

Lesson: Subnetting & CIDR

What you'll learn

- What a **subnet mask** is and what the `/24` in `10.100.100.0/24` means.
- How to split an address into its **network part** and **host part**.
- Why the **network address** and **broadcast address** can't be used for hosts.
- How to look at any two addresses and decide whether they're on the **same network**.

This is the chapter that makes the "local or remote?" decision from Lesson 1 *concrete*.

The lesson

1. Why subnets exist

You can't put every machine in the world on one flat network — it wouldn't scale, and you'd want to separate groups for security and management. So we carve the address space into **subnets**: smaller networks, each a contiguous block of addresses. Our lab is one such subnet:

`10.100.100.0/24`.

2. Network part vs host part

Recall an IPv4 address is 32 bits. A subnet splits those 32 bits into two pieces:

```
10.100.100.7 /24
└───┬───┬──┘ └─┘
  first 24 bits  last 8 bits
  = NETWORK      = HOST
  (which network) (which machine on it)
```

- The **network part** is shared by every machine on the subnet — it's the network's "identity".
- The **host part** is unique per machine within that subnet.

3. The mask and the /prefix

The **subnet mask** says *where the split is*. It's 32 bits: 1s for the network part, 0s for the host part.

```
/24 = 11111111.11111111.11111111.00000000 = 255.255.255.0
      └── 24 ones ───┬── 8 zeros ─┘
```

So these two notations mean exactly the same thing:

- **CIDR notation:** 10.100.100.0/24 ← the modern, compact form (CIDR = *Classless Inter-Domain Routing*)
- **Mask notation:** network 10.100.100.0, mask 255.255.255.0

The number after the slash = how many leading bits are the network part. Bigger prefix = more network bits = *fewer* hosts per subnet.

```
/24 → 8 host bits → 2^8 = 256 addresses (254 usable)
/25 → 7 host bits → 2^7 = 128 addresses (126 usable)
/16 → 16 host bits → 2^16 = 65,536 addresses
```

4. The two addresses you can't assign

In every subnet, two host values are reserved:

```
10.100.100.0 ← NETWORK address (host bits all 0) – names the subnet itself
10.100.100.255 ← BROADCAST address (host bits all 1) – "everyone on this subnet"
```

That's why a /24 has 256 total addresses but only **254 usable** for machines (.1 through .254). In our lab, .254 is the Jumpbox and .1/the gateway live at the low end — the usable middle is where VMs sit.

5. The skill: "are these two on the same network?"

This is the practical payoff. To decide if address A can talk to address B *directly* (local) or must go via the gateway (remote), compare their **network parts**.

For /24 it's easy because the split lands on a dot — just compare the first three octets:

```
10.100.100.7   and  10.100.100.50   → first 3 octets match → SAME network → local
10.100.100.7   and  10.100.101.50  → 3rd octet differs   → DIFFERENT network → remote (via
gateway)
```

For non-`/24` masks you compare *bits*, not octets — that's the **AND** operation:

```
address AND mask = network address
10.100.100.7     = 00001010.01100100.01100100.00000111
255.255.255.0   = 11111111.11111111.11111111.00000000
AND result      = 00001010.01100100.01100100.00000000 = 10.100.100.0
```

Do this for both addresses; if the network addresses match, they're on the same subnet.

6. See it on the lab

```
ip addr show          # look for an address like 10.100.100.X/24 – the /24 IS the prefix
ipcalc 10.100.100.7/24 # prints network, broadcast, usable range (install: apt install
ipcalc)
```

`ipcalc` is the fastest way to check your reasoning while it's still new.

Dig deeper

- PracticalNetworking — *Subnetting Mastery* (the best free visual series on this): <https://www.practicalnetworking.net/stand-alone/subnetting-mastery/>
- Cloudflare Learning — *What is a subnet?*: <https://www.cloudflare.com/learning/network-layer/what-is-a-subnet/>
- An online subnet calculator to check your hand calculations: <https://www.subnet-calculator.com/>

Search terms

- `subnetting explained for beginners`
- `CIDR notation explained /24 /16`
- `subnet mask 255.255.255.0 meaning`
- `network address vs broadcast address`
- `how to tell if two IP addresses are on the same subnet`

Check yourself

1. In `10.100.100.0/24`, how many bits are the network part? How many usable host addresses are there?
2. What is the subnet mask for a `/24`, written in dotted-decimal?
3. Which two addresses in any subnet are reserved, and what is each called?
4. Are `10.100.100.5` and `10.100.100.200` on the same network? How did you decide?
5. Are `10.100.100.5` and `10.100.99.200` (both `/24`) on the same network? What happens when `.5` tries to reach `.200` here?

Revision #3

Created 2026-05-11 17:00:00 UTC by Eslam Shapsough

Updated 2026-05-11 17:04:00 UTC by Eslam Shapsough