**Relatório Técnico – Lab Segmentação de Rede**

**Autor:** Antonio Agostinho Gomes Bezerra

**Data:** 24 de julho de 2025

**Versão:** 1.0

**Introdução**

Este relatório analisa a configuração de rede de um sistema Linux que atua como um ponto central de interconexão para três redes distintas: Infraestrutura (10.10.30.0/24), Corporativa (10.10.10.0/24) e Convidados (10.10.50.0/24). A análise do comando ip a e da tabela ARP revela que o sistema possui interfaces dedicadas para cada sub-rede, indicando sua função como roteador/gateway. Os principais achados incluem a identificação de diversos servidores críticos na rede de infraestrutura (FTP, LDAP, MySQL, Zabbix, Samba), estações de trabalho na rede corporativa e dispositivos de usuários na rede de convidados. Recomenda-se manter essa arquitetura segmentada para garantir a segurança, o isolamento de tráfego e a aplicação de políticas de acesso diferenciadas, protegendo os ativos mais sensíveis da organização.

**Objetivo**

Analisar a rede simulada para identificar exposição, segmentação e riscos operacionais.

**Escopo**

Ambiente docker simulado com múltiplos hosts e redes segmentadas.

**Metodologia**

- Ferramentas: nmap, rustscan, netdiscover, ping, etc.

- Coleta ativa de dados de rede

- Análise manual e documentada

1. **Redes Identificadas**

|  |  |  |
| --- | --- | --- |
| **Nome Estimado** | **Sub-rede (DNS Domain)** | **Finalidade Suposta** |
| eth0 | 10.10.30.0/24 (infra\_net) | Rede de Infraestrutura (Servidores) |
| eth1 | 10.10.10.0/24 (corp\_net) | Rede Corporativa (Workstations) |
| eth2 | 10.10.50.0/24 (guest\_net) | Rede de Convidados (dispositivos pessoais) |

1. **Dispositivos por Rede**

Esta interface está conectada à rede de infraestrutura ( projeto\_final\_opcao\_1\_infra\_net ). O sistema com IP 10.10.30.2 (o sistema analisado) conhece os seguintes dispositivos nesta rede:

|  |  |  |  |
| --- | --- | --- | --- |
| **eth0 (Infraestrutura - 10.10.30.0/24)** | | | |
| **IP** | **Nome do Host** | **MAC Address** | **Observações** |
| 10.10.30.10 | ftp-serve | 62:81:5f:1a:ce:ed | Servidor FTP |
| 10.10.30.11 | Mysql-serve | C2:d9:cd:27:a6:61 | Servidor MySQL |
| 10.10.30.15 | Samba-server | 9e:f5:8b:5f:64:e6 | Servidor Samba (compartilhamento de arquivos) |
| 10.10.30.17 | Openldap | 3a:48:b2:0f:e1:0f | Servidor LDAP (autenticação centralizada) |
| 10.10.30.117 | Zabbix-server | ae:09:dc:f9:e5:57 | Servidor de monitoramento (Zabbix) |
| 10.10.30.227 | Legacy-server | ee:5b:93:4e:56:7a | Servidor legado (possivelmente antigo) |
| 10.10.30.1 | (Gateway) | 5a:28:3f:ca:1f:6c | Roteador/switch da rede de infraestrutura |

Esta interface está conectada à rede corporativa ( projeto\_final\_opcao\_1\_corp\_net ). O sistema com IP 10.10.10.2 (o sistema analisado) conhece os seguintes dispositivos nesta rede:

|  |  |  |  |
| --- | --- | --- | --- |
| **eth1 (Corporativa - 10.10.10.0/24)** | | | |
| IP | Nome do host | MAC Address | Observações |
| 10.10.10.10 | WS\_001 | 42:c7:9f:c6:69:b2 | Workstation 1 |
| 10.10.10.101 | WS\_002 | 56:fe:df:0d:46:ba | Workstation 2 |
| 10.10.10.127 | WS\_003 | 4a:55:33:09:07:06 | Workstation 3 |
| 10.10.10.222 | WS\_004 | 92:7a:01:85:69:43 | Workstation 4 |
| 10.10.10.1 | (Gateway) | ea:21:9d:77:31:f1 | Roteador/switch da rede corporativa |

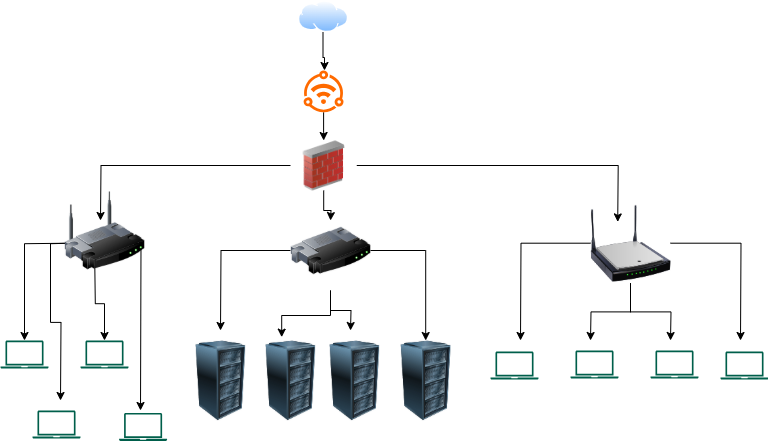
Esta interface está conectada à rede de convidados ( projeto\_final\_opcao\_1\_guest\_net ). O sistema com IP 10.10.50.6 (o sistema analisado) conhece os seguintes dispositivos nesta rede:

|  |  |  |  |
| --- | --- | --- | --- |
| **eth2 (Convidados - 10.10.50.0/24)** | | | |
| IP | Nome do host | MAC Addess | Observações |
| 10.10.50.1 | (Gateway) | fe:d3:9f:dc:ab:23 | Roteador da rede de convidados |
| 10.10.50.2 | Notebook-carlos | 42:e7:53:52:38:8e | Dispositivo pessoal (Carlos) |
| 10.10.50.3 | Laptop-luiz | 56:14:38:38:ed:69 | Dispositivo pessoal (Luiz) |
| 10.10.50.4 | Laptop-vastro | 76:84:2b:8b:05:40 | Dispositivo pessoal (Vastro) |
| 10.10.50.5 | Macbook-aline | 32:e9:2a:59:66:62 | Dispositivo pessoal (Aline, Apple) |

1. **Conclusão**

Com base na análise das configurações de rede e da tabela ARP, conclui-se que o sistema em questão desempenha um papel crucial como roteador/gateway ou servidor multifunção em um ambiente de rede segmentado. Ele possui conectividade direta com três redes distintas: Rede de Infraestrutura (10.10.30.0/24): Contém servidores críticos como FTP, LDAP, Samba, MySQL e Zabbix. Rede Corporativa (10.10.10.0/24): Abriga as estações de trabalho dos usuários corporativos. Rede de Convidados (10.10.50.0/24): Destinada a dispositivos de usuários visitantes ou temporários. Essa arquitetura de rede, com segmentação clara e um ponto central de interconexão, é uma prática recomendada para segurança e organização. Ela permite isolar o tráfego, aplicar políticas de segurança diferenciadas para cada segmento e proteger os ativos mais sensíveis da infraestrutura de acessos não autorizados ou maliciosos de outras redes. Os endereços x.x.x.1 em cada sub-rede são consistentemente identificados como prováveis gateways, reforçando a função de roteamento do sistema analisado.

1. **Diagrama de rede**

****