Packet Tracer – Desafio de Integração de Habilidades (Versão do Instrutor)

**Nota do Instrutor**: Cor vermelha da fonte ou realces em cinza indicam o texto que aparece apenas na cópia do instrutor.

# Tabela de Endereçamento

| Dispositivo | Interface | Endereço IP / Prefixo | Gateway padrão |
| --- | --- | --- | --- |
| R1 | G0/0 | 192.168.0.1 /25 | N/D |
| R1 | G0/0 | 2001:db8:acad::1/64 | N/D |
| R1 | G0/0 | fe80::1 | N/D |
| R1 | G0/1 | 192.168.0.129 /26 | N/D |
| R1 | G0/1 | 2001:db8:acad:1::1/64 | N/D |
| R1 | G0/1 | fe80::1 | N/D |
| R1 | G0/2 | 192.168.0.193 /27 | N/D |
| R1 | G0/2 | 2001:db8:acad:2: :1/64 | N/D |
| R1 | G0/2 | fe80::1 | N/D |
| R1 | S0/0/1 | 172.16.1.2 /30 | N/D |
| R1 | S0/0/1 | 2001:db 8:2: :1/64 | N/D |
| R1 | S0/0/1 | fe80::1 | N/D |
| Central | S0/0/0 | 209.165.200.226 /30 | N/D |
| Central | S0/0/0 | 2001:db 8:1: :1/64 | N/D |
| Central | S0/0/0 | fe80::2 | N/D |
| Central | S0/0/1 | 172.16.1.1 /30 | N/D |
| Central | S0/0/1 | 2001:db 8:2: :2/64 | N/D |
| Central | S0/0/1 | fe80::2 | N/D |
| S1 | VLAN 1 | 192.168.0.2 | 192.168.0.1 |
| S2 | VLAN 1 | 192.168.0.130 /26 | 192.168.0.129 |
| S3 | VLAN 1 | 192.168.0.194 /27 | 192.168.0.193 |
| Staff | NIC | 192.168.0.3 /25 | 192.168.0.1 |
| Staff | NIC | 2001:db8:acad: :2/64 | fe80::1 |
| Staff | NIC | fe80::2 | fe80::1 |
| Vendas | NIC | 192.168.0.131 /26 | 192.168.0.129 |
| Vendas | NIC | 2001:db8:acad:1::2/64 | fe80::1 |
| Vendas | NIC | fe80::2 | fe80::1 |
| TI | NIC | 192.168.0.195 /27 | 192.168.0.193 |
| TI | NIC | 2001:db8:acad:2: :2/64 | fe80::1 |
| TI | NIC | fe80::2 | fe80::1 |
| Web | NIC | 64.100.0.3 /29 | 64.100.0.1 |
| Web | NIC | 2001:db8:café: :3/64 | fe80::1 |
| Web | NIC | fe80::2 | Fe80::1 |

# Histórico/Cenário

Os roteadores Central, do cluster do ISP e o servidor Web estão completamente configurados. Você deve criar um novo esquema de endereçamento IPv4 que acomode 4 sub-redes usando a rede 192.168.0.0/24. O maior departamento de TI precisa de 25 hosts. O maior departamento de vendas (Sales) precisa de 50 hosts. A sub-rede para o restante da equipe (staff) precisa de 100 hosts. Uma sub-rede para convidados (guest) será futuramente adicionada para acomodar 25 hosts. Você também deve concluir as configurações básicas de segurança e as configurações de interface no R1. Em seguida, você definirá a interface SVI e as configurações básicas de segurança nos comutadores S1, S2 e S3.

# Instruções

Endereçamento IPv4

* Use 192.168.0.0/24 para criar sub-redes que atendem aos requisitos do host.
* Equipe (Staff): 100 hosts
* Departamento de Vendas (Sales): 50 hosts
* TI: 25 hosts
* Sub-rede de convidados (Guest) futuramente adicionada: 25 hosts
* Documente os endereços IPv4 que foram atribuídos na Tabela de Endereçamento.
* Registre a sub-rede da rede Convidado:

Digite suas respostas aqui.

192.168.0.224/27

Configurações dos computadores

* Defina as configurações de endereço IPv4, máscara de sub-rede e gateway padrão atribuídos nos funcionários, vendas e computadores de TI, usando seu esquema de endereçamento.
* Atribua o unicast IPv6 e vincule os endereços locais e os gateways padrão às equipes, vendas e redes de TI, de acordo com a Tabela de endereçamento.

Configurações de R1

* Configure o nome do dispositivo conforme a Tabela de Endereçamento.
* Desative a pesquisa do DNS.
* Atribua **Ciscoenpa55** como a senha criptografada do modo EXEC privilegiado.
* Atribua **Ciscoconpa55** como a senha de console e habilite o login.
* Exija que um mínimo de **10** caracteres seja usado para todas as senhas.
* Criptografe todas as senhas em texto simples.
* Crie um banner para avisar às pessoas que o acesso não autorizado é proibido.
* Configure e ative todas as interfaces Gigabit Ethernet.
* Configure endereços IPv4 de acordo com seu esquema de endereçamento.
* Configure endereços IPv6 de acordo com a Tabela de Endereçamento.
* Configure o SSH em R1:
* Defina o nome de domínio como **CCNA-lab.com**
* Gere uma chave RSA de **1024** bits.
* Configure as linhas VTY para acesso SSH.
* Use perfis de usuário local para autenticação.
* Crie um usuário **Admin1** com um privilégio de nível **15** usando a senha criptografada para **Admin1pa55**.
* Configure o console e as linhas VTY para encerrar sessão após cinco minutos de inatividade.
* Bloqueie durante três minutos qualquer pessoa que não conseguiu fazer log in depois de quatro tentativas em um período de dois minutos.

Configuração de switches

* Configure o nome do dispositivo conforme a Tabela de Endereçamento.
* Configure a interface SVI com endereço e máscara de sub-rede IPv4 de acordo com o seu esquema de endereçamento.
* Configure o gateway padrão.
* Desative a pesquisa do DNS.
* Atribua **Ciscoenpa55** como a senha criptografada do modo EXEC privilegiado.
* Atribua **Ciscoconpa55** como a senha de console e habilite o login.
* Configure o console e as linhas VTY para encerrar a sessão após cinco minutos de inatividade.
* Criptografe todas as senhas em texto simples.

Requisitos de conectividade

* Usando navegadores Web nos computadores Staff, Sales e TI, navegue para **www.cisco.pka**.
* Usando navegadores Web nos computadores Staff, Sales e TI, navegue para **www.cisco6.pka**.
* Todos os PCs devem poder executar ping em todos os outros dispositivos.

Fim do documento

# Scripts de Execução

Configuração do R1

enable

config t

service password-encryption

security passwords min-length 10

hostname R1

login block-for 30 attempts 2 within 120

enable secret 5 $1$mERr$Amm/da5NtiazLuZDbgqZ60

ipv6 unicast-routing

username Admin1 secret 5 $1$mERr$Ty/EkWXcSXEwIckISrps8/

no ip domain-lookup

ip domain-name CCNA-lab.com

interface GigabitEthernet0/0

ip address 192.168.0.1 255.255.255.128

duplex auto

speed auto

ipv6 address FE80::1 link-local

ipv6 address 2001:DB8:ACAD::1/64

no shutdown

interface GigabitEthernet0/1

ip address 192.168.10.129 255.255.255.192

duplex auto

speed auto

ipv6 address FE80::1 link-local

ipv6 address 2001:DB8:ACAD:1::1/64

no shutdown

interface GigabitEthernet0/2

ip address 192.168.33.193 255.255.255.224

duplex auto

speed auto

ipv6 address FE80::1 link-local

ipv6 address 2001:DB8:ACAD:2::1/64

no shutdown

interface Serial0/0/1

ip address 172.16.1.2 255.255.255.252

ipv6 address FE80::1 link-local

ipv6 address 2001:DB8:2::1/64

no shutdown

banner motd ^CAny text^C

line con 0

exec-timeout 5 0

password 7 0802455D0A1606181C1B0D517F

Login

line vty 0 4

exec-timeout 5 0

login local

transport input ssh

exit

crypto key generate rsa general-keys modulus 1024

finalizar

Configuração do S1

enable

conf t

service password-encryption

hostname S1

enable secret 5 $1$mERr$Amm/da5NtiazLuZDbgqZ60

no ip domain-lookup

interface Vlan1

ip address 192.168.10.2 255.255.255.128

no shutdown

ip default-gateway 192.168.0.1

line con 0

password 7 0802455D0A1606181C1B0D517F

Login

exec-timeout 5 0

line vty 0 4

exec-timeout 5 0

Login

line vty 5 15

exec-timeout 5 0

Login

end

Configuração do S2

enable

conf t

service password-encryption

hostname S2

enable secret 5 $1$mERr$Amm/da5NtiazLuZDbgqZ60

no ip domain-lookup

interface Vlan1

ip address 192.168.0.130 255.255.255.192

no shutdown

ip default-gateway 192.168.0.129

line con 0

password 7 0802455D0A1606181C1B0D517F

Login

exec-timeout 5 0

line vty 0 4

exec-timeout 5 0

Login

line vty 5 15

exec-timeout 5 0

Login

end

Configuração do S3

enable

conf t

service password-encryption

hostname S3

ativar segredo 5 $1$merr$amm/da5ntiazluzdbgqz60

no ip domain-lookup

interface Vlan1

ip address 192.168.33.193 255.255.255.224

no shut

ip default-gateway 192.168.0.193

line con 0

password 7 0802455D0A1606181C1B0D517F

Login

exec-timeout 5 0

line vty 0 4

exec-timeout 5 0

Login

line vty 5 15

exec-timeout 5 0

Login

end