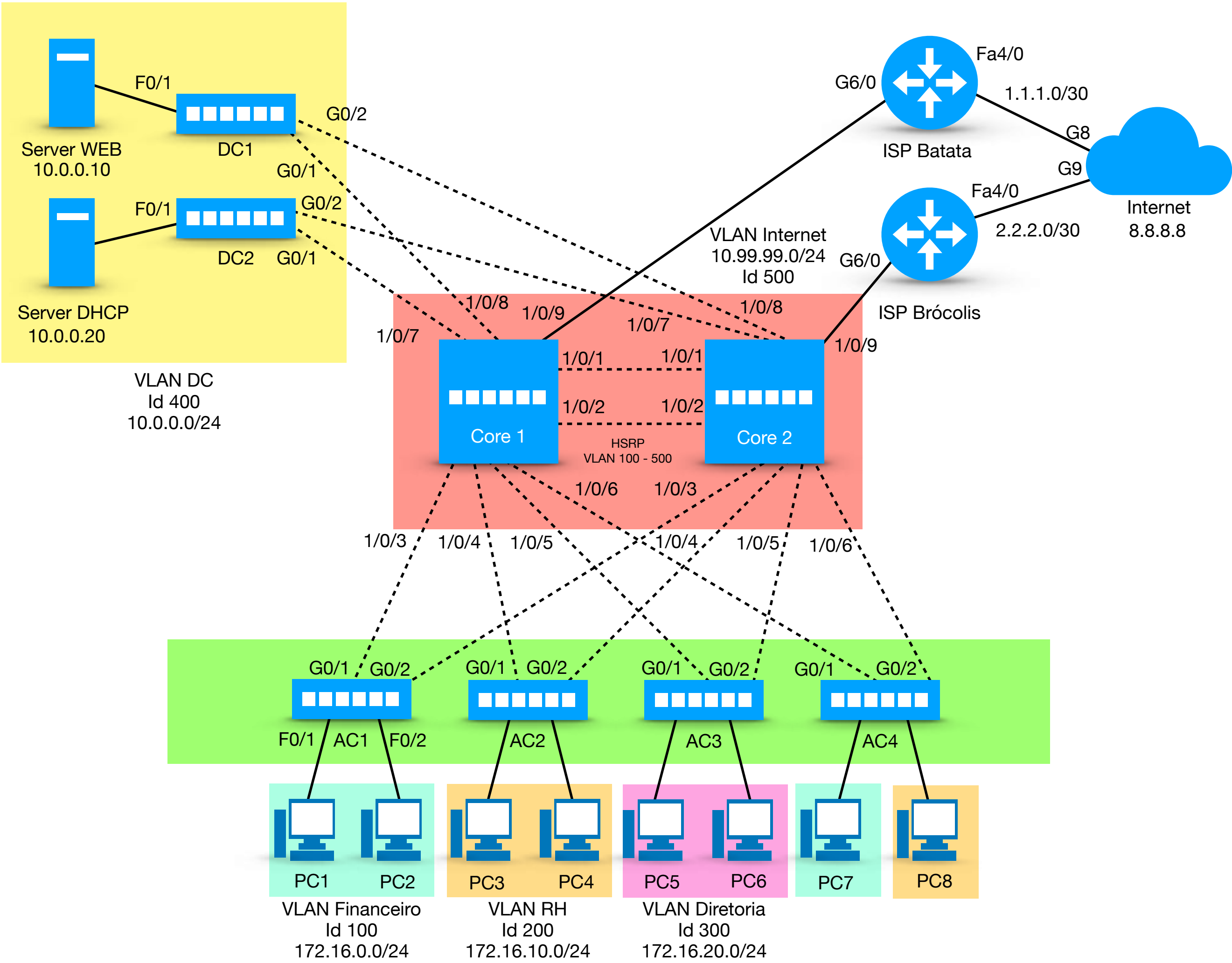


Olá pessoas! Sejam bem vindas! Nesse pequeno curso aprenderemos conceitos básicos de redes e alguns até avançados, no final no curso teremos configurado a rede do desenho abaixo, esse desenho é chamado de topologia e representa os equipamentos, conexões e endereçamento básico dos dispositivos.



Apesar de parecer complexo, iremos por etapas e você vai ver que tudo vai se encaixar, a ideia é você ir aprendendo gradativamente através da prática, lembrando que a teoria é extremamente importante e caso você tenha interesse em determinado assunto, que você busque mais informações para fixar seu aprendizado.

Para montar esse nosso LAB, utilizaremos um software chamado Packet Tracer, que nada mais é que um simulador de dispositivos de rede desenvolvido pelo fabricante Cisco, esse software é totalmente gratuito, basta fazer um pequeno cadastro no site do fabricante para poder fazer o download.

Entre no site: <https://www.netacad.com/pt-br/courses/packet-tracer> e clique em Inscreva-se para baixar o packet tracer, na próxima página clique em Inscreva-se hoje mesmo e em English, na próxima página faça o seu cadastro (sim eu seu, são muitas páginas.)

1

Como fazer o download do Packet Tracer

Para baixar o Packet Tracer, siga estas etapas para se inscrever na Networking Academy:

- Clique no botão "Inscreva-se para fazer o download do Packet Tracer"
- Inscreva-se no curso Introduction to Packet Tracer
- Complete seu registro da Networking Academy
- Inicie o curso Introduction to Packet Tracer
- As instruções de download podem ser encontradas no curso

Inscreva-se para baixar Packet Tracer

2

Inscreva-se, faça o download e comece a receber dicas importantes e as melhores práticas para a ferramenta de simulação inovadora da Cisco, o Packet Tracer. Este curso individualiza o aprendizado para iniciantes sem conhecimento prévio de rede. Ele ensina as operações básicas da ferramenta com várias atividades práticas que ajudam você a visualizar uma rede usando exemplos, incluindo a Internet das Coisas (IoT). O curso introdutório é muito útil para quem planeja cursos da Networking Academy que usa a eficiente ferramenta de simulação.

Inscreva-se hoje mesmo!

English

3

Introduction to Packet Tracer 0420

Detalhes do curso

Cisco Virtual Academy

Explore

02 Apr - 30 Sep 2020

Sandra Ray2, Kimberly Little, Elaine Sherwood

Inscreva-se agora

Nome *

Sobrenome *

E-mail (para receber o link de ativação) *

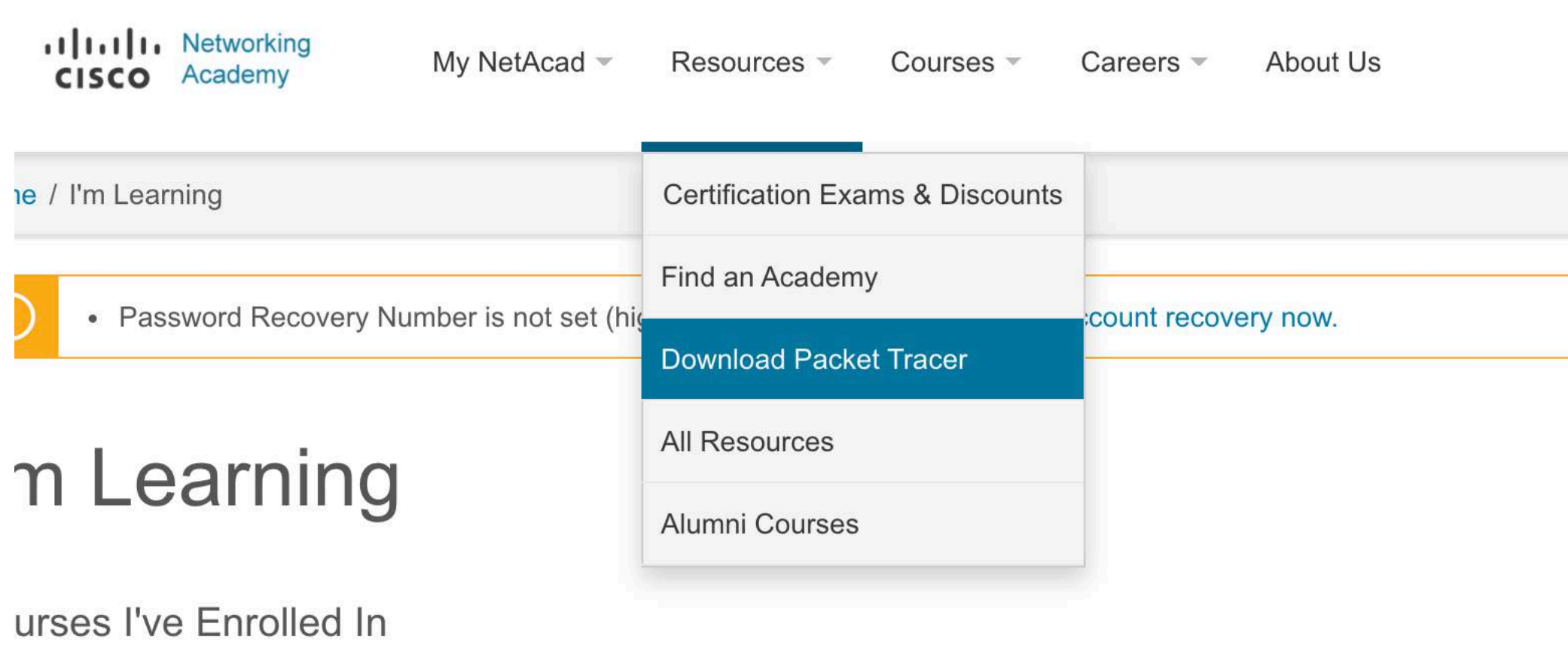
☐ Envie atualizações sobre meu curso e oportunidades

CODERES

#60243

gustavokalau.com.br

Ao efetuar o login no site, vá no menu superior em resource e depois em Download Packet Tracer:



Basta agora escolher o download de acordo com o seu sistema operacional:

Download

Choose the OS you are using and download the relevant files. Read the [FAQ](#). View [Tutorial](#)

Packet Tracer requires authentication with your login and password when you first use

Considering to upgrade?

For CCNA 7, Packet Tracer 7.3.0 is the minimal version that supports CCNA 7.
For CCNA 6 (and older versions), we recommend instructors and students stay with Packet Tracer 6.0.1.
If you are learning/teaching both CCNA 6 and 7, please use Packet Tracer 7.3.0.
When using Packet Tracer 7.3.0 for CCNA 6, there is a small possibility you may encounter a warning message.
If so, you may disregard the message. It is simply a warning that scripts in this file need to be updated.

Windows Desktop Version 7.3.0 English

[64 Bit Download](#) [32 Bit Download](#)

Linux Desktop Version 7.3.0 English

[64 Bit Download](#)

macOS Version 7.3.0 English

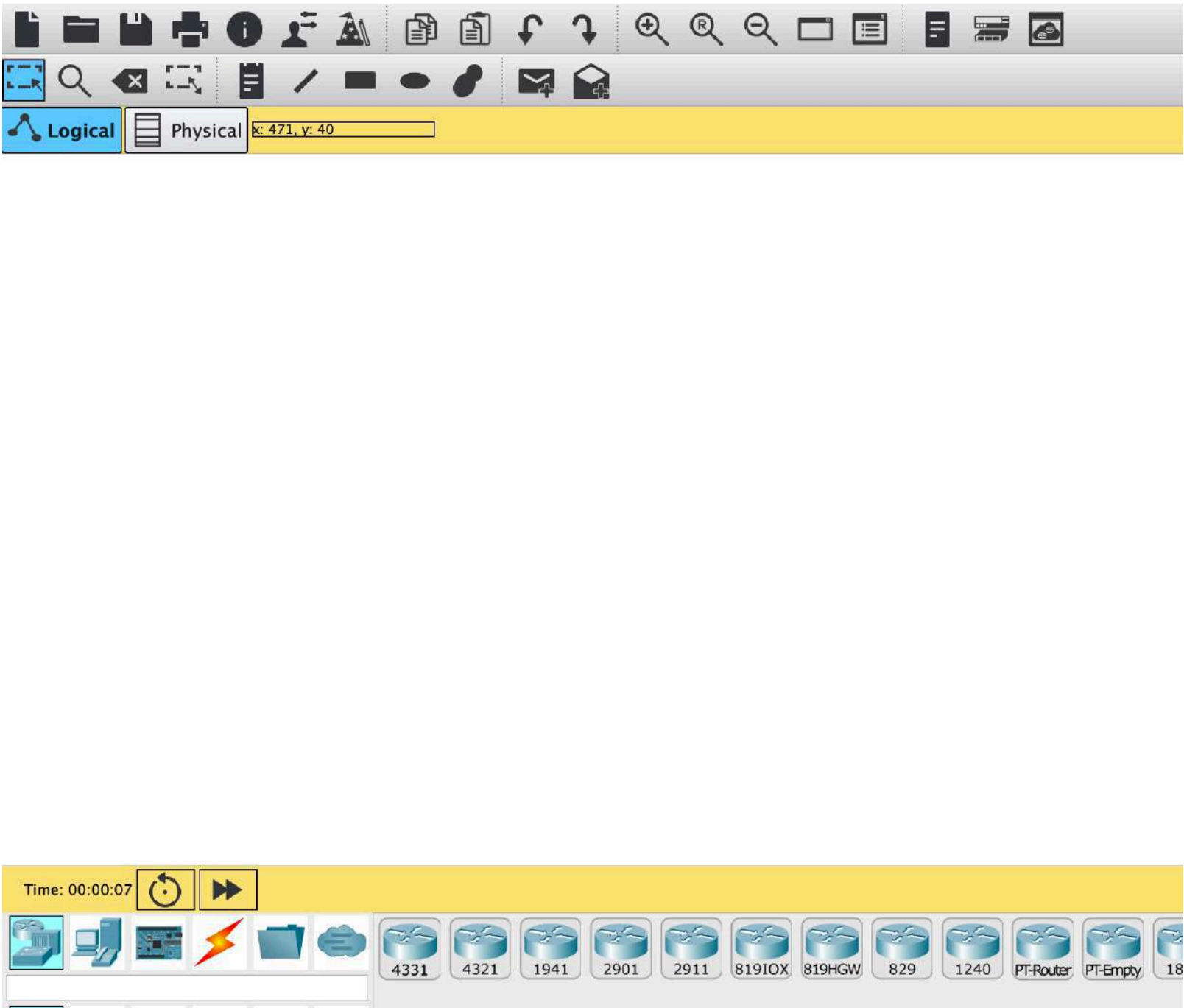
[Download](#)

No curso utilizarei a versão 7.3, caso tenha problema com essa versão tente instalar uma mais antiga.

Para instalar, basta executar o instalador que você acabou de baixar.

Para utilizar o packet tracer e conseguir usar sem limitação será necessário uma conexão com a internet, pois ao abrir o software ele vai pedir para você autentica no site da Cisco com o seu user e senha criado anteriormente.

Abaixo a tela do programa.

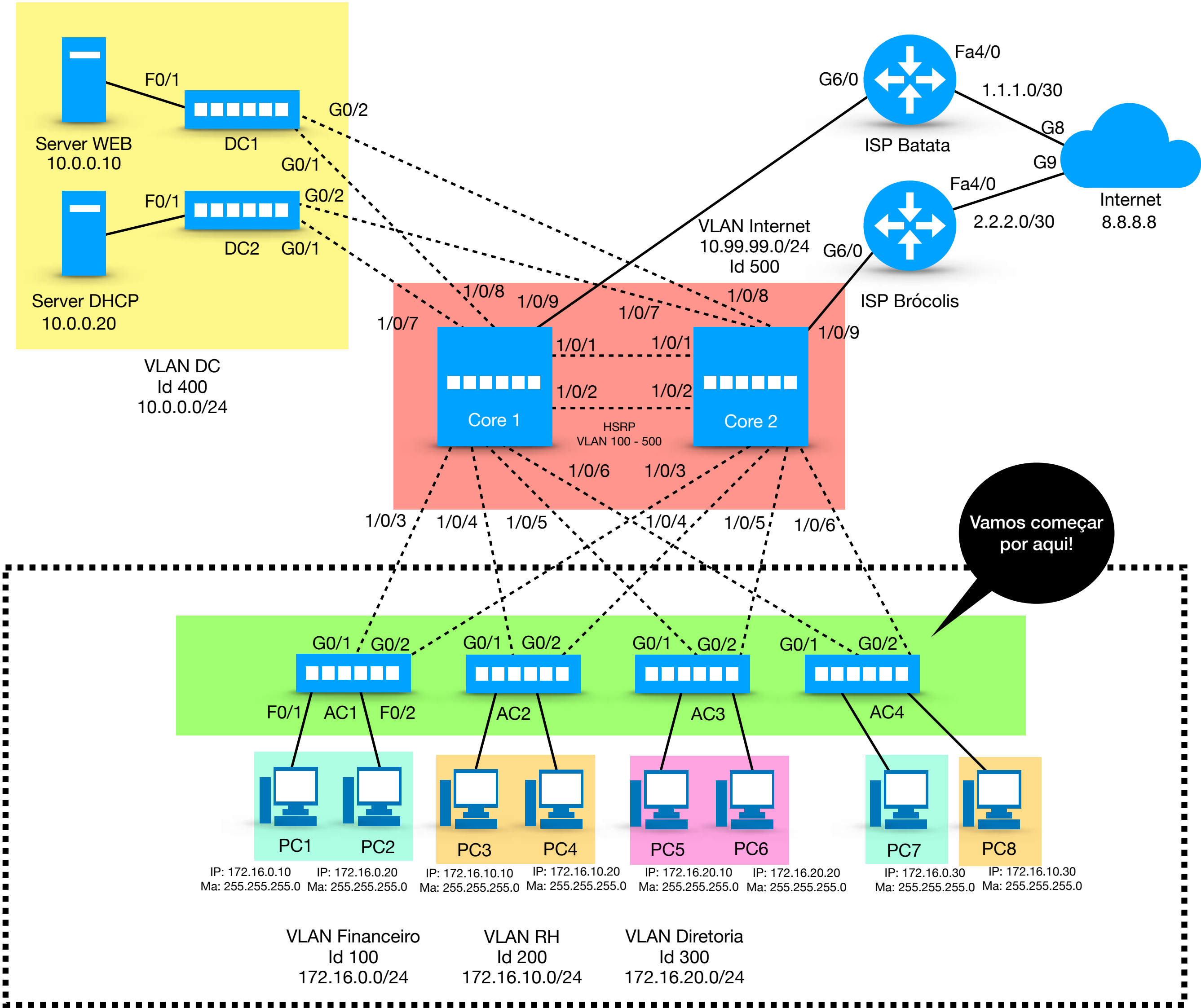


Aula 2

Curso de Rede Básico - Mão na massa

Olá pessoas! Sejam bem vindas! Na aula 2 iremos conhecer um conceito básico de redes chamado switching e para fazer isso vamos utilizar um equipamento chamado switch.

Para entender como ele funciona teremos uma base teórica, lembrando que esse é curso para despertar interesse e não se trata de um curso completo, bora lá!

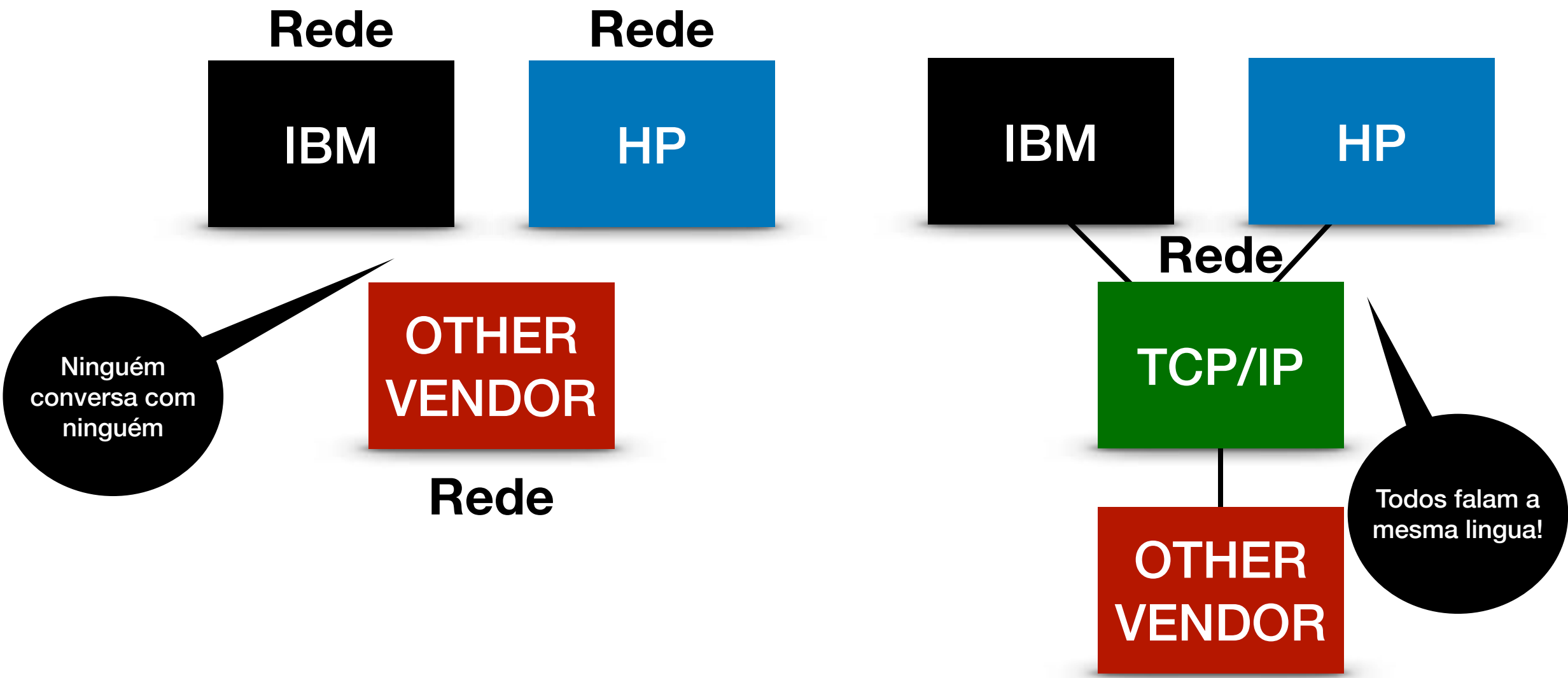


Devemos antes de tudo entender o que é um protocolo e para que existe um padrão de comunicação utilizada em redes de computadores.

Um protocolo nada mais que um conjunto de regras, nós seres humanos seguimos protocolos a todo momento.

Um mundo SEM padrão

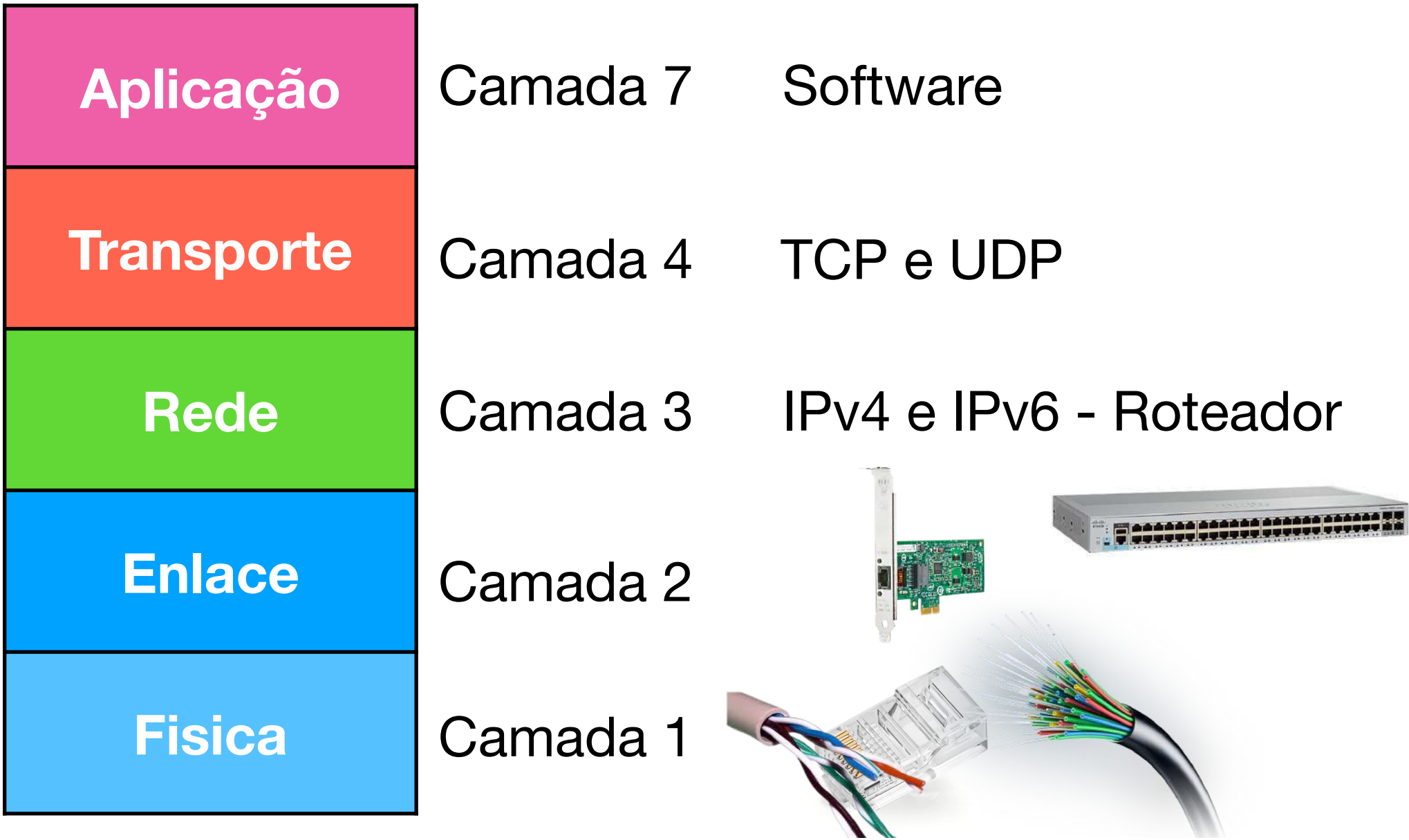
Um mundo COM padrão



Para resolver um problema tão complexo quanto o envio de dados em rede, os engenheiros e pesquisadores decidiram quebrar o problema em partes, a velha tática de dividir pra conquistar, com isso nasceu o modelo ou pilha TCP/IP, que deixa claro as tarefas de cada camada, imagine esse modelo como um carro, onde cada camada tem uma função específica, se o carro só tiver motor não adianta muita coisa pois faltara outros componentes como rodas, pneus, bancos etc, é o conjunto de tudo que faz o carro ser o carro. Aqui podemos ter a mesma abordagem.

Entender como a pilha TCP/IP funciona é o mais importante para os profissionais de rede, ao entender a relação entre as camadas e os protocolos ajuda a desenvolver melhor os projetos de rede e na detecção e resolução de problemas.

TCP/IP



O Switch:

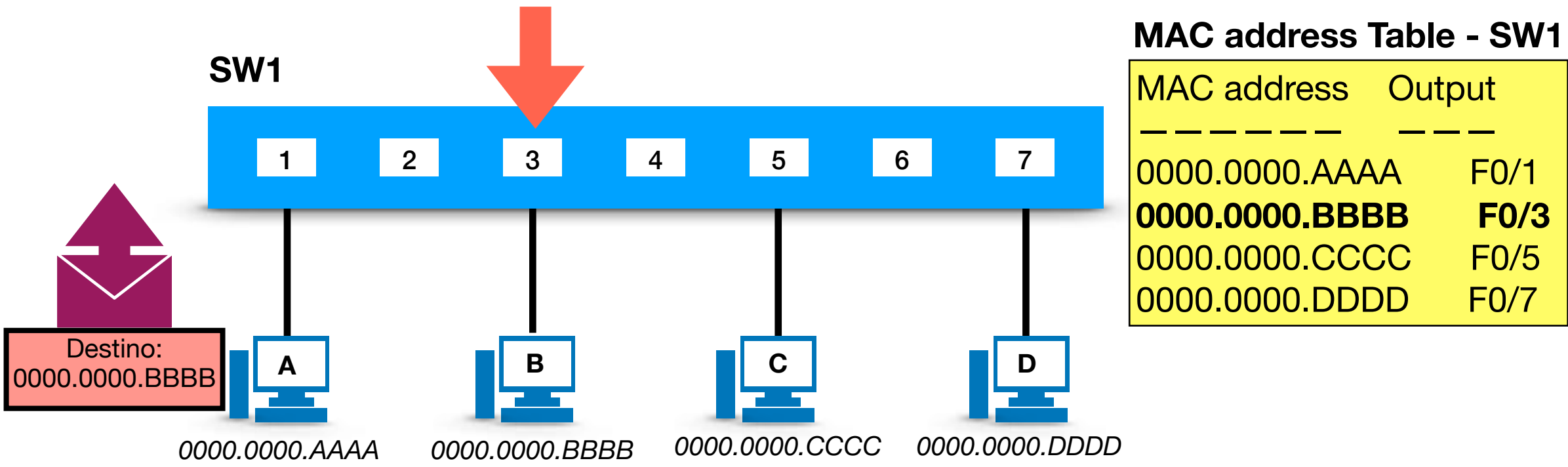


O papel de um switch LAN é encaminhar Frames Ethernet.

Seu trabalho principal é: encaminhar frames para o endereço de destino correto (MAC).

As LANs existem como um conjunto de dispositivos de usuário, servidores e outros dispositivos que se conectam a switches, com os switches conectados entre si.

E para atingir esse objetivo, os switches usam lógica - lógica baseada no endereço MAC de origem e destino no cabeçalho Ethernet de cada frame.



Comando utilizados na aula:

```
Switch> enable
Switch# show mac-address-table
Switch# configure terminal
Switch(config)# hostname AC1
AC1(config)# end
AC1# wr
```

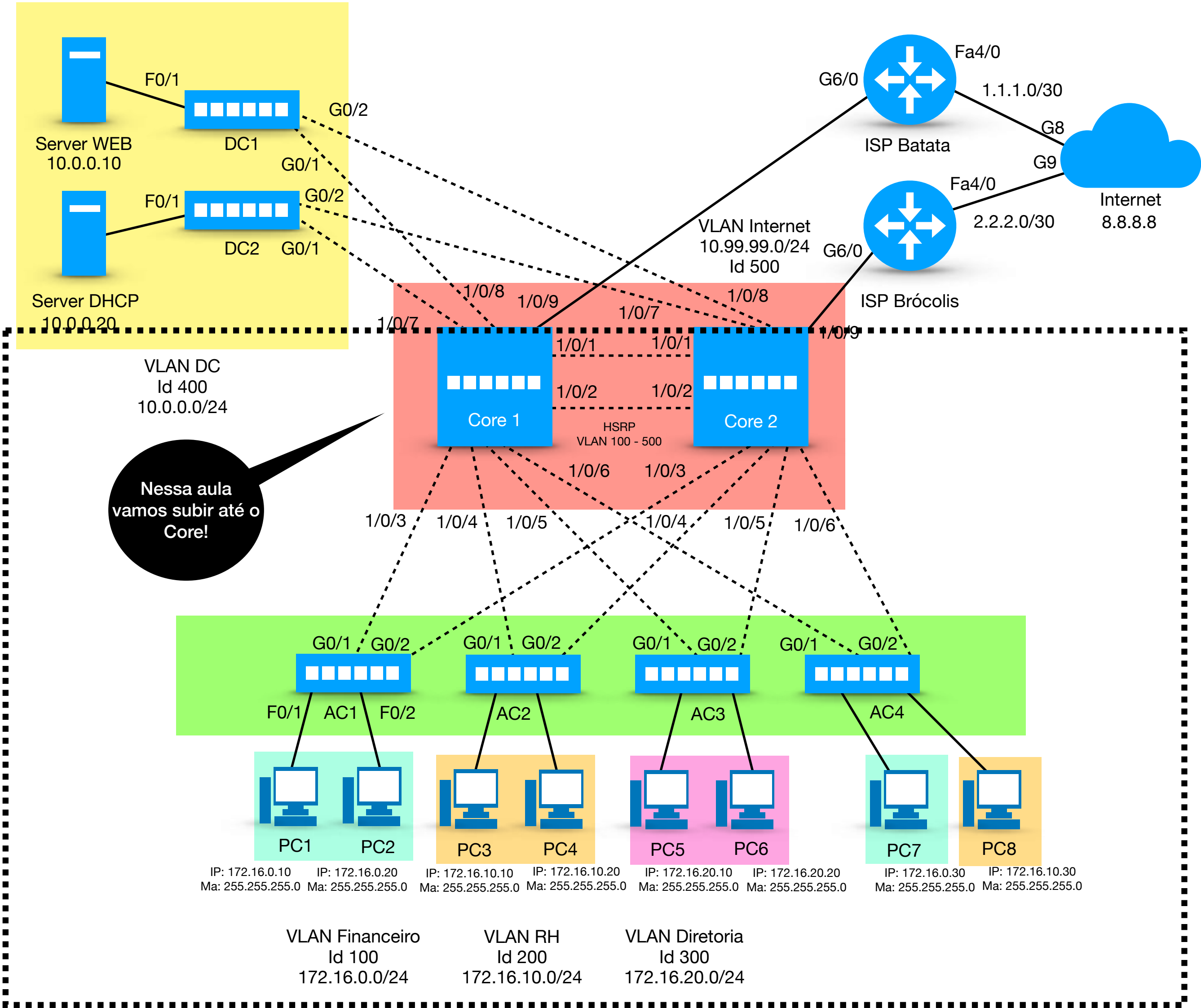


Aula 3

Curso de Rede Básico - Mão na massa

Olá pessoas! Sejam bem vindas! Na aula 2 iremos conhecer um conceito básico de redes chamado switching e para fazer isso vamos utilizar um equipamento chamado switch.

Para entender como ele funciona teremos uma base teórica, lembrando que esse é curso para despertar interesse e não se trata de um curso completo, bora lá!



Virtual LAN Conceitos

O que é uma LAN?

Uma LAN inclui todos os dispositivos de usuário, servidores, comutadores, roteadores, cabos e pontos de acesso sem fio em um local.

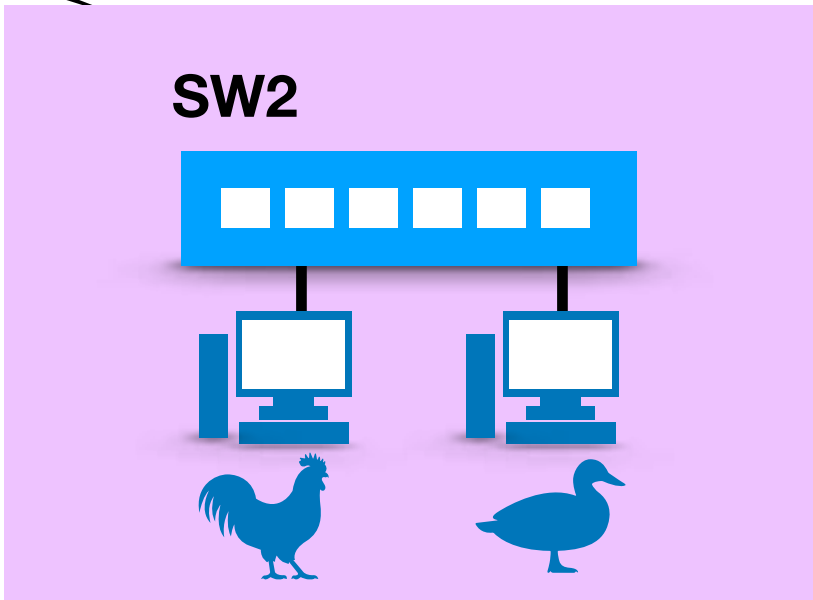
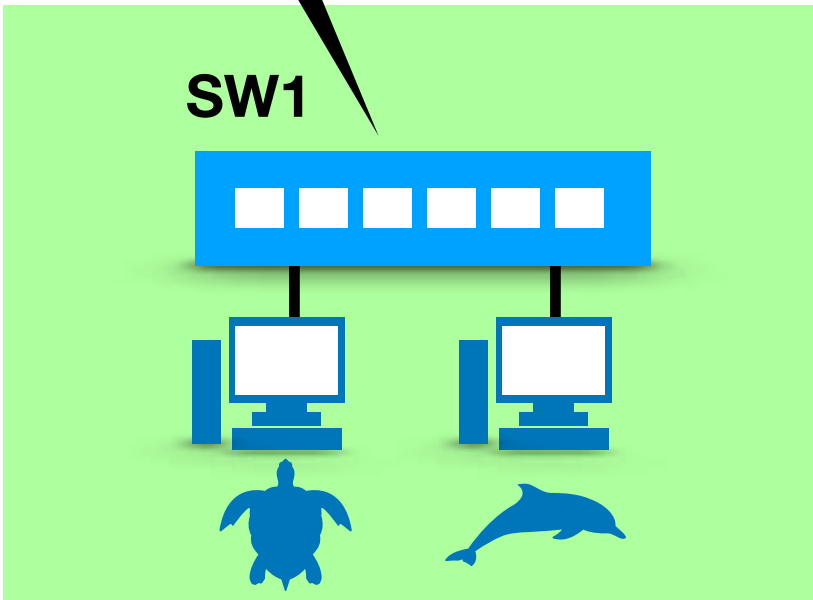
Uma LAN inclui **todos** os dispositivos no **mesmo domínio de broadcast**.

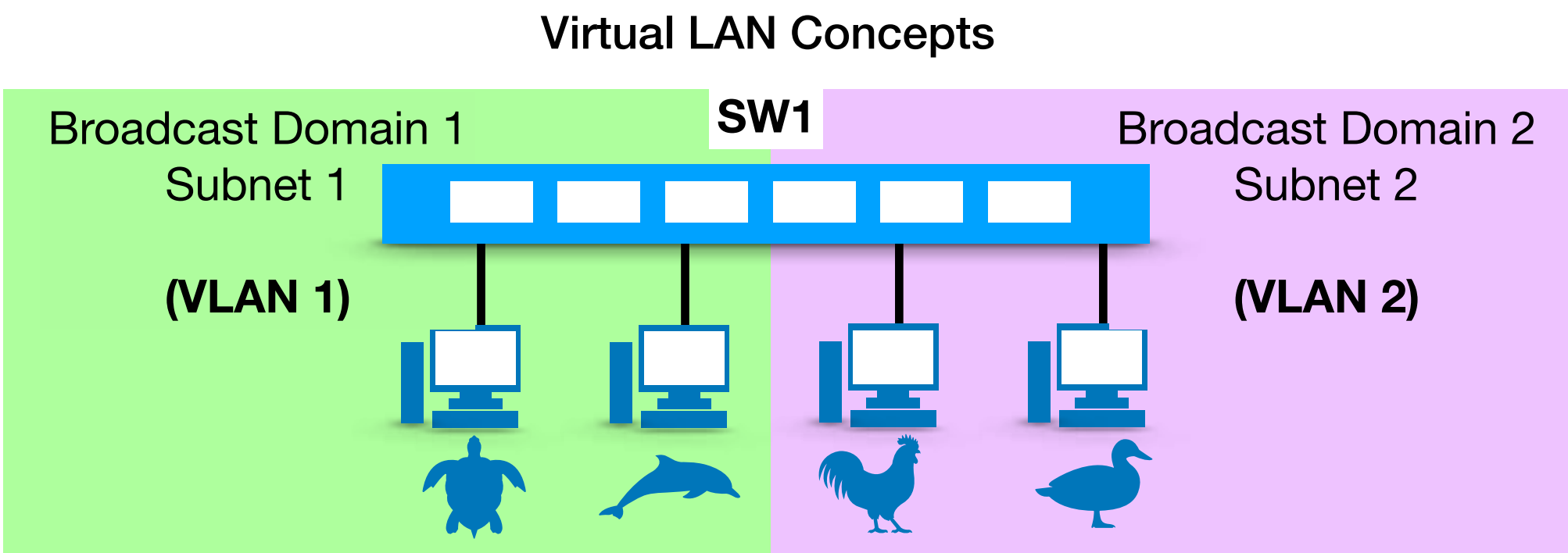
Essas redes não se falam pois estão em domínios de broadcast diferentes e não existe um dispositivo que ligue essas duas redes

Quando um dispositivo envia um Frame broadcast, todos os outros dispositivos obtêm uma cópia desse Frame.

Broadcast Domain 1
Subnet 1

Broadcast Domain 2
Subnet 2





Mas pra que criar domínios de broadcast menores?

Para reduzir o CPU overhead em cada dispositivo, melhorando o desempenho do host, reduzindo o número de dispositivos que recebem cada broadcast frame;

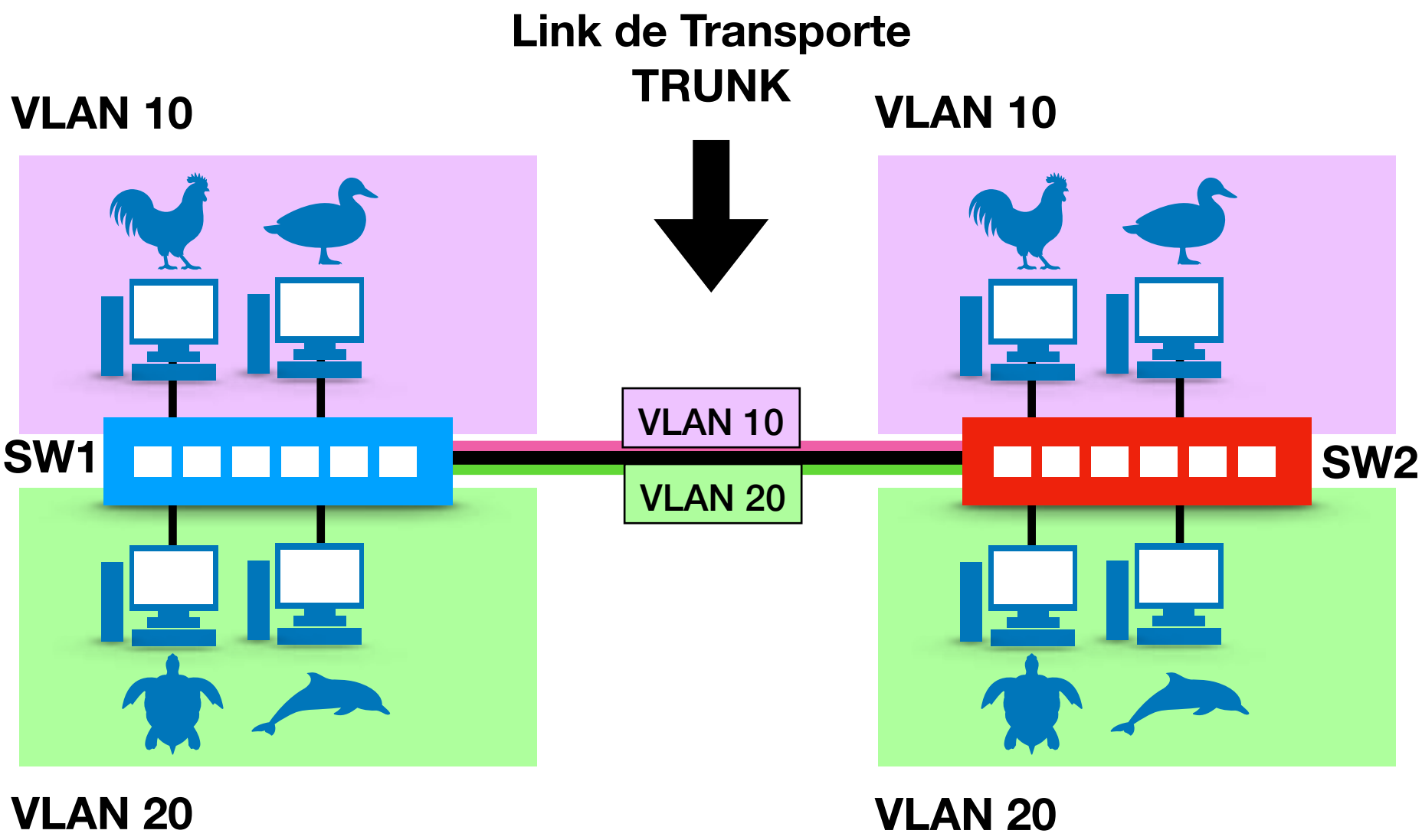
Para reduzir os riscos de segurança, reduzindo o número de hosts que recebem cópias de frames inundados pelos switches (broadcasts, multicasts, and unknown unicasts);

Para melhorar a segurança dos hosts por meio da aplicação de diferentes políticas de segurança por VLAN

Para resolver problemas mais rapidamente, porque o domínio de falha para muitos problemas é o mesmo conjunto de dispositivos que estão no mesmo domínio de broadcast.

Para criar designs mais flexíveis que agrupam usuários por departamento ou por grupos que trabalham juntos, em vez de por local físico

Creating Multiswitch VLANs Using Trunking



VLAN Tagging Concepts



TAG do tênis, aparentemente isso é moda



Quem sou eu? (Gustavo Kalau uai...)

Pai do Arthur, apaixonado por infraestrutura de TI, formado em Sistemas de Informação pela PUC MG, especialista em gestão de Infraestrutura de TI utilizando Software Livre e especialista em Redes de Computadores também pela PUC MG, atua há mais de 10 anos com redes de computadores e possui as seguintes certificações: CCIE R&S #60243, CCNAv3 R&S, CCNP R&S, CCDA, ITILv3F, MTA NF, JNCIA, AWS Associate: SysOps, Architect e Developer, LPIC-1 e LinuxEssentials e morando em Belo Horizonte.

Idealizador do treinamento CCNA/CCNP RiscoZero

A ideia do treinamento é passar o conteúdo da forma mais didática e diferente possível, fugindo do método de ensino chato.

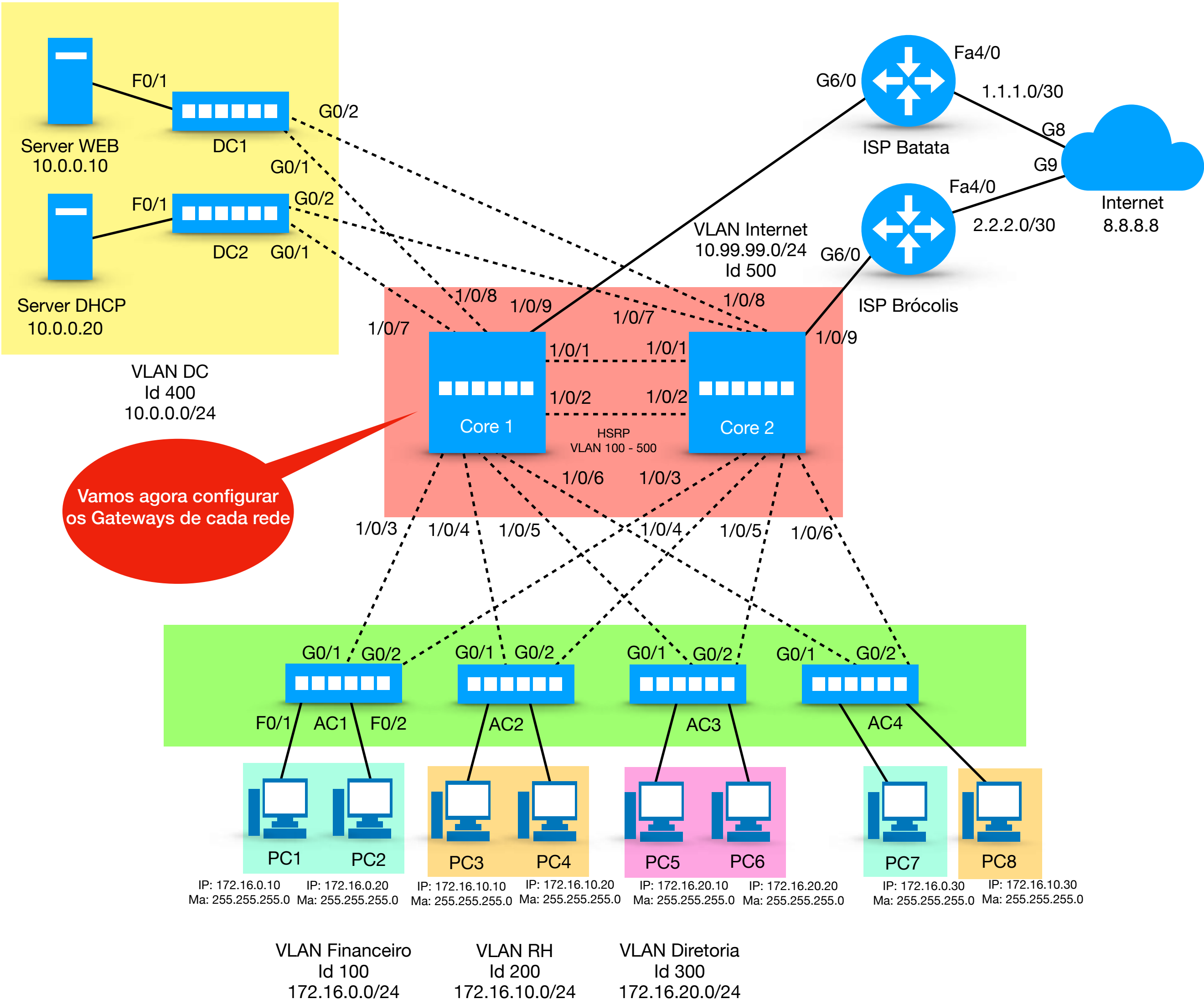
Além disso ao comprar o modo Risco Zero, o candidato tem uma segurança maior, pois se for reprovado, eu devolvo o dinheiro investido (descontado impostos e tarifas de operadora), o que dá ao aluno a chance de fazer a prova novamente, normalmente sem custo

Obrigado por acessar esse conteúdo e me ajude a espalhar conhecimento, compartilhe com seus amigos!



Olá pessoas! Sejam bem vindas! Na aula 2 iremos conhecer um conceito básico de redes chamado switching e para fazer isso vamos utilizar um equipamento chamado switch.

Para entender como ele funciona teremos uma base teórica, lembrando que esse é curso para despertar interesse e não se trata de um curso completo, bora lá!





Gateway



Em uma **REDE** o **gateway** é o IP utilizado pelos dispositivos para encaminhar os pacotes destinados a outras redes, **GATE é portão me inglês**, podemos fazer uma analogia com a sua casa:

quando vc quer se comunicar pessoalmente com alguém que está fora da sua casa você não tem que SAIR da sua casar? E para sair da sua casa você precisa passar por uma porta ou **PORTÃO** (GATE).

O gateway da rede deve ser um dispositivo capaz de encaminha pacotes entre redes diferentes, esse processo é chamado de roteamento e o dispositivo que normalmente faz esse papel é o Roteador, mas pode ser também um switch layer 3 ou até mesmo um computador ou firewall.



Configurações realizadas até o momento:

SWITCH AC1:

```
enable
conf t
hostname AC1
vlan 100
  name FINANCEIRO
exit
!
interface FastEthernet0/1
  switchport access vlan 100
  switchport mode access
exit
!
interface FastEthernet0/2
  switchport access vlan 100
  switchport mode access
exit
end
wr
```

Entrar em modo usuário privilegiado

Entrar em modo de configuração

Mudar o nome do dispositivo

SWITCH AC2:

```
enable
conf t
hostname AC2
vlan 200
  name RH
exit
!
interface FastEthernet0/1
  switchport access vlan 200
  switchport mode access
exit
!
interface FastEthernet0/2
  switchport access vlan 200
  switchport mode access
exit
end
wr
```

Criar VLAN e colocar um nome nela

Sair do modo de configuração de VLAN

SWITCH AC3:

```
enable
conf t
hostname AC3
vlan 300
  name DIRETORIA
exit
!
interface FastEthernet0/1
  switchport access vlan 300
  switchport mode access
exit
!
interface FastEthernet0/2
  switchport access vlan 300
  switchport mode access
exit
end
wr
```

Configurar uma interface

Colocar uma interface em uma VLAN específica

Voltar para o modo usuário privilegiado

SWITCH AC4:

```
enable
conf t
hostname AC4
vlan 100
  name FINANCEIRO
exit
vlan 200
  name RH
exit
!
interface FastEthernet0/1
  switchport access vlan 100
  switchport mode access
exit
!
interface FastEthernet0/2
  switchport access vlan 200
  switchport mode access
exit
end
wr
```

Salvar a configuração



```
SWITCH CORE 1:

enable
conf t
hostname CORE1
vlan 100
  name FINANCEIRO
  exit
vlan 200
  name RH
  exit
vlan 300
  name DIRETORIA
  exit
!
ip routing
!
interface GigabitEthernet1/0/3
  switchport trunk encapsulation dot1q
  switchport mode trunk
  exit
!
interface GigabitEthernet1/0/4
  switchport trunk encapsulation dot1q
  switchport mode trunk
  exit
!
interface GigabitEthernet1/0/5
  switchport trunk encapsulation dot1q
  switchport mode trunk
  exit
!
interface GigabitEthernet1/0/6
  switchport trunk encapsulation dot1q
  switchport mode trunk
  exit
!
interface Vlan100
  ip address 172.16.0.1 255.255.255.0
  exit
!
interface Vlan200
  ip address 172.16.10.1 255.255.255.0
  exit
!
interface Vlan300
  ip address 172.16.20.1 255.255.255.0
  exit
end
wr
```

Habilitar a funcionalidade de roteamento no switch camada 3

Configurar a porta em modo de transporte (tronco)

Pode ser configurado em apenas um dos lados, aqui configuramos na porta do CORE, os switches AC formarão o tronco automaticamente

Criando as interfaces VLAN que servirão de gateway para as redes de cada VLAN

Devem ser executados em modo usuário privilegiado *switch#*, esses comandos não funcionam em modo de configuração *switch(config)#*

Comandos de verificação:

```
sh vlan brief
sh running-config
sh interfaces trunk
```

Não se esqueça de configurar os computadores (IP, Máscara e o Gateway correto)





Quem sou eu? (Gustavo Kalau uai...)

Pai do Arthur, apaixonado por infraestrutura de TI, formado em Sistemas de Informação pela PUC MG, especialista em gestão de Infraestrutura de TI utilizando Software Livre e especialista em Redes de Computadores também pela PUC MG, atua há mais de 10 anos com redes de computadores e possui as seguintes certificações: CCIE R&S #60243, CCNAv3 R&S, CCNP R&S, CCDA, ITILv3F, MTA NF, JNCIA, AWS Associate: SysOps, Architect e Developer, LPIC-1 e LinuxEssentials e morando em Belo Horizonte.

Idealizador do treinamento CCNA/CCNP RiscoZero

A ideia do treinamento é passar o conteúdo da forma mais didática e diferente possível, fugindo do método de ensino chato.

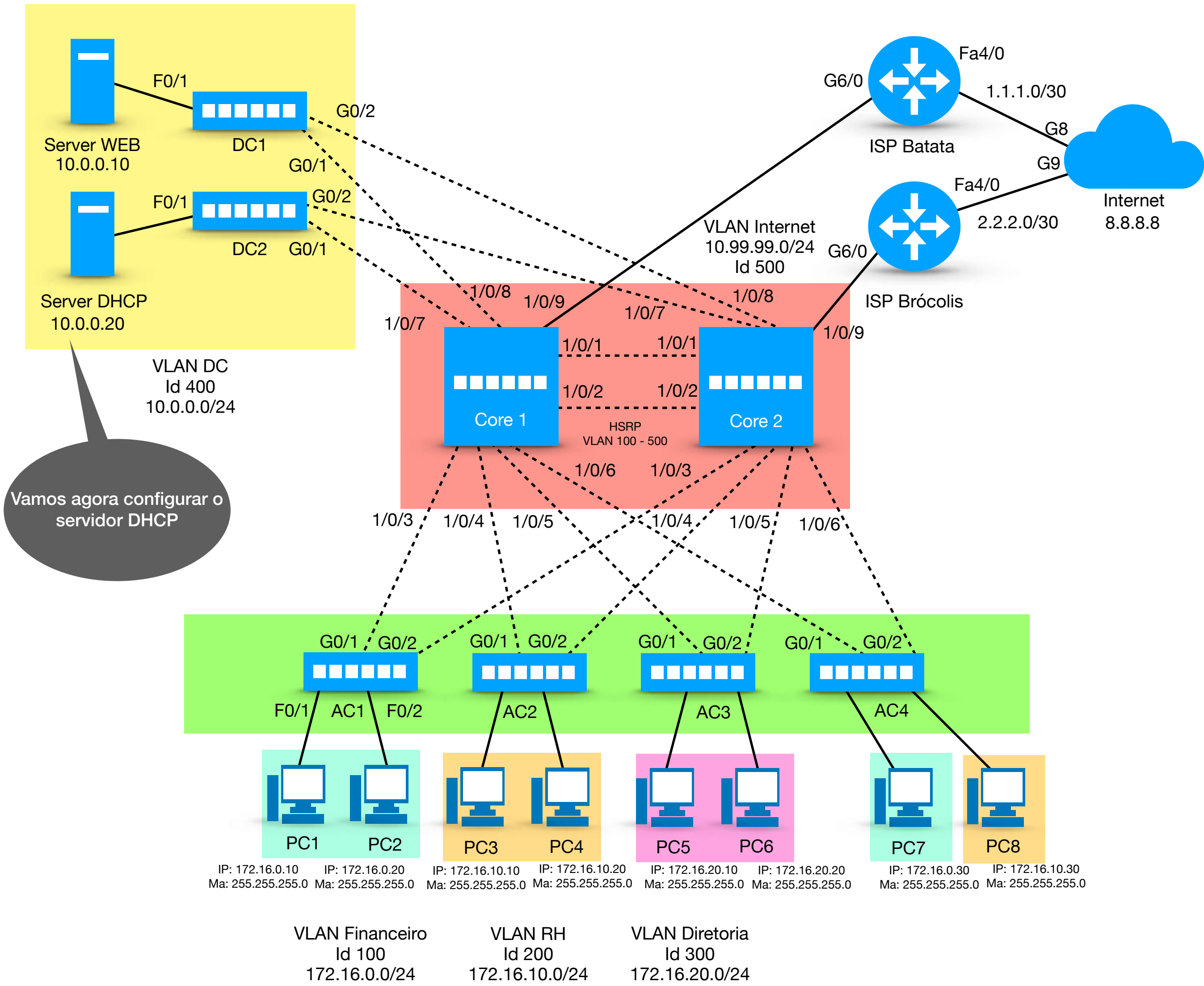
Além disso ao comprar o modo Risco Zero, o candidato tem uma segurança maior, pois se for reprovado, eu devolvo o dinheiro investido (descontado impostos e tarifas de operadora), o que dá ao aluno a chance de fazer a prova novamente, normalmente sem custo

Obrigado por acessar esse conteúdo e me ajude a espalhar conhecimento, compartilhe com seus amigos!



Olá pessoas! Sejam bem vindas! Na aula 5 iremos conhecer o serviço chamado DHCP/

Para entender como ele funciona teremos uma base teórica, lembrando que esse é curso para despertar interesse e não se trata de um curso completo, bora lá!



DHCP

O DHCP, Dynamic Host Configuration Protocol (protocolo de configuração dinâmica de host), é um protocolo que oferece configuração dinâmica de de endereços IP, máscara de sub-rede, default gateway (gateway padrão), DNS e outros atributos para dispositivos em rede.

Sem o DHCP teríamos que configurar o IP “na mão” em todos os dispositivos da rede, imagine o trabalho que daria em uma rede com 100 computadores, ou com 1000!

Um dispositivo precisa “descobrir” servidor DHCP em sua rede, para isso ele utiliza msgs broadcast, o que gera um problema se o servidor DHCP estiver em uma rede diferente (o que acontece 99% das vezes, o servidor fica na rede do Data Center e dispositivo em outra), roteadores não propagam broadcast de uma rede para outra, somente unicast.

Para resolver esse problema foi criado o DHCP RELAY, na Cisco é utilizado o comando ip helper-address



Configurações realizadas na aula 5

Entrar em modo de configuração

Criar VLAN e colocar um nome nela

Colocar uma interface em uma VLAN específica

Entrar em modo usuário privilegiado

Mudar o nome do dispositivo

Configurar uma interface

Salvar a configuração

Voltar para o mode usuário privilegiado

Sair do modo de configuração de VLAN

Switch DC2

en

conf t

hostname DC2

vlan 400

name DC

interface fastEthernet 0/1

switchport mode access

switchport access vlan 400

exit

interface vlan 400

ip add 10.0.0.1 255.255.255.0

end

wr

Criando a interface VLAN que servirá de gateway para a rede da VLAN do DC

Configurar a porta em modo de transporte (tronco)

Pode ser configurado em apenas um dos lados, aqui configuramos na porta do CORE, o switch DC2 formara o tronco automaticamente

Configurando o DHCP relay na interface VLAN da rede local da VLAN 100, esse comando serve para enviar as solicitações de DHCP que chegam dos PCs da VLAN 100 em formato broadcast para o servidor DHCP que está no DC, o relay transforma essa msgs em Unicast, permitindo assim o envio através de redes diferentes (lembre-se que o Roteador não propaga broadcast), sem o relay, teríamos que configurar um servidor DHCP em cada rede o que seria inviável.

Sua tarefa ness aula é configurar os demais relays e escopos DHCP, além de adicionar mais um PC em cada VLAN, esse novo PC deve receber IP de forma automática via DHCP

Switch CORE1

en

conf t

interface gigabitEthernet 1/0/7

switchport trunk encapsulation dot1q

switchport mode trunk

exit

interface vlan 100

ip helper-address 10.0.0.20

end

wr

gustavokalau.com.br

CCIE R&S

#60243



Quem sou eu? (Gustavo Kalau uai...)

Pai do Arthur, apaixonado por infraestrutura de TI, formado em Sistemas de Informação pela PUC MG, especialista em gestão de Infraestrutura de TI utilizando Software Livre e especialista em Redes de Computadores também pela PUC MG, atua há mais de 10 anos com redes de computadores e possui as seguintes certificações: CCIE R&S #60243, CCNAv3 R&S, CCNP R&S, CCDA, ITILv3F, MTA NF, JNCIA, AWS Associate: SysOps, Architect e Developer, LPIC-1 e LinuxEssentials e morando em Belo Horizonte.

Idealizador do treinamento CCNA/CCNP RiscoZero

A ideia do treinamento é passar o conteúdo da forma mais didática e diferente possível, fugindo do método de ensino chato.

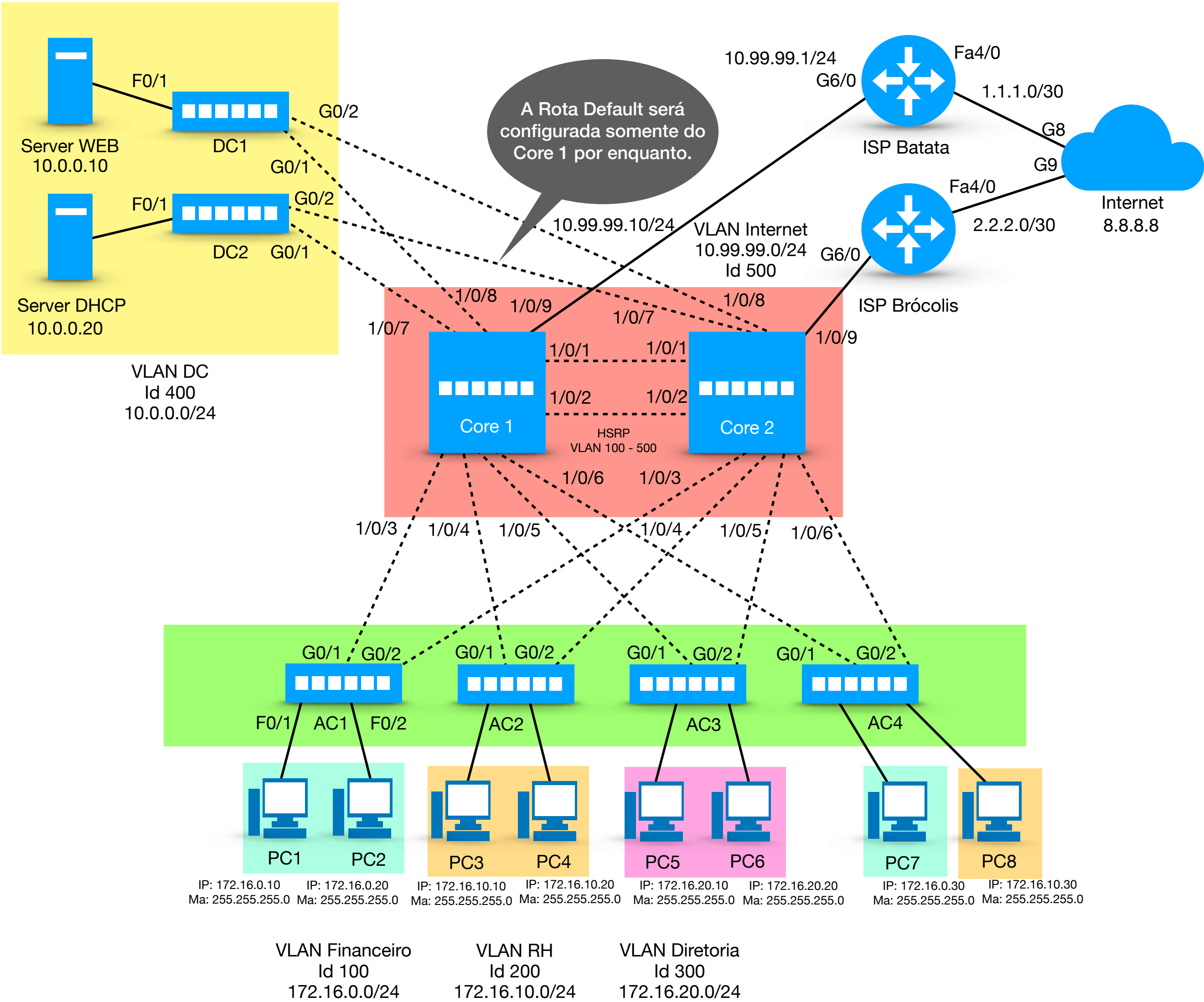
Além disso ao comprar o modo Risco Zero, o candidato tem uma segurança maior, pois se for reprovado, eu devolvo o dinheiro investido (descontado impostos e tarifas de operadora), o que dá ao aluno a chance de fazer a prova novamente, normalmente sem custo

Obrigado por acessar esse conteúdo e me ajude a espalhar conhecimento, compartilhe com seus amigos!



Olá pessoas! Sejam bem vindas! Na aula 6 iremos configurar uma rota estática.

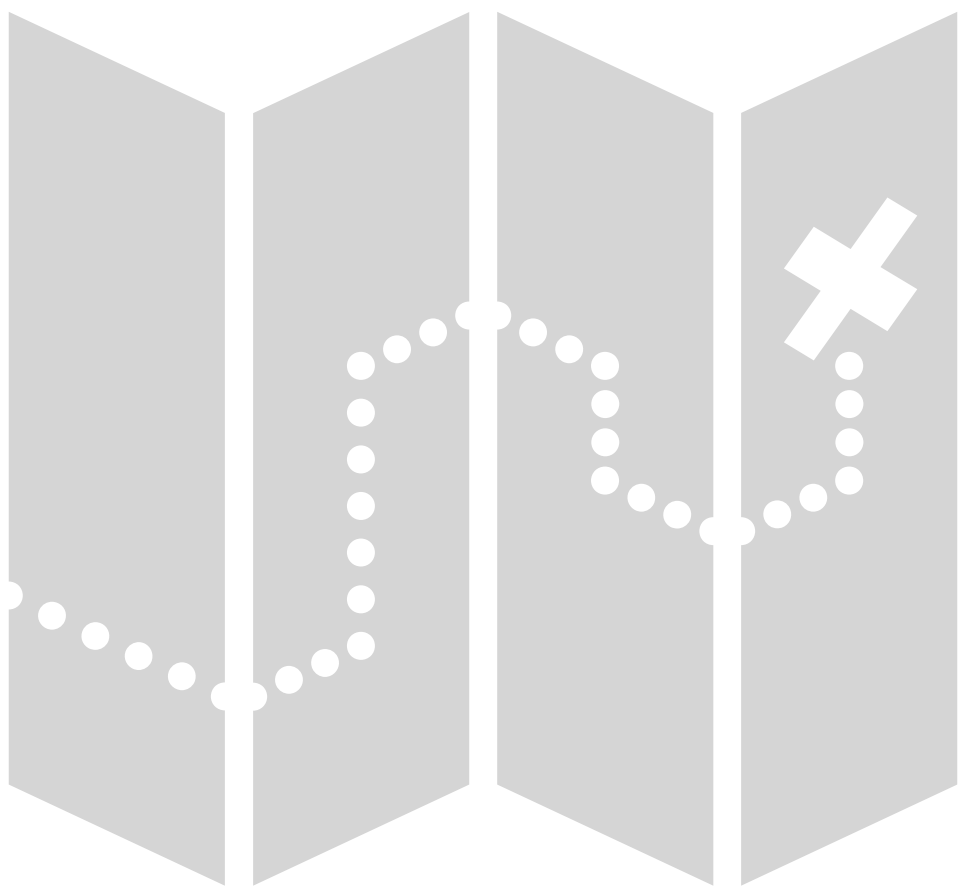
Para entender como ele funciona teremos uma base teórica, lembrando que esse é curso para despertar interesse e não se trata de um curso completo, bora lá!



Rota Default

Uma rota padrão (Default Route), também conhecida como “gateway de último recurso”, é a rota de rede utilizada por um roteador quando não há nenhuma outra rota conhecida existente para o endereço de destino de um pacote IP. Todos os pacotes para destinos desconhecidos pela tabela do roteador são enviados para o endereço de rota padrão. Esta rota geralmente direciona para outro roteador, que trata o pacote da mesma forma: Se a rota é conhecida, o pacote será direcionado para a rota conhecida. Se não, o pacote é direcionado para o “default route” desse roteador que geralmente direciona a outro roteador. E assim sucessivamente.

Fonte https://pt.wikipedia.org/wiki/Rota_padrão



Configurações realizadas na aula 6

```
AC2(config)#int f0/3
AC2(config-if)#switchport access vlan 200
AC2(config-if)#end
AC2#wr
```

Adicionar as portas F0/3 dos switches AC2 e AC3 nas respectivas VLANs

```
AC3(config)#int f0/3
AC3(config-if)#switchport access vlan 300
AC3(config-if)#end
AC3#wr
```

```
CORE1(config)#int vlan 200
CORE1(config-if)#ip helper-address 10.0.0.20
CORE1(config-if)#int vlan 300
CORE1(config-if)#ip helper-address 10.0.0.20
CORE1(config-if)#
```

Salvar a configuração

Configurar o DHCP relay para que os computadores nas VLANs 200 e 300 consigam pegar IP de forma dinâmica

```
Router(config)#hostname ISP-BATATA
ISP-BATATA(config)#interf g6/0
ISP-BATATA(config-if)#ip address 10.99.99.1 255.255.255.0
ISP-BATATA(config-if)#no shutdown
```

Configurar o IP na interface VLAN 500 que servirá de VLAN para conexão com os dispositivos do ISP

```
CORE1(config)#int vlan 500
CORE1(config-if)#ip address 10.99.99.10 255.255.255.0
CORE1(config-if)#no shutdown
CORE1(config-if)#exit
CORE1(config)#int g1/0/9
CORE1(config-if)#switchport mode access
CORE1(config-if)#switchport access vlan 500
CORE1(config-if)#exit
CORE1(config)#ip route 0.0.0.0 0.0.0.0 10.99.99.1
```

Adicionando a rota default, execute o comando IP ROUTE seguido de 0.0.0.0 que significa qualquer rede e depois outro 0.0.0.0 que significa qualquer máscara, por último temos o IP do próximo salto, ou seja, o IP para onde devemos enviar o tráfego.





Quem sou eu? (Gustavo Kalau uai...)

Pai do Arthur, apaixonado por infraestrutura de TI, formado em Sistemas de Informação pela PUC MG, especialista em gestão de Infraestrutura de TI utilizando Software Livre e especialista em Redes de Computadores também pela PUC MG, atua há mais de 10 anos com redes de computadores e possui as seguintes certificações: CCIE R&S #60243, CCNAv3 R&S, CCNP R&S, CCDA, ITILv3F, MTA NF, JNCIA, AWS Associate: SysOps, Architect e Developer, LPIC-1 e LinuxEssentials e morando em Belo Horizonte.

Idealizador do treinamento CCNA/CCNP RiscoZero

A ideia do treinamento é passar o conteúdo da forma mais didática e diferente possível, fugindo do método de ensino chato.

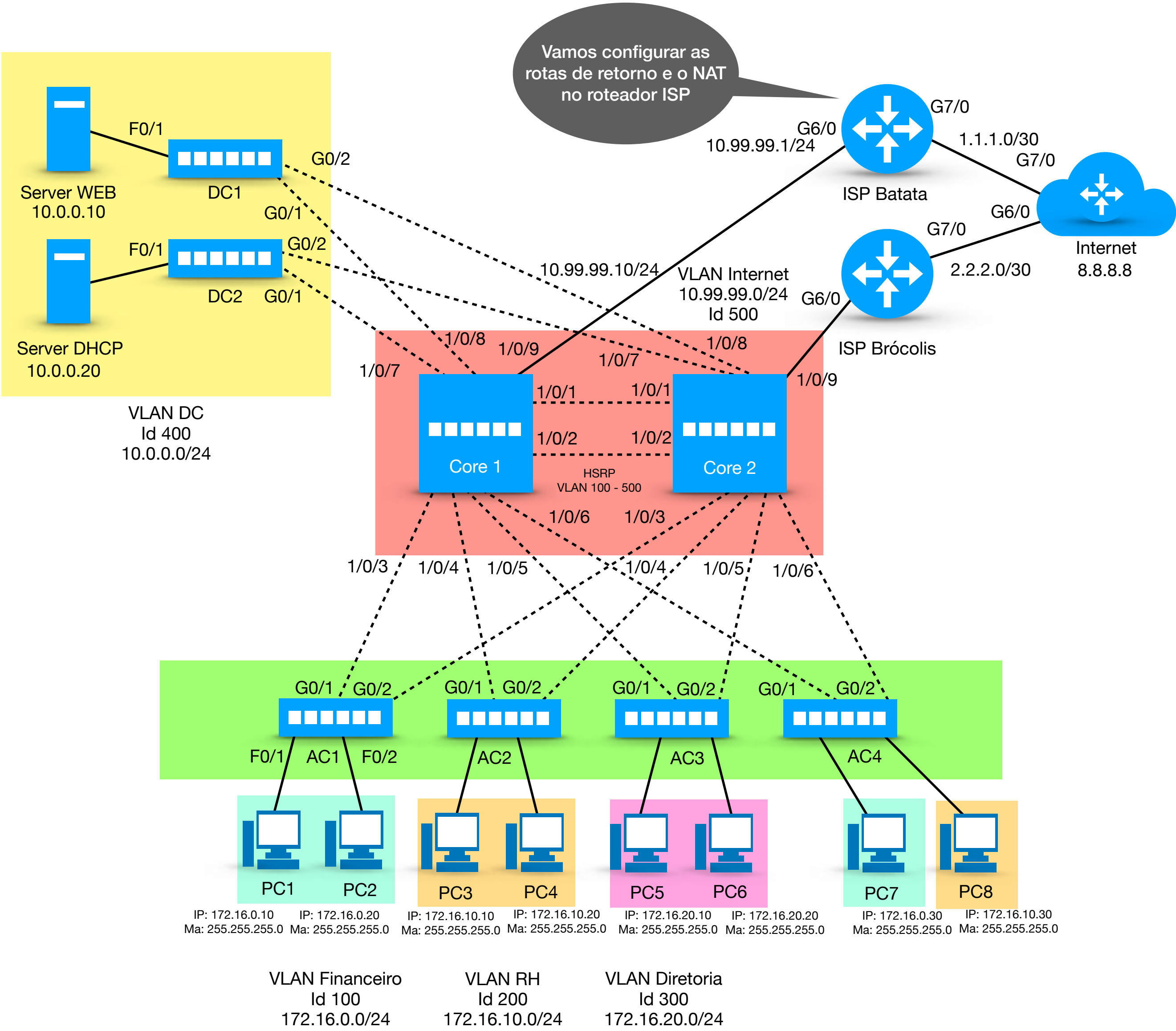
Além disso ao comprar o modo Risco Zero, o candidato tem uma segurança maior, pois se for reprovado, eu devolvo o dinheiro investido (descontado impostos e tarifas de operadora), o que dá ao aluno a chance de fazer a prova novamente, normalmente sem custo

Obrigado por acessar esse conteúdo e me ajude a espalhar conhecimento, compartilhe com seus amigos!



Olá pessoas! Sejam bem vindas! Na aula 6 iremos configurar uma rota estática.

Para entender como ele funciona teremos uma base teórica, lembrando que esse é curso para despertar interesse e não se trata de um curso completo, bora lá!



NAT

Por se tratar de uma rede privada, os números de IP interno da rede (como 10.0.0.0/8, 172.16.0.0/12 e 192.168.0.0/16) nunca poderiam ser passados para a Internet pois não são roteados nela e o computador que recebesse um pedido com um desses números não saberia para onde enviar a resposta. Sendo assim, os pedidos teriam de ser gerados com um IP global do router. Mas quando a resposta chegasse ao router, seria preciso saber a qual dos computadores presentes na LAN pertencia aquela resposta.

A solução encontrada foi fazer um mapeamento baseado no IP interno e na porta local do computador. Com esses dois dados o NAT gera um número de 16 bits usando a tabela hash, este número é então escrito no campo da porta de origem.

O pacote enviado para fora leva o IP global do router e na porta de origem o número gerado pelo NAT. Desta forma o computador que receber o pedido sabe para onde tem de enviar a resposta. Quando o router recebe a resposta faz a operação inversa, procurando na sua tabela uma entrada que corresponda aos bits do campo da porta. Ao encontrar a entrada, é feito o direcionamento para o computador correto dentro da rede privada.

Esta foi uma medida de reação face à previsão da exaustão do espaço de endereçamento IP, e rapidamente adaptada para redes privadas também por questões econômicas (no início da Internet os endereços IP alugavam-se, quer individualmente quer por classes/grupos).

https://pt.wikipedia.org/wiki/Network_address_translation



Configurações realizadas na aula 7

Roteadores utilizados na aula:

PT-Router

Interfaces utilizadas nos roteadores:

NM-1CGE

ISP-BATATA:

Habilitando a Interface Interna (rede local) para o NAT

Habilitando a Interface Externa (Internet) para o NAT

Criando um grupo (ACL) para ser usado no NAT, basicamente essa ACL permite que qualquer IP seja nateado

O comando NAT inside indica que vc quer utilizar o NAT de “dentro para fora” da sua rede

Tudo que bater na ACL 1 será permitido, ou seja, qualquer IP

Tudo que vier da rede interna terá seu IP de origem alterado para o IP da interface G7/0

```
interface GigabitEthernet6/0
 ip nat inside
!
interface GigabitEthernet7/0
 ip address 1.1.1.1 255.255.255.252
 ip nat outside
!
access-list 1 permit any
!
ip nat inside source list 1 interface GigabitEthernet7/0 overload
!
!
ip route 172.16.0.0 255.255.255.0 10.99.99.10
ip route 172.16.10.0 255.255.255.0 10.99.99.10
ip route 172.16.20.0 255.255.255.0 10.99.99.10
ip route 10.0.0.0 255.255.255.0 10.99.99.10
ip route 0.0.0.0 0.0.0.0 1.1.1.2
```

INTERNET

```
hostname INTERNET

interface Loopback0
 ip address 8.8.8.8 255.255.255.0
!
interface GigabitEthernet7/0
 ip address 1.1.1.2 255.255.255.252
```





Quem sou eu? (Gustavo Kalau uai...)

Pai do Arthur, apaixonado por infraestrutura de TI, formado em Sistemas de Informação pela PUC MG, especialista em gestão de Infraestrutura de TI utilizando Software Livre e especialista em Redes de Computadores também pela PUC MG, atua há mais de 10 anos com redes de computadores e possui as seguintes certificações: CCIE R&S #60243, CCNAv3 R&S, CCNP R&S, CCDA, ITILv3F, MTA NF, JNCIA, AWS Associate: SysOps, Architect e Developer, LPIC-1 e LinuxEssentials e morando em Belo Horizonte.

Idealizador do treinamento CCNA/CCNP RiscoZero

A ideia do treinamento é passar o conteúdo da forma mais didática e diferente possível, fugindo do método de ensino chato.

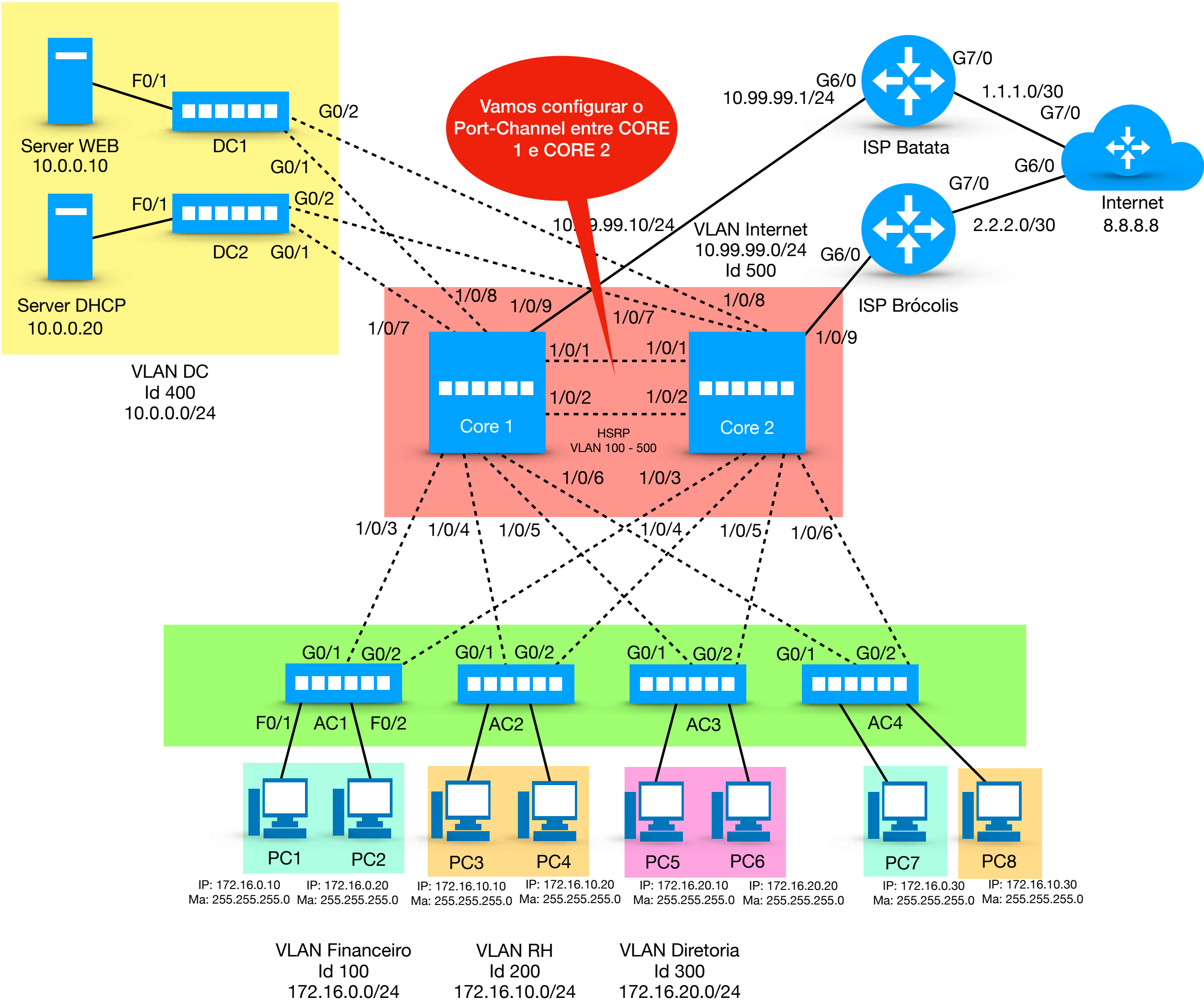
Além disso ao comprar o modo Risco Zero, o candidato tem uma segurança maior, pois se for reprovado, eu devolvo o dinheiro investido (descontado impostos e tarifas de operadora), o que dá ao aluno a chance de fazer a prova novamente, normalmente sem custo

Obrigado por acessar esse conteúdo e me ajude a espalhar conhecimento, compartilhe com seus amigos!



Olá pessoas! Sejam bem vindas! Na aula 8 iremos configurar uma rota estática.

Para entender como ele funciona teremos uma base teórica, lembrando que esse é curso para despertar interesse e não se trata de um curso completo, bora lá!



EtherChannel

A ideia aqui é juntar várias interfaces físicas em uma interface lógica, fazemos isso para “enganar” o switch e evitar que caminhos alternativos sejam bloqueados pelos Spanning-tree, dessa forma teremos mais banda e e nenhum caminho ficará bloqueado, essa configuração só pode ser feita entre pares de switches (existe também o VPC que pode ser feito entre trios de switches mas faz parte do escopo de Data Center).

Basicamente temos duas formas de trabalhar com o Etherchannel, onde teríamos dois padrões:

- LACP (Link Aggregation Control Protocol): Protocolo padrão IEEE, disponível quase todos switches gerenciáveis.
- PAgP (Port Aggregation Protocol): Protocolo disponível em equipamentos Cisco

Temos configurar ambas as pontas no mesmo padrão, senão se uma determinada ponta ficar em padrão distinto nosso canal etherchannel não irá negociar



Configurações realizadas na aula 8

```
CORE 1 e CORE 2
```

```
en
```

```
conf t
```

```
interface range g1/0/1 - 2
```

```
channel-group 1 mode active
```

Criando a interface Port-channel 1

Utilizando o protocolo LACP

```
show etherchannel summary
```

Para verificar o Port-Channel





Quem sou eu? (Gustavo Kalau uai...)

Pai do Arthur, apaixonado por infraestrutura de TI, formado em Sistemas de Informação pela PUC MG, especialista em gestão de Infraestrutura de TI utilizando Software Livre e especialista em Redes de Computadores também pela PUC MG, atua há mais de 10 anos com redes de computadores e possui as seguintes certificações: CCIE R&S #60243, CCNAv3 R&S, CCNP R&S, CCDA, ITILv3F, MTA NF, JNCIA, AWS Associate: SysOps, Architect e Developer, LPIC-1 e LinuxEssentials e morando em Belo Horizonte.

Idealizador do treinamento CCNA/CCNP RiscoZero

A ideia do treinamento é passar o conteúdo da forma mais didática e diferente possível, fugindo do método de ensino chato.

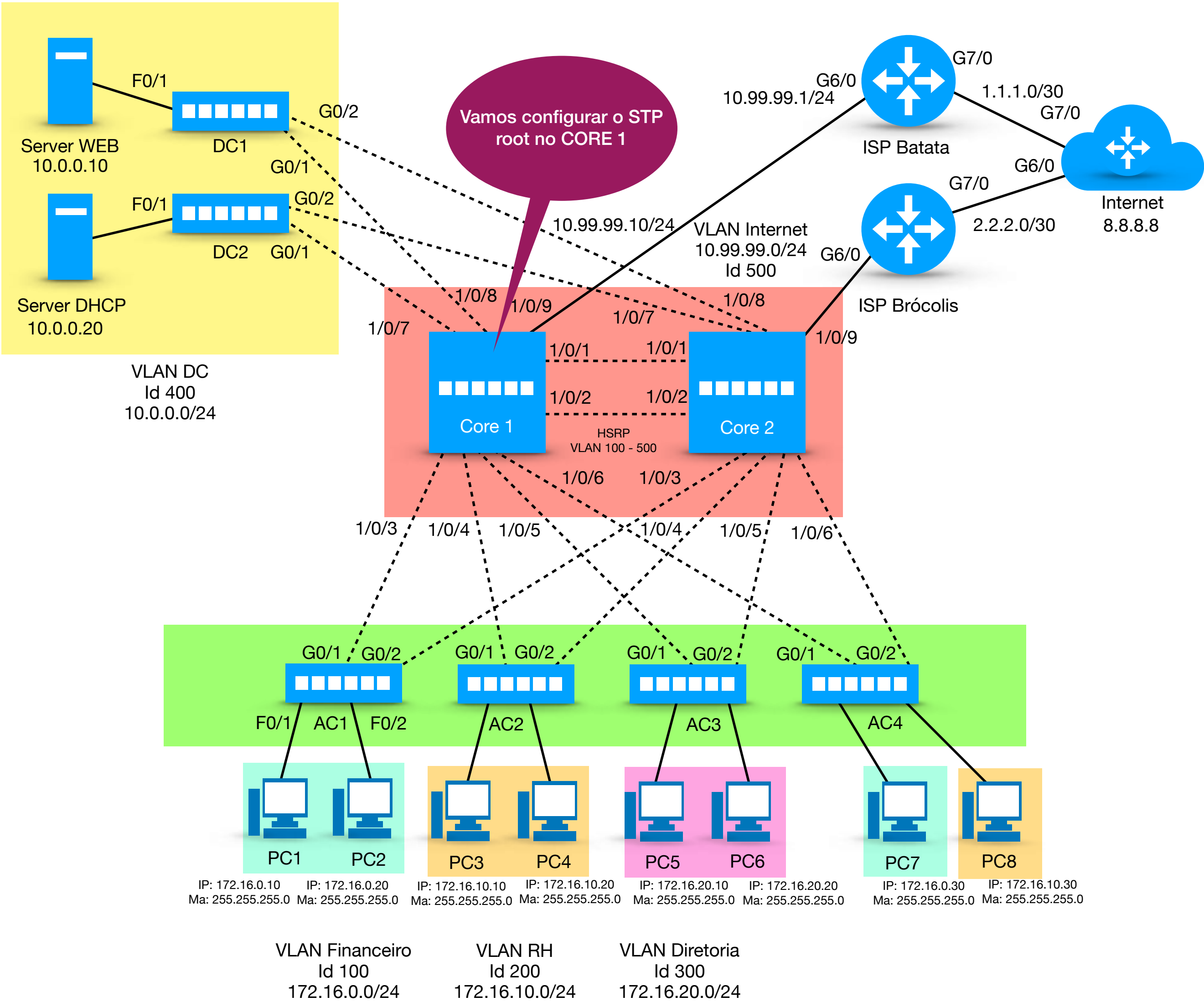
Além disso ao comprar o modo Risco Zero, o candidato tem uma segurança maior, pois se for reprovado, eu devolvo o dinheiro investido (descontado impostos e tarifas de operadora), o que dá ao aluno a chance de fazer a prova novamente, normalmente sem custo

Obrigado por acessar esse conteúdo e me ajude a espalhar conhecimento, compartilhe com seus amigos!



Olá pessoas! Sejam bem vindas! Na aula 9 iremos configurar o STP root no sw CORE 1.

Para entender como ele funciona teremos uma base teórica, lembrando que esse é curso para despertar interesse e não se trata de um curso completo, bora lá!



Spanning-Tree Protocol (STP)

Spanning Tree Protocol (STP) é um protocolo para equipamentos de rede que permite resolver problemas de loop em redes comutadas (ligações entre switches) cuja topologia introduza anéis nas ligações, auxiliando na melhor performance da rede.

O protocolo STP possibilita a inclusão de ligações redundantes entre os switches, provendo caminhos alternativos no caso de falha de uma dessas ligações. Nesse contexto, ele serve para evitar a formação de loops entre os switches e permitir a ativação e desativação automática dos caminhos alternativos.



Configurações realizadas na aula 9

CORE 1

```
spanning-tree vlan 100,200 priority 0
```

CORE 2

```
spanning-tree vlan 100,200 priority 4096
```

Alterando a prioridade STP das VLANs 100 e 200 para 0 no CORE 1(a melhor prioridade possível)

Alterando a prioridade STP das VLANs 100 e 200 para 4096 no CORE 2 (a segunda melhor prioridade possível)

```
CORE1#show spanning-tree vlan 100
```

```
VLAN0100
Spanning tree enabled protocol ieee
Root ID    Priority    100
           Address      0010.11C9.5DC4
           This bridge is the root
           Hello Time  2 sec    Max Age 20 sec    Forward Delay 15 sec

Bridge ID  Priority    100 (priority 0 sys-id-ext 100)
           Address      0010.11C9.5DC4
           Hello Time  2 sec    Max Age 20 sec    Forward Delay 15 sec
           Aging Time   20
```

Isso significa que o CORE 1 é o STP Root da vlan 100

Interface	Role	Sts	Cost	Prio.Nbr	Type
-----	----	---	-----	-----	
Gi1/0/4	Desg	FWD	4	128.4	P2p
Gi1/0/7	Desg	FWD	4	128.7	P2p
Gi1/0/3	Desg	FWD	4	128.3	P2p
Gi1/0/5	Desg	FWD	4	128.5	P2p
Gi1/0/6	Desg	FWD	4	128.6	P2p
Po1	Desg	FWD	3	128.29	Shr





Quem sou eu? (Gustavo Kalau uai...)

Pai do Arthur, apaixonado por infraestrutura de TI, formado em Sistemas de Informação pela PUC MG, especialista em gestão de Infraestrutura de TI utilizando Software Livre e especialista em Redes de Computadores também pela PUC MG, atua há mais de 10 anos com redes de computadores e possui as seguintes certificações: CCIE R&S #60243, CCNAv3 R&S, CCNP R&S, CCDA, ITILv3F, MTA NF, JNCIA, AWS Associate: SysOps, Architect e Developer, LPIC-1 e LinuxEssentials e morando em Belo Horizonte.

Idealizador do treinamento CCNA/CCNP RiscoZero

A ideia do treinamento é passar o conteúdo da forma mais didática e diferente possível, fugindo do método de ensino chato.

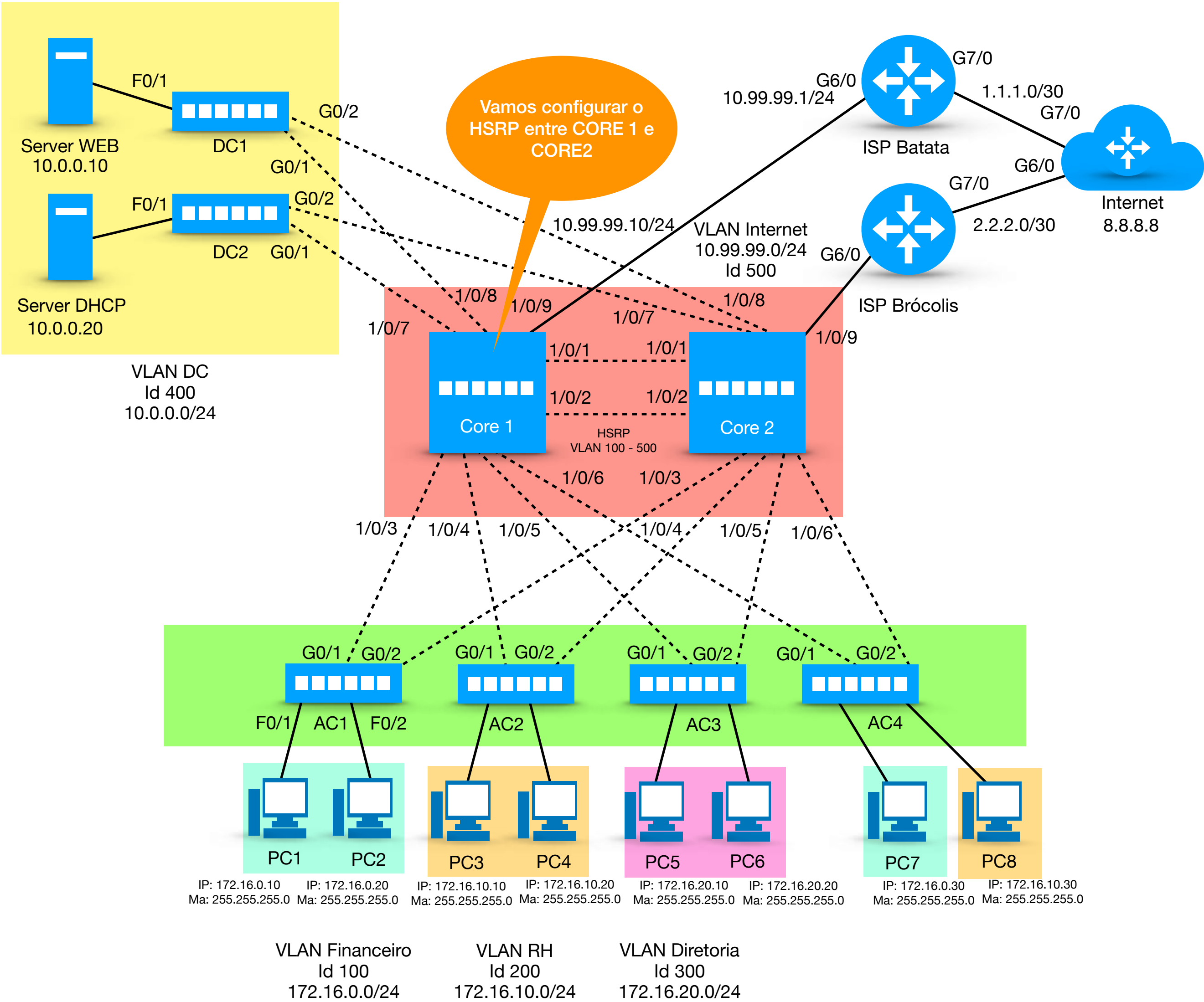
Além disso ao comprar o modo Risco Zero, o candidato tem uma segurança maior, pois se for reprovado, eu devolvo o dinheiro investido (descontado impostos e tarifas de operadora), o que dá ao aluno a chance de fazer a prova novamente, normalmente sem custo

Obrigado por acessar esse conteúdo e me ajude a espalhar conhecimento, compartilhe com seus amigos!



Olá pessoas! Sejam bem vindas! Na aula 10 iremos configurar o HSRP no CORE 1 e CORE 2.

Para entender como ele funciona teremos uma base teórica, lembrando que esse é curso para despertar interesse e não se trata de um curso completo, bora lá!



Hot Standby Router Protocol (HSRP)

Quando alta disponibilidade se torna uma necessidade, utilizamos os First Hop Redundancy Protocols (FHRPs) que nos permitem configurar mais de um roteador físico para agir como se fossem logicamente um. Existem protocolos proprietários como HSRP, GLBP e VRRP que é um protocolo definido pelo IEEE.

Falaremos hoje sobre o Hot Standby Router Protocol (HSRP), desenvolvido pela Cisco, e que é utilizado para fornecer redundância de gateway em redes locais.

Geralmente rodando na camada de distribuição, o HSRP utiliza endereço MAC e IP virtuais compartilhado pelos membros do grupo HSRP, que deve conter um Active Router (responsável por realizar o encaminhamento dos pacotes) e um ou mais Standby Router, que assumirá o papel de Active somente em caso de falha. O HSRP não foi projetado para ser um substituto para os protocolos de roteamento dinâmico e eles devem ser utilizados sempre que possível.

Fonte: <https://brainwork.com.br/2017/01/03/hsrp-ha>



Configurações realizadas na aula 10

```
CORE 1

interface Vlan100
ip address 172.16.0.2 255.255.255.0
standby 100 ip 172.16.0.1
standby 100 priority 120
standby 100 preempt
```

Alteramos o IP “real” da interface

O Comando STANBY configura o HSRP na interface:
Primeiro configuramos o IP que será o IP virtual que flutuará entre os participantes do grupo HSRP

No CORE1 alteramos a prioridade para 120, o equipamento que tiver a maior prioridade será o MASTER HSRP, isso significa que ele assumirá o VIP e será então o gateway dessa rede

O comando preempt indica para o CORE1 tomar de volta o VIP caso retorne de alguma queda (se a prioridade dele for maior)

```
CORE 2

interface Vlan100
ip address 172.16.0.3 255.255.255.0
standby 100 ip 172.16.0.1
```

Verificando o HSRP, nesse caso o CORE 1 é o Master (active = local)

```
CORE1#sh standby brief
                P indicates configured to preempt.
                |
Interface      Grp  Pri  P State      Active      Standby      Virtual IP
Vl100          100  120  P Active     local       172.16.0.3   172.16.0.1
```





Quem sou eu? (Gustavo Kalau uai...)

Pai do Arthur, apaixonado por infraestrutura de TI, formado em Sistemas de Informação pela PUC MG, especialista em gestão de Infraestrutura de TI utilizando Software Livre e especialista em Redes de Computadores também pela PUC MG, atua há mais de 10 anos com redes de computadores e possui as seguintes certificações: CCIE R&S #60243, CCNAv3 R&S, CCNP R&S, CCDA, ITILv3F, MTA NF, JNCIA, AWS Associate: SysOps, Architect e Developer, LPIC-1 e LinuxEssentials e morando em Belo Horizonte.

Idealizador do treinamento CCNA/CCNP RiscoZero

A ideia do treinamento é passar o conteúdo da forma mais didática e diferente possível, fugindo do método de ensino chato.

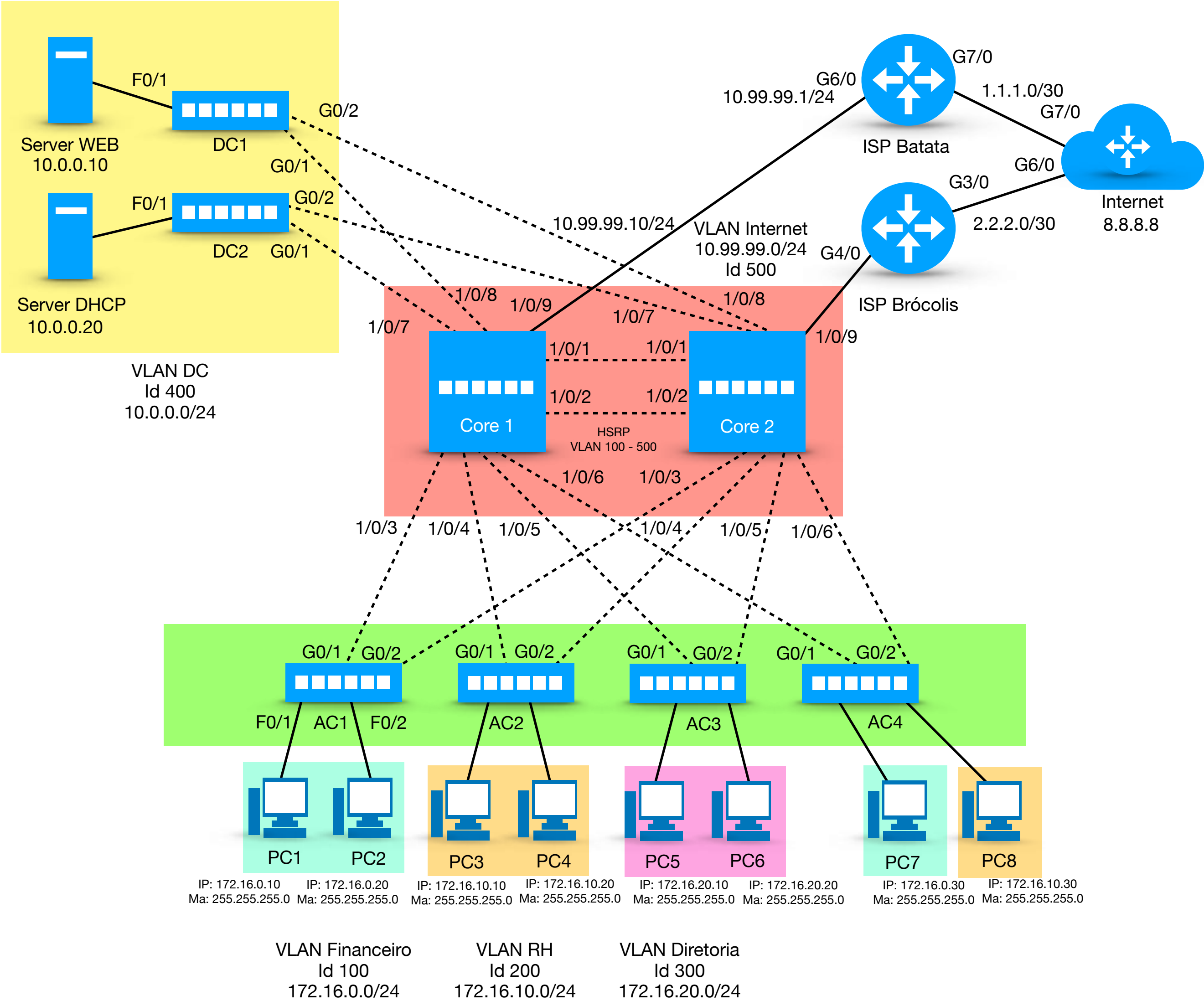
Além disso ao comprar o modo Risco Zero, o candidato tem uma segurança maior, pois se for reprovado, eu devolvo o dinheiro investido (descontado impostos e tarifas de operadora), o que dá ao aluno a chance de fazer a prova novamente, normalmente sem custo

Obrigado por acessar esse conteúdo e me ajude a espalhar conhecimento, compartilhe com seus amigos!



Olá pessoas! Sejam bem vindas! Na aula 11 iremos juntar todas as peças e testar nossas configs.

Para entender como ele funciona teremos uma base teórica, lembrando que esse é curso para despertar interesse e não se trata de um curso completo, bora lá!



Configurações realizadas na aula 11

```
CORE 1

interface Vlan100
 ip address 172.16.0.2 255.255.255.0
 ip helper-address 10.0.0.20
 standby version 2
 standby 100 ip 172.16.0.1
 standby 100 priority 120
 standby 100 preempt
!
interface Vlan200
 ip address 172.16.10.2 255.255.255.0
 ip helper-address 10.0.0.20
 standby version 2
 standby 200 ip 172.16.10.1
 standby 200 priority 120
 standby 200 preempt
!
interface Vlan300
 ip address 172.16.20.2 255.255.255.0
 ip helper-address 10.0.0.20
 standby version 2
 standby 300 ip 172.16.20.1
 standby 300 priority 120
 standby 300 preempt
!
interface Vlan400
 ip address 10.0.0.2 255.255.255.0
 standby version 2
 standby 400 ip 10.0.0.1
 standby 400 priority 120
 standby 400 preempt
```

```
CORE 2

interface Vlan100
 ip address 172.16.0.3 255.255.255.0
 standby version 2
 standby 100 ip 172.16.0.1
!
interface Vlan200
 ip address 172.16.10.3 255.255.255.0
 standby version 2
 standby 200 ip 172.16.10.1
!
interface Vlan300
 ip address 172.16.20.3 255.255.255.0
 standby version 2
 standby 300 ip 172.16.20.1
!
interface Vlan400
 ip address 10.0.0.3 255.255.255.0
 standby version 2
 standby 400 ip 10.0.0.1
!
interface Vlan500
 ip address 10.99.99.11 255.255.255.0
!
ip routing
ip route 0.0.0.0 0.0.0.0 10.99.99.2
!
interface GigabitEthernet1/0/9
 switchport access vlan 500
 switchport mode access
```



Configurações realizadas na aula 11

```
ISP-BROCOLIS
```

```
interface GigabitEthernet3/0
 ip address 2.2.2.1 255.255.255.252
 ip nat outside
!
interface GigabitEthernet4/0
 ip address 10.99.99.2 255.255.255.0
 ip nat inside

access-list 1 permit any

ip nat inside source list 1 interface GigabitEthernet3/0 overload

ip route 172.16.0.0 255.255.255.0 10.99.99.11
ip route 172.16.10.0 255.255.255.0 10.99.99.11
ip route 172.16.20.0 255.255.255.0 10.99.99.11
```

```
Internet
```

```
interface GigabitEthernet6/0
 ip address 2.2.2.2 255.255.255.252
!
ip route 10.0.0.0 255.255.255.0 10.99.99.11
ip route 0.0.0.0 0.0.0.0 2.2.2.2
```





Quem sou eu? (Gustavo Kalau uai...)

Pai do Arthur, apaixonado por infraestrutura de TI, formado em Sistemas de Informação pela PUC MG, especialista em gestão de Infraestrutura de TI utilizando Software Livre e especialista em Redes de Computadores também pela PUC MG, atua há mais de 10 anos com redes de computadores e possui as seguintes certificações: CCIE R&S #60243, CCNAv3 R&S, CCNP R&S, CCDA, ITILv3F, MTA NF, JNCIA, AWS Associate: SysOps, Architect e Developer, LPIC-1 e LinuxEssentials e morando em Belo Horizonte.

Idealizador do treinamento CCNA/CCNP RiscoZero

A ideia do treinamento é passar o conteúdo da forma mais didática e diferente possível, fugindo do método de ensino chato.

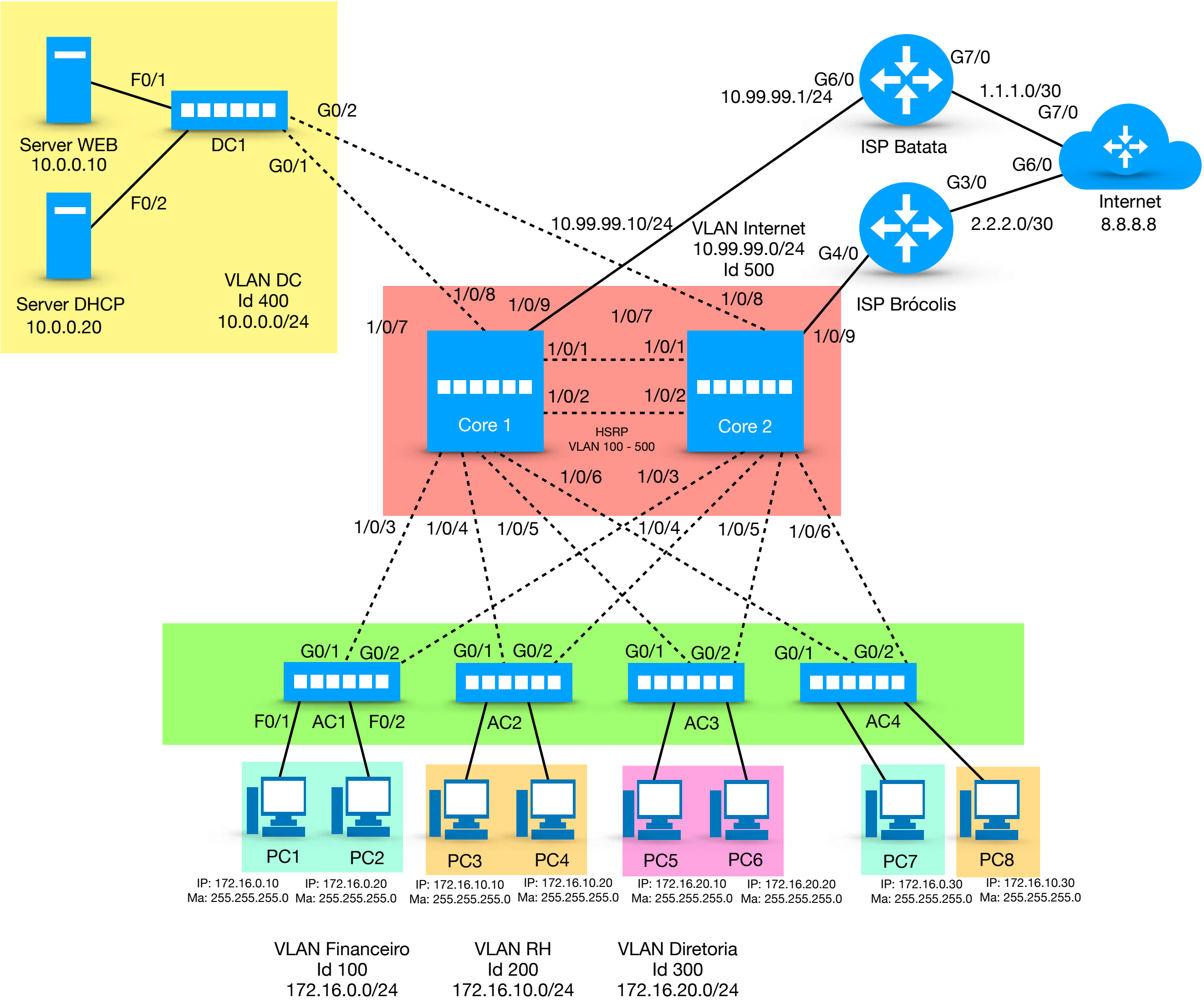
Além disso ao comprar o modo Risco Zero, o candidato tem uma segurança maior, pois se for reprovado, eu devolvo o dinheiro investido (descontado impostos e tarifas de operadora), o que dá ao aluno a chance de fazer a prova novamente, normalmente sem custo

Obrigado por acessar esse conteúdo e me ajude a espalhar conhecimento, compartilhe com seus amigos!



Olá pessoas! Sejam bem vindas! Na aula 12 iremos fazer uma revisão do que foi apresentado e vamos configurar uma ACL.

Para entender como ele funciona teremos uma base teórica, lembrando que esse é curso para despertar interesse e não se trata de um curso completo, bora lá!



Access Control Lists ou, em bom Português: listas de controle de acesso. OK... mas acesso de quem???

Acesso de pacotes IP, basicamente. Mas como pacotes IP transportam qualquer tipo de informação em uma rede, as ACLs controlam o acesso de TUDO e de TODOS! Quando você tenta acessar um router via Telnet, por exemplo, este acesso nada mais é do que uma série de pacotes IP, certo? Routers (e switches que suportem ACLs) podem permitir ou negar que determinados pacotes o atravessem.

Existem apenas 2 parâmetros quando configuramos uma ACL: PERMIT ou DENY. Estes parâmetros são seguidos das definições DO QUE se deve permitir (PERMIT) ou negar (DENY). Estas, basicamente, são as opções:

- ANY (tudo)
- HOST [IP do host]
- [subrede + wildcard]
- [protocolo]

Quando se trata de ACLs, os equipamentos Cisco trabalham com o conceito de negar tudo e permitir somente o que lhes for informado. Ou seja, TODA ACL criada em um roteador Cisco termina com um DENY ANY implícito, negando TUDO, à todos. Por este motivo, é preciso ter muito cuidado com a aplicação de uma ACL, pois se ela for mal planejada poderá isolar uma (ou várias) redes de uma só vez, inclusive impedindo o acesso ao router via Telnet, o que o impedirá de reverter a situação.

Fonte (veja o post completo no blog do Marco, vale a pena): <https://blog.ccna.com.br/2007/10/21/tutorial-basico-acls-para-o-exame-ccna/>



Configurações realizadas na aula 12

CORE 1

```
interface Vlan400
 ip access-group 100 out
!
access-list 100 deny tcp 172.16.0.0 0.0.0.255 host 10.0.0.30 eq www
access-list 100 deny tcp 172.16.0.0 0.0.0.255 host 10.0.0.30 eq 443
access-list 100 permit ip any any
```

Aplica a ACL criada na interface VLAN 400 e no sentido OUT

ACL criada que impede que a rede 172.16.0.0/24 que impede acesso ao host 10.0.0.30 nas portas 80 e 443 (HTTP) e (HTTPS)

DC2

```
interface FastEthernet0/2
 switchport access vlan 400
 switchport mode access
```

Porta do servidor WEB colocada na VLAN400





Quem sou eu? (Gustavo Kalau uai...)

Pai do Arthur, apaixonado por infraestrutura de TI, formado em Sistemas de Informação pela PUC MG, especialista em gestão de Infraestrutura de TI utilizando Software Livre e especialista em Redes de Computadores também pela PUC MG, atua há mais de 10 anos com redes de computadores e possui as seguintes certificações: CCIE R&S #60243, CCNAv3 R&S, CCNP R&S, CCDA, ITILv3F, MTA NF, JNCIA, AWS Associate: SysOps, Architect e Developer, LPIC-1 e LinuxEssentials e morando em Belo Horizonte.

Idealizador do treinamento CCNA/CCNP RiscoZero

A ideia do treinamento é passar o conteúdo da forma mais didática e diferente possível, fugindo do método de ensino chato.

Além disso ao comprar o modo Risco Zero, o candidato tem uma segurança maior, pois se for reprovado, eu devolvo o dinheiro investido (descontado impostos e tarifas de operadora), o que dá ao aluno a chance de fazer a prova novamente, normalmente sem custo

Obrigado por acessar esse conteúdo e me ajude a espalhar conhecimento, compartilhe com seus amigos!

