジナルの著作物です。無断での転載・複製・再配布・二次販売はできません。お気づきの点はinfo@shikaku-doujou.com までご連絡ください。