Universidade Estadual do Oeste do Paraná

Curso de Ciência da Computação

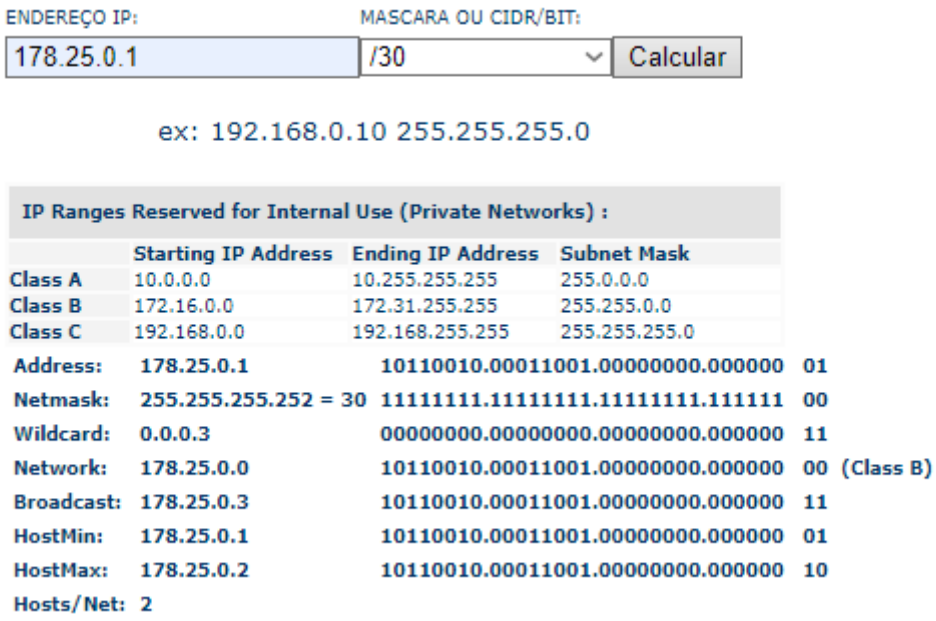
Relatório de Redes:
Trabalho 2

Aluno: Natã Rafael Cruz de Jesus
Professor Orientador: Renato Bobsin

Maio de 2021

Foi requisitado um link com saída externa para a RNP com o endereço 178.25.0.1/30. Com isso em mente foi atribuído para o roteador do campus o endereço 178.25.0.2, para que fosse uma extensão do primeiro.

Para os seguintes roteadores, referentes aos centros, foram atribuídos endereços internos nas faixas de 192.168.X.1 e 172.16.X.1, que foram escolhidos de acordo com cálculos feitos para endereços de 30 bits utilizando o endereço inicial de 178.25.0.1, como demonstrado na imagem abaixo.



ENDEREÇO IP: MASCARA OU CIDR/BIT:

178.25.0.1 /30 Calcular

ex: 192.168.0.10 255.255.255.0

IP Ranges Reserved for Internal Use (Private Networks) :

	Starting IP Address	Ending IP Address	Subnet Mask
Class A	10.0.0.0	10.255.255.255	255.0.0.0
Class B	172.16.0.0	172.31.255.255	255.255.0.0
Class C	192.168.0.0	192.168.255.255	255.255.255.0

Address:	178.25.0.1	10110010.00011001.00000000.000000	01
Netmask:	255.255.255.252 = 30	11111111.11111111.11111111.111111	00
Wildcard:	0.0.0.3	00000000.00000000.00000000.000000	11
Network:	178.25.0.0	10110010.00011001.00000000.000000	00 (Class B)
Broadcast:	178.25.0.3	10110010.00011001.00000000.000000	11
HostMin:	178.25.0.1	10110010.00011001.00000000.000000	01
HostMax:	178.25.0.2	10110010.00011001.00000000.000000	10
Hosts/Net:	2		

Mas, essa conta também pode ser feita de maneira manual, somente somando os octanos da máscara, para descobrir qual usar, mas de maneira lógica podemos dizer que como a rede de 8, 16 e 24 possuem os valores de 255.0.0.0; 255.255.0.0 e 255.255.255.0, respectivamente, para uma máscara de 30 bits podemos perceber que, caso o último valor (normalmente destinado para o host) fosse 255 podemos diminuir 3 bits obtendo 252, sendo essa a máscara de 30 bits. Já que nos números binários 1 equivale a 1 e 2 equivale a 11, em binário. Pode-se também usar a imagem a seguir para confirmação técnica

128	64	32	16	8	4	2	1

A tabela 1 apresenta com mais detalhes os cursos com seus respectivos endereços

Tabela 1 – Cursos e os endereços requisitados e utilizados

Cursos	Centro	Endereços
Ciência da computação (CC)	CECE	192.168.0.254
Engenharia Mecânica (EM)	CECE	172.16.0.254
Letras (LT)	CELS	192.168.1.254
Enfermagem (ENF)	CELS	172.16.1.254
Ciências Contábeis (CCont)	CCSA	192.168.2.254
Administração(ADM)	CCSA	172.16.2.254

Fonte: http://calculadoraip.com.br

Com isso, foi calculado as máscaras necessárias para as redes, obedecendo a regra de 30 bits foram utilizadas as máscaras de 255.255.255.252.

Para cada centro foi determinado os roteadores na faixa de 10.0.X.X, sendo eles:

Tabela 3 – Centro e seus respectivos IPs.

Centro	IP	IP CAMPUS FOZ	MASCARA
CECE	10.0.0.2	10.0.0.1	255.255.255.252
CELS	10.0.1.2	10.0.1.1	255.255.255.252
CCSA	10.0.2.2	10.0.2.1	255.255.255.252

Para a criação da estrutura da rede, foi utilizado o *Cisco Packet Tracer,* onde é possível simular uma rede de internet. Primeiro foi criado um roteador principal que tem o acesso aos outros roteadores dos cursos e o roteador da RNP. Esse roteador tem o nome de CAMPOS UNIOESTE-FOZ e é utilizado portas seriais de número 2, 3, 4 e 5 e a porta Fast Internet 1/0 para a conexão com o servidor. Conectado a cada uma dessas portas seriais é localizado cada roteador dos centros, sendo: CECE; RNP; CELS e; CCSA, respectivamente.

Cada roteador de centro tem um *Switch* conectado para fornecer uma rede Lan para cada curso, e cada switch tem um computador como *Host*, e o switch do curso é conectado ao roteador CECE/UNIOESTE-FOZ pelo IP privado 10.0.X.X, sendo cada um dos roteadores um IP diferente (10.0.1.1, 10.0.2.1, ..., 10.0.2.1). Conforme conectado e configura cada computador e cada roteador, o esquema da rede fica apresentado na próxima figura.

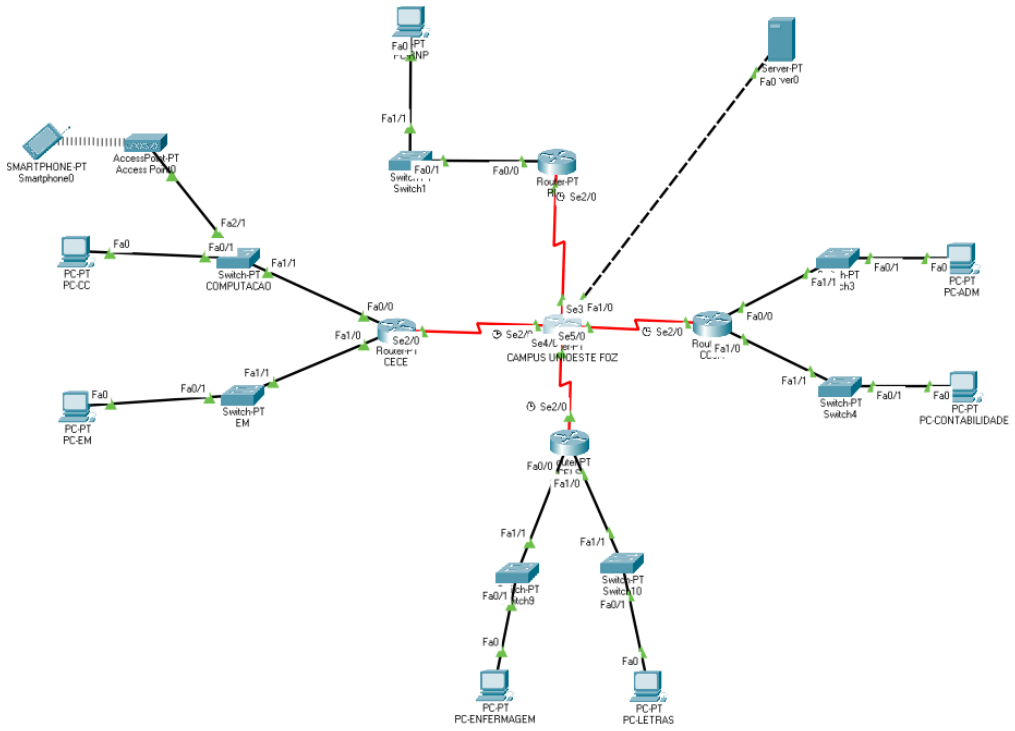


Figura 1 – Arquitetura de Rede desenvolvida

Com essa rede em mente, o próximo passo é fazer uso do NAT e do DHCP. Para configurar um DHCP, não foi utilizado um servidor devido ao roteador utilizado possuir a opção via comandos no terminal para a criação do *pool* de IPs, assim como a configuração do DNS e do IPs exclusivos da rede. Os comandos utilizados foram:

- *ip dhcp pool POOL_NAME* (nome qualquer que será utilizado para criar o *pool* de DHCP, esse comando cria uma pool de DHCP com o nome escolhido)
- *network 192.168.X.0 255.255.Y.0* (Define o intervalo a qual os IPs serão extraídos, onde X é início do intervalo da sub-rede do curso, e Y é a máscara para a sub-rede do curso)
- *default-router* 192.168.X.254 (Define qual o IP do roteador principal) (gateway)
- *dns-server* 200.248.122.254 (Define o IP do servidor DNS)

Com esses comandos executados, qualquer computador daquela sub-rede terá a possibilidade de utilizar a função DHCP quando tiver definido o IP do computador.

NAT

Para a utilização do NAT na rede, foi atribuído o valor de saída como o ip do Campus (178.25.0.2).

As configurações necessárias para implementação do NAT foram feitas via CLI, por linhas de códigos e foram as seguintes:

int Fa0/0 – para *int* significa interface, comando para entrar na interface de certa porta

ip nat inside - define como interno, que será alterado na saída

exit - para sair da interface

REPETE PARA OS OUTROS SWITCHS/ENDS

Para o roteador de saída

int Se2/0 – escolhe a porta de saída

ip nat outside – para definir como *outside*, que será o IP resultante do NAT

exit

Depois disso pode-se criar uma lista de acesso para as redes, que podem ser permitidas ou negadas

access-list 10 permit 192.168.X.254 0.0.0.255 (mascara invertida -wild card mask)

O processo se repete para cada rede

Configurando o NAT (da primeira rede pública ou roteavel até a última que pode ser acessada, no nosso caso por enquanto só uma)

E mascara

ip nat pool NOME_POOL 178.25.0.1 178.25.0.1 netmask 255.255.255.0

Quem vai ter os IP traduzido e por onde serão encaminhados/encapsulados

ip nat inside source list 10 interface Se2/0 overload

ACABOU O NAT

Só configurar rede para alcançar remota 1 para 1

conf t

Ordem: de qualquer rede alvo; de qualquer mascara siga para

ip route 0.0.0.0 0.0.0.0 178.16.0.1

exit

No próximo modem só checa o 0.0.0.0 0.0.0.0 178.16.0.2

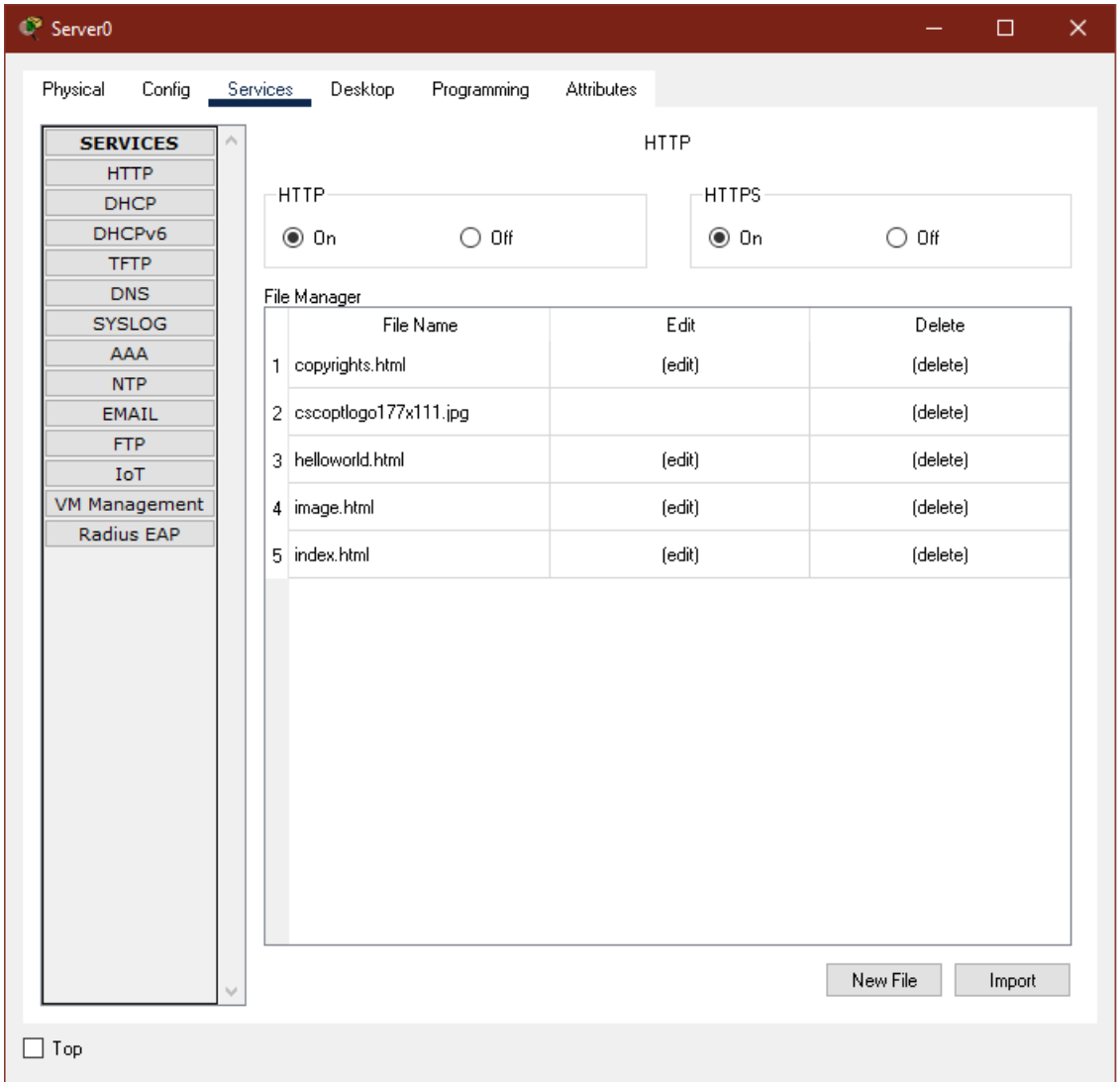
Que verifica o caminho de volta entre os dois.

WiFi

Para configuração do *wi-fi* somente foi atribuído um *Acess-point* ao switch do curso de CC e atribuído o mesmo DHCP do curso, manualmente

Servidor Web-DNS Unioeste

Para o servidor foi atribuído o IP 200.248.122.254 e ativado as funções de DHCP e DNS, em serviços



E, por último, nos computadores hosts, foram atribuídos o DNS do servidor, por meio de linhas de comandos CLI.

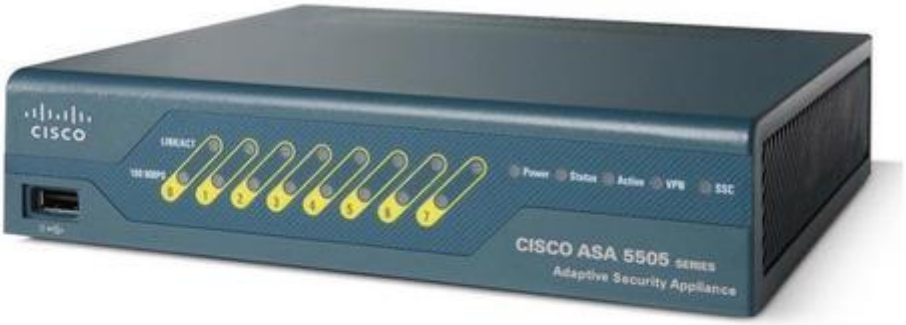
Firewall

Para a configuração do firewall existem mais de uma possibilidade, sendo uma via software e outra via hardware, porém, para nosso exemplo foi escolhido a via software por questões de econômicas, já que pode ser implementada no próprio servidor e não precisa adquirir tipos especiais de roteadores, mas para a configuração via hardware os mais comuns são:

ASA8 ou 5506-X

Fonte: https://www.cisco.com/c/pt_br/support/security/asa-5506-x-firepower-services/model.html

ASA7 ou 5505



Fonte: https://produto.mercadolivre.com.br/MLB-1543025498-firewall-cisco-asa5505-50-aip5-k9v-_JM

Porém, como nossa demonstração será somente via software, não apresentaremos tutoriais onde esses seriam implantados.

Configurando o FIREWALL

Pode-se determinar a partir de uma sigla, o que pode ou não ser permitido através do firewall de um grupo de redes, sendo eles:

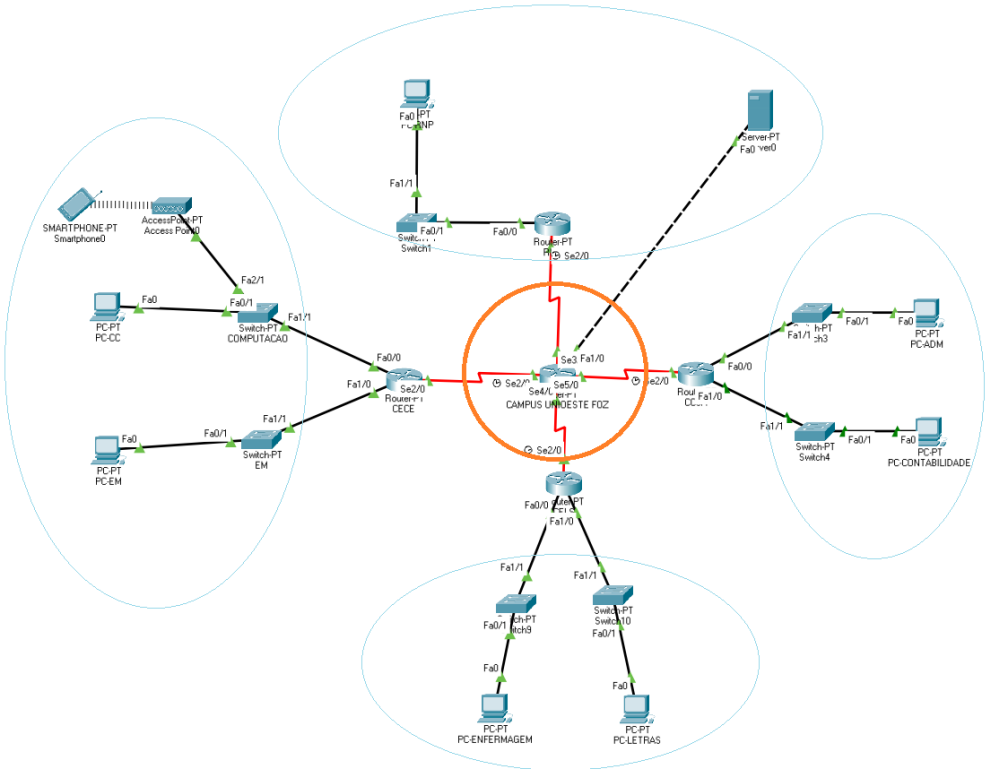
ICMP = ping

FTP = transferência de arquivos

WEB = conexões web, por exemplo o web-browsing

DNS = uso de DNS, por exemplo para fazer um ping via prompt de comando deverá ser usado o IP da rede.

Nosso recurso usado para a criação do firewall foi por meio de linhas de comando no roteador central de nossas conexões, já que todos os roteadores e hosts podem conversar entre si, mas todos devem passar por esse roteador. Pode-se notar isso olhando para as configurações *statics*(sua rota) de cada roteador de centro, e em nosso caso o roteador central é o CAMPUS UNIOSTE FOZ como demonstrado, em alaranjado, na imagem a seguir.



Vale ressaltar que sempre pode-se usar o símbolo “?” para verificar opções de comandos ou se o comando está completo ou correto.

Então, dentro das configurações desse roteador, no CLI a partir de configure terminal devemos utilizar os comandos:

Access-list - Criar uma template de regras do que pode ou não, que são de 1 a 99 os padrões e de 100 a 199 as entendidas, em nosso exemplo usaremos as entendidas, já que tem mais recursos;

Access-list 100

A partir daqui devemos dizer se é para negar ou permitir. Podemos nesse exemplo negar protocolos icmp, o ping

Access-list 100 deny icmp any any hos

O primeiro any significa de onde, já o segundo para onde, no nosso caso de qualquer lugar para qualquer lugar, outra opção seria dizer o host de quem negaria e/ou para quem negaria. Hos é um atalho para o comando host não alcançável, que seria a mensagem recebida após a tentativa de ping

Podemos então entrar na interface do roteador, usando o comando interface e sua porta (F1/0)

E dentro da porta podemos ativar a configuração anterior com os comandos:

Ip access-group 100 in = essa lista de permissões eu quero atribuir a 100. Entrada

Outro serviço configurável, por exemplo, pode ser para o servidor em relação a TCP na conexão com a internet

Mais uma vez em modo de configuração, eu acesso minha lista 100 podemos permitir o protocolo TCP

Access-list 100 permit tcp any any eq = o comando eq me mostra quais portas são usadas para cada tipo de protocolo mas podemos não o usar para permitir todos tipos de protocolos TCP.

Existe também o comando UDP que da opção de configurações de DNS.

Para finalizar, podemos utilizar um comando para mostrar todas configurações que tem em minha access-list, utilizando o comando:

Show access-list 100