

ASS

ASS全称为”Autonomous system scanner“中文名为“自主系统扫描器”，被设计用于查找路由器的As(Autonomous system，自治系统)，他支持IRDP、IGRP、EIGRP、RIPv1、RIPv2、CDP、HSRP和OSPF等协议。

——FX

<http://www.phenoelit.de>

一，帮助手册

Usage is trivial:

ass -i 网卡 -ApcMS -P IER12

-a 从自治系统开始 -b 要停止的自治系统

-S 设置源地址 -D 设置目标地址[^如果不指定地址，将会使用每个协议适当的地址]

-T 设置延迟数[^T1是最慢的扫描，T -100也许变得不死那么可靠]

-r 文件名

Where:

-v 详细输出

-A 设置ASS为活动模式

-M 设置ASS为被动模式

-P 见下文用法

-M EIGRP系统使用多播地址来进行扫描，而不是通过枚举和直接查询进行扫描

-p 不在乱七八糟的环境下运行（也许这是一个坏的主意）

-c 扫描后终止，这也许不是一个好的建议，因为信息可能会晚一点到达，你可以会看到一些没有显示的界面。

```
[-v[v[v]]] -i <interface> [-ApcMs] [-P IER12]
  [-a <autonomous system start> -b <autonomous system stop>]
  [-S <spoofed source IP>] [-D <destination ip>]
  [-T <packets per delay>]
  [-r <filename>]
```

二，模式介绍

ASS主要分为被动模式和活动模式，两者功能和特点均不相同：

被动模式

只监听路由协议数据包（比如广播和多播）

活动模式

试图通过询问信息来发现路由器，这是对每个协议的适当地址（广播或多播地址来进行）进行，如果指定目标地址，则使用此模式，但不可能像默认值那样有效

对于活动模式，可以选择需要扫描的协议，如果不选择，则全部都会被扫描。通过 -P选项 来搭配字符进行任意选择。

I = IGRP

E = EIGRP

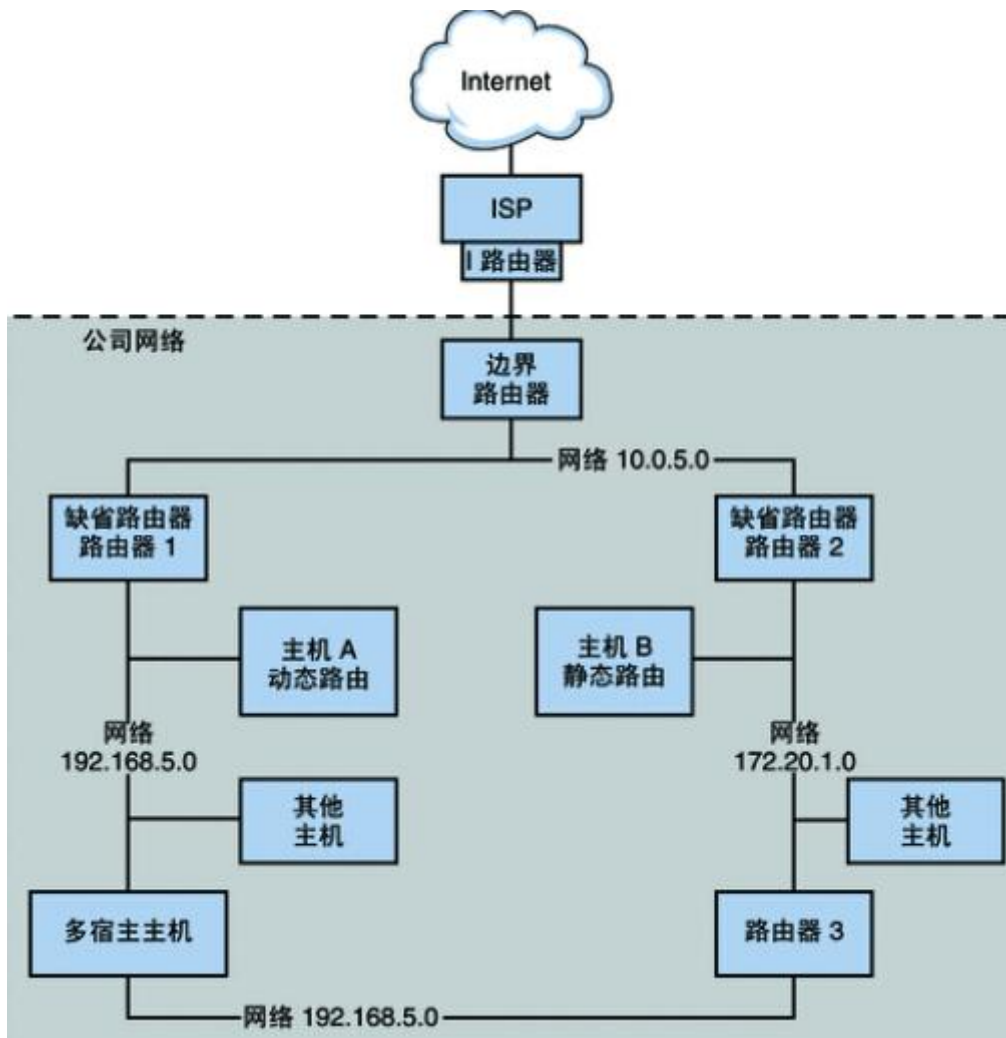
R = IRDP

1 = RIPv1

2 = RIPv2

EIGRP扫描是不同的，在扫描的时，ASS监听数据流，然后直接扫描自己的路由器上的AS。可以通过给出目标来强制让EIGRP扫描到iGRP使用的相同扫描行为，或者通过 -M参数进行强制多播扫描。

三，自治系统



自治系统（Autonomous system）相当与处于一个小型话将下的路由器和网络群组，他可以是一个路由器直接连接到另一个局域网上，然后同时连接到互联网上。

在自治系统中，所有的路由器都必须相互连接，并且运行相同的路由协议，同时分配用一个自治系统号。

四、-V 参数详解

<pre> [Autonomous System Scanner] \$Revision: 1.24 \$ (c) 2k++ FX <fx@phenoelit.de> Phenoelit (http://www.phenoelit.de) IRPAS build XXXIX scanning scanning IRDP ... scanning RIPv1 ... scanning RIPv2 ... scanning IGRP ... </pre>	<pre> 1789 138.874842878 192.168.0.105 118.150.165.78 IGRP 60 Request 1792 140.094844503 192.168.0.105 118.150.165.78 IGRP 60 Request 1794 142.138789226 192.168.0.105 118.150.165.78 IGRP 60 Request 1796 142.850790619 192.168.0.105 118.150.165.78 IGRP 60 Request 1801 149.062829516 192.168.0.105 118.150.165.78 IGRP 60 Request 1804 161.790798639 192.168.0.105 118.150.165.78 IGRP 60 Request 1810 163.830785978 192.168.0.105 118.150.165.78 IGRP 60 Request 1813 165.366826169 192.168.0.105 118.150.165.78 IGRP 60 Request 1817 168.850787940 192.168.0.105 118.150.165.78 IGRP 60 Request 1822 173.046848788 192.168.0.105 118.150.165.78 IGRP 60 Request 1825 182.155110913 192.168.0.105 118.150.165.78 IGRP 60 Request 1828 184.815083008 192.168.0.105 118.150.165.78 IGRP 60 Request </pre>
---	--

IGRP

IGRP路由信息显示目标网络，在括号中显示（延迟、宽带、MTU、可靠性、负载和跳数）

IRDP

IRDP信息被限制到宣布网关（路由器）和他的偏爱之中

RIPv1

RIPv1信息只给出了分类的目标网络（请记住RIPv1网络边界）和他的度量

RIPv2

RIPv2信息包含目标网络之后的以下信息，网络掩码，下一跳，任意标记和度量。如果在协议中启用了身份验证可能会在路由器部分位置出现另一行，对于文本验证，密码都在哪里

EIGRP基本

基本的EIGRP路由部分取决与路由的类型，所有这些字段包括的目标网络、目标掩码和最后一行的延迟、宽带、MTU、可靠性、负载和跳数、外部路由还包括路由、发起的自治系外部度量和该路由的源

EIGRP路由

EIGRP路由部分取决与路由的类型，所有这些字段包括目标网络、目标掩码和最后一行的延迟数、宽带、MTU、可靠性、负载和跳数，外部路由还包括发起路由、发起自治系统、外部度量和该路由的源

HSRP

HSRP信息不是路由，因此第三个字段是备用组的虚拟IP地址，其次是状态、auth字符、Hello、Hold的优先级值

OSPF

OSPF信息包括目标网络及IP格式的区域、使用身份信息验证（如果适用、还有auth字符串），网络掩码、制定路由器和备份路由器、以及Dead、Priority和Hello的值