



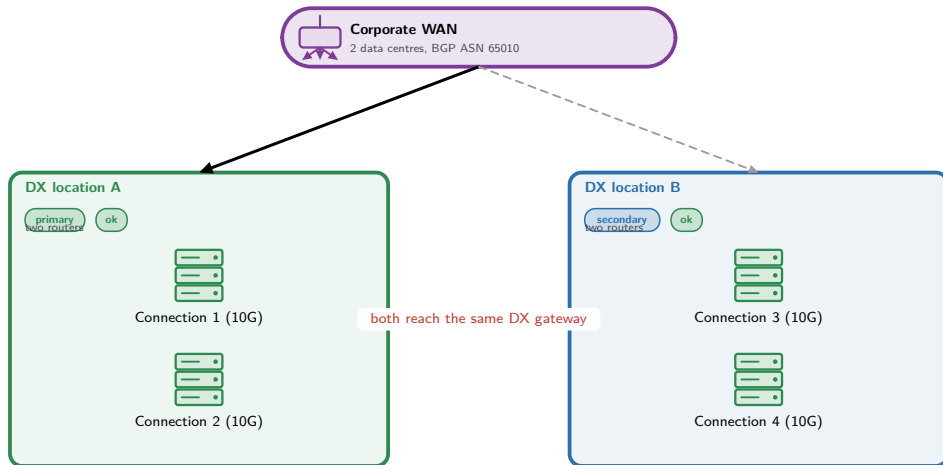
ANS-C01: Direct Connect, VPN and BGP

AWS Certified Advanced Networking Specialty exam guide, as of 2026 | Direct Connect connections and VIFs, Direct Connect gateway, resiliency models, Site-to-Site and Client VPN, BGP path control, MTU, MACsec

ANS-C01 Domain 1 Domain 2 Direct Connect VPN BGP

Direct Connect building blocks

Element	Key facts	Exam trap
Dedicated connection	1/10/100 Gbps (400 in some locations), LOA-CFA to the colocation provider for the cross-connect, weeks to provision	you own the port; MACsec only here
Hosted connection	from a DX partner, 50 Mbps to 10 Gbps (higher at some partners), one VIF per hosted connection	need several VIFs → several hosted connections
Private VIF	to one VGW, or to a DXGW reaching many VPCs; jumbo frames up to 9001	≤ 100 prefixes advertised by you per session or BGP goes idle
Public VIF	AWS public prefixes (S3, DynamoDB, public endpoints) over DX; needs public IPs and ASN you own (or AWS-provided)	not encrypted; add IPsec VPN over it for privacy
Transit VIF	DXGW → Transit Gateways; MTU up to 8500	one transit VIF per dedicated connection (check current quota)
DX gateway	global, any Region, multiple accounts by association proposal	no VPC-to-VPC or VIF-to-VIF routing through it
SiteLink	on-prem site to site via DX locations, by-passing Regions	enabled per VIF, billed per hour



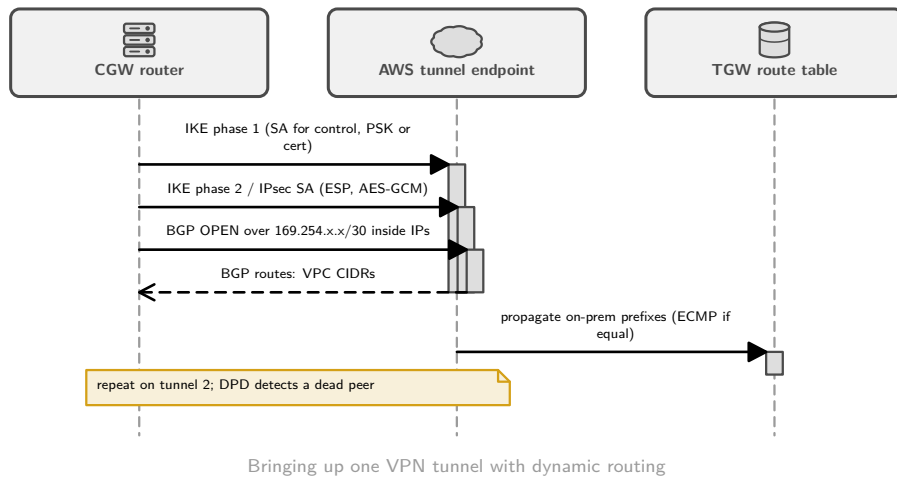
Maximum resiliency: 2 locations × 2 connections on separate devices (99.99 % SLA model); High resiliency = 1 per location

💡 Resiliency Toolkit models

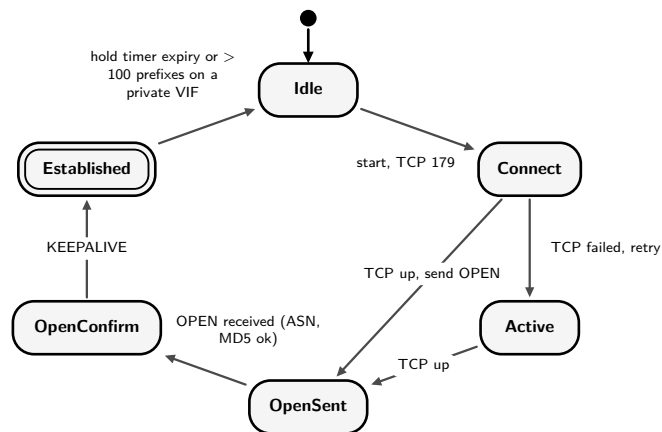
Maximum resiliency (2 locations, 2 connections each, separate devices), **High resiliency** (2 locations, 1 connection each), **Development and test** (1 location, 2 connections on separate devices). A VPN as backup of DX is cheaper but slower and capped by tunnel bandwidth.

Site-to-Site and Client VPN

Feature	Value / behaviour
Tunnels	2 per VPN connection, in different AWS endpoints; up to 1.25 Gbps per tunnel (large-bandwidth tunnels announced 2025, check)
Termination	VGW (one VPC, no ECMP) or Transit Gateway (ECMP across tunnels and connections) or Cloud WAN
Routing	static, or BGP (recommended: failover and ECMP)
MTU / MSS	1446 bytes MTU, 1406 MSS; fragmented ICMP issues → clamp MSS
IKE	IKEv1 or IKEv2, pre-shared key or certificate (Private CA); DPD timeout action clear/restart/none
Private IP VPN	IPsec over a DX transit VIF to TGW using private addresses: encryption over DX
Accelerated VPN	Global Accelerator in front of tunnels, TGW only, cannot be changed after creation
Client VPN	OpenVPN clients; auth mutual TLS, AD, SAML IdP; authorization rules per CIDR/group; split-tunnel off by default



⚡ BGP and path control



BGP finite-state machine: stuck in Active = TCP 179 not reachable (VLAN, IPs, ACL); stuck before Established = ASN or MD5 mismatch

Goal	Lever	Where it acts
AWS → on-prem: prefer DX A over DX B	local preference community 7224:7300 on A, 7224:7100 on B (or AS_PATH prepend on B)	your advertisements on private/transit VIFs
On-prem → AWS: prefer DX A	local preference on your routers (inbound routes from AWS)	your side only
Prefer a specific path for one subnet	advertise a more specific prefix there (longest prefix wins first)	both directions
Keep public VIF prefixes local	scope communities 7224:9100 (local Region), 9200 (continent), 9300 (global)	AWS → you on public VIF

Do not let AWS re-advertise	NO_EXPORT community on public VIF	AWS side
Active/passive DX and VPN	AWS prefers DX over VPN for identical prefixes	VGW/TGW route selection

- 1 Longest prefix match** /24 beats /16 whatever the source
- 2 Static routes in the VPC route table** beat propagated routes
- 3 Propagated: DX BGP routes** preferred over VPN
- 4 Propagated: VPN static routes** then VPN BGP routes
- 5 Among BGP routes** shortest AS_PATH, then lowest MED (for VPN), then ECMP where supported

VGW route selection for the same destination (as documented, check for TGW nuances)

Conditions	DX	DX + crypto	VPN	Users
Need private, consistent latency	Y	Y	N	N
Need encryption in transit	N	Y	Y	--
Need it within days	N	N	Y	--
Remote users, not sites	N	N	N	Y
Actions				
DX private / transit VIF	X	X		
IPsec over DX (private IP VPN) or MACsec		X		
Site-to-Site VPN (TGW, BGP, ECMP)			X	
AWS Client VPN				X

Picking the hybrid link

Worked example and recap

VPN bandwidth with ECMP on a Transit Gateway

PROBLEM A branch needs 8 Gbps to AWS over the internet before DX arrives. How many Site-to-Site VPN connections on a Transit Gateway?

GIVEN

- Each tunnel: up to 1.25 Gbps
- Each VPN connection: 2 tunnels
- TGW ECMP balances flows across equal BGP paths; one flow stays on one tunnel

1 Bandwidth per connection

$2 \times 1.25 = 2.5 \text{ Gbps}$

Why: both tunnels active with BGP + ECMP

2 Connections needed

$\text{ceil}(8 / 2.5) = 4 \text{ connections}$

Why: $4 \times 2.5 = 10 \text{ Gbps}$ aggregate

3 Routing

BGP, same prefixes and AS_PATH on all 8 tunnels, VPN ECMP support enabled on the TGW

Why: unequal paths disable ECMP

4 Single-flow limit

one TCP flow $\leq 1.25 \text{ Gbps}$

Why: ECMP hashes per flow

ANSWER 4 VPN connections (8 tunnels) to the Transit Gateway; a VGW could not do it (no ECMP).

CHECK ✓ TGW metrics BytesIn per attachment should be roughly equal across tunnels.

MYTH

✗ Direct Connect traffic is encrypted

✗ A DX gateway lets two VPCs talk to each other

✗ A VGW load-balances over both VPN tunnels

✗ Advertise as many prefixes as you like on a private VIF

FACT

✓ DX is private but not encrypted
Add MACsec (dedicated ports) or an IPsec VPN over a transit/public VIF.

✓ DXGW only connects VIFs to gateways
Use a Transit Gateway or peering for VPC-to-VPC.

✓ VGW uses one tunnel at a time
ECMP needs a Transit Gateway.

✓ More than 100 IPv4 prefixes puts the session in Idle
Summarise routes.

Key takeaways

01

DX = private, consistent, not encrypted

private, public, transit VIFs; DXGW is global

02

Resiliency = locations $\times$ connections

maximum = 2×2 on separate devices

03

VPN on TGW for ECMP and acceleration

1.25 Gbps per tunnel, MTU 1446

04

Path control

longest prefix, then local-pref communities, then AS_PATH

05

Encrypt DX

MACsec on dedicated ports or IPsec over DX

Q1 Which VIF type reaches S3 public endpoints over DX?

A Public VIF (or a private/transit path to an S3 interface endpoint).

Q2 Which VIF connects DX to a Transit Gateway?

A Transit VIF through a Direct Connect gateway.

Q3 Community that makes AWS prefer this DX path towards you the most?

A 7224:7300 (high local preference).

Q4 BGP stuck in Active on a new VIF. First checks?

A VLAN ID, peer IPs, TCP 179 reachability, ACLs on the router; then ASN and MD5 key.

Q5 Maximum MTU on a private VIF and on a transit VIF?

A 9001 bytes on private VIFs, 8500 on transit VIFs (jumbo frames enabled per VIF).

Q6 Which DX feature encrypts at layer 2?

A MACsec, on dedicated 10/100/400 Gbps connections at supported locations.

Q7 Need faster failover than BGP hold timers?

A Enable BFD on the customer router (AWS side is on by default).

Q8 Remote employees need access to VPCs with SAML SSO?

A AWS Client VPN with a SAML identity provider and authorization rules.

Q9 Same prefix learnt over DX and VPN on a VGW: which wins?

A Direct Connect BGP route.