Tailscale Subnet Router

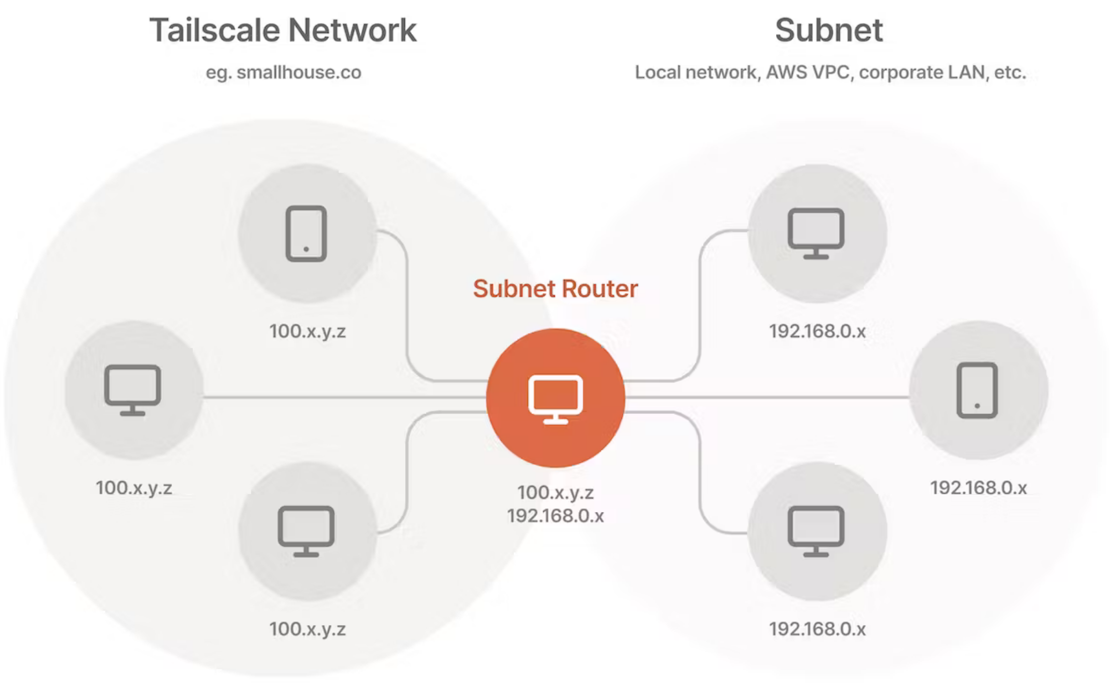
Subnet routers and traffic relay nodes

Tailscale works best when the client app is installed directly on every client, server, and VM in your organization. That way, traffic is end-to-end encrypted, and no configuration is needed to move machines between physical locations.

However, in some situations, you can't or don't want to install Tailscale on each device:

- With embedded devices, like printers, which don't run external software
- When connecting large quantities of devices, like an entire AWS VPC
- When incrementally deploying Tailscale (eg. on legacy networks)

In these cases, you can set up a "subnet router" (previously called a relay node or relaynode) to access these devices from Tailscale. Subnet routers act as a gateway, relaying traffic from your Tailscale network onto your physical subnet. Subnet routers respect features like access control policies, which make it easy to migrate a large network to Tailscale without installing the app on every device.



Step 1: Install the Tailscale client https://tailscale.com/download/linux

Step 2: Connect to Tailscale as a subnet router Enable IP forwarding

If your Linux system has a /etc/sysctl.d directory, use:

```
echo 'net.ipv4.ip_forward = 1' | sudo tee -a /etc/sysctl.d/99-tailscale.conf
echo 'net.ipv6.conf.all.forwarding = 1' | sudo tee -a /etc/sysctl.d/99-tailscale.conf
sudo sysctl -p /etc/sysctl.d/99-tailscale.conf
```

Otherwise, use:

```
echo 'net.ipv4.ip_forward = 1' | sudo tee -a /etc/sysctl.conf
echo 'net.ipv6.conf.all.forwarding = 1' | sudo tee -a /etc/sysctl.conf
sudo sysctl -p /etc/sysctl.conf
```

If your Linux node uses firewalld, you may need to also allow masquerading due to a known issue. As a workaround, you can allow masquerading with this command:

`firewall-cmd --permanent --add-masquerade`

Other distros may require different steps.

When enabling IP forwarding, ensure your firewall is set up to deny traffic forwarding by default. This is a default setting for common firewalls like ufw and firewalld, and ensures your device doesn't route traffic you don't intend. Advertise subnet routes

`sudo tailscale up --advertise-routes=192.168.0.0/24,192.168.1.0/24`

Replace the subnets in the example above with the right ones for your network. Both IPv4 and IPv6 subnets are supported.

If the device is authenticated by a user who can advertise the specified route in autoApprovers, then the subnet router's routes will automatically be approved. You can also advertise any subset of the routes allowed by autoApprovers in the tailnet policy file. If you'd like to expose default routes (0.0.0.0/0 and ::/0), consider using exit nodes instead.

Revision #1
Created 6 April 2024 08:13:19 by Suraj
Updated 6 April 2024 08:21:05 by Suraj