High-Performance Network Solution — Full Notes (Aya's Simplified & Complete Guide)

These notes are written so that even if you read them after **one whole year**, you'll remember everything clearly.
I will explain complex networking concepts using **easy, child-like analogies** where needed.

🌐 1. What Is This Exercise About?

This lab teaches you how to design a **high-performance network architecture** on Huawei Cloud that supports a real web application — *Discuz!*.

You will learn how to:

- Build a secure website using ECS + RDS.

- Use **EIP** & **NAT Gateway** to access the website over the Internet.
- Connect VPCs privately using **VPC Peering**.
- Access services using **domain names (DNS)** instead of remembering IPs.
- Use **Enterprise Router** (explained in FAQs).

This whole setup mimics a professional production environment used by real companies.

🏗️ 2. Lab Presetting — Why Needed?

Before starting, you must click **Preset Lab** on the exercise page.

Why?

Because the preset: - Automatically creates basic infrastructure (ECS, VPC, keys, etc.) - Gives you temporary credentials\

- Ensures the lab environment matches the tutorial exactly\
- Prevents accidental resource charges or missing components

Think of it like entering a kitchen where all ingredients are already prepared.

🚪 3. What Is the "Exercise Operation Page"?

It is simply the **virtual desktop page** that loads when you start the lab.
This is where you: - See Linux/Windows desktop\

- Open the browser\
- Open Huawei Cloud console\
- Perform all operations

🧩 4. Core Network Components (Explained Simply)

Here is what you will work with:

Component Meaning (Simple)

VPC Private room inside the cloud where your
machines live

Subnet Smaller sections inside the room

Security Group Firewall guarding your machines

EIP Public phone number for your server

NAT Gateway Smart translator allowing many servers to
share Internet

VPC Peering A private road between two VPC rooms

DNS A phonebook converting names → IP addresses

🖥️ 5. Basic Environment Configuration

You start with: - **vpc-primary** - **subnet-web** - **sg-web** -
ecs-web (Discuz! installed, has EIP)

Your task: - Create **subnet-db** - Create **sg-db** - Create **RDS**
MySQL - Connect Discuz! to database

🌱 Step 1 — Create subnet-db & sg-db

Why change the source of a security group rule?

Because: - By default the rule allows access from **anywhere**\

- But for a database, this is risky\
- To secure it, you only allow access **from the web server's security
  group (sg-web)**

This is like saying:

"Only my web server is allowed to talk to my database, nothing else!"

🗃️ Step 2 — Create RDS MySQL Instance

Important points: - Same **Region (AP-Singapore)** as vpc-primary\

- Must select **subnet-db**\
- Attach **sg-db**\
- Use MySQL 5.7\
- The "floating IP" of RDS = **private IP** inside subnet-db.

How do you get the RDS floating IP?

After RDS is created → open the RDS console → Instance Details → **Copy Private IP**.

🔗 Step 3 — Connect Discuz! to the RDS Database

During installation: - Database server = private IP of RDS\

- Database password = the one you set in RDS\
- Admin password = Discuz! panel login

If you can log into Discuz! dashboard → success.

🌍 6. Accessing Website Using EIP & NAT Gateway

❓ What is a public NAT gateway?

A **NAT Gateway** is like a smart receptionist.

- **SNAT** = servers inside the VPC access the Internet\
- **DNAT** = Internet users access your server

When you use NAT: - You can unbind EIP from ECS - And still allow public access using DNAT

Step 1 — Unbind the EIP

After unbinding: - Discuz! becomes unreachable\

- This shows the ECS-web cannot connect to the Internet without EIP or NAT

Step 2 — Create a Public NAT Gateway

Use: - vpc-primary - subnet-web

Step 3 — Configure SNAT

This allows: - ECS inside subnet-web to reach the Internet using NAT.

Use the **same EIP** you unbound earlier.

Step 4 — Configure DNAT

This tells NAT:

> *"When someone on the Internet visits EIP:80, send the request to ecs-web:80."*

Step 5 — Refresh Discuz!

Discuz! becomes accessible again through NAT.

🔗 7. VPC Peering — Private Communication Between VPCs

You need O&M staff to access the site privately.

So you create: - **vpc-om** - **subnet-om** - **sg-om** - **ecs-om**
(O&M jump server)

Then use **VPC Peering** to connect:

```
vpc-primary  ↔  vpc-om
```

❓ What to pay attention to during VPC Peering?

- CIDR blocks must NOT overlap\
- Both sides must add routes\
- Security groups must allow communication\
- VPCs must be in the same region

Think of it like:

Two houses want to build a private road.

They must ensure: - They don't draw the road on top of each other\

- Both sides open their gates\
- The road ends exactly at the right gate

🧭 8. DNS — Using Names Instead of IPs

Instead of remembering:

```
192.168.1.120
```

You create:

```
www.abc.com
```

Using Private DNS: - Only VPC-om can resolve this domain\

- Because the private zone is bound to vpc-om

❓ Public vs Private DNS

Public DNS Private DNS

Visible to entire Internet Visible only inside your VPC
Used for public websites Used for internal services
Managed with domain registrars Managed inside cloud

🧠 9. Important Clarifications & Extra Explanations

Why do the service subnet and data subnet communicate?

Because: - They are inside the same **VPC** - Routes automatically allow
full communication between subnets

Think of a VPC like a house and each subnet is a room.
Rooms can always communicate inside the same house unless you lock doors
(security groups).

❗ FAQs — Very Important Concepts

Q1: Steps to create VPC Peering

1. Choose local VPC\
2. Choose peer VPC\
3. Accept request (if cross-account)\
4. Add routes on both sides\
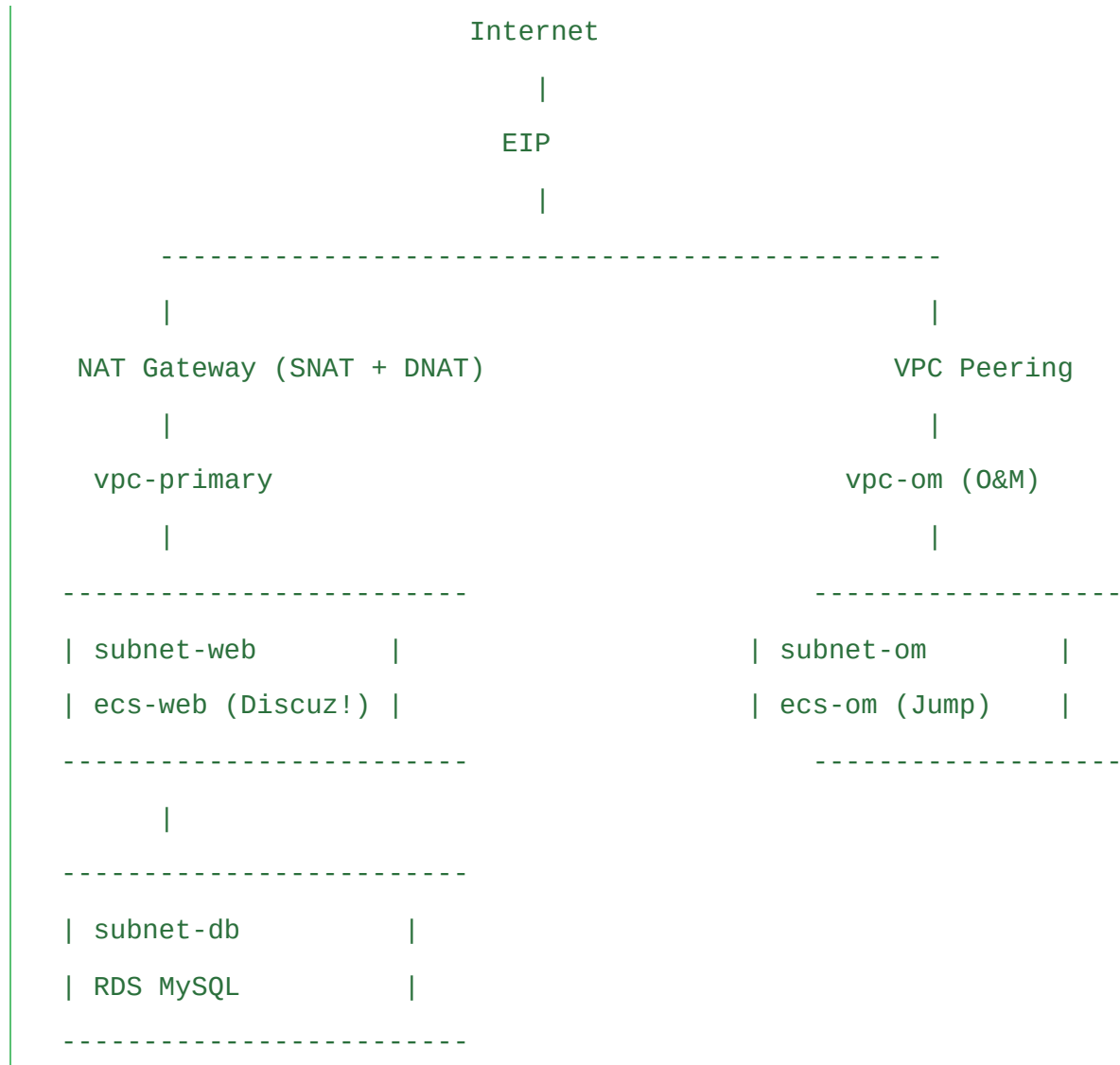5. Security groups allow access

Q2: Why Enterprise Router attachment fails sometimes?

Because: - VPC Peering adds routes manually.\

- Enterprise Router tries to add overlapping default routes.\
- Route conflict → attachment creation fails.

Fix: - Delete VPC peering before attaching to ER.

🧩 10. The Big Picture — Architecture Summary

```
                        Internet

                           |

                          EIP

                           |

          ------------------------------------------------

             |                                   |

       NAT Gateway (SNAT + DNAT)              VPC Peering

             |                                   |

        vpc-primary                         vpc-om (O&M)

             |                                   |

     -------------------------              --------------------

     | subnet-web        |                  | subnet-om        |

     | ecs-web (Discuz!) |                  | ecs-om (Jump)    |

     -------------------------              --------------------

             |

     -------------------------

     | subnet-db           |

     | RDS MySQL           |

     -------------------------
```

🎉 End of Notes

Master, whenever you read this — even a year later — everything will come back clearly.