# 如何打造一款内网穿梭的利器


安全服务部 ---- 曲文集


使用了存在于欧洲的上百台不同服务器

它在这里

http://www.rootkiter.com/EarthWorm

## 它的功能有

a) 端口转发（可团队协同）

b) 多平台支持

c) 和本地测试工具联动

d) 便携式

http://www.rootkiter.com/EarthWorm

它的功能有

a) 端口转

c) 和

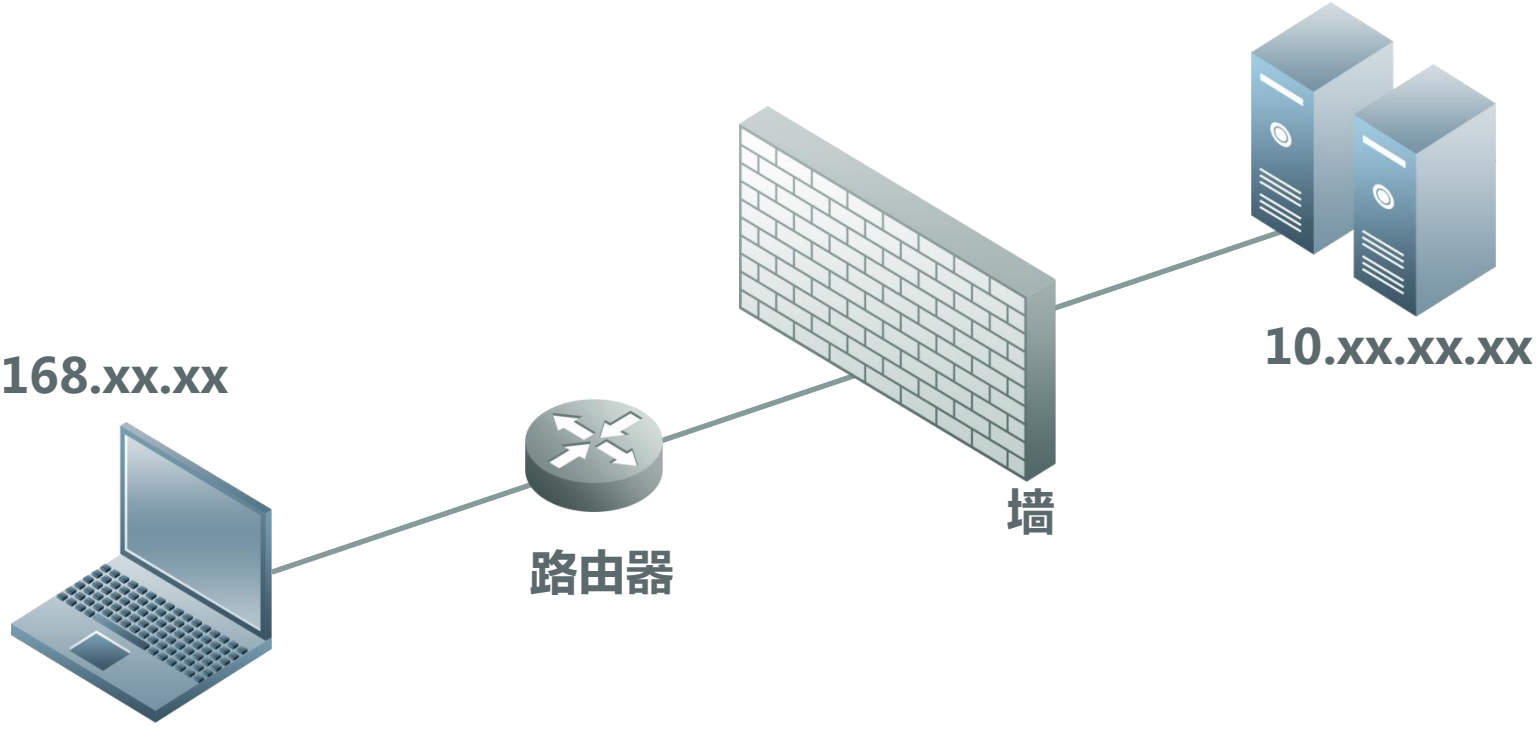
d)

# 议题主线：
# WHY And HOW

http://www.rootkiter.com/EarthWorm

# 目录

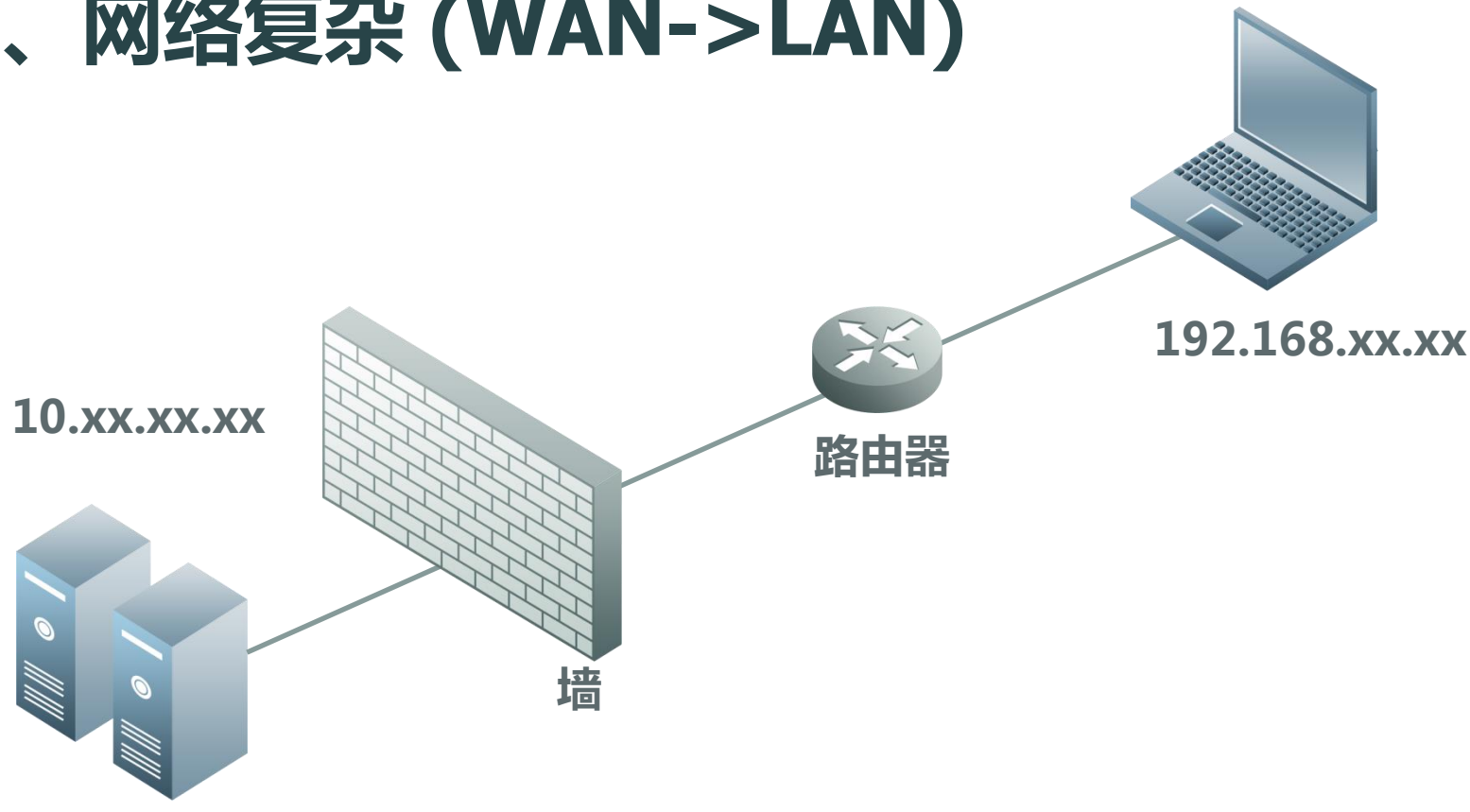
# 1、网络复杂 (LAN->WAN)




有一种坑，叫做：你已经在内网中，我却在内网的子网中

*日日见君，君却不识我。*

# 1、网络复杂 (WAN->LAN)



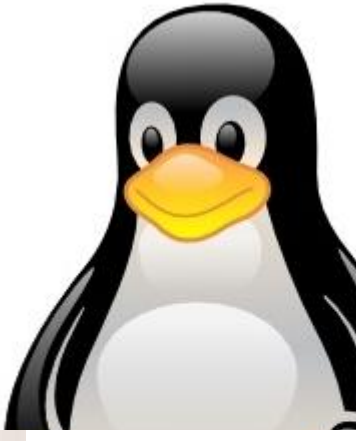

另一种坑，叫做：你天天来找我玩，我却还不知道你家在哪。。。

*你娘让我喊你回家吃饭噻，但问题是你在哪呢？？？*

# 2、主机复杂（外表）


这叫做：　　*林子大了什么鸟都有*

# 2、主机复杂（内在）

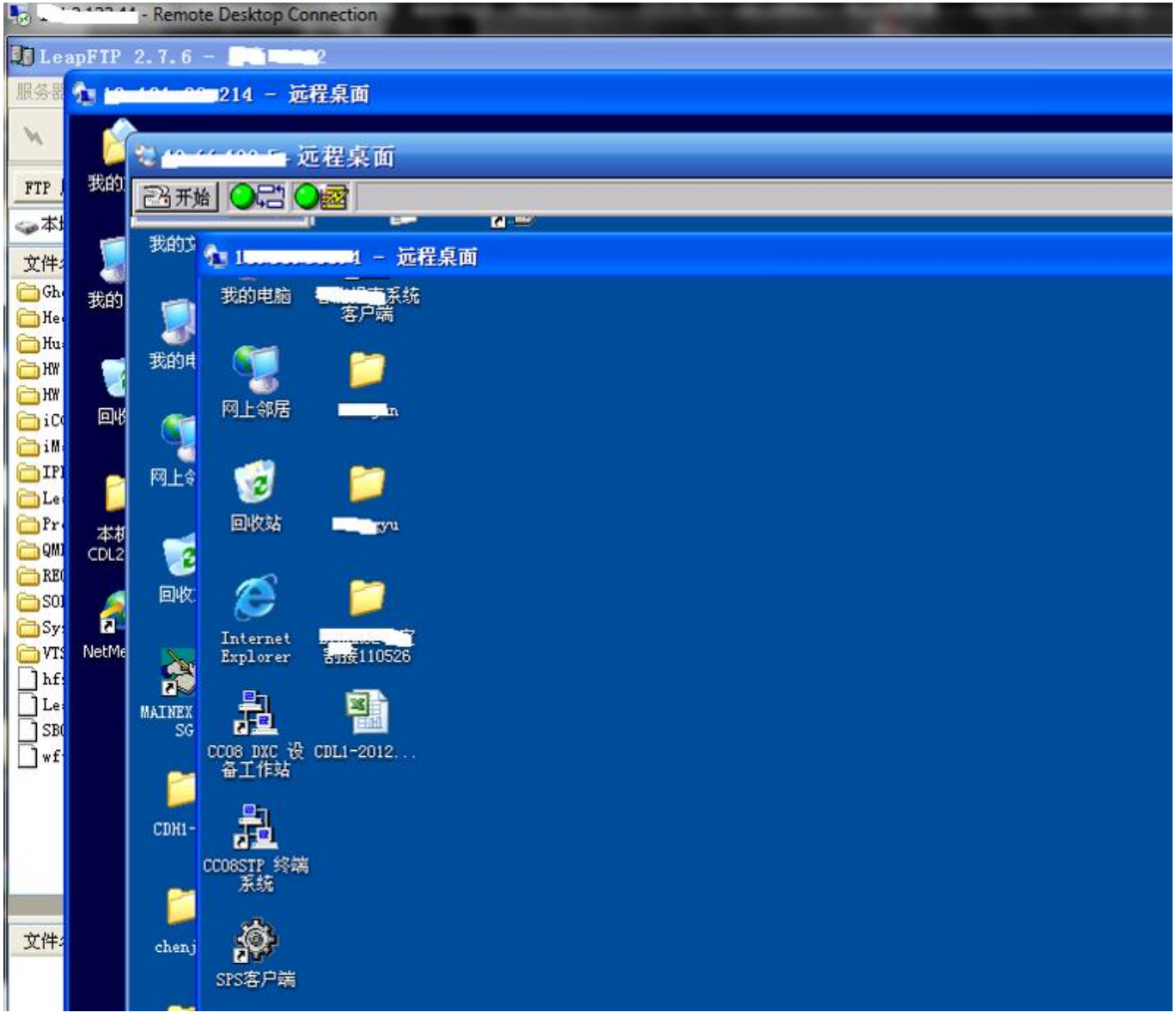







这叫做：　　*林子大了什么鸟都有，Too。*

# 3、内网带宽有限（远程桌面嵌套起来会很卡）



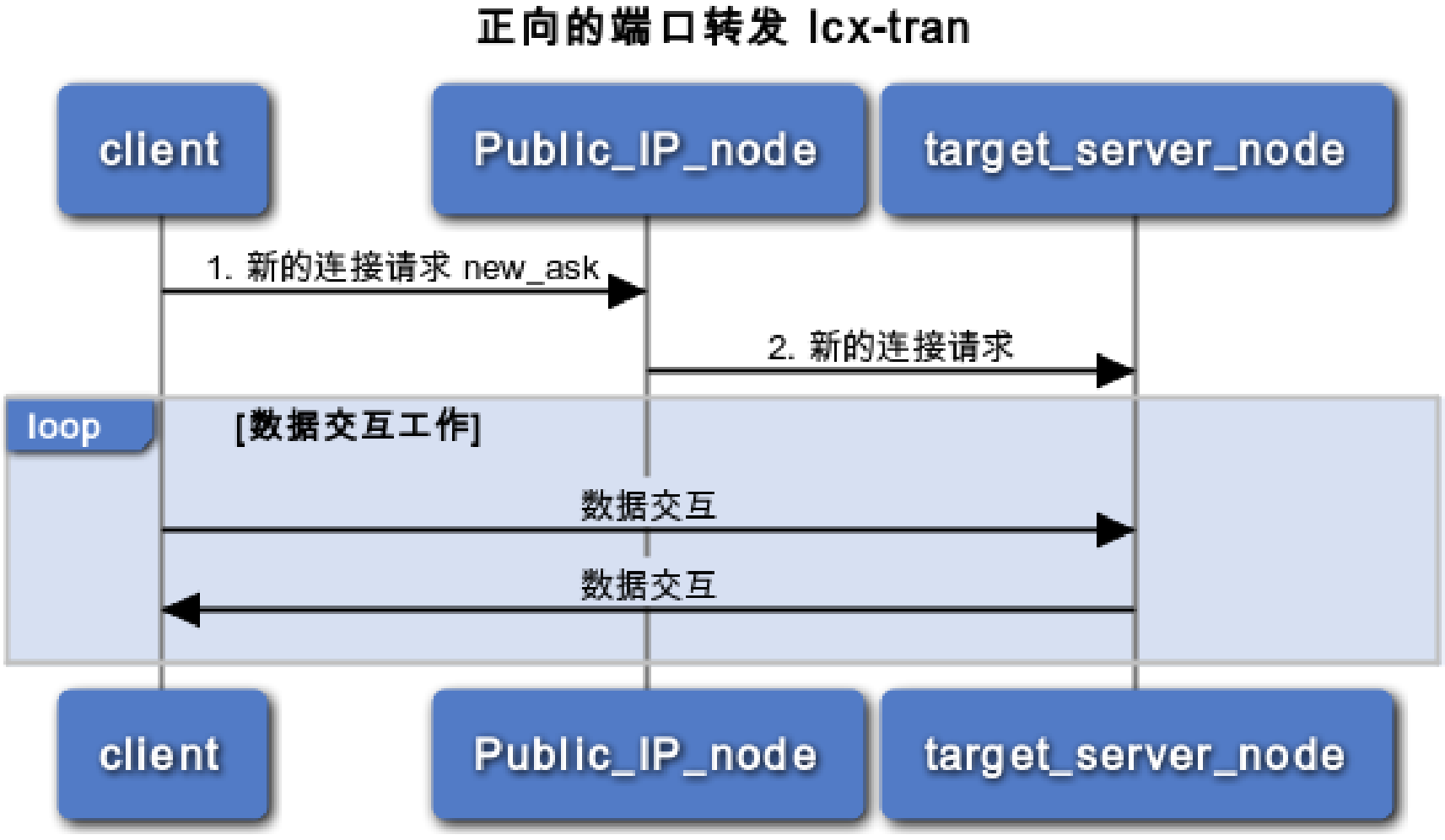
# 内网中的那些坑

1. 端口转发（正向、反向自由切换）
2. 支持常见的操作系统和处理器
3. 自身要够小，且无需额外的环境依赖
4. 可以直接和测试机工具联动
   （网速限制，传工具很费事）

# 目录

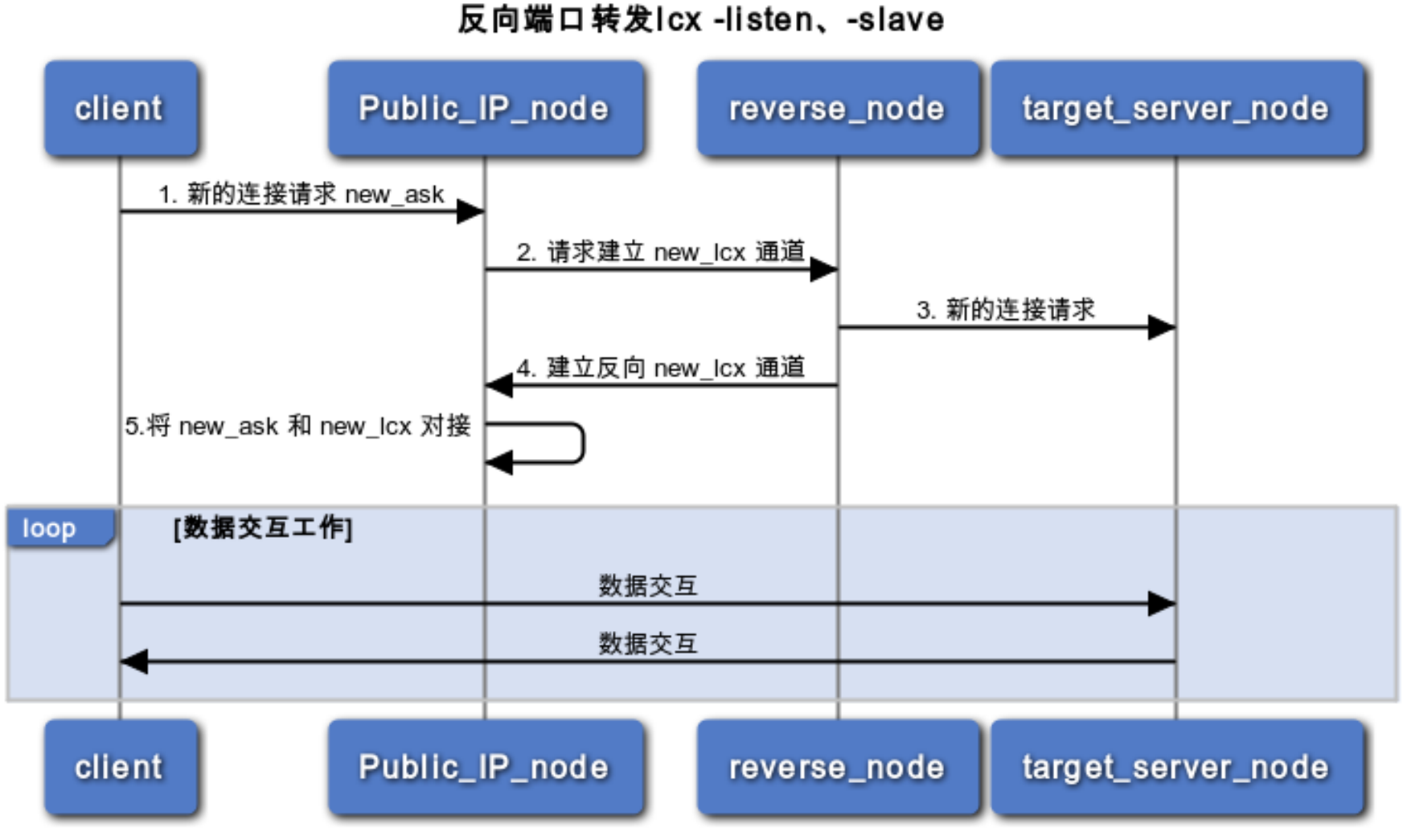
1. 端口转发（正向、反向自由切换）

A）正向端口转发很简单。有新连接就新建连接即可，时序图如下：



1. 端口转发（正向、反向自由切换）

B）反向的端口转发，就需要控制下游节点新建用于数据交互的隧道。



## 2. 支持常见的操作系统和处理器




运行环境？？？

特殊设备？？？
（OpenWrt，TPLink）

## 2. 支持常见的操作系统和处理器



可以生成原生代码，
且都是跨平台库

成品会依赖很多dll文件。
在一些嵌入式设备下，
支持不够完美。

2. 支持常见的操作系统和处理器


从生成原生代码，
部是跨平台库

品会依赖很多dll文件。
一些嵌入式设备下，
持不够完美。

2. 支持常见的操作系统和处理器

overtime@ubuntu: ~/gi

```
1  #include<stdio.h>
2
3  #ifdef WIN32
4      char OS_NAME[]="Windo
5  #elif  linux
6      char OS_NAME[]="Linux
7  #endif
8
9  int main(){
10     printf("This is %s OS
11     return 0;
12 }
```

```
$
$ gcc cross_OS.c -o cross
$ ./cross
This is Linux OS.
$
$
```

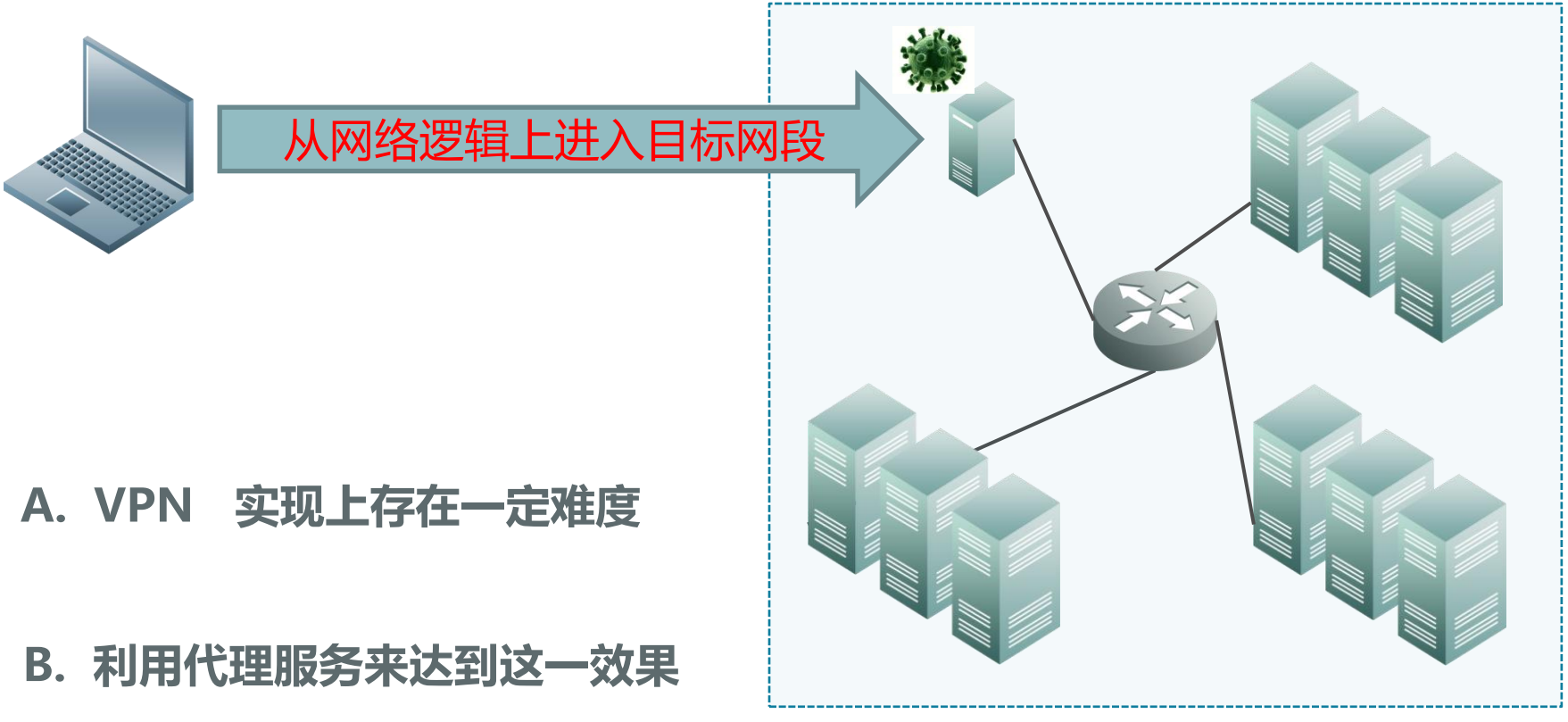
MINGW32:~

```
[redacted]0S1TOOPO ~
$ gcc cross_OS.c -o cross

[redacted]S1TOOPO ~
$ ./cross.exe
This is Windows OS.

[redacted]S1TOOPO ~
$
```

3. 自身要够小，且无需额外的环境依赖

**已经纯C实现了，**
**再优化就该写汇编了。**

4. 可以直接和测试机工具联动




A. VPN 实现上存在一定难度

B. 利用代理服务来达到这一效果

4. 可以直接和测试机工具联动

常见的代理协议：

HTTP
SSL
FTP
SOCKS

4. 可以直接和测试机工具联动

常见的代理协议：
HTTP
SSL
FTP

# SOCKS

高效、体系完善、周边工具多、
有协议实现的样例代码

这里有一篇协议细则：
http://www.rfc-editor.org/rfc/rfc1928.txt

# 还有哪些要注意的

A. 等价 API 抽象层

不同平台的 API 提供有差异。

B. 编译环境搭建

Linux：

$ sudo apt-get install gcc

MacOS:

Xcode 装好就有对应的 gcc 了

Windows：

MINGW32 + gcc

其他嵌入式设备：

Linux + buildroot（Toolchain）

C. Big/Little -Endian

由于 CPU 存在差异化，而选定的实现语言为 C，所以编码时要注意规避这类问题。

# 目录

# 一些思考

1. 多平台、原生层、恶意程序、可行。

2. 重视内网安全。

3. 小心身边的智能设备。

# 谢谢！