UNIVERSIDADE da MADEIRA

CTeSP

CURSOS TÉCNICOS SUPERIORES PROFISSIONAIS

TRABALHO

Projeto

Fabrício Rodrigues

Nº 2015418

Tecnologias e Programação de Sistemas de Informação

UNIDADE CURRICULAR:

Segurança Informática

DOCENTE:

Filipe André Freitas

DATA:

12 de janeiro de 2020

ESCOLA SUPERIOR DE TECNOLOGIAS E GESTÃO

Cofinanciado por:

MADEIRA 14-20

REGIÃO AUTÓNOMA DA MADEIRA

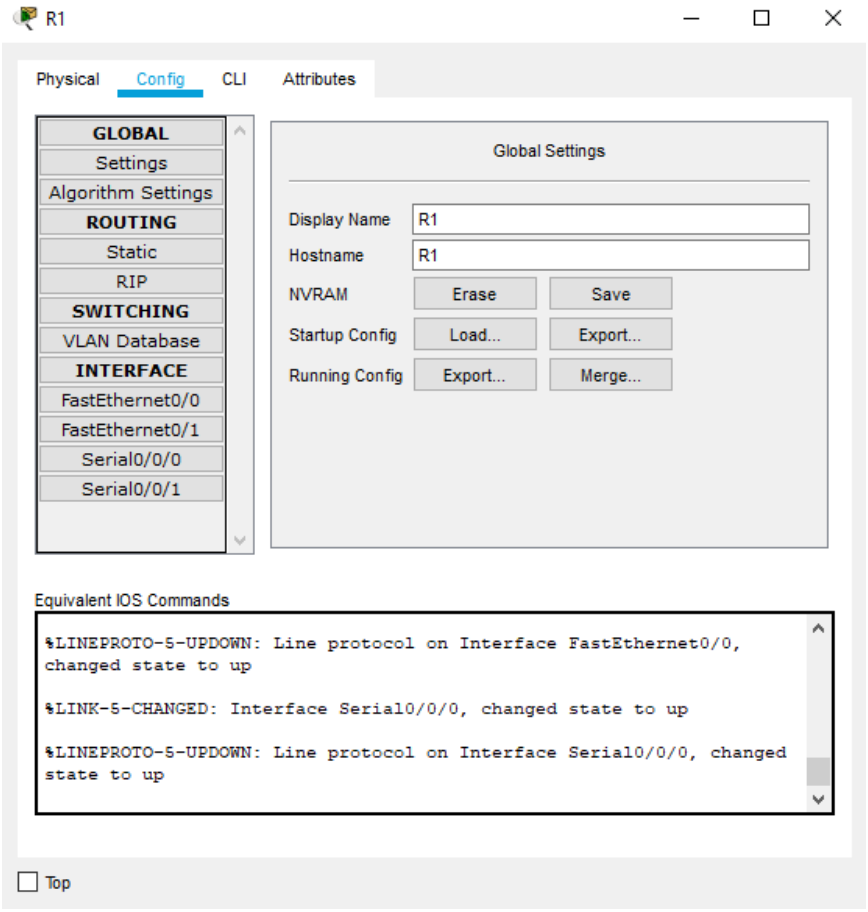
PORTUGAL 2020

UNIÃO EUROPEIA

Fundo Social Europeu

Etapa 1: Atribua o nome aos equipamentos

A atribuição do nome aos equipamentos é feita no próprio dispositivo a partir da tab config, alterando o Display Name e Hostname para o que desejamos.



Etapa 2: Configure um banner

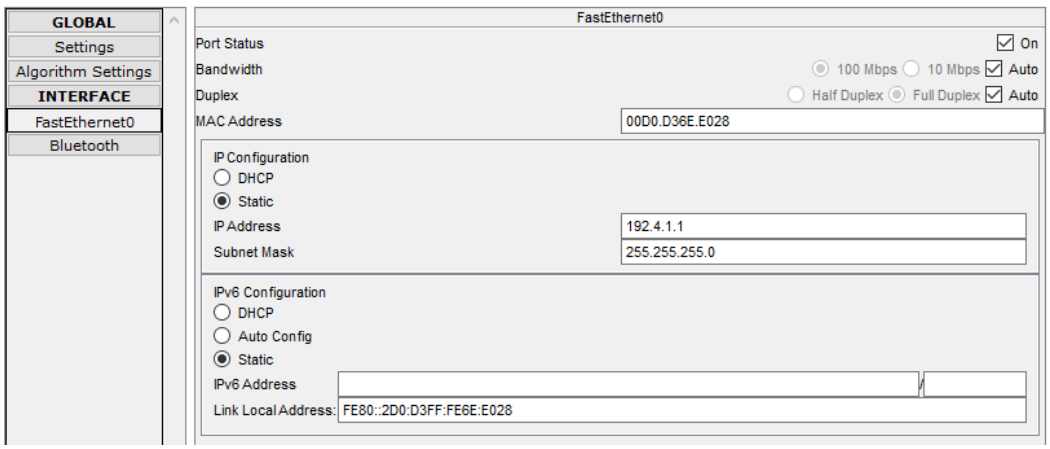
Para configurar um banner apenas temos de utilizar o seguinte comando:

R1(config)# banner motd #*Bem-Vindo*#

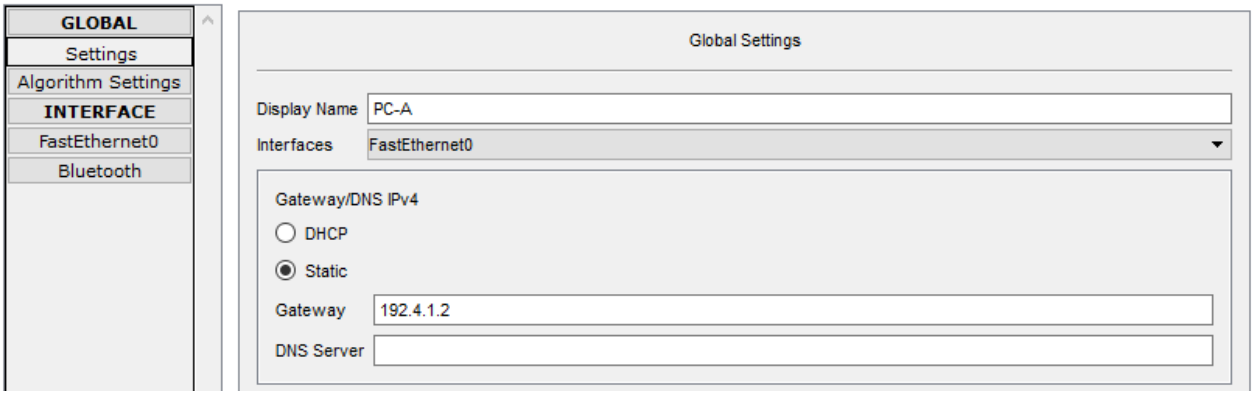
Etapa 3: Configure os IPs nos equipamentos

PC's

Nos PC's temos de ir à interface Fa0/0 e definir o seu IP, neste caso o seu IP acaba em 1. (repetindo este passo para os restantes PC's alterando apenas os IP'S e máscaras).

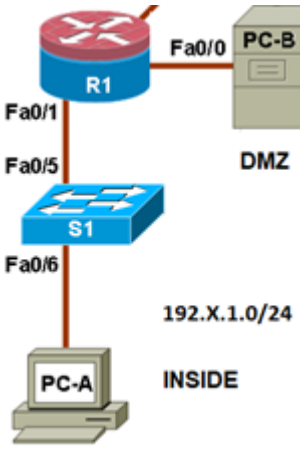


De seguida, ainda nos Pc's, é definido o gateway que é o que vai permitir a sua ligação ao router que se situa na sua mesma rede. (o IP do gateway varia consoante a sua rede)

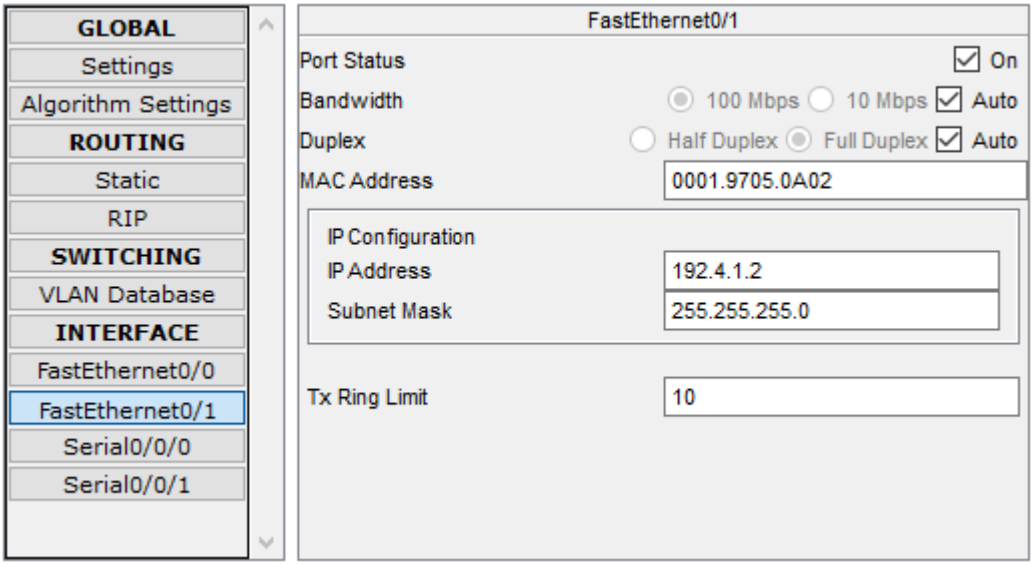


Routers

Nos routers, a interface onde é definido os IP'S depende da estrutura da rede, por exemplo:



A interface do router R1 onde vamos definir o IP 192.4.1.2 é a interface Fa0/1 pois é a partir dela que o PC-A vai comunicar.



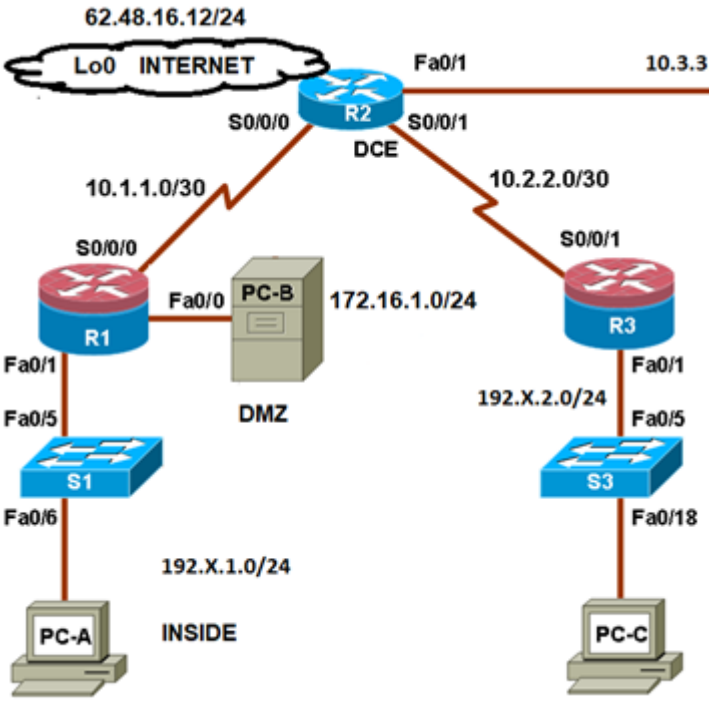
No router R2 foi criado também um Loopback0 com os seguintes comandos:

R2(config)#interface loopback0

R2(config-if)#ip address 62.48.16.12 255.255.255.0

Etapa 4: Configure as rotas estaticas para colocar todos os equipamentos a comunicar

A configuração das rotas estáticas permite a comunicação entre componentes que não estejam na mesma lan, por exemplo:



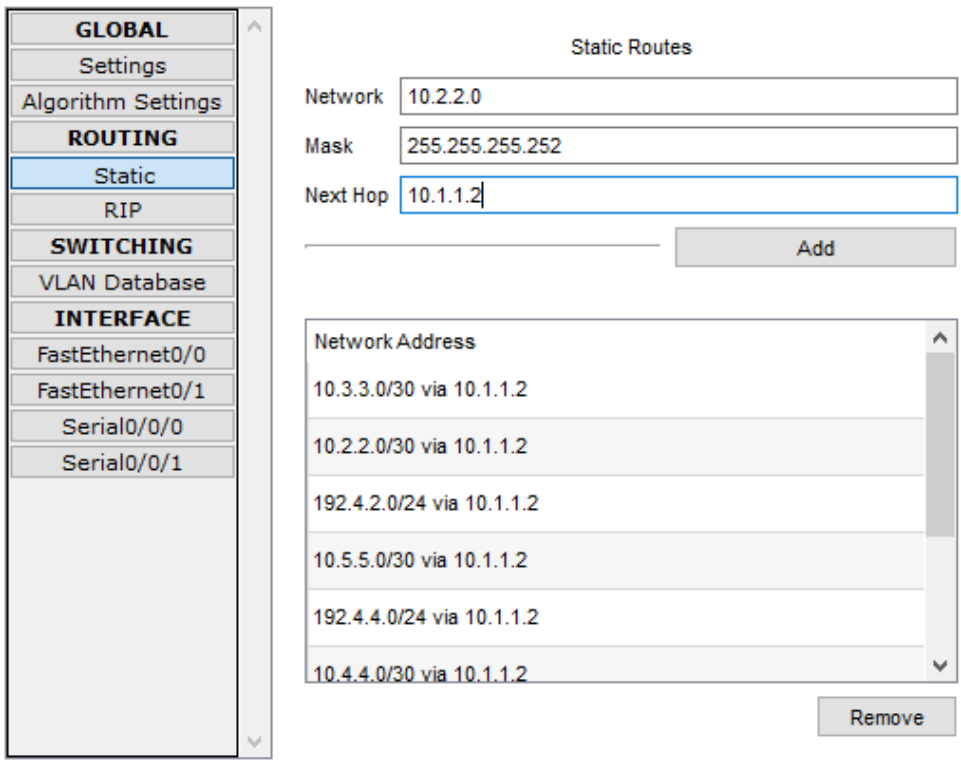
O router R1 para comunicar com o R3 tem de ter uma rota estática que interligue os dois, esta sairá do router R1, passará pelo router R2 e depois então irá chegar ao router R3.

Isto é feito da seguinte forma:

O Network é a rede que queremos chegar, neste caso é a rede: 10.2.2.0

A Mask é a máscara definida para essa rede, esta é /30, ou seja: 255.255.255.252

O Next Hop é o IP da interface do primeiro router que o router R1 tem de passar. Neste caso o router R1 passa primeiro pela Interface s0/0/0 do router R2 que tem o IP 10.1.1.2



Etapa 5: Configure a password com um tamanho mínimo de 10 caracteres

Para configurar o tamanho mínimo de uma password usamos o seguinte comando:

R1(config)# security passwords min-length 10

Etapa 6: Configure a password de enable com "cisco12345"

Para criar uma password de enable usamos o seguinte comando:

R1(config)# enable secret cisco12345

Etapa 7: Configure um utilizador com privilégios 15 em todos os routers e switches e configure a line vty com este user/pass e com o método de transporte SSH

Para criar um utilizador com privilégios 15 usamos o comando:

R1(config)# username admin privilege 15 secret mypwd

De seguida a line vty com o método de transporte SSH é feito da seguinte forma:

R1(config)# line vty 0 4

R1(config-line)# privilege level 15

R1(config-line)# login local

R1(config-line)# transport input ssh

R1(config-line)# exit

R1(config)# ip domain-name ccnasecurity.com

R1(config)# crypto key generate rsa general-keys modulus 1024

R1(config)# ip ssh version 2

R1(config)# ip ssh time-out 90

R1(config)# ip ssh authentication-retries 2

R1(config)# exit

Etapa 8: Configure em todos os routers o acesso remoto apenas através do PC-A

Para permitir o acesso remoto apenas do PC-A, temos de criar uma ACL em cada router com o seguinte comando:

R1(config)# access-list 1 permit host 192.4.1.1

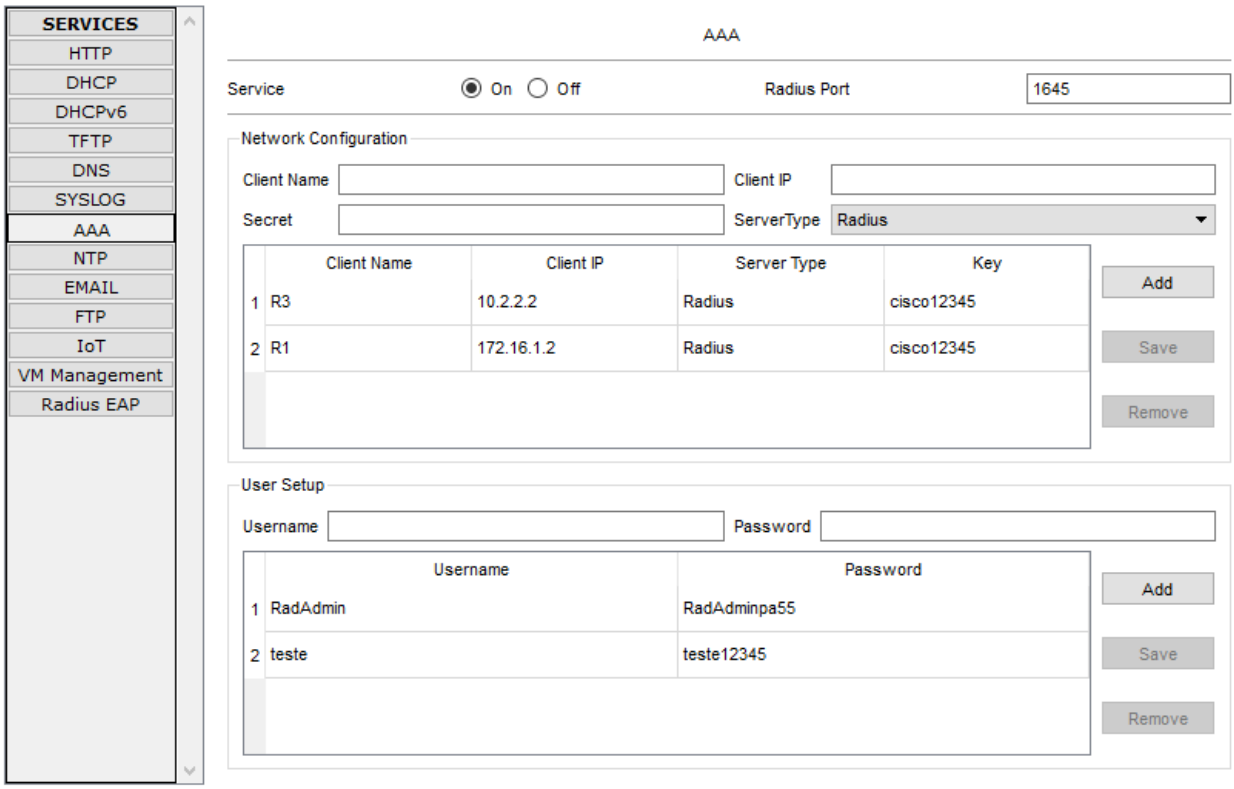
R1(config)# line vty 0 4

R1(config-line)# access-class 1 in

Etapa 9: Configure um servidor RADIUS no PC-A e crie o utilizador com username "RadAdmin" e a password "RadAdminpa55"

A configuração foi feita no PC-B porque o PC-A é um PC normal e não suporta servidor RADIUS

Para configurar um servidor RADIUS, nele próprio, vamos à config/AAA e inserimos as duas configurações de rede, R1 e R2. Depois criamos o utilizador RadAdmin.



Etapa 10: Crie um modelo AAA no R1 e R3, em que o primeiro metodo é o servidor RADIUS e o segundo metodo de autenticação é a base de dados local do router

Para criar um modelo AAA foram usados os seguintes comandos em ambos os routers:

R1(config)# aaa new-model

R1(config)# aaa authentication login default group radius local

R1(config)# radius-server host 172.16.1.1 auth-port 1645

R1(config)# radius-server key cisco12345

R1(config)# line vty 0 4

R1(config-line)# access-class 1 in

R1(config-line)# login authentication default

R1(config-line)# transport input ssh

Etapa 12: Crie uma Zone Base Firewall no R1 com 3 zonas: Internet, DMZ e Inside. Inspecione todo o tráfego entre a zona Inside para a internet nos protocolos tcp, udp e icmp. Permita o tráfego entre o servidor da DMZ para a internet nos protocolos DNS, HTTP e HTTPS

Para criar uma Zone Base Firewall usamos os seguintes comandos:

R1(config)# zone security INTERNET

R1(config)# zone security DMZ

R1(config)# zone security INSIDE

R1(config)# class-map type inspect match-any INSIDE_PROTOCOLS

R1(config-cmap)# match protocol tcp

R1(config-cmap)# match protocol udp

R1(config-cmap)# match protocol icmp

R1(config)# class-map type inspect match-any DMZ_PROTOCOLS

R1(config-cmap)# match protocol http

R1(config-cmap)# match protocol https

R1(config-cmap)# match protocol dns

R1(config)# policy-map type inspect INSIDE_TO_INTERNET

R1(config-pmap)# class type inspect INSIDE_PROTOCOLS

R1(config-pmap-c)# inspect

R1(config)# policy-map type inspect DMZ_TO_INTERNET

R1(config-pmap)# class type inspect DMZ_PROTOCOLS

R1(config-pmap-c)# inspect

R1(config)# zone-pair security INSIDE_TO_INTERNET source INSIDE destination INTERNET

R1(config-sec-zone-pair)# service-policy type inspect INSIDE_TO_INTERNET

R1(config)# zone-pair security DMZ_TO_INTERNET source DMZ destination INTERNET

R1(config-sec-zone-pair)# service-policy type inspect DMZ_TO_INTERNET

Após criar as zonas temos de as aplicar aos várias interfaces:

R1(config)# interface fa0/0

R1(config-if)# zone-member security DMZ

R1(config)# interface fa0/1

R1(config-if)# zone-member security INSIDE

R1(config)# interface s0/0/1

R1(config-if)# zone-member security INTERNET

Etapa 14: Crie um Tunel IPSec entre o R4 e o R6 de forma que as LAN do R4 e R6 comuniquem em segurança

Para criar um Tunel IPSEC entre o R4 e o R6 usamos o seguinte comando:

R4(config)# access-list 110 permit ip 192.4.3.0 0.0.0.255 192.4.4.0 0.0.0.255

(Define o tráfego do R4 ao R6 como interesting para que quando isto aconteça o IPsec VPN seja ativado)

R4(config)# crypto isakmp policy 10

R4(config-isakmp)# encryption aes 256

R4(config-isakmp)# authentication pre-share

R4(config-isakmp)# group 5

R4(config-isakmp)# exit

R4(config)# crypto isakmp key vpnpa55 address 10.5.5.2

R4(config)# crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac

R4(config)# crypto map VPN-MAP 10 ipsec-isakmp

(pode dar erro, fazer exit e tentar de novo)

R4(config-crypto-map)# description VPN connection to R6

R4(config-crypto-map)# set peer 10.5.5.2

R4(config-crypto-map)# set transform-set VPN-SET

R4(config-crypto-map)# match address 110

R4(config-crypto-map)# exit

R4(config)# interface s0/0/0

R4(config-if)# crypto map VPN-MAP

R6(config)# access-list 110 permit ip 192.4.4.0 0.0.0.255 192.4.3.0 0.0.0.255

R6(config)# crypto isakmp policy 10

R6(config-isakmp)# encryption aes 256

R6(config-isakmp)# authentication pre-share

R6(config-isakmp)# group 5

R6(config-isakmp)# exit

R6(config)# crypto isakmp key vpnpa55 address 10.4.4.2

R6(config)# crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac

R6(config)# crypto map VPN-MAP 10 ipsec-isakmp

(pode dar erro, fazer exit e tentar de novo)

R6(config-crypto-map)# description VPN connection to R4

R6(config-crypto-map)# set peer 10.4.4.2

R6(config-crypto-map)# set transform-set VPN-SET

R6(config-crypto-map)# match address 110

R6(config-crypto-map)# exit

R6(config)# interface s0/0/1

R6(config-if)# crypto map VPN-MAP