Redsocks 实践

当然！我将指导您如何使用您的 Mac 电脑设置 **Shadowsocks** 代理，并配置您的 **OpenWRT** 路由器，通过此代理将所有连接设备的流量路由。此设置主要包括以下几个步骤：

1. **在 macOS 上设置 Shadowsocks 客户端（使用 Shadowsocks-NG 或 Clash）**
2. **配置 macOS 以允许外部代理连接**
3. **为您的 Mac 分配静态 IP**
4. **在 OpenWRT 上安装和配置 Redsocks**
5. **通过 macOS 代理重定向 OpenWRT 的流量**
6. **测试代理设置**

让我们详细了解每个步骤。

---

1. 在 macOS 上设置 Shadowsocks 客户端

您可以使用 **Shadowsocks-NG** 或 **Clash** 作为您的 Shadowsocks 客户端。以下是两者的使用说明。

选项 A：使用 Shadowsocks-NG

Shadowsocks-NG 是一个流行且用户友好的 macOS Shadowsocks 客户端。

步骤 1：下载并安装 Shadowsocks-NG

1. **下载 Shadowsocks-NG：**
   - 访问 Shadowsocks-NG GitHub 发布页面。
   - 下载最新的 `.dmg` 文件。
2. **安装应用程序：**
   - 打开下载的 `.dmg` 文件。
   - 将 **ShadowsocksX-NG** 应用拖到您的 **应用程序** 文件夹中。
3. **启动 Shadowsocks-NG：**
   - 从 **应用程序** 文件夹中打开 **ShadowsocksX-NG**。
   - 您可能需要在 **系统偏好设置** 中授予应用必要的权限。

步骤 2：配置 Shadowsocks-NG

1. **打开偏好设置：**
   - 点击菜单栏中的 **ShadowsocksX-NG** 图标。
   - 选择 “**Open ShadowsocksX-NG**” > “**Preferences**”。
2. **添加新服务器：**

- 转到 “**Servers**”标签。
- 点击 “+”按钮添加新服务器。

3. **导入 Shadowsocks URL**：
   - **复制您的 Shadowsocks URL**：

     `ss://[ENCRYPTED_PASSWORD]@xxx.xxx.xxx.xxx:xxxxx/?outline=1`
   - **导入方法**：
     - 点击 “**Import**”。
     - 粘贴您的 Shadowsocks URL。
     - Shadowsocks-NG 应该会自动解析并填写服务器详情。
4. **设置本地代理**：
   - 确保勾选 “**Enable SOCKS5 Proxy**”。
   - 注意 **本地端口**（默认通常为 `1080`）。
5. **保存并激活**：
   - 点击 “**OK**”保存服务器。
   - 切换 “**Enable Shadowsocks**”开关至 **ON**。

选项 B：使用 Clash

Clash 是一个多功能的代理客户端，支持包括 Shadowsocks 在内的多种协议。

步骤 1：下载并安装 Clash

1. **下载适用于 macOS 的 Clash**：
   - 访问 Clash GitHub 发布页面。
   - 下载最新的 **Clash for macOS** 二进制文件。
2. **安装应用程序**：
   - 将下载的 **Clash** 应用移动到您的 **应用程序** 文件夹中。
3. **启动 Clash**：
   - 从 **应用程序** 文件夹中打开 **Clash**。
   - 您可能需要在 **系统偏好设置** 中授予必要的权限。

步骤 2：配置 Clash

1. **访问配置文件**：
   - Clash 使用 YAML 配置文件。您可以使用 **TextEdit** 或 **Visual Studio Code** 等文本编辑器创建或编辑它。
2. **添加您的 Shadowsocks 服务器**：
   - 创建一个配置文件（例如 `config.yaml`），内容如下：

```yaml
port: 7890
socks-port: 7891
allow-lan: true
mode: Rule
log-level: info

proxies:
  - name: "MyShadowsocks"
    type: ss
    server: xxx.xxx.xxx.xxx
    port: xxxxx
    cipher: chacha20-ietf-poly1305
    password: "xxxxxx"

proxy-groups:
  - name: "Default"
    type: select
    proxies:
      - "MyShadowsocks"
      - "DIRECT"

rules:
  - MATCH,Default
```

注意事项：

- **port** 和 **socks-port** 定义了 Clash 监听的 HTTP 和 SOCKS5 代理端口。
- **allow-lan: true** 允许局域网设备使用代理。
- **proxies** 部分包括您的 Shadowsocks 服务器详情。
- **proxy-groups** 和 **rules** 决定了流量的路由方式。

3. **使用配置文件启动 Clash**：
   - 启动 Clash 并确保它使用您的 `config.yaml` 文件。
   - 您可能需要在启动 Clash 时指定配置路径。
4. **验证代理是否运行**：
   - 确保 Clash 正在连接到您的 Shadowsocks 服务器。
   - 检查菜单栏图标的状态。

---

2. 配置 macOS 以允许外部代理连接

默认情况下，Shadowsocks 客户端将代理绑定到 `localhost` (`127.0.0.1`)，这意味着只有 Mac 可以使用该代理。要允许您的 OpenWRT 路由器使用此代理，您需要将代理绑定到 Mac 的局域网 IP。

对于 Shadowsocks-NG：

1. **打开偏好设置：**
   - 点击菜单栏中的 **ShadowsocksX-NG** 图标。
   - 选择 “**Open ShadowsocksX-NG**” > “**Preferences**”。
2. **转到高级选项卡：**
   - 导航到 “**Advanced**”标签。
3. **设置监听地址：**
   - 将 “**Listen Address**”从 `127.0.0.1` 更改为 `0.0.0.0` 以允许来自任何接口的连接。
   - 或者，指定 Mac 的局域网 IP（例如 `192.168.1.xxx`）。
4. **保存并重启 Shadowsocks-NG：**
   - 点击 “**OK**”保存更改。
   - 重启 Shadowsocks-NG 客户端以应用新设置。

对于 Clash：

1. **编辑配置文件：**
   - 确保在您的 `config.yaml` 中启用了 `allow-lan: true` 设置。
2. **绑定到所有接口：**
   - 在配置中，设置 `allow-lan: true` 通常会将代理绑定到所有可用接口，包括局域网。
3. **重启 Clash：**
   - 重启 Clash 客户端以应用更改。

---

3. 为您的 Mac 分配静态 IP

为了确保 OpenWRT 路由器与 Mac 之间的连接稳定，请在您的本地网络中为 Mac 分配一个静态 IP。

在 macOS 上分配静态 IP 的步骤：

1. **打开系统偏好设置：**
   - 点击 **Apple** 菜单，选择 “**系统偏好设置**”。
2. **导航到网络设置：**
   - 点击 “**网络**”。
3. **选择您的活动连接：**

- 从左侧栏中选择 “**Wi-Fi**”或 “**以太网**”，具体取决于您的 Mac 如何连接到路由器。

4. **配置 IPv4 设置**：
   - 点击 “**高级…**”。
   - 转到 “**TCP/IP**”标签。
   - 将 “**配置 IPv4**”从 “**使用 DHCP**”更改为 “**手动**”。
5. **设置静态 IP 地址**：
   - **IP 地址**：选择一个路由器 DHCP 范围之外的 IP 以防止冲突（例如 `192.168.1.xxx`）。
   - **子网掩码**：通常为 `255.255.255.0`。
   - **路由器**：您路由器的 IP 地址（例如 `192.168.1.1`）。
   - **DNS 服务器**：您可以使用路由器的 IP 或其他 DNS 服务，如 `8.8.8.8`。
6. **应用设置**：
   - 点击 “**OK**”，然后点击 “**应用**”保存更改。

---

4. 在 OpenWRT 上安装和配置 Redsocks

Redsocks 是一个透明的 SOCKS 重定向器，允许您通过 SOCKS5 代理路由网络流量。我们将使用 Redsocks 将 OpenWRT 的流量重定向到在 Mac 上运行的 Shadowsocks 代理。

步骤 1：安装 Redsocks

1. **更新软件包列表**：

```
ssh root@<router_ip>
opkg update
```

2. **安装 Redsocks**：

```
opkg install redsocks
```

如果 *Redsocks* 在您的 *OpenWRT* 仓库中不可用，您可能需要手动编译或使用替代软件包。

步骤 2：配置 Redsocks

1. **创建或编辑 Redsocks 配置文件**：

```
vi /etc/redsocks.conf
```

2. **添加以下配置**：

```
base {
    log_debug = on;
    log_info = on;
```

```
    log = "file:/var/log/redsocks.log";
    daemon = on;
    redirector = iptables;
}

redsocks {
    local_ip = 0.0.0.0;
    local_port = 12345;  # Redsocks 监听的本地端口
    ip = xxx.xxx.xxx.xxx;  # Mac 的静态 IP
    port = xxxxx;          # Shadowsocks-NG 的本地 SOCKS5 代理端口
    type = socks5;
    login = "";           # 如果您的代理需要认证
    password = "";
}
```

注意事项：

- `local_port`：Redsocks 用于监听来自 iptables 重定向的连接的端口。
- `ip` 和 `port`：指向您的 Mac 上的 Shadowsocks SOCKS5 代理（基于前面的步骤为 `xxx.xxx.xxx.xxx:xxxxx`）。
- `type`：设置为 `socks5`，因为 Shadowsocks 提供 SOCKS5 代理。

3. **保存并退出：**
   - 按 `ESC`，输入 `:wq`，然后按 `Enter`。
4. **创建日志文件：**

```
touch /var/log/redsocks.log
chmod 644 /var/log/redsocks.log
```

步骤 3：启动 Redsocks 服务

1. **启用 Redsocks 开机启动：**

```
/etc/init.d/redsocks enable
```

2. **启动 Redsocks：**

```
/etc/init.d/redsocks start
```

3. **验证 Redsocks 是否在运行：**

```
ps | grep redsocks
```

您应该会看到 Redsocks 进程正在运行。

---

5. 通过 macOS 代理重定向 OpenWRT 的流量

现在，Redsocks 已在 OpenWRT 上设置完毕，接下来配置 iptables，将所有出站的 TCP 流量通过 Redsocks 重定向，而 Redsocks 再通过您的 Mac 的 Shadowsocks 代理路由流量。

步骤 1：配置 iptables 规则

1. **添加 iptables 规则以重定向流量：**

```
# 将所有 TCP 流量重定向到 Redsocks（除了流向代理本身的流量）
iptables -t nat -N REDSOCKS
iptables -t nat -A REDSOCKS -d xxx.xxx.xxx.xxx -p tcp --dport xxxxx -j RETURN
iptables -t nat -A REDSOCKS -p tcp -j REDIRECT --to-ports 12345

# 将 REDSOCKS 链应用于所有出站流量
iptables -t nat -A OUTPUT -p tcp -j REDSOCKS
iptables -t nat -A PREROUTING -p tcp -j REDSOCKS
```

解释：

- **创建新链：** REDSOCKS
- **排除代理流量：**确保目的地为代理本身的流量不被重定向。
- **重定向其他 TCP 流量：**将其他 TCP 流量转发到 Redsocks 的监听端口（12345）。

2. **保存 iptables 规则：**

为了使这些规则在重启后依然有效，将它们添加到防火墙配置中。

```
vi /etc/firewall.user
```

添加 iptables 规则：

```
# 将所有 TCP 流量重定向到 Redsocks（除了代理）
iptables -t nat -N REDSOCKS
iptables -t nat -A REDSOCKS -d xxx.xxx.xxx.xxx -p tcp --dport xxxxx -j RETURN
iptables -t nat -A REDSOCKS -p tcp -j REDIRECT --to-ports 12345

# 应用 REDSOCKS 链
iptables -t nat -A OUTPUT -p tcp -j REDSOCKS
iptables -t nat -A PREROUTING -p tcp -j REDSOCKS
```

保存并退出：

- 按 ESC，输入 :wq，然后按 Enter。

3. **重启防火墙以应用更改**：

```
/etc/init.d/firewall restart
```

步骤 2：验证流量是否被重定向

1. **检查 Redsocks 日志**：

```
cat /var/log/redsocks.log
```

您应该会看到日志显示流量正在通过 Redsocks 处理。

2. **从客户端设备进行测试**：

- 连接设备到您的 OpenWRT 路由器。
- 访问一个网站或执行一个使用互联网的操作。
- 通过检查外部 IP 地址（例如通过 WhatIsMyIP.com）验证流量是否通过代理路由。

---

6. 测试代理设置

通过执行以下测试，确保整个设置按预期工作。

步骤 1：验证 Mac 上的 Shadowsocks 连接

1. **检查 Shadowsocks 客户端状态**：
   - 确保 Shadowsocks-NG 或 Clash 正在连接到 Shadowsocks 服务器。
   - 验证本地代理（例如 xxx.xxx.xxx.xxx:xxxxx）是否可访问。
2. **在本地测试代理**：
   - 在您的 Mac 上，打开浏览器并将其配置为使用 localhost:1080 作为 SOCKS5 代理。
   - 访问 WhatIsMyIP.com 以确认 IP 是否与 Shadowsocks 服务器匹配。

步骤 2：验证 OpenWRT 的流量是否通过代理路由

1. **检查 OpenWRT 的外部 IP**：
   - 从连接到 OpenWRT 的设备访问 WhatIsMyIP.com，查看 IP 是否反映 Shadowsocks 服务器的 IP。
2. **监控 Redsocks 日志**：
   - 在 OpenWRT 上，监控 Redsocks 日志以确保流量被重定向。

```
tail -f /var/log/redsocks.log
```

3. **必要时进行故障排除**：
   - 如果流量未正确路由：
     - 确保 Mac 上的 Shadowsocks 客户端正在运行并可访问。
     - 验证 iptables 规则是否正确设置。
     - 检查 Mac 和 OpenWRT 上的防火墙设置。

附加考虑事项

1. 安全性

- **保护您的代理**：
  - 确保只有可信设备可以访问代理。由于您正在通过 Redsocks 重定向所有流量，请确保 Mac 的防火墙仅允许来自 OpenWRT 路由器的连接。

  在 macOS 上：
  - 进入 **系统偏好设置** > **安全性与隐私** > **防火墙**。
  - 配置防火墙，仅允许来自 OpenWRT 路由器 IP 的代理端口 (`xxxxx`) 的传入连接。
- **认证**：
  - Shadowsocks 已通过加密提供了一定程度的安全性。确保使用强密码和加密方法。

2. 性能

- **路由器资源**：
  - 运行像 Redsocks 这样的代理服务可能会消耗 OpenWRT 路由器的额外 CPU 和内存。确保您的路由器有足够的资源。
- **Mac 性能**：
  - 确保您的 Mac 保持开启并连接到网络，以维持代理的可用性。

3. 维护

- **监控日志**：
  - 定期检查 Redsocks 和 Shadowsocks 的日志，以发现任何异常活动或错误。
- **更新软件**：
  - 保持 OpenWRT、Redsocks 以及您的 Shadowsocks 客户端更新，以受益于安全补丁和性能改进。

4. 替代方法

虽然使用 Mac 作为中介代理服务器是可行的，但考虑以下替代方案可能会简化设置：

- **直接将 OpenWRT 配置为 Shadowsocks 客户端**：
  - OpenWRT 通过 `shadowsocks-libev` 等软件包直接支持 Shadowsocks。这种方法无需 Mac 作为中介。
- **使用专用的代理/VPN 设备**：
  - 如 Raspberry Pi 等设备可以运行代理服务，作为专用网关使用。

结论

通过遵循上述步骤，您已将 Mac 设置为 Shadowsocks 代理服务器，并配置了 OpenWRT 路由器，通过此代理将所有连接设备的流量路由。此设置通过利用 Shadowsocks 协议，增强了您网络的隐私和控制。

关键点回顾：

1. **Mac 上的 Shadowsocks 客户端**：
   - 使用您提供的 Shadowsocks URL 安装并配置了 Shadowsocks-NG 或 Clash。
   - 配置客户端监听 Mac 的局域网 IP。
2. **代理可访问性**：
   - 为 Mac 分配了静态 IP，以确保代理访问的一致性。
   - 配置了 macOS 防火墙以允许传入的代理连接。
3. **OpenWRT 配置**：
   - 安装并配置了 Redsocks，通过 Shadowsocks 代理重定向所有出站 TCP 流量。
   - 应用了必要的 iptables 规则以强制流量重定向。
4. **测试**：
   - 通过检查外部 IP 地址验证了连接设备的流量通过 Shadowsocks 代理路由。

建议：

- **确保稳定性**：保持 Mac 开启并连接，以维持代理的可用性。
- **安全优先**：定期更新所有组件并监控日志，以防止未经授权的访问。
- **考虑直接路由器配置**：为了更简化的设置，探索直接在 OpenWRT 路由器上配置 Shadowsocks。

如果您在配置过程中遇到任何问题或需要进一步的帮助，请随时联系我们!

```
base {
    log_debug = on;
    log_info = on;
```

```
    log = "file:/var/log/redsocks.log";
    daemon = on;
    redirector = generic;
}

redsocks {
    local_ip = 0.0.0.0;
    local_port = 7891;
    ip = xxx.xxx.xxx.xxx;
    port = xxxxx;
    type = http-connect;
    login = "";
    password = "";
}
```