# 地址转换协议NAT

# 网络地址转换协议

**地址地址转换协议（NAT）：在私有地址和全局可路由地址之间转换的协议。**

**RFC3022**
**RFC2993**
**RFC3235**
**RFC3027**

## 引入NAT协议的动机

- 增加内部网络的安全性
- 内联网用户需要访问因特网
- DHCP只能部分缓解IP地址资源的不足
- 小型企业和家庭用户需要全程在线连接因特网

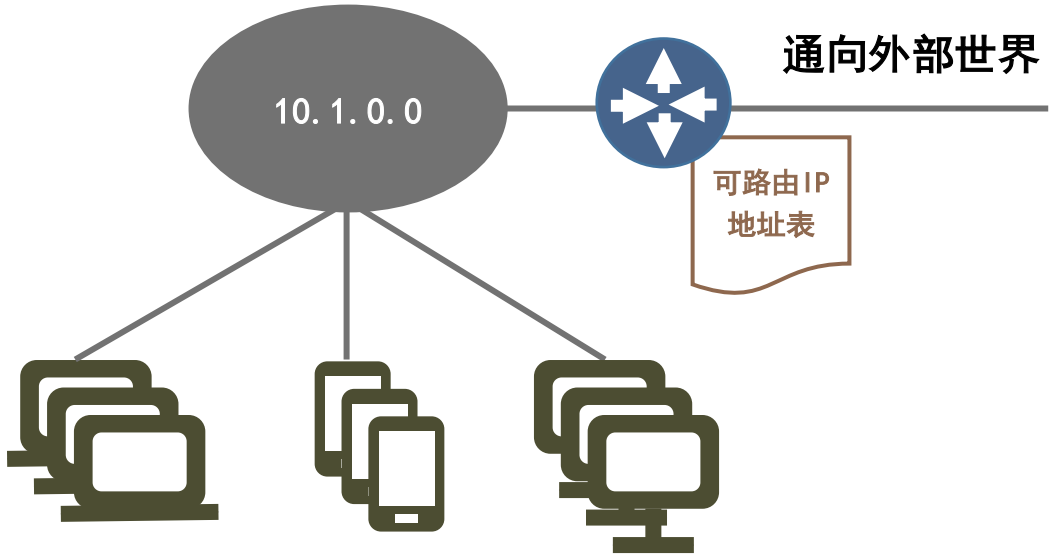
# 静态和动态NAT

## 动态NAT

- 动态配置NAT是建立内部本地地址和外部可路由地址的临时映射关系，并且映射关系具有一定的时效性。

## 静态NAT

- 路由器维护一张可路由IP地址分配表
- 路由器负责建立内网本地地址和外部可路由地址的一对一永久映射关系
- 当外部网络需要通过固定的全局可路由地址访问内部服务器时，静态NAT尤为重要




Router(config)#ip nat inside source static
local-ip global-ip
/*将内网地址映射成外网地址

Router #ip nat inside 10.1.0.2 125.1.2.3

# 基于端口的NAT

**网络端口地址转换（NAPT）：将多个内部地址映射为一个合法的可路由地址，但以不同的协议端口号和内部地址对应于端口号和可路由地址。**

| 内部地址<br>内部端口 | vs | 全局地址<br>外部端口 |
|---|---|---|

路由器维护一张NAT转换表

- 通过转换端口号以及地址来提供并发性
- 除了一对源和目的IP地址以外，还包括一对源和目的协议端口号，以及NAT使用的一个协议端口号。

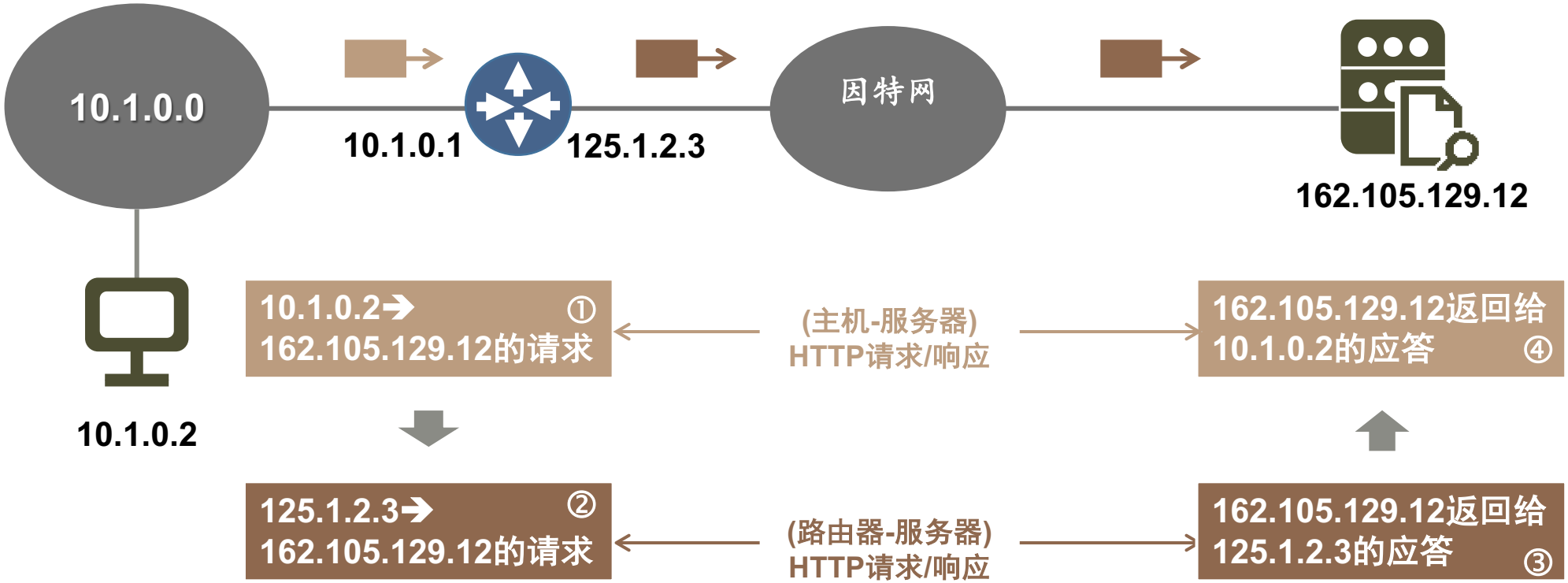
NAT转换表

| NAPT特点 | NAPT优势 | NAPT缺点 |
|---|---|---|
| • “多对一”的NAT<br>• 可将中小型网络隐藏在一个合法IP地址后面 | 能够使用一个全球有效IP地址访问因特网。 | 仅限于TCP或UDP高层协议 |

# NAPT协议——工作过程

假设：内网主机访问外部网络web服务器

- 主机访问WEB服务器的方式没有变化
- 服务器响应主机请求的方式没有变化






内网IP包 外网IP包

# NAT路由器功能

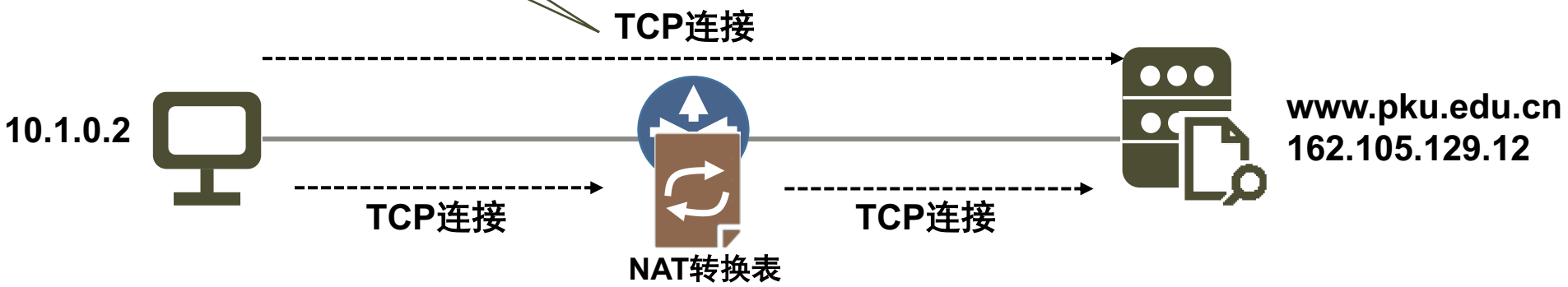
**NAT路由器：负责IP包的源IP地址和目的IP地址转换，地址转换可以静态或者动态设置。**

客户机和服务器的连接被拆分成两段：

- 客户机-路由器
- 路由器-服务器

## NAT路由器的任务

- 针对出境包源地址进行替换：(源IP地址, port #)→(路由器IP地址, 新port #)
- 在NAT转换表中记录映射关系：(源IP地址, port #)→(路由器IP地址, 新port #)
- 针对入境包目标地址进行替换：(路由器IP地址, 新port #) →(源IP地址, port #)



# NAT实现——地址转换表

NAT转换表

| 源主机 | 源IP地址 | 源Port号 | 路由器IP地址 | NAT指定Port号 |
|---|---|---|---|---|
| H1 | 10.1.0.2 | 80 | 125.1.2.3 | 102 |
| H2 | 10.1.0.3 | 3000 | 125.1.2.3 | 103 |
| H3 | 10.1.0.4 | 4000 | 125.1.2.3 | 104 |

## 对于出境包

- 路由器给该包分配一个未用的port号，并用NAT路由器的IP地址和该port号替换包的源IP地址和源port号
- 在NAT地址转换表中添加一项，将源port号源IP地址映射成新分配的port号NAT路由器IP地址

## 对于入境包

- 路由器以目的port号作为索引查找转换表，以对应的源IP地址和port号置换回去
- 转换表中的有关条目动态在空闲超时后删除

# NAT协议——支持/不支持的应用

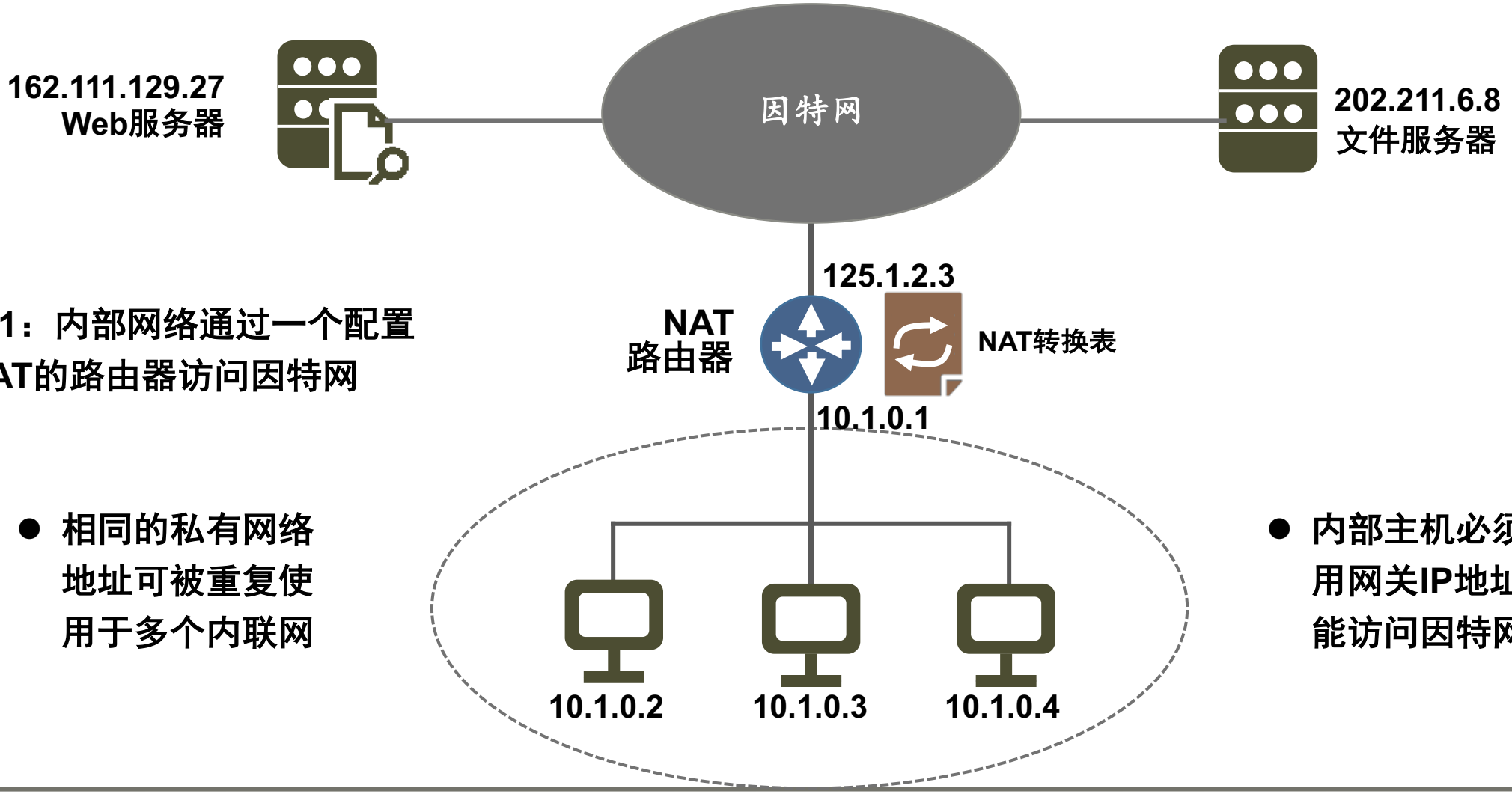
## NAT支持的应用

- 数据部分不包含IP地址的TCP/UDP流
- 在数据部分包含IP地址的IP包
- ICMP、FTP
- NetBIOS over TCP
- RealAudio
- CUSeeMe (White Pines)
- Streamworks
- DNS “A” and “PTR” 查询
- H.323 (NetMeeting)
- VDOLive、Vxtreme

**NAT不支持**

- IP组播
- DNS Zone Transfers
- BOOTP
- Talk, ntalk
- SNMP
- NetShow

# NAT典型应用场景——内联网




示例1：内部网络通过一个配置成NAT的路由器访问因特网

- 相同的私有网络地址可被重复使用于多个内联网
- 内部主机必须使用网关IP地址才能访问因特网

# NAT协议地址转换示例

**内网上的请求包**

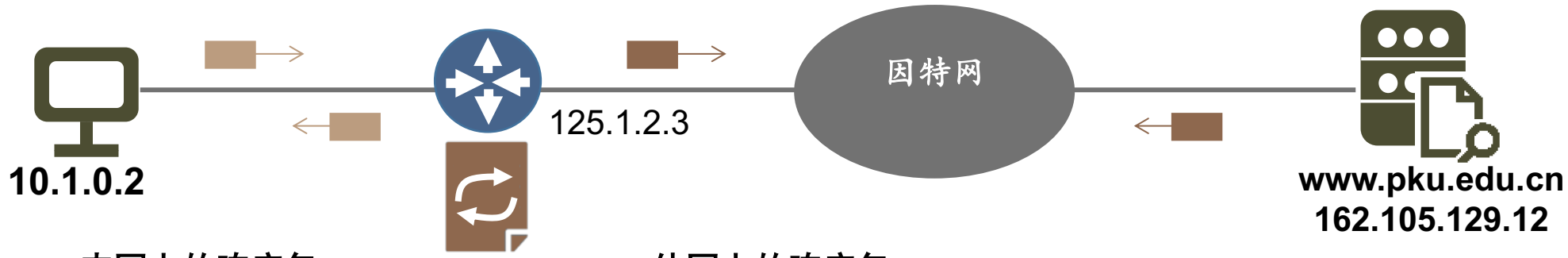
| | |
|---|---|
| Proto | TCP |
| Saddr | 10.1.0.2 |
| Daddr | 162.105.129.12 |
| Sport | 1049 |
| Dport | 80 |

**外网上的请求包**

| | |
|---|---|
| Proto | TCP |
| Saddr | 125.1.2.3 |
| Daddr | 162.105.129.12 |
| Sport | 102 |
| Dport | 80 |

示例2：一个内网主机作为客户机访问外网的一个门户网站

试问：IP包在内外网上的地址转换情况？




**内网上的响应包**

| | |
|---|---|
| Proto | TCP |
| Saddr | 162.105.129.12 |
| Daddr | 10.1.0.2 |
| Sport | 80 |
| Dport | 1049 |

**外网上的响应包**

| | |
|---|---|
| Proto | TCP |
| Saddr | 162.105.203.12 |
| Daddr | 125.1.2.3 |
| Sport | 80 |
| Dport | 102 |

# NAT协议的不足

内网上的请求包

| Proto | TCP |
|---|---|
| Saddr | 10.1.0.2 |
| Daddr | 162.105.129.12 |
| Sport | 1049 |
| Dport | 80 |

外网上的请求包

| Proto | TCP |
|---|---|
| Saddr | 125.1.2.3 |
| Daddr | 162.105.129.12 |
| Sport | 102 |
| Dport | 80 |

**NAT协议不足**

- 破坏了端-端连接语义
- 没有根本解决地址资源不足