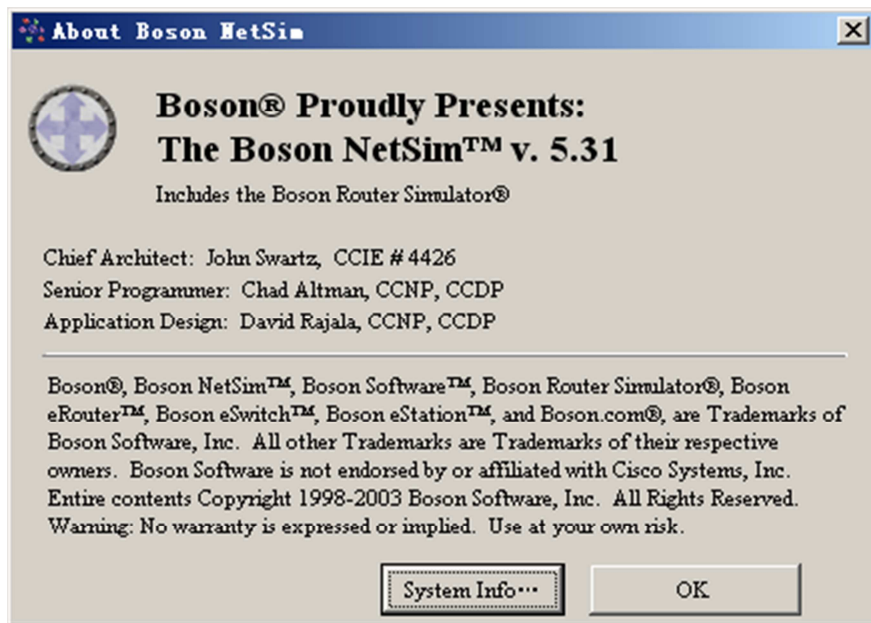


Netsim 使用说明

NetSim 软件介绍

NetSim 是 Boson 公司开发的一个针对 Cisco 认证的路由器配置模拟软件，主要模拟 Cisco 路由器的命令行配置。软件还提供一个拓扑设计功能，使用者可以使用软件提供的缺省拓扑或自己设计的拓扑进行网络配置实验。目前版本是 NetSim6，本实验室安装的是 NetSim5.31。



关于 NetSim 的中文使用资料参见：

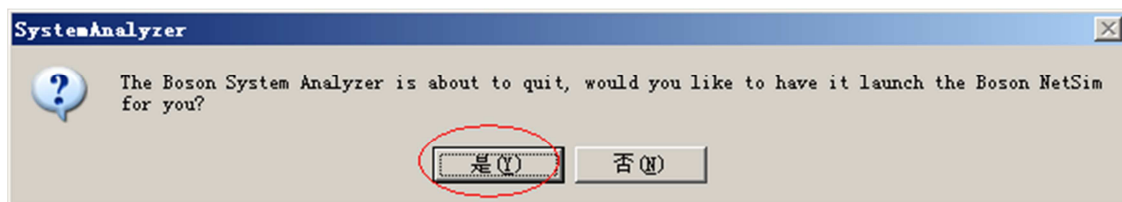
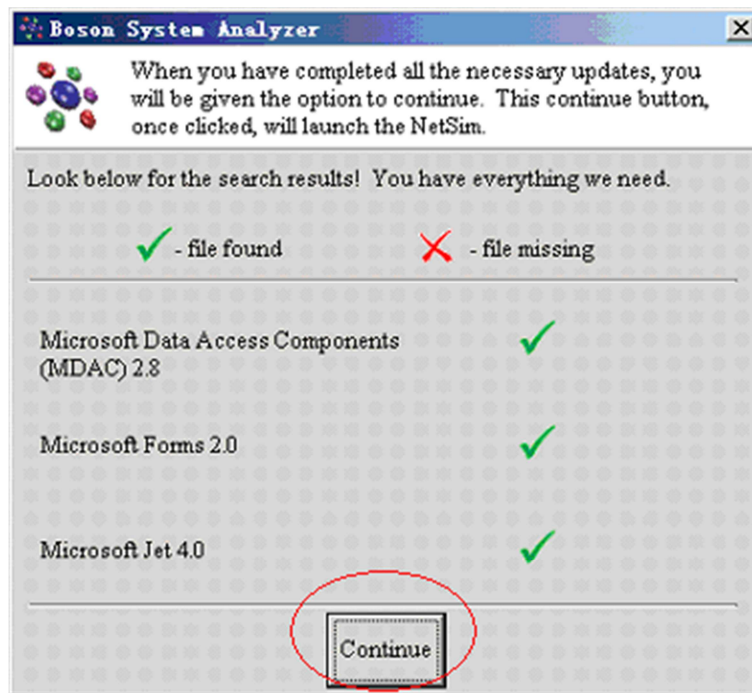
[Boson NetSim 入门进阶.pdf](#)

[Boson NetSim 入门进阶 II .pdf](#)

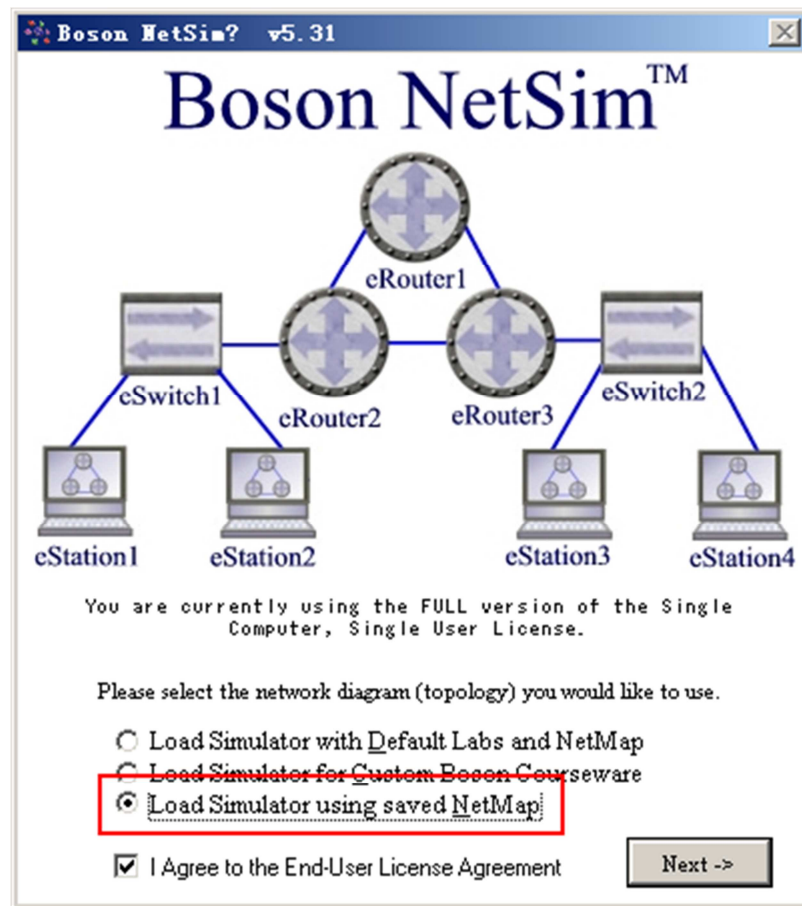
在机房使用 NetSim 说明

在实验室首次使用 Netsim 的时候，Netsim 需要做一些检查：





检查完成以后就可以开始使用 Netsim 了。由于绘制网络拓扑（即 NetSim 中的 NetMap）是比较浪费时间的，实验过程中建议按照所提供的 NetMap 文件(*.top) 加载如下图所示。



Cisco 路由器常用命令：

1. 改变命令状态：

任务	命令
进入特权命令状态	enable
退出特权命令状态	disable
进入全局设置状态	config terminal / 缩写：conf t
退出全局设置状态	end
进入端口设置状态	interface <i>type slot/number</i> 例：int eth 0
激活端口状态	no shut
进入路由设置状态	router <i>protocol</i> 例：动态路由 route rip network 202.38.73.0 network 202.38.77.0

退出局部设置状态	exit
配置静态路由	ip route <i>net net_mask next_hop</i> 例：ip route 202.38.73.0 255.255.255.0 202.38.75.254

2. 显示命令：

任务	命令
查看运行设置	show running-config
显示端口信息	show interface <i>type slot/number</i>
显示路由信息	show ip router

访问控制列表的配置：

访问控制列表简称为 ACL，访问控制列表使用包过滤技术，在路由器上读取第三层及第四层包头中的信息如源地址，目的地址，源端口，目的端口等，根据预先定义好的规则对包进行过滤，从而达到访问控制的目的。该技术初期仅在路由器上支持，近些年来已经扩展到三层交换机，部分最新的二层交换机也开始提供 ACL 的支持了。

依据不同的分类标准，访问控制列表可以进行如下分类：

根据路由器引用 ACL 方式的不同，访问控制列表可以分为：Numbered ACL 和 Named ACL，这两者实质上没有太多区别，只是路由器引用不同的访问控制列表时所使用的方式不同。本实验仅讨论 Numbered ACL。

根据对报文过滤内容的不同，访问控制列表又可以分为：Standard ACL（标准访问控制列表）和 Extended ACL（扩展访问控制列表）。标准访问控制列表仅通过使用 IP 包中的源 IP 地址来进行过滤，在使用 Numbered ACL 的情况下，标准 ACL 使用访问控制列表号 1 到 99 来创建相应的 ACL；而扩展访问控制列表则可以使用源 IP 地址、目的 IP 地址、IP 包协议类型以及协议相关信息（例如 TCP、UDP 的端口号）来进行过滤，在使用 Numbered ACL 的情况下，扩展访问控制列表使用访问控制列表号 100-199 来创建相应的 ACL。

具体地，配置一个 Numbered Standard ACL 的步骤如下：

1. 使用 access-list 命令创建 ACL 中的表项：

access-list 1-99 permit|deny source IP_address [wildcard_mask]

需要注意的是每次使用上述命令给相应的访问控制列表添加一条表项时，该表项总是作为最后一条表项添加到该 ACL 中来。

2. 激活访问控制列表，将步骤 1 中的访问控制列表在某个接口(Interface)上激活：

interface type [module_#]port_#：进入相应的接口配置界面，

ip access-group ACL_# in|out: 在该接口上激活编号为 ACL_# 的访问控制列表;

而配置 Numbered Extended ACL 的过程和上述配置 Numbered Standard ACL 的过程基本一致, 所不同的是步骤 1 的命令中的内容将更加详尽, 如下:

```
access-list 100-199 permit|deny IP_protocol source_address  
source_wildcard_mask\ [protocol_information] destination_address  
destination_wildcard_mask\ [protocol_information] [log]
```

其中:

IP_protocol 为协议域, 可以为: IP、TCP、UDP、ICMP 等;

protocol_information 为协议信息域, 其内容依具体协议有所不同, 具体请查阅参考资料: Cisco_ACL.pdf

最后需要强调的是, 对于一个访问控制列表中有多条表项的情况下, Cisco 设备将遵从如下原则进行处理:

1. ACL 表项将按照从上到下的顺序进行处理;
2. 一旦匹配到某条表项, 则依据该表项做出相应的处理, 并且将不再继续处理后续的表项条目;
3. 如果所有的表项都没有匹配到, 则丢弃此包。

详细内容请查阅参考资料: Cisco_ACL.pdf