实验六 多网段网络组建与静态路由配置

一、实验目的

通过设计有两个路由器的网络及静态路由的配置理解静态路由原理。

**二、实验内容**

1、按照给出的参考拓扑图构建逻辑拓扑图。

2、按照给出的配置参数表配置各个设备。

3、练习静态路由的配置。

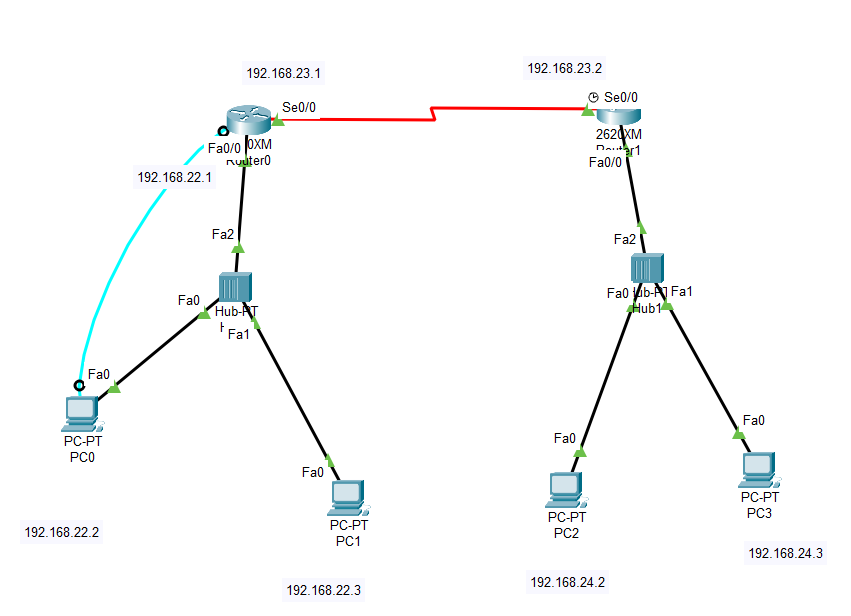
4、完成连通性测试和包传输路径跟踪测试。

**三、实验要求**

1、能够在静态路由上进行配置。

2、在静态路由上进行连通性测试和包传输路径跟踪测试。

**四、拓扑结构**



**五、参数列表**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 路由器信息(子网掩码均为255.255.255.0) | | | | | | |
| 路由器名称 | | 类型 | IP地址 | | 时钟频率 | |
| Router 0 | | 2620XM | Fa0/0: 192.168.22.1  S0/0: 192.168.23.1 | | 56000 | |
| Router 1 | | 2620XM | Fa0/0: 192.168.24.1  S0/0: 192.168.23.2 | |  | |
| PC信息(子网掩码均为 255.255.255.0) | | | | | | |
| 主机名 | | IP 地址 | | 缺省网关 | | 所属网段 |
| PC0 | | 192.168.22.2 | | 192.168.22.1 | | 192.168.22.0 |
| PC1 | | 192.168.22.3 | | 192.168.22.1 | | 192.168.22.0 |
| PC2 | | 192.168.23.2 | | 192.168.23.1 | | 192.168.23.0 |
| PC3 | | 192.168.23.3 | | 192.168.23.1 | | 192.168.23.0 |
| Hub信息 | | | | | | |
| Hub名称 | 类型 | | 所属网段 | | | |
| Hub 0 | Hub-PT | | 192.168.21.0 | | | |
| Hub 1 | Hub-PT | | 192.168.23.0 | | | |

**六、实验步骤**

步骤1：参考附录中PackeTracer的使用方法，按照拓扑图构建逻辑拓扑图。并按照参数配置表配置各个设备。

步骤1.1：Router 0的配置。

步骤1.1.1：配置以太网端口。

步骤1.1.2：配置串行端口。

步骤1.2：PC0和PC1的配置。

步骤1.3：对Router 1进行相同的配置。

步骤2：配置静态路由。

步骤2.1：配置静态路由0。

步骤2.1.1：登陆到路由器Router a 的CLI。

步骤2.1.2：进入全局模式，键入命令：Ra (config) # ip route 192.168.23.0 255.255.255.0 192.168.22.2。

步骤2.1.3：检查配置的路由信息是否在路由表中。用show ip route命令。

步骤2.1.4：在特权配置模式下输入：Ra # copy running-config startup-config.

步骤2.2：对Router1进行相同的配置。

步骤3：连通性和包传输路径的跟踪测试；

步骤3.1：连通性测试。

步骤3.1.1：主机间连通性测试。

步骤3.1.2 按例完成其他主机间连通性测试。

步骤3.1.3 路由器间连通性测试。

步骤3.2 包传输路径跟踪测试。

**七、实验结论及分析**

本次实验进行多网段的组建与静态路由的配置，并进行不同网络主机的连通性的测试，实验表明PC0与PC2可以通信，验证结果与事实一致。同时了解了静态路由配置的过程，向路由中加入网络号，子网掩码，以及下一跳，静态路由便配置成功，掌握了静态路由配置的办法。

实验七 多网段网络组建与动态路由配置

一、实验目的

1、理解RIP动态路由原理。

2、练习动态路由配置。

3、掌握对路由器有关状态获取和分析的方法。

**二、实验内容**

1、按照拓扑构建一个小型局域网。

2、配置PC机的IP地址及网关。

3、配置路由器的各个接口、RIP路由协议。

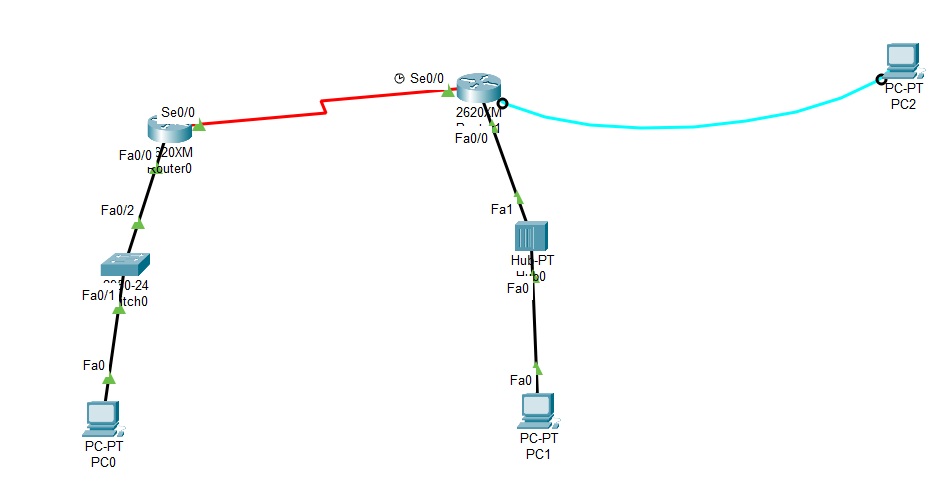
4、完成连通性和包传输路径基本测试。

**三、实验要求**

1、能够在进行动态路由的配置，理解RIP算法。

2、在静态路由上进行连通性测试和包传输路径跟踪测试。

**四、拓扑结构**



**五、参数列表**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 路由器信息（子网掩码均为255.255.255.0） | | | | | |
| 主机名 | 类型 | | IP地址 | RIP路由网络 | 时钟频率 |
| Router1 | 2620XM | | Fa0/0:192.168.22.1  Ser0/0:192.168.23.1 | 192.168.22.0  192.168.23.0 | 56000 |
| Router2 | 2620XM | | Fa0/0:192.168.24.1  Ser0/0:192.168.23.2 | 192.168.23.0  192.168.24.0 |  |
| PC信息（子网掩码均为255.255.255.0） | | | | | |
| 主机名 | | | IP地址 | 默认网关 | |
| PC0 | | | 192.168.22.2 | 192.168.22.1 | |
| PC1 | | | 192.168.24.3 | 192.168.24.1 | |
| 交换机和HUB信息 | | | | | |
| 主机名 | | 类型 | | | |
| Hub 0 | | Hub-PT | | | |
| Switch 0 | | 2950-24 | | | |

**六、实验步骤**

**步骤1** 对路由器进行配置。

步骤1.1 先进入全局配置模式，执行命令“earase startup-config” ,清除缓存的配置文件。使用“reload”命令重启路由器。

步骤1.2 接下来进入接口配置模式对路由器的接口进行配置，包括IP地址，开启接口，对DCE进行时钟设置。

**步骤2** 对各主机按以上拓扑所规定的IP地址子网掩码以及缺省网关进行配置,并检查连通性。

**步骤3** 路由器的全局模式使用“router rip”进入路由器配置，对各路由器使用“network 端口所在的网络地址”进行RIP路由协议配置。

步骤3.1 对Router1进行RIP路由配置。

步骤3.2 对Router2进行RIP路由配置。

步骤3.3 使用“copy running-config startup-config”将配置从running-config保存到startup-config。

**步骤4** 检查路由器的基本配置。

**步骤5** 观察RIP路由的更新。

**七、实验结论及分析**

本次实验进行多网段的组建与动态路由的配置，实验的核心内容是利用router rip以及network命令设置路由的直连的网络，内容较为简单。观察RIP路由更新的过程才能更好的展示rip协议的是如何更新，遵守原来不存在直接添加，存在时若下一跳相同则更新，当下一跳不相同时，距离小时进行更新。

实验八 网络访问控制与基本包过滤配置

一、实验目的

通过本实验理解基于IP源地址的包过滤原理和应用方法。掌握标准访问控制列表的设计、配置和测试。

**二、实验内容**

1、参照拓扑图建立网络拓扑。

2、配置路由器和PC，确保网络拓扑的连通性。

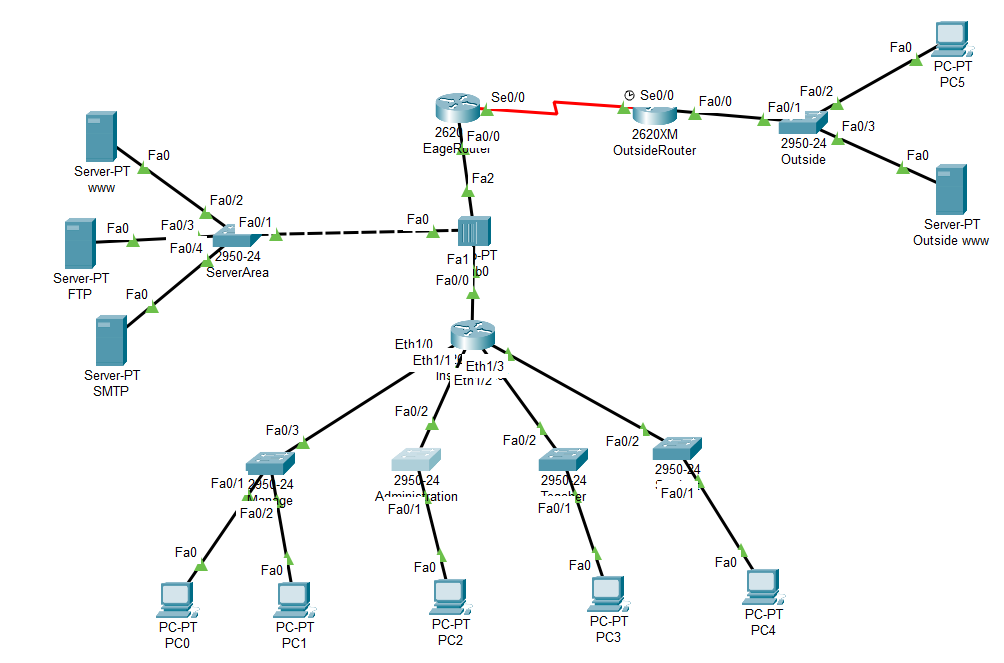
3、配置标准访问控制列表满足应用需求。

**三、实验要求**

1、能够成功配置标准访问控制表。

2、查看各个网段的访问情况，并根据情况进行调整。

**四、拓扑结构**



**五、参数列表**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 路由器配置信息（子网掩码均为255.255.255.0） | | | | | | | | | | |
| 主机名 | 类型 | | | IP 地址 | | | RIP路由网络 | | | 时钟频率 |
| InsideRouter | 2620XM | | | Fa0/0: 192.22.1.2  Eth1/0: 192.22.2.1  Eth1/1: 192.22.3.1  Eth1/2: 192.22.4.1  Eth1/3: 192.22.5.1 | | | 192.22.1.0  192.22.2.0  192.22.3.0  192.22.4.0  192.22.5.0 | | |  |
| EageRouter | 2620XM | | | Fa0/0: 192.22.1.1  Ser0/0: 218.22.59.91 | | | 192.22.1.0  218.22.59.0 | | |  |
| OutsideRouter | 2620XM | | | Fa0/0: 218.22.100.1  Ser0/0: 218.22.59.90 | | | 218.22.59.0  218.22.100.0 | | | 9600 |
| PC和Server配置信息（子网掩码均为255.255.255.0） | | | | | | | | | | |
| 主机名 | | | IP 地址 | | | 默认网关 | | | 所属网段 | |
| PC0 | | | 192.22.2.2 | | | 192.22.2.1 | | | 192.22.2.0 | |
| PC1 | | | 192.22.2.3 | | | 192.22.2.1 | | | 192.22.2.0 | |
| PC2 | | | 192.22.3.2 | | | 192.22.3.1 | | | 192.22.3.0 | |
| PC3 | | | 192.22.4.2 | | | 192.22.4.1 | | | 192.22.4.0 | |
| PC4 | | | 192.22.5.2 | | | 192.22.5.1 | | | 192.22.5.0 | |
| PC5 | | | 218.22.100.2 | | | 218.22.100.1 | | | 218.22.100.0 | |
| WWW | | | 192.22.1.3 | | | 192.22.1.1 | | | 192.22.1.0 | |
| FTP | | | 192.22.1.4 | | | 192.22.1.1 | | | 192.22.1.0 | |
| SMTP | | | 192.22.1.5 | | | 192.22.1.1 | | | 192.22.1.0 | |
| Outside WWW | | | 218.22.100.3 | | | 218.22.100.1 | | | 218.22.100.0 | |
| 交换机和Hub配置信息 | | | | | | | | | | |
| 主机名 | | 类型 | | | 所属网段 | | | 备注 | | |
| Manage | | 2950-24 | | | 192.22.2.0 | | | 所属校园网管理网段 | | |
| Administration | | 2950-24 | | | 192.22.3.0 | | | 所属校园网行政网段 | | |
| Teach | | 2950-24 | | | 192.22.4.0 | | | 所属校园网教学网段 | | |
| Student | | 2950-24 | | | 192.22.5.0 | | | 所属校园网宿舍网段 | | |
| Server Area | | 2950-24 | | | 192.22.1.0 | | | DMZ区 | | |
| Outside | | 2950-24 | | | 218.22.100.0 | | | 所属校外网 | | |
| Hub 0 | | Hub-PT | | | Hub-PT | | |  | | |

**六、实验步骤**

**步骤1** 建立网络拓扑并确保其连通性。

**步骤2** 配置标准访问控制列表满足应用需求

步骤2.1在InsideRouter上创建标准访问控制列表access–list 1，将其应用到InsideRouter的Eth1/1端口上

步骤2.2查看建立的访问控制列表。

步骤2.3实验结果分析

**七、实验结论及分析**

本次实验学习了新的概念标准访问控制列表，标准访问控制列表匹配IP包中的源地址或源地址中的一部分，可对匹配的包采取拒绝或允许两个操作，这是他的特点也是他的局限性，只能对源地址作用，而无法对目的地址判断。同时本次标准访问控制列表的配置比较繁琐，复杂，容易出错。标准访问控制列表对基本包的控制只是低级的过滤，达到安全校园局域网的标准还需进一步的包过滤配置。

实验九 网络访问控制与扩展包过滤配置

一、实验目的

通过本实验理解基于IP地址、协议和端口的包过滤原理和应用方法，掌握扩展访问控制列表的设计、配置和测试。

**二、实验内容**

1、参照拓扑图建立网络拓扑。

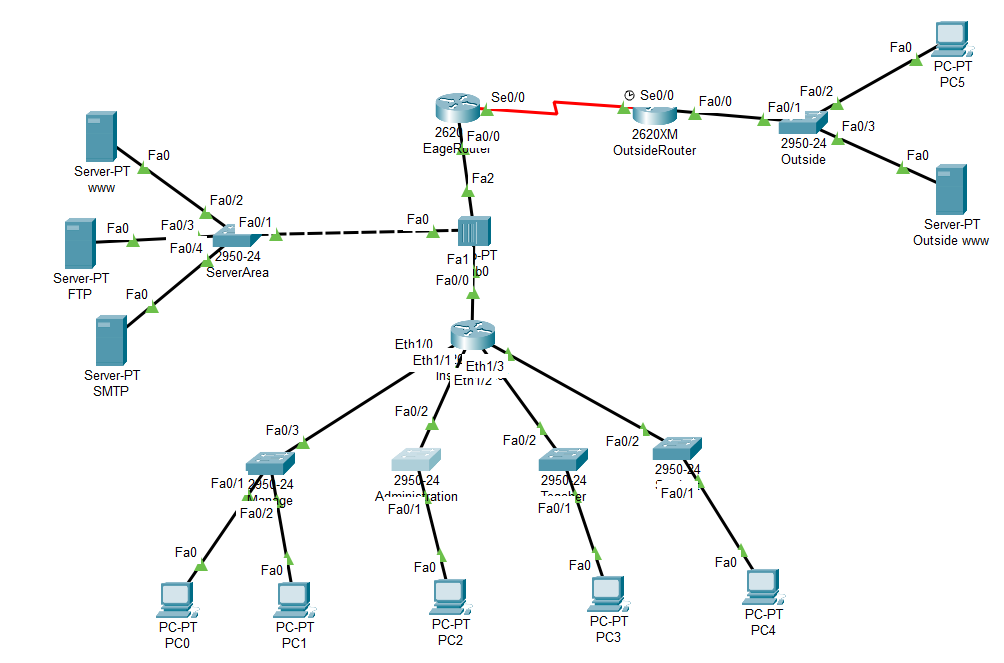
2、在实验八的基础上，配置扩展访问控制列表满足应用需求。

**三、实验要求**

1、能够成功配置标准访问控制表，使其能够对扩展包进行过滤。

2、查看各个网段的访问情况，并根据情况进行调整。

**四、拓扑结构**



**五、参数列表**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 路由器配置信息（子网掩码均为255.255.255.0） | | | | | | | | | | |
| 主机名 | 类型 | | | IP 地址 | | | RIP路由网络 | | | 时钟频率 |
| InsideRouter | 2620XM | | | Fa0/0: 192.22.1.2  Eth1/0: 192.22.2.1  Eth1/1: 192.22.3.1  Eth1/2: 192.22.4.1  Eth1/3: 192.22.5.1 | | | 192.22.1.0  192.22.2.0  192.22.3.0  192.22.4.0  192.22.5.0 | | |  |
| EageRouter | 2620XM | | | Fa0/0: 192.22.1.1  Ser0/0: 218.22.59.91 | | | 192.22.1.0  218.22.59.0 | | |  |
| OutsideRouter | 2620XM | | | Fa0/0: 218.22.100.1  Ser0/0: 218.22.59.90 | | | 218.22.59.0  218.22.100.0 | | | 9600 |
| PC和Server配置信息（子网掩码均为255.255.255.0） | | | | | | | | | | |
| 主机名 | | | IP 地址 | | | 默认网关 | | | 所属网段 | |
| PC0 | | | 192.22.2.2 | | | 192.22.2.1 | | | 192.22.2.0 | |
| PC1 | | | 192.22.2.3 | | | 192.22.2.1 | | | 192.22.2.0 | |
| PC2 | | | 192.22.3.2 | | | 192.22.3.1 | | | 192.22.3.0 | |
| PC3 | | | 192.22.4.2 | | | 192.22.4.1 | | | 192.22.4.0 | |
| PC4 | | | 192.22.5.2 | | | 192.22.5.1 | | | 192.22.5.0 | |
| PC5 | | | 218.22.100.2 | | | 218.22.100.1 | | | 218.22.100.0 | |
| WWW | | | 192.22.1.3 | | | 192.22.1.1 | | | 192.22.1.0 | |
| FTP | | | 192.22.1.4 | | | 192.22.1.1 | | | 192.22.1.0 | |
| SMTP | | | 192.22.1.5 | | | 192.22.1.1 | | | 192.22.1.0 | |
| Outside WWW | | | 218.22.100.3 | | | 218.22.100.1 | | | 218.22.100.0 | |
| 交换机和Hub配置信息 | | | | | | | | | | |
| 主机名 | | 类型 | | | 所属网段 | | | 备注 | | |
| Manage | | 2950-24 | | | 192.22.2.0 | | | 所属校园网管理网段 | | |
| Administration | | 2950-24 | | | 192.22.3.0 | | | 所属校园网行政网段 | | |
| Teach | | 2950-24 | | | 192.22.4.0 | | | 所属校园网教学网段 | | |
| Student | | 2950-24 | | | 192.22.5.0 | | | 所属校园网宿舍网段 | | |
| Server Area | | 2950-24 | | | 192.22.1.0 | | | DMZ区 | | |
| Outside | | 2950-24 | | | 218.22.100.0 | | | 所属校外网 | | |
| Hub 0 | | Hub-PT | | | Hub-PT | | |  | | |

**六、实验步骤**

**步骤1**

步骤1.1 首先我们配置扩展访问控制列表满足禁止宿舍网段访问FTP服务器上的ftp资源的应用需求。

步骤1.2 查看建立的访问控制列表。

步骤1.3 实验结果分析

0号PDU Failed状态说明宿舍网段无法访问FTP服务器。

1号PDU Successful状态说明宿舍网段可以访问WWW服务器。

2号PDU Successful状态说明宿舍网段可以访问FTP服务器。

**步骤2**

步骤2.1 创建扩展访问控制列表access–list 101，将其应用到EageRouter 的Fa0/0端口上，以满足其他的应用需求。

步骤2.2查看建立的访问控制列表。

步骤2.3 实验结果分析

0号PDU 的Failed状态说明外网不能访问内网的FTP服务器。

1号PDU 的Successful状态说明外网能访问内网的WWW服务器。

2号PDU 的Successful状态说明外网能访问内网的SMTP服务器。

**七、实验结论及分析**

本次实验学习了扩展ACL，通过配置，实现教学网段和宿舍网段不能访问行政网段，管理网段中只允许PC1访问行政网段，行政网段可以访问DMZ中的WWW、FTP、SMTP服务器。可以看出扩展ACL具有更加强大的功能，可以使用扩展ACL来做到针对协议及其参数的更精细的包过滤,如TCP,UDP,ICMP和IP。在扩展ACL中,要指定上层TCP或UDP端口号,从而选择允许或拒绝的协议。

实验十 内外网结构下的网络地址转换（NAT/PAT）

一、实验目的

通过本实验理解网络地址转换的原理和技术，掌握扩展NAT/PAT设计、配置和测试。

**二、实验内容**

1、配置静态网络地址转换并完成相应的测试。

2、配置动态网络地址转换并完成相应的测试。

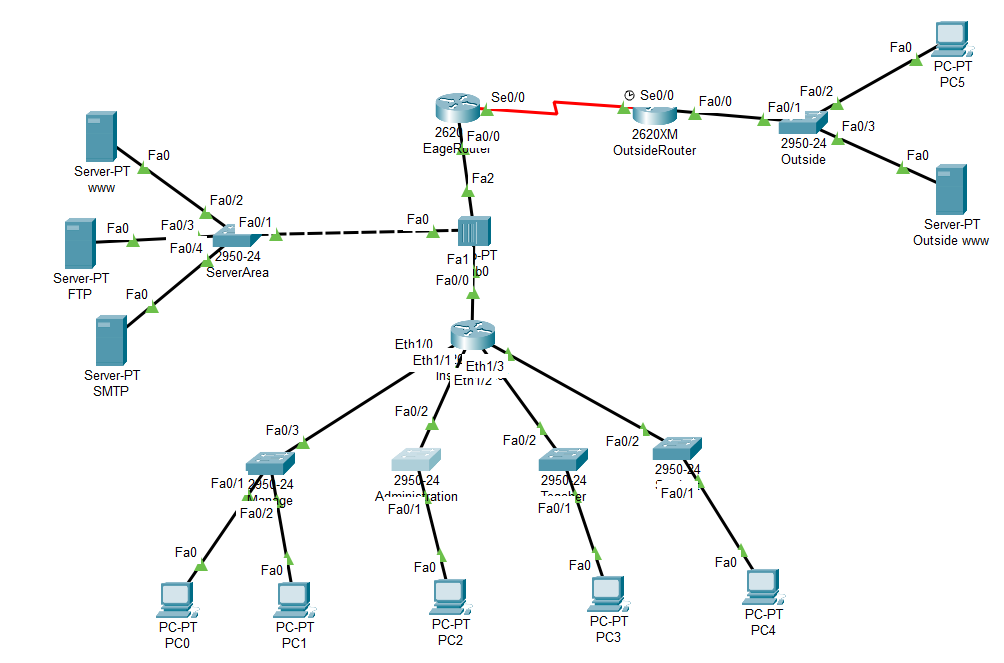
3、配置端口地址转换（PAT）并完成相应的测试。

**三、实验要求**

1、在前两次实验的基础上，利用NAT和PAT技术实现私有地址和公有地址的相互转换，进一步增强校园网的安全性。

2、查看各个网段的访问情况，并根据情况进行调整。

**四、拓扑结构**



**五、参数列表**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 路由器配置信息（子网掩码均为255.255.255.0） | | | | | | | | | | |
| 主机名 | 类型 | | | IP 地址 | | | RIP路由网络 | | | 时钟频率 |
| InsideRouter | 2620XM | | | Fa0/0: 192.22.1.2  Eth1/0: 192.22.2.1  Eth1/1: 192.22.3.1  Eth1/2: 192.22.4.1  Eth1/3: 192.22.5.1 | | | 192.22.1.0  192.22.2.0  192.22.3.0  192.22.4.0  192.22.5.0 | | |  |
| EageRouter | 2620XM | | | Fa0/0: 192.22.1.1  Ser0/0: 218.22.59.91 | | | 192.22.1.0  218.22.59.0 | | |  |
| OutsideRouter | 2620XM | | | Fa0/0: 218.22.100.1  Ser0/0: 218.22.59.90 | | | 218.22.59.0  218.22.100.0 | | | 9600 |
| PC和Server配置信息（子网掩码均为255.255.255.0） | | | | | | | | | | |
| 主机名 | | | IP 地址 | | | 默认网关 | | | 所属网段 | |
| PC0 | | | 192.22.2.2 | | | 192.22.2.1 | | | 192.22.2.0 | |
| PC1 | | | 192.22.2.3 | | | 192.22.2.1 | | | 192.22.2.0 | |
| PC2 | | | 192.22.3.2 | | | 192.22.3.1 | | | 192.22.3.0 | |
| PC3 | | | 192.22.4.2 | | | 192.22.4.1 | | | 192.22.4.0 | |
| PC4 | | | 192.22.5.2 | | | 192.22.5.1 | | | 192.22.5.0 | |
| PC5 | | | 218.22.100.2 | | | 218.22.100.1 | | | 218.22.100.0 | |
| WWW | | | 192.22.1.3 | | | 192.22.1.1 | | | 192.22.1.0 | |
| FTP | | | 192.22.1.4 | | | 192.22.1.1 | | | 192.22.1.0 | |
| SMTP | | | 192.22.1.5 | | | 192.22.1.1 | | | 192.22.1.0 | |
| Outside WWW | | | 218.22.100.3 | | | 218.22.100.1 | | | 218.22.100.0 | |
| 交换机和Hub配置信息 | | | | | | | | | | |
| 主机名 | | 类型 | | | 所属网段 | | | 备注 | | |
| Manage | | 2950-24 | | | 192.22.2.0 | | | 所属校园网管理网段 | | |
| Administration | | 2950-24 | | | 192.22.3.0 | | | 所属校园网行政网段 | | |
| Teach | | 2950-24 | | | 192.22.4.0 | | | 所属校园网教学网段 | | |
| Student | | 2950-24 | | | 192.22.5.0 | | | 所属校园网宿舍网段 | | |
| Server Area | | 2950-24 | | | 192.22.1.0 | | | DMZ区 | | |
| Outside | | 2950-24 | | | 218.22.100.0 | | | 所属校外网 | | |
| Hub 0 | | Hub-PT | | | Hub-PT | | |  | | |

**六、实验步骤**

**步骤1**

步骤1.1 我们首先将192.168.1.3 静态转换到218.58.59.93

步骤1.2 查看配置并进行实验结果分析。

**步骤2**

步骤2.1首先将192.168.1.5 静态转换到218.58.59.94。

步骤2.2 查看配置并进行实验结果分析。

**步骤3**

步骤3.1 将管理网段（192.168.2.0）、行政网段（192.168.3.0）的内部私有IP动态转换到218.58.59.95和218.58.59.96。

步骤3.2 测试配置并进行实验结果分析。

**步骤4**

步骤4.1 我们将教学网段（192.168.4.0）、宿舍网段（192.168.5.0）的内部私有IP 通过端口地址转换转换到218.58.59.97。

步骤3.2 测试配置并进行实验结果分析。

**七、实验结论及分析**

本次实验学习了NAT和PAT，利用这两种新技术实现了私有地址和公有地址的相互转换，NAT不仅能解决IP地址不足的问题，而且还能够有效地避免来自网络外部的攻击，隐藏并保护网络内部的计算机，对于校园网的安全保护达到了一个可接受的程度。端路多口复用PAT是目前网络中应用最多技术，使内部网络共用一个ip，能够最大限度地节约IP地址资源。同时又可隐藏网络内部的所有主机保护网络。