



Routing *Inside* and *Into* the Cloud

The Basics of VPCs and Transit Gateways

Agenda

- About Me!
- Who's Who in the *Neighborhood Zoo*
- Directing all the *Neighborhood Traffic*
- Connecting Neighborhoods Together
- Planning for Scale – *World Domination*

About Me! *William Collins*

CONNECT
CLOUD NETWORKING VIRTUAL SUMMIT

2005

Help Desk

Access Management

Senior Network Engineer

Network Architect

Cloud Architect

Principal Cloud Architect

2025

Tech Evangelist

20 years

Let's Connect!

<https://linktr.ee/MacroEngineered>



Hosted by  Megaport



Who's Who in the Neighborhood Zoo



Virtual Private Cloud (VPC)

Foundational service in AWS that allows resources to communicate privately with each other. VPCs are like neighborhoods

172.16.0.0
172.16.1.0
172.16.2.0

Route Table

Get attached to subnets and direct traffic. Route Tables are like road signs in the neighborhood



Subnet

Segment VPCs into small manageable blocks. Subnets are like houses in the neighborhood



Access Lists (NACLs)

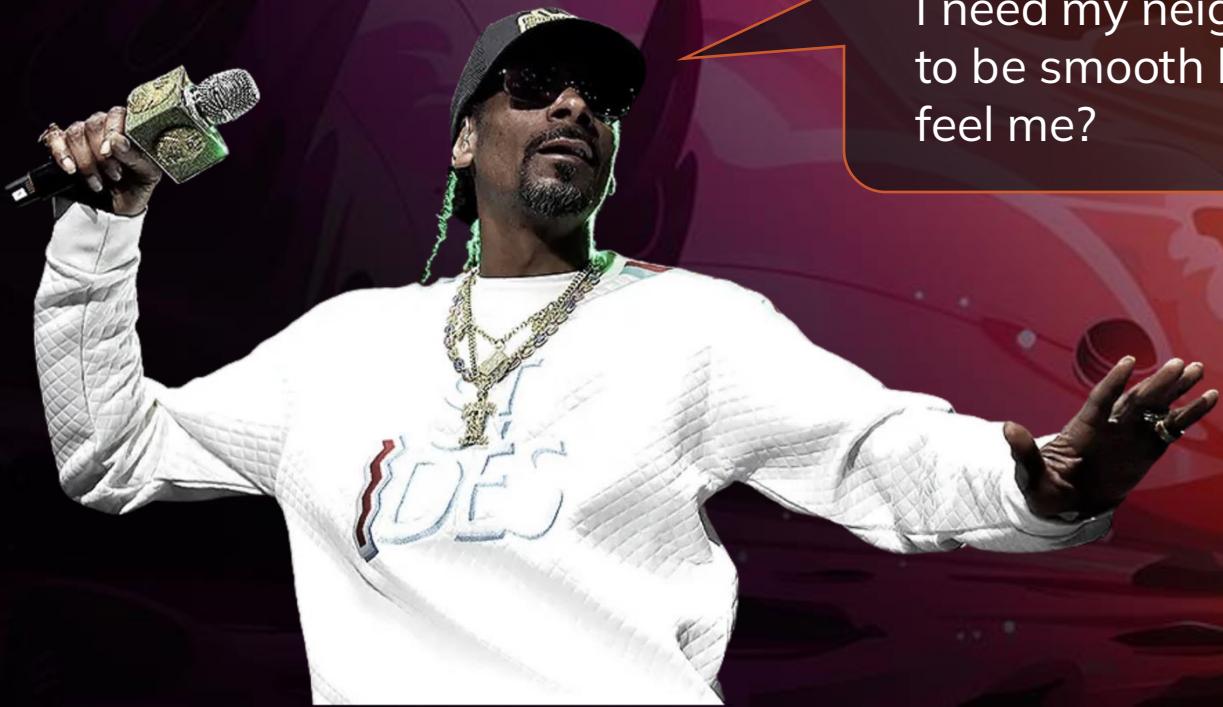
Stateless One-to-many security checkpoints at the subnet level. NACLs are like security checkpoints for the whole neighborhood

✓
✓
✗

Security Group

Stateful traffic controls applied at the `instance` / VM in AWS. Security Groups are like private security for only the people in your home

Directing all the Neighborhood Traffic



I need my neighborhood's traffic
to be smooth like my flows, you
feel me?

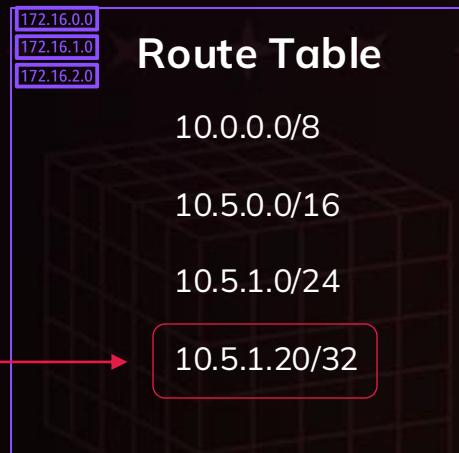
Directing all the Neighborhood Traffic



I need to get to Destination IP: **10.5.1.20**



Longest prefix
match gets used

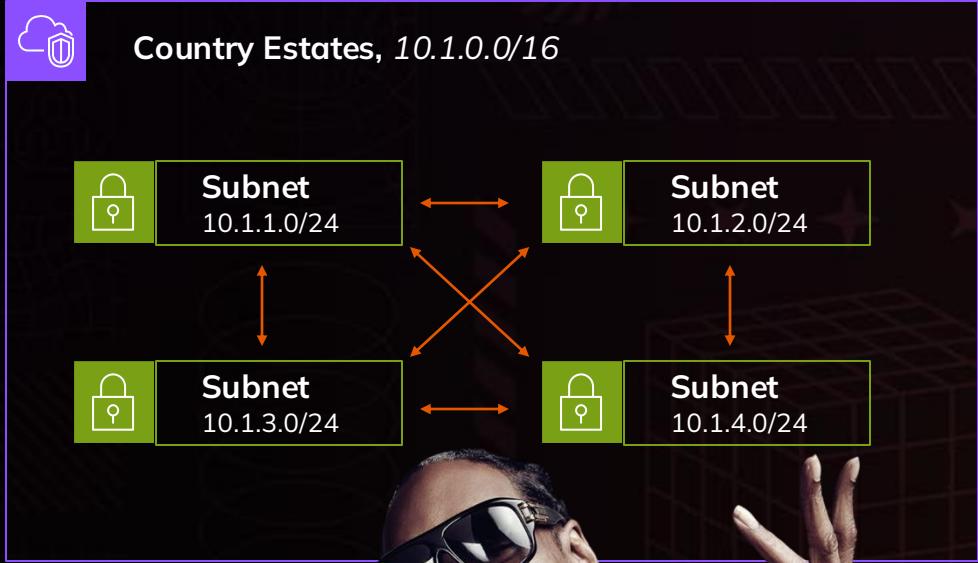


AWS uses longest prefix match – which is a term for selecting the most specific route (largest number of matching bits or the most specific subnet mask). Route priority is based on table entries, with local routes being preferred over propagated and custom routes.

Priority

- 1.) Local Routes (*VPC CIDR*)
- 2.) Custom Routes
- 3.) Propagated VPN/TGW Routes

Directing all the Neighborhood Traffic



Country Estates, 10.1.0.0/16

VPC Defaults

Main Route Table

- Destination: 10.1.0.0/16
- Target: local

Security Group

- Allows all inbound traffic (using default group)
- Allows all outbound to (0.0.0.0/0)

BLOCK
PARTY!!

Connecting Neighborhoods Together



I heard Willow Heights has a
poppin' party! I need to get up
on over there!

Directing all the Neighborhood Traffic



VPC Peering
↔



VPC Peering

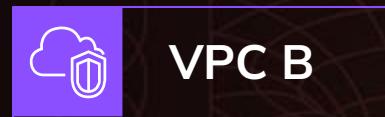
Great for connecting two VPCs
(Complexity increases with additional VPCs)

Directing all the Neighborhood Traffic



Scaling Challenges

What is *Transitive Routing*?



VPC A can peer
directly with **VPC B**

Directing all the Neighborhood Traffic



Scaling Challenges

What is *Transitive Routing*?



VPC A can peer
directly with **VPC B**



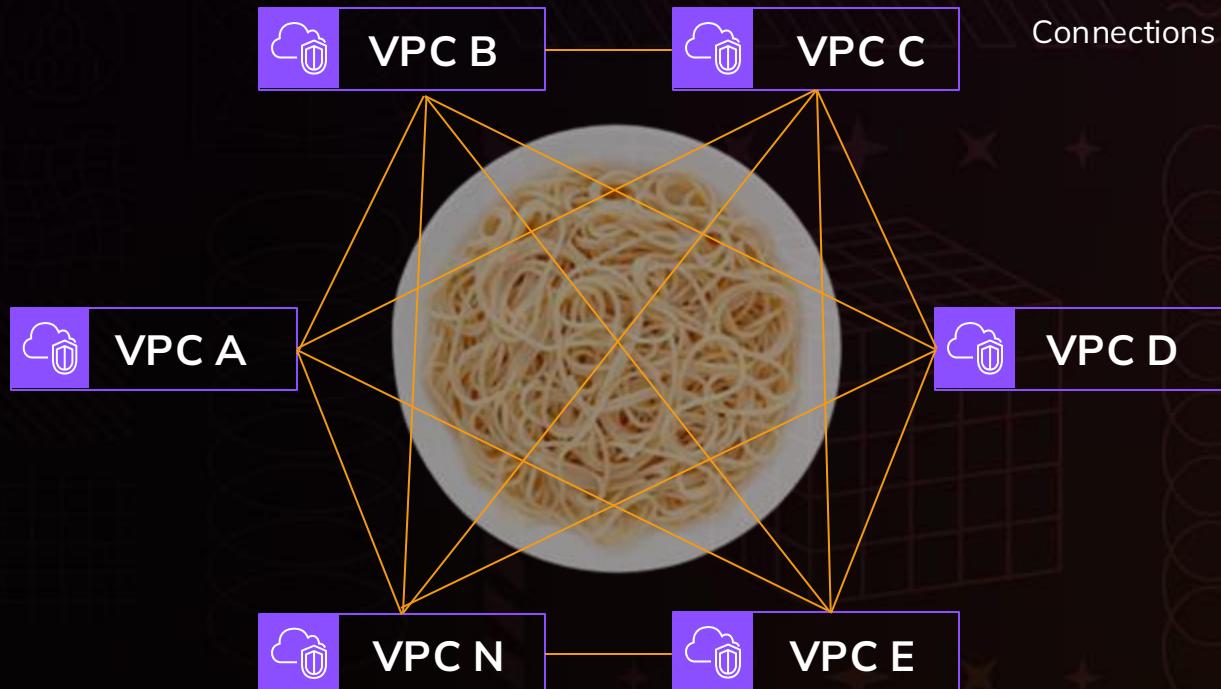
VPC A cannot reach
VPC N through **VPC B**



Directing all the Neighborhood Traffic



Full Mesh Peering at Scale = *Complexity + Tech Debt*



$$\text{Connections} = n * (n - 1) / 2$$

$$6 * (6 - 1) / 2$$

$$6 * 5 / 2$$

$$30 / 2$$

15 Connections!

Planning for Scale – World Domination



I need better options to get to
more places faster!

Planning for Scale – World Domination



Transit Gateway

Cloud-native, regional network hub that interconnects VPCs and on-premises networks.



Cloud WAN

Managed Wide Area Network (WAN) that allows for building and operating a global network.



Interconnection

Private, high-performance connections to cloud providers, service providers, and other data centers.

Planning for Scale – World Domination

Research, Plan, Organize, and ***Don't Rush!***



Ask good Questions!



Is on-premises a factor?



How many VPCs?



Are there 3rd party integration requirements?



What security requirements exist for segmentation and encryption?



What are the business requirements for High Availability and DR?



**WILD
CARD**



Who is responsible for building new components and maintaining existing components? How will you ensure consistency?



Thank you!

CONNECT

CLOUD NETWORKING VIRTUAL SUMMIT

Hosted by  Megaport