

FCEE
25/05/2025

RELATÓRIO

Redes e Comunicação de Dados

Projeto Packet Tracer



Discentes

Aashish Kumar Thapa (2024623)
Cláudio Fernandes (2186622)

Docentes

Lina Maria Pestana Leão de Brito
Lisandro Henrique Gouveia de Olim Marote

Resumo

Neste trabalho o principal objetivo é implementar uma rede nacional em contexto virtual. A rede é constituída pelas ilhas (Madeira e Açores) e por Portugal Continental, tendo cada região a sua respetiva rede e sendo possível fazer a ligação com outra através da Internet.

Na Internet temos *routers* de uma certa operadora de telecomunicações (Nos, Meo e Vodafone) , em que cada uma está conectada a uma certa área. Estes *routers* vão ser os principais responsáveis por conectar todas as redes. Existe também um router principal que está diretamente associado aos três routers das operadoras e a duas redes adicionais , uma com um servidor *DNS* e outra com um servidor *WEB* , em que a principal função é que se consiga através de qualquer computador aceder ao *site* listado no servidor *DNS*.

Para cada combinação de pares dos *routers* da Internet, existe uma rede própria (*WAN*) que é uma rede de longo alcance que serve para ligar redes que englobam áreas grandes. No nosso caso temos 5 conexões entre *routers ISP*'s e um *router AWS* e 3 entre um *router ISP* e o respetivo *router* da região.

Para cada rede (*LAN*) que é uma rede de curto alcance, existem 6 sub-redes (*Vlan's*) com diferentes *ids*: 10 (*Printers*) , 15 (*lot*) , 55 (Atendimento) , 90 (*Wireless*) , 130 (Servidores ou Contabilidade) e 500 (Gestão).

Permitem agrupar dispositivos iguais/semelhantes numa rede própria mas não isolada , pois através da criação de sub-interfaces no *Router* da rede principal permitem com que todos se comuniquem, de maneira fluida e eficaz.

Em todas as regiões , existe um número de *hosts* mínimo obrigatório para cada sub-rede, que será respeitado através do comprimento do prefixo da máscara de sub-rede, em que se identifica através da compreensão do seu número, o número de hosts disponíveis para cada uma. Por exemplo /30, corresponde à máscara de sub-rede 255.255.255.252, estando disponíveis 2 *ip*'s para *hosts* (dispositivos finais) e ficando 1 *ip* para a identificação da rede e outro para *broadcast*. De notar que o número de *hosts* não é igual em sub-redes iguais em diferentes redes. De esclarecer também que neste projeto só é usado o tipo de endereçamento IPv4 , que significa que cada *ip* tem um valor que corresponde a uma palavra de 32 *bits* dividida em 4 *bytes*.

Para um melhor aproveitamento do número de *hosts* , não desperdiçando assim *ip*'s que não são necessários, utilizou-se o método de *subnetting VLSM* (máscara de sub-rede com comprimento variado) , para as redes Madeira e Açores, ficando o Continente com o método *subnetting standard* em que a máscara de sub-rede é igual para todos os dispositivos da rede. Já com o *VLSM* observando o número de *hosts*, é possível “ajustar” a máscara de sub-rede de acordo com o número de *hosts* necessários. Para chegar a uma distribuição eficiente e lógica dos *ips* , realizou-se vários cálculos, principalmente no método *subnetting VLSM* , pois o método *standard* é trivial. Através das tabelas de endereçamento dos dispositivos e de cada sub-rede, é possível identificar todos os *ip*'s presentes no nosso trabalho, a sua respetiva máscara e o seu *gateway* padrão (endereço *ip* da *sub-interface* presente no *router* da rede). Estas *sub-interfaces* servem para que se

consiga comunicar com diferentes *vlan*'s de forma eficiente, sendo que caso não existissem a conexão não seria possível. Obviamente também servem como uma fonte de saída de algum tipo de mensagem por parte de um dispositivo da rede, para outra rede, através do *router* que possui essas *interfaces*. Como sabemos este funciona como uma “ponte” para a passagem de um sinal, pois a sua principal função é ligar redes diferentes e transmitir os dados sem qualquer perda de informação. Uma nota importante é que é usado o primeiro *ip* de cada sub-rede como *gateway* padrão e que todos os *ip*'s das redes são privados, sendo assim necessário configurar a *Nat* para que transforme esses *ip*'s privados em públicos com a finalidade dos equipamentos comunicarem entre si em diferentes redes, pois a *Internet* (obrigatória a passagem por ela para aceder a um dispositivo noutra rede) só lida com endereços *ip*'s públicos.

Algo que é bastante usado, para verificarmos a conexão entre algum dispositivo de uma rede com outro noutra, é uma mensagem em formato de *PDU* (Unidade de dados de protocolo) executada pelo protocolo *ICMP*, por exemplo o famoso “*PING*” é feito por este protocolo. É muito útil, pois assegura que existe uma conexão entre dois dispositivos, etapa fundamental para o desenvolvimento deste projeto.

Em relação ao software e à configuração dos equipamentos/dispositivos são precisas várias configurações básicas e outras mais complexas para que o trabalho funcione de maneira eficiente e correta. Aspetos como o tipo de roteamento, nome do dispositivo, tipos de *interfaces* e as suas descrições, *passwords*, *logins*, endereço *ip* por *dhcp*, formas de um computador aceder a um *site*, etc, são características/funcionalidades que abordaremos mais à frente.

Índice - Páginas

Introdução.....	1
Configurações básicas.....	2 á 5
Restantes configurações.....	5 á 9
Sub-redes criadas com o Subnetting VLSM.....	15 e 16
Sub-redes criadas com o Subnetting Standard.....	16 e 17
Problemas encontrados e possíveis soluções.....	17 á 19
Testes e Resultados.....	19 e 20
Conclusão.....	21
Anexos.....	22

Índice - Figuras

Fig.1- Palavra passe relativa ao modo executivo privilegiado.....	10
Fig.2- Chaves SSH criadas.....	10
Fig.3- Interface em modo administratively down.....	10
Fig.4- Atribuição do nome de utilizador e a respetiva palavra-passe.....	11
Fig.5- Running-config.....	11
Fig.6- Start-up config.....	11
Fig.7- POOL em um servidor DHCP.....	12
Fig.8- Identificação num computador do IP, Máscara ,DG e servidor DNS.....	12
Fig.9- Output de uma página WEB.....	12
Fig.10- Implementação de VLANs e configuração de trunk entre os switches.....	13
Fig.11- Exemplo de ligação LACP entre dois switches em modo passivo (Madeira).....	13
Fig.12- Utilização do NAT overload para passar de um end.privado para público.....	14
Fig.13- Resultado de um teste de conexão entre dois dispositivos.....	14
Fig.14- Insucesso no pedido do IP por DHCP.....	14
Fig.15- Insucesso numa requisição do domínio ao servidor DNS.....	14
Fig.16- Mensagem de erro após 3 tentativas falhadas a aceder remotamente.....	14

Índice - Tabelas

Tabela das sub-redes da rede Madeira.....	15
Tabela de endereçamento da rede Madeira.....	15
Tabela das sub-redes da rede Açores.....	16
Tabela de endereçamento da rede Açores.....	16
Tabela das sub-redes da rede Continente.....	17
Tabela de endereçamento da rede Continente.....	17

Introdução

É usada a aplicação *Cisco Packet Tracer*, da *Cisco Systems*, para implementar uma rede virtual. Vamos ao longo do nosso relatório falar sobre as técnicas que usámos para executar com sucesso todas as alíneas pedidas.

Cada configuração básica foi feita em todos os dispositivos de rede (*switches/routers*) , sendo algumas só limitadas a um só equipamento. O resto das configurações exigiu mais complexidade e atenção ao detalhe, porque na maior parte dessas, foram feitas modificações que afetam toda a rede e não só um equipamento em particular, por exemplo aceder a um certo *site*. Outros sistemas físicos como computadores, servidores... foram também configurados, dependendo de certa instrução pedida.

Através de exemplos/demonstrações iremos mostrar como chegámos a um certo resultado e o seu significado. Na secção “Lista de Figuras” estão vários exemplos visuais em formato de *prints*, sobre diversos componentes , servindo como referência e ajuda para perceber o que está a ser feito. Quando houver alguma referência de uma figura, esta estará neste segmento.

As tabelas de endereçamento e as várias sub-redes estão quer na parte das sub-redes criadas com *subnetting VLSM* (Madeira e Açores), quer na sub-rede criada com *subnetting Standard* (Continente). Ao longo da execução do trabalho surgiram algumas complicações , dúvidas, sendo estas resolvidas com soluções viáveis ou indicando uma possível mudança que possa ser feita na rede. Por último, foram realizados vários testes aos diversos equipamentos presentes na rede, para verificar se o que foi pensado primeiramente estava na prática a funcionar (secção “Testes e Resultados”).

Configurações equipamentos

Em relação às configurações dos equipamentos vamos apresentar primeiro as configurações básicas. São implementações mais específicas e diretas. A maior parte destas tem só a ver com o próprio equipamento e não afetam a rede.

Configuração do *host name* - em todos os dispositivos de rede (*switches/routers*), foi implementada esta configuração, dando um certo nome ao equipamento de acordo com a sua localização e a sua função. No que toca aos *routers* principais de cada rede e aos *ISP*’s (*router* fornecido por uma companhia de serviços de Internet), o nome possui: quer a região, no caso dos regionais , quer o tipo de empresa, no caso dos *ISP*’s. No que toca ao *router AWS*, escolhemos “*MainRouter*” identificando que é um router importante pois através das suas redes, é possível fazer a conexão de um certo computador em qualquer rede, com o servidor *DNS* presente numa das suas conexões. Também pelo fato de todas as redes se conectarem a ele diretamente ou indiretamente. O comando para obter sucesso nesta funcionalidade é: modo executivo privilegiado -> *config* -> *hostname X* .

Configuração do *banner motd* - em todos os dispositivos de rede (*switches/routers*), foi implementada esta configuração, que basicamente é uma mensagem em que quando

alguém entra no *CLI - Command Line Interface* (Linha de comandos dos *routers/switches*) , é notificado com um aviso que pode ser personalizado no modo executivo privilegiado -> *config* -> *banner* -> *motd* -> # mensagem # , sendo que a mensagem tem de estar entre cardinais. No nosso caso, o recado alerta o utilizador de que qualquer acesso não autorizado é proibido e que tem de ter permissão para configurar o equipamento.

Configuração da *password* de acesso ao modo privilegiado - em todos os dispositivos de rede (*switches/routers*), foi implementada esta configuração, que adiciona uma *password* para o acesso ao modo administrador. É uma segurança, pois impede que qualquer utilizador configure as funcionalidades mais críticas num dispositivo. O comando é executado pelos seguintes subcomandos : modo executivo privilegiado -> *config* -> *enable secret X*. O valor X aparece de seguida, obviamente encriptado (**fig.1**) no comando *show running-config*, presente no modo executivo do utilizador e que é responsável por mostrar todas as configurações relativas ao equipamento no seu estado atual.

Configuração da *password* de acesso à ligação por consola - em todos os dispositivos de rede (*switches/routers*), foi implementada esta configuração, que adiciona uma *password* ao modo executivo do utilizador. Quando um certo utilizador entra no *CLI*, é pedida uma palavra-passe de acesso ao modo mais básico (modo este que só serve para visualizar informação, dados do equipamento e não permite configurar). É a forma mais segura de combater contra utilizadores indevidos, pois não têm qualquer acesso aos detalhes do dispositivo. Quando estamos a aceder a um equipamento de rede , é através da linha de consola presente no mesmo, que poderemos alterar/configurar as suas funcionalidades/características. Uma *password* é a maneira mais eficiente de bloquear qualquer acesso indevido. Para uma correta implementação a sequência de comandos é : modo exec privilegiado -> *config* -> *line console 0* -> *password X* . O 0 refere-se à única (geralmente) linha de consola disponível.

Configuração da *password* de acesso às linhas virtuais (*telnet ssh*) - em todos os dispositivos de rede (*switches/routers*), foi implementada esta configuração, que atribui uma *password* quando queremos modificar remotamente certo equipamento. O utilizador pode discriminar quantas entidades podem ter acesso ao dispositivo simultaneamente. No nosso caso, escolhemos 5 sessões ativas no máximo, ao mesmo tempo. Existem dois protocolos por detrás desta configuração e da futura ligação (comunicação) entre utilizador e dispositivo, que são o *Telnet* e o *SSH*. Escolhemos devido à impossibilidade de usarmos os dois, o protocolo *SSH*. É muito mais seguro, pois encripta todos os dados (ao contrário de *Telnet* que deixa informação crítica visível) , como por exemplo a *password* que definimos. Como o nome indica (“*SSH = Secure Shell*”) , serve como um escudo contra ataques maliciosos. Será abordado noutra configuração, o facto de o protocolo só funcionar, se forem geradas chaves *SSH*. Feito através dos comandos -> modo exec privilegiado -> *config* -> *line vty 0 4* -> *password X* -> *login local* -> *transport input ssh*.

Configuração de bloquear o *login* nos equipamentos contra ataques de *brute-force* - Em todos os dispositivos de rede (*switches/routers*), foi implementada esta configuração. Ataques de “*brute-force*” são ataques que pretendem manipular certa chave/*password* codificada, executando tentativas exaustivas até acertar na sequência

correta de caracteres. Pode ser feito com um algoritmo e é extremamente perigoso. Com esta implementação, esse risco de acesso indesejado é diminuído/retirado (dependendo do tempo de bloqueio) e necessita de que o *NAT overload* esteja configurado na rede e que todos os routers tenham o protocolo *RIPv2* implementado. O comando é simples : modo exec privilegiado -> *config* -> *login block-for X attempts Y within Z*, em que X é o tempo máximo em segundos , de Y tentativas. Se não acertarmos na chave, o campo de inserção fica bloqueado durante Z segundos. No nosso caso, fizemos com que se o utilizador se enganasse 3 vezes em 30 segundos, o acesso ficaria suspenso durante 60 segundos.

X é o tempo que fica bloqueado, e Z é o tempo que temos para as Y tentativas

Configuração de criar o utilizador “*netadmin*” como administrador dos equipamentos de rede - em todos os dispositivos de rede (*switches/routers*), foi implementada esta configuração. É simples de ser efetuada , pois necessita de um simples comando. Como o nome indica, o utilizador “*netadmin*” será o nome do administrador/utilizador do dispositivo de rede, ou seja a entidade que configura ou acede ao equipamento será esta. Esta funcionalidade será útil, por exemplo, para quando acedermos à distância por *SSH* a um dispositivo de rede. Foi também adicionado, para além do nome do utilizador , uma palavra passe para reforçar a segurança. O comando que executa esta funcionalidade é : modo exec privilegiado -> *config* -> *username X secret Y* (**Fig.4**). X é o nome do administrador e Y é a palavra-passe. Também podemos adicionar para completar o comando, o grau de acesso que um certo utilizador tem. Sendo 0 = praticamente não pode fazer nada no *router/switch* e 15 = acesso total a todos os comandos no dispositivo. ~~Antes da palavra-passe poderá ser adicionado um número, que identifica o grau de encriptação da password~~

Configuração nos equipamentos da política de password maior de 12 caracteres - em todos os dispositivos de rede (*switches/routers*), foi implementada esta configuração. Serve para definir um limite mínimo de caracteres das *passwords* implementadas. No nosso caso temos que o comprimento da chave é 12. O comando é : modo exec privilegiado -> *config* -> ~~service password encryption~~ X, em que X é o valor.

security passwords min-length X

Configuração em todos os equipamentos de rede a utilização do servidor NTP

- o servidor *NTP* serve para fornecer um relógio interno nos dispositivos de rede. O administrador da rede pode modificar a hora sempre que quiser, basta que no próprio servidor , o serviço *NTP* esteja ativo e que a conexão esteja bem feita com o equipamento de rede. Para haver essa ligação entre ambos, basta executar o comando : modo exec privilegiado-> *config* -> *ntp server X* , onde X é o *IP* do servidor *NTP* na rede/sub-rede. No nosso projeto, temos dois servidores *NTP* nas redes Madeira e Açores.

Configuração do domínio de rede como *cam.gov.pt* - em todos os dispositivos de rede (*switches/routers*), foi implementada esta configuração, que identifica a rede em formato de nome, em vez de *IP* . Estará presente nas chaves públicas (*SSH*), na resolução de nomes para *IP*’s (*DNS*), entre outras funcionalidades. É vantajoso, pois é mais legível para o humano (mais fácil de perceber). O seu comando é simples: modo exec privilegiado -> *config* -> *ip domain-name X* , em que X é o nome do domínio.

Configuração da encriptação das *passwords* - em todos os dispositivos de rede (*switches/routers*), foi implementada esta configuração, que encripta/codifica todas as

passwords presentes no equipamento de rede, embora com a qualidade de encriptação baixa. Tirando este aspecto, é bastante útil, pois não necessitamos de encriptar individualmente cada palavra-passe que adicionamos. Comando : modo exec privilegiado -> *config* -> *service password-encryption*. Nota : Modifica também as *passwords*, que não estavam encriptadas antes do comando.

Podemos implementar as *passwords* de duas maneiras diferentes : *enable secret* (palavra-passe encriptada de raiz) ou *password* (palavra-passe não encriptada). Dependendo do comando, uma/ambas serão aceites , porém a que garante melhor desempenho em termos de segurança, é o *enable secret* (encriptação forte).

Configuração das chaves SSH para acesso remoto nos equipamentos de rede

Como já tínhamos mencionado, para aceder através do protocolo *SSH* a um dispositivo de rede remotamente, é necessário gerar chaves *SSH*. É constituída pelo nome do dispositivo de rede, juntamente com o nome do domínio, a informação de onde será usada e os seus dados. Quando um certo utilizador quer aceder a um *router/switch*, autentica-se usando estas chaves, fazendo assim a conexão entre ambos. Para além desta chave que pertence à conexão administrador/rede, temos outra que também é dada automaticamente quando este comando é executado. É a chave temporária que serve para fazer a encriptação durante as sessões ativas (*line vty*). Para o sucesso desta configuração, é necessário também já ter no seu dispositivo o nome de utilizador e a respetiva palavra-passe. Para gerarmos as chaves podemos fazer o seguinte comando : modo exec privilegiado -> *config* -> *crypto key generate rsa general-keys X* -> em que X é o número de bits presentes na chave. Para visualizar as chaves que foram geradas usamos o comando: modo exec privilegiado -> *config* -> *show crypto key mypubkey rsa* (**fig. 2**).

Configuração das portas que não estão a ser utilizadas nos switches, com a finalidade dos dispositivos não conseguirem se conectar com sucesso - para que outros equipamentos não consigam se conectar com sucesso, é necessário desativar completamente todas as suas *interfaces* (que não estão em uso). Com isto fechamos qualquer possibilidade de conexão com as mesmas. Normalmente por padrão as *interfaces* estão em modo “*down*” quando são criadas , o que significa que não estão desativadas. Para que isso aconteça, temos que fazê-lo manualmente, através do comando -> modo exec privilegiado -> *config* -> *interface X* -> *shutdown*. Assim, qualquer conexão com um possível dispositivo, está desabilitada nesta *interface*. Na (**fig.3**) é possível visualizar o estado da mesma depois de ser desconectada.

Configuração da gravação do ficheiro de configuração na memória NVRAM dos equipamentos - depois de todas estas configurações estarem implementadas nos *routers/switches*, é necessário gravar na memória, para que quando se desconecte do equipamento, não se perca todas as modificações feitas. Para isso usamos o comando: modo exec -> *write memory*. Estamos sobrepondo as nossas mudanças na configuração padrão do equipamento e é como se a nossa configuração passasse a ser a da raiz do sistema. No comando -> *show start-up config* (**fig.6**) é possível vermos as alterações

feitas. Há outro comando para visualizar as transformações, porém este fornece a configuração atual, sem estar na memória *NVRAM*, logo serão perdidos os dados, quando houver o abandono do utilizador ao dispositivo. Comando este que é o *show running-config*. (**fig.5**).

Configuração de descrições em todas as *interfaces*, de todos os dispositivos de rede - através do comando modo exec privilegiado -> *config* -> *interface X* -> *description Y*, descrevemos em um/a pequeno/a texto/frase a função da *interface* respetiva.

Concluímos assim as configurações básicas nos equipamentos de rede.

De acordo com a tabela de endereçamento, as *interfaces* dos routers são identificadas dando um certo *IP* a cada uma. As *interfaces* “normais” (que só servem para fazer a conexão ponto a ponto entre dois equipamentos), são ativadas (*UP*) usando o comando : modo exec privilegiado -> *config* -> *interface X* -> *no shutdown*. Por exemplo, nos *routers* *ISP*’s e *AWS* , são habilitadas desta maneira, enquanto que nos das redes Madeira, Açores e Continente, são criadas *sub-interfaces* com o *default-gateway* de cada *vlan* existente na sub-rede. Assim garante-se que todos os equipamentos da rede, mesmo que pertençam a sub-redes diferentes, consigam comunicar entre si. Este tema será mais aprofundado na secção de sub-redes criadas com *Subnetting Standard* e *VLSM*.

Configuração dos *IP*’s nos computadores das redes via protocolo *DHCP*

No caso da Madeira e Açores, todos os *IP*’s dos computadores foram atribuídos de maneira dinâmica, através de um servidor *DHCP*. Este é responsável por designar num certo intervalo de endereços, presentes na tabela de sub-rede, um *IP* (número que identifica o dispositivo na rede). Como já foi mencionado, todos os aparelhos neste projeto (os que é possível atribuir um *IP*) são referenciados com base no protocolo *IPv4* (32 bits). No caso destas duas sub-redes, a *VLAN* onde estão os computadores é a que tem o *id* 55 (atendimento). O número de hosts necessário para cada uma, em cada sub-rede, difere, logo o número máximo de *IP*’s que podem ser distribuídos pelo servidor *DHCP* será diferente. Para o sucesso desta configuração, foi necessário que os serviços dentro do servidor estejam corretamente efetuados; como o pedido *DHCP* é feito em sinal de *broadcast* (para todos os dispositivos na rede) e pelo facto do servidor não estar na sub-rede de atendimento e desconhecer-se à partida a existência da sub-rede servidores, quando o *request* chega ao *default-gateway* é necessário este enviar para o respetivo servidor. Sendo assim, é fulcral no *router* (na *sub-interface* que receberá a solicitação), configurar um comando que é o *ip helper-address* que indica que quando recebermos um pedido em *broadcast* (neste caso de um dispositivo da *VLAN* 55), encaminharmos para o servidor *DHCP*. Comando : modo exec privilegiado -> *config* -> *interface X* -> *ip helper-address Y*, em que X é a *interface* que recebe o sinal em *broadcast* e Y é o *IP* do servidor.

Como se pode ver na **fig.7**, é necessário criar uma *POOL* (identificação de um certo serviço *DHCP*), com todos os detalhes fundamentais, para que quando houver uma

solicitação de um *IP* por *DHCP* e este estiver no range de *IP*'s possíveis para atribuir (na mesma *vlan* que o dispositivo que está pedindo), a atribuição seja feita de maneira eficiente. Reparemos que é necessário colocar o *IP* inicial (*IP* da sub-rede) e a respetiva máscara. Através desta já se sabe a quantidade de endereçamentos. Por exemplo na sub-rede Açores, como temos uma máscara de sub-rede 255.255.255.128, há 7 *bits* para a parte dos *hosts*, logo existem 126 dispositivos disponíveis para colocação do *IP*. Depois da correta formatação do servidor, no dispositivo que queremos atribuir o *IP*, colocamos a opção *DHCP* em vez de estático no campo *IPv4*. De notar que o servidor *DHCP* não só atribui o *IP* de identificação do equipamento, mas sim também a máscara de sub-rede (neste caso), o *IP* do *default gateway* e o *IP* do servidor *DNS* (**fig.8**).

Na rede Continente, como não possuímos servidor *DHCP*, a atribuição dos *IP*'s tem de ser feita no próprio *router*. Existe um conjunto de comandos que permitem fazer basicamente a mesma coisa que um servidor faz, só que é um pouco mais trabalhoso, especialmente se estivermos em redes grandes, devido ao facto de termos de efetuar manualmente a exclusão dos *IP*'s que não podem ser endereçados, por exemplo o do *default-gateway*. No servidor *DHCP*, este processo é feito de forma automática.

No nosso projeto, temos nesta rede dois tipos de computadores : o fixo e o portátil. Ambos estão em sub-redes diferentes ; consequência disto é ser preciso criar duas *POOLS* em que cada uma referencia uma sub-rede. Quando houver um pedido de *IP* por *DHCP*, o equipamento vai aceder à *POOL* correspondente da sua sub-rede, devido ao facto de essa *POOL* ter o mesmo *default gateway* que a *VLAN* do dispositivo. Por motivos de escalabilidade, o *router* tem *POOLS* de todas as *VLANS*. Devido ao facto de termos poucos *hosts* nas sub-redes dos computadores, se quisermos inserir um *PC* noutra sub-rede já temos a configuração *DHCP* feita.

Configuração dos servidores *DNS* e *HTTP*

Para a configuração de pode aceder ao *site* *cam.gov.pt*, através de um *web browser*, a partir de um computador na rede Açores, é necessário formatar os servidores *DNS* e *HTTP*. Para o servidor *DNS* temos de obviamente ativar o serviço *DNS* e adicionar um nome de domínio e o seu respetivo *IP*. Quando o dispositivo aceder ao *site*, a parte do domínio presente no *URL*, tem de estar presente no servidor *DNS*, senão não conseguimos aceder ao *site*. Este processo serve para o computador saber o *IP* de um certo *URL*. Quando souber fica armazenado na sua *cache* (memória não volátil e muito rápida), fazendo assim com que quando houver um 2º pedido para o mesmo domínio já não precisa de pedir ao servidor *DNS* o *IP* respetivo. Se esta solicitação for feita com sucesso, o dispositivo já sabe que para aquele domínio, o *IP* é X, sendo X (no nosso trabalho) o *IP* do servidor *WEB*. Então, de seguida é feita uma requisição *HTTP* ao servidor *WEB*, que tem as páginas *HTML/CSS* preparadas e envia-as como resposta ao pedido. O *browser* interpreta o código e dá como “*output*” a página correspondente. Na **fig.9** é possível observar a página gerada.

Em relação às redes adicionais conectadas às *interfaces* do *router AWS*, foram configuradas com máscaras de rede /24 (8 *bits* para a parte do *host*) para facilitar a implementação. Numa existe um servidor *WEB* e noutra um servidor *DNS Cloudflare*.

Usou-se ao contrário dos outros servidores *DNS*, o servidor *DNS Cloudflare* que se destaca pela velocidade, segurança e custo. Por exemplo, quando para um certo utilizador,

um certo domínio chega a este servidor e resolve para um *IP*, o *IP* do dispositivo que fez o pedido ao servidor não fica guardado neste. É gratuito e o seu *IP* é público (1.1.1.1), de maneira a que qualquer empresa/entidade que queira acedê-lo consegue fazê-lo com eficácia. Devido à limitação da aplicação, não é possível implementar este tipo de servidor (só podemos configurar um servidor *DNS* padrão). Para acedermos ao site *miutmadeira.com* a partir de qualquer computador em qualquer rede, foi necessário configurar o domínio respectivo nos servidores *DNS* dos Açores e do Continente. Para a rede Madeira, usou-se o servidor *DNS* dos Açores. Atribuímos a esse domínio, o *IP* do servidor *WEB* da rede *Internet* (172.67.185.68) e tal como fizemos no caso do site *cam.gov.pt* nos Açores, customizámos as páginas *HTML* para o site ficar mais apelativo e credível.

Protocolo *RIPv2*

Utilizámos para o *routing* o protocolo *RIPv2* em vez do estático. Para o correto funcionamento, foi preciso configurar todos os *routers* de maneira dinâmica. Por termos uma rede “grande”, esta implementação é mais rápida e menos exaustiva, pois se fizéssemos de maneira estática, teríamos que para cada rede/sub-rede existente configurar nos *routers* todos os saltos. Seria um processo bastante confuso, demoroso e nada prático.

Através do *RIPv2*, só identificando as redes que estão á volta (conectadas) de cada *router*, o próprio protocolo encarregue-se de fazer a conexão de forma automática, percebendo por exemplo para certa rede, num certo *router*, que temos de “apontar” para a outra *interface* do outro *router* para chegarmos à rede requisitada. Se nesse *router* não estiver a rede numa das suas *interfaces*, continuaremos o processo até encontrarmos a rede. Caso não exista, o campo *TTL* que contém um certo número à partida e que é decrementado em cada salto, chegará a zero e o pacote será excluído da rede. Podemos pensar como se fosse uma comunicação indireta entre todos os *routers* que têm o seu *routing* definido com o protocolo *RIPv2*, o processo de interconexão das interfaces e redes correspondentes de cada *router*.

Para integrarmos este tipo de roteamento num *router*, podemos fazer esta sequência de comandos: modo exec privilegiado -> *config* -> *router rip* -> *version 2* -> *no auto-summary* -> *network X* -> *passive-interface Y*, em que *X* é a rede conectada a uma das *interfaces*.

O comando *passive-interface* serve para uma rede que não contenha *routers*, não receba atualizações *RIPv2* (há a verificação depois de algum tempo, da entrada de alguma *interface* ou *Router RIPv2*, modificando possivelmente a tabela de roteamento de cada *router*), portanto convém omitirmos estes *updates* na *interface* respetiva (Y). O *no auto-summary* permite que certa máscara de uma rede, que é a mesma de uma porta do *router*, seja identificada de maneira correta, ou seja com a sub-máscara correta. Se *no auto-summary* não estivesse ativo, iria identificar a sub-rede com /8 ou /16 ou /24 (*classless*), mesmo que não fosse efetivamente o comprimento de prefixo da sub-rede. No nosso caso é fulcral estar ligado, pois como lidamos com *VLSM* (redes com máscaras não fixas), não a podemos definir de maneira errada, caso assim fosse teríamos potenciais problemas no roteamento.

Configuração da *Interface de Gestão (VLAN 500)*

Para ativar a gestão remota dos *switches* da Madeira, Açores e Continente, a *VLAN* 500 foi configurada como a *VLAN* de gestão. Um endereço *IP* estático dentro da sub-rede apropriada foi atribuído a cada *switch* através da interface *VLAN* 500. O *gateway* predefinido também foi configurado para garantir a conectividade com redes externas. Esta configuração permite aos administradores gerir os *switches* por meio de *SSH* ou *Telnet*.

Para configurar a *VLAN* de gestão, execute os seguintes comandos: modo exec privilegiado -> *config* -> *interface vlan 500* -> *ip address X Y* (substituir X e Y pelo *IP* e pela máscara de sub-rede desejados) -> *exit* -> *ip default-gateway Z*. Esta configuração garante que o *switch* possa ser gerido remotamente utilizando protocolos como *SSH* ou *Telnet* através da *VLAN* 500.

Configuração do *Trunk* entre os *Switches* e os *Routers*

Para permitir a comunicação entre *VLANs* em diferentes *switches* e garantir o encaminhamento (*routing*) realizado pelo *router*, foi configurado o modo *trunk* nas *interfaces* que ligam os *switches* entre si e aos *routers*. O modo *trunk* permite que múltiplas *VLANs* circulem através de uma ligação física. Apenas as *VLANs* estritamente necessárias (10, 15, 55, 90, 130) foram permitidas nas portas *trunk*, com o objetivo de otimizar o desempenho e aumentar a segurança, evitando a propagação de *VLANs* desnecessárias. Para configurar o modo *trunk* e permitir apenas as *VLANs* exigidas, foi utilizada a seguinte sequência de comandos: modo exec privilegiado -> *config* -> *interface X* (substituir X pela *interface* correspondente, ex: *FastEthernet0/1*) -> *switchport trunk encapsulation dot1q* -> *switchport mode trunk* -> *switchport trunk allowed vlan 10,15,55,90,130*.

A configuração foi aplicada às *interfaces* que ligam:

- *Switch-to-Switch* (por exemplo, Pld-S1 a Pld-S2)
- *Switch-to-Router* (por exemplo, Pld-S1 a Pld-Router)

Esta ligação pode ser observada na **fig.10** e este conjunto de configurações garante que apenas o tráfego das *VLANs* necessárias, seja transportado através das ligações *trunk*, mantendo a eficiência da rede e a segmentação adequada.

Configuração da agregação de *links* entre *switches* usando *LACP* (Modo Passivo)

Para aumentar a largura de banda e garantir redundância entre os *switches*, foi implementado o protocolo de controlo de agregação de *links* (*LACP* – *Link Aggregation Control Protocol*). Ao agrupar várias *interfaces* físicas numa única *interface* lógica

(*Port-Channel*), o tráfego é distribuído de forma equilibrada (*load balancing*) e é estabelecido um mecanismo de tolerância a falhas (*failover*).

O *LACP* foi configurado em modo passivo em ambas as extremidades, o que significa que cada lado aguarda que o outro inicie o processo de agregação, assegurando uma negociação estável. Sequência de comandos utilizada : modo exec privilegiado -> *config* -> *interface range f0/8 - 9* -> *channel-group 1 mode passive* -> *exit* -> *interface Port-channel 1* -> *switchport mode trunk* -> *switchport trunk allowed vlan 10,15,55,90,130*.

Esta configuração agregou as *interfaces FastEthernet0/8* e *FastEthernet0/9* entre os *switches Pld-S1* e *Pld-S2* na *interface lógica Port-channel1*, permitindo a passagem apenas das *VLANs* necessárias através da ligação *trunk*. A implementação pode ser confirmada através do comando: *show etherchannel summary*, que exibe o estado do *LACP* e as *interfaces* agregadas, conforme demonstrado na **fig.11**. Esta configuração melhora a comunicação entre *switches*, proporcionando balanceamento de carga e alta disponibilidade.

Configuração da *NAT Overload (PAT)* para acesso à *Internet*

Para permitir que os *hosts* das *VLANs* internas acedam à *Internet*, foi configurado o *NAT Overload (PAT)* nos *routers* das redes regionais. Esta técnica permite que múltiplos endereços *IP* privados partilhem um único endereço *IP* público, utilizando diferentes portas de origem para distinguir as sessões.

O *NAT Overload* é essencial quando há um número limitado de endereços *IP* públicos e vários dispositivos internos necessitam de conectividade externa.

A configuração envolveu a marcação das *interfaces* internas (conectadas às *VLANs* internas) com o comando *ip nat inside* e da *interface* externa (ligada ao *ISP*) com o comando *ip nat outside*. Foi então criada uma lista de acesso (*access list*) para definir quais endereços *IP* internos podem ser traduzidos, seguida da aplicação da regra de *NAT* com a palavra-chave *overload* na *interface* de saída.

A sequência de comandos usada (exemplo na rede Açores) foi : *access-list permit 10.210.34.0 0.0.0.0 -> interface fastEthernet 0/0.X* , em que X é o *IP* do *default gateway* de cada sub-rede -> *ip nat inside -> exit -> interface Serial1/0 -> ip nat outside -> ip nat inside source list 1 interface Serial 1/0 overload*.

Esta configuração garante que os dispositivos nas *VLANs* internas possam aceder às redes externas (como a *Internet*) de forma eficiente e segura. O funcionamento pode ser confirmado na **fig.12**.

Lista de Figuras

```
!
!
enable secret 5 $1$mERr$p0.rGLvw6oWWiTTkVdABH/
!
!
```

Fig.1 - Palavra passe relativa ao modo executivo privilegiado , encriptada no comando show running-config.

```
PldRouter# show crypto key mypubkey rsa
% Key pair was generated at: 14:12:44 UTC março 19 2025
Key name: PldRouter.cam.gov.pt
Storage Device: not specified
Usage: General Purpose Key
Key is not exportable.
Key Data:
00005827 00004aa9 000010e4 00006261 0000490f 00006c85 000000d4 00007841
00002397 000020b1 00005040 0000206a 0000591b 0000226c 00005f7f 000043a3
000051d4 00001157 000006b9 00007442 0000464f 0000351f 00005afb 6ef1
% Key pair was generated at: 14:12:44 UTC março 19 2025
Key name: PldRouter.cam.gov.pt.server
Temporary key
Usage: Encryption Key
Key is not exportable.
Key Data:
00004d1d 0000245b 0000498a 000018b2 000070cd 000052b8 00007d78 00001e21
00006217 00004a53 00004376 000017f9 00001a5a 00001466 00005fe9 000058da
00000249 00001527 00000b40 0000484a 000070e0 00005eed 00000884 6ef9
```

Fig.2 - Chaves SSH criadas. Chave pública (uso geral) e chave temporária.

```
PLD-S1#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
PLD-S1(config)#interface f0/1
PLD-S1(config-if)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down
```

Fig.3 - Interface em modo administratively down, depois de ser desabilitada manualmente.

```
PldRouter#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
PldRouter(config)#username netadmin privilege 15 secret 5 testetestetesteste
PldRouter(config)#exit
```

Fig.4 - Atribuição do nome de utilizador e a respetiva palavra-passe a um dispositivo de rede.

```
FldRouter#show running-config
Building configuration...
!
Current configuration : 3116 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
security passwords min-length 12
!
hostname FldRouter
!
login block-for 30 attempts 3 within 60
login on-failure log
login on-success log
!
!
enable secret 5 $1$ERr$RVupf0bTLZgsowKqFC9fS1
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
username netadmin privilege 15 secret 5 testetestetestete
!
!
license udi pid CISCO2811/K9 sn FTX10174LH5-
!
!
!
!
!
--More-- |
```

Fig.5 - Estado atual das funcionalidades presentes no dispositivo de rede.

```
FldRouter#show startup-config
Using 3139 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
security passwords min-length 12
!
hostname FldRouter
!
login block-for 30 attempts 3 within 60
login on-failure log
login on-success log
!
enable secret 5 $1$ERr$RVupf0bTLZgsowKqFC9fS1
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
username netadmin privilege 15 secret 5 $1$ERr$Y1CkLMcTYWwkFlCndt11.
!
license udi pid CISCO2811/K9 sn FTX10174LH5-
!
!
!
!
no ip domain-lookup
```

Fig.6 - Estado gravado na memória (NVRAM) das funcionalidades presentes no dispositivo de rede.

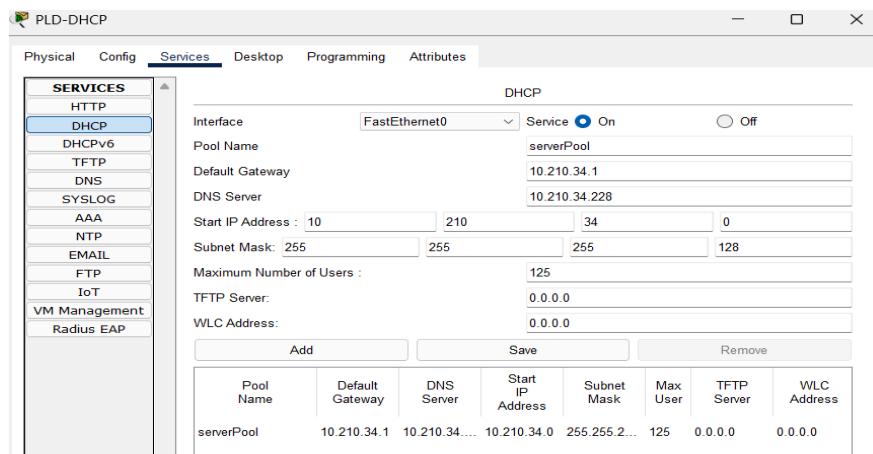


Fig.7 - POOL em um servidor DHCP e as suas especificações.

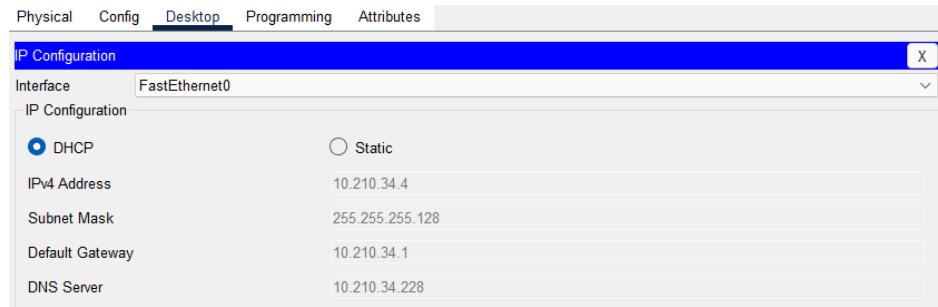


Fig.8 - Secção num computador da rede Açores, que identifica o tipo de endereçamento (DHCP ou estático), o IP , o IP da máscara de sub-rede, o IP do default gateway e o IP do Servidor DNS.



Fig.9 - Output do ficheiro index.html (página principal).

```
LisS1#show vlan brief
VLAN Name          Status    Ports
----  -----
1    default        active    Po1, Fa0/11, Fa0/12, Fa0/13
                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                Giga0/2
10   Printers       active    Fa0/4
15   IoT            active    Fa0/2, Fa0/3
55   Atendimento   active    Fa0/10
90   Wireless      active    Fa0/9
130  Contabilidade active    Fa0/5, Fa0/6
500  default        active
1002 fddi-default  active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default  active
LisS1#show interfaces trunk
Port   Mode      Encapsulation  Status      Native vlan
Fa0/1  on        802.1q         trunking    1

Port   Vlans allowed on trunk
Fa0/1  10,15,55,90,130

Port   Vlans allowed and active in management domain
Fa0/1  10,15,55,90,130

Port   Vlans in spanning tree forwarding state and not pruned
Fa0/1  10,15,55,90,130
```

Fig.10- Implementação de VLANs e configuração de trunk entre os switches (a partir do LisS1) e o router do Continente.

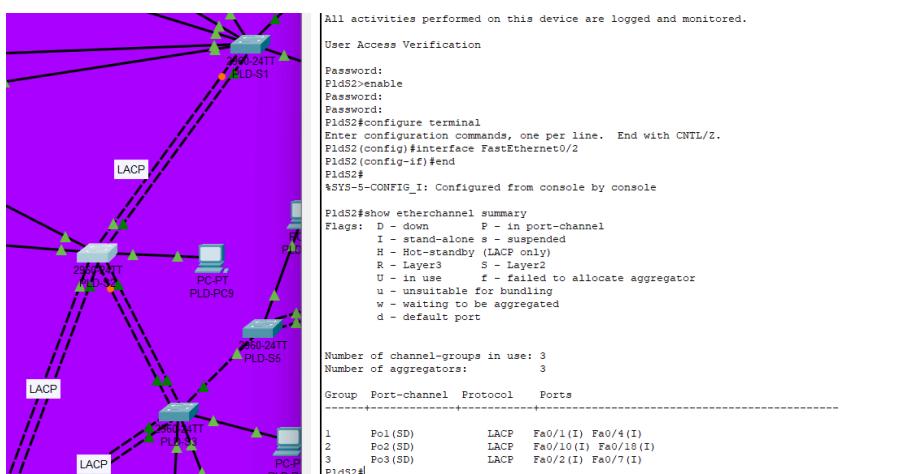
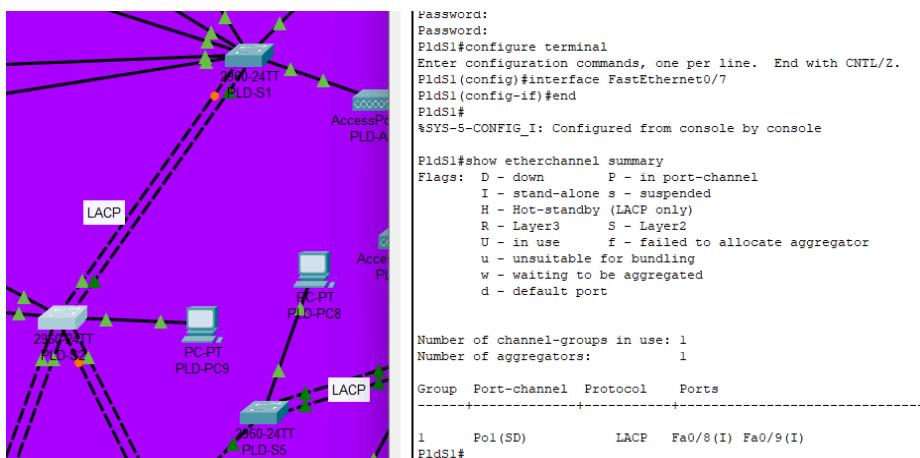


Fig.11 - Exemplo de ligação LACP entre PLD S-1 e PLD S-2 em modo passivo (Madeira).

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PLD-P1	FNC-PC1	ICMP		0.000	N	0	(edit)	(delete)
<pre>P1dRouter#show ip nat statistics Total translations: 0 (0 static, 0 dynamic, 0 extended) Outside Interfaces: Serial1/0 Inside Interfaces: FastEthernet0/0.10 , FastEthernet0/0.15 , FastEthernet0/0.55 , FastEthernet0/0.90 , FastEthernet0/0.130 , FastEthernet0/0.500 Hits: 0 Misses: 116 Expired translations: 0 Dynamic mappings: P1dRouter#show ip nat translations Pro Inside global Inside local Outside local Outside global icmp 62.223.143.101:1 10.210.34.242:1 172.16.34.3:1 172.16.34.3:1 icmp 62.223.143.101:2 10.210.34.242:2 172.16.34.3:2 172.16.34.3:2 P1dRouter#</pre>										

Fig.12- Após estabelecer a comunicação entre a VLAN 10 (Impressora PLD-P1) e a VLAN 55 (FNC-PC1), esta é a tradução de endereços de rede, de privada para pública utilizando NAT overload no router dos Açores.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PLD-...	NOS	ICMP		0.000	N	0	(edit)	(delete)
	Failed	PLD-...	LIS-LT1	ICMP		0.000	N	1	(edit)	(delete)

Fig.13 - Resultado de um teste de conexão entre dois dispositivos.

IP Configuration	
<input checked="" type="radio"/> DHCP	<input type="radio"/> Static
IPv4 Address	
169.254.113.37	

Fig.14 - Insucesso no pedido do IP por DHCP.

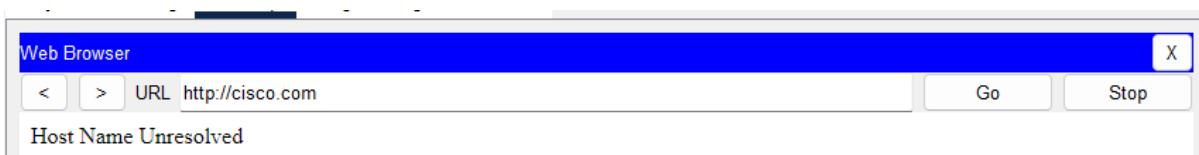


Fig.15 - Insucesso numa requisição do domínio ao servidor DNS.

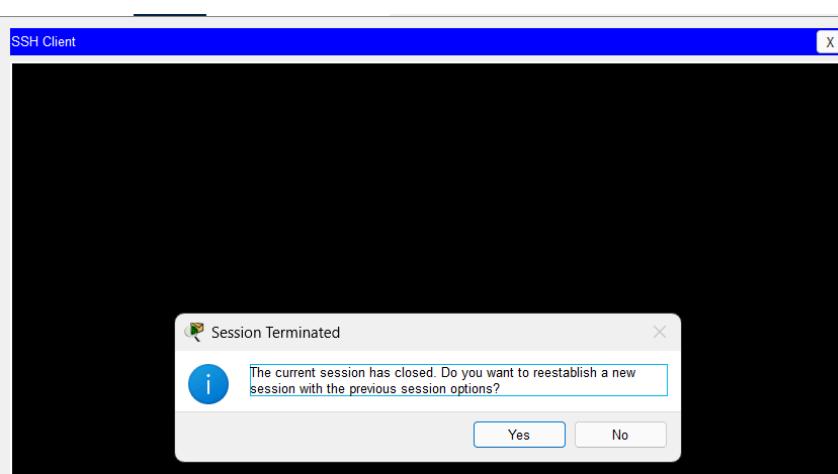


Fig.16 - Mensagem de erro após 3 tentativas falhadas ao tentar aceder remotamente um router, por meio do protocolo SSH.

Sub-redes criadas com *Subnetting VLSM*

Para a criação das sub-redes na Madeira e Açores usou-se o *Subnetting VLSM*, que consiste em implementar numa rede várias sub-redes de diferente comprimento de prefixo de máscara. O principal benefício é evitar perda de *IPs* desnecessariamente, ajustando o tamanho da máscara de acordo com o número de *hosts* que queremos, porém é mais trabalhoso do que o *Standard*. De notar que o número de *hosts* de cada sub-rede difere em cada rede, por exemplo na sub-rede “Atendimento”, nos Açores são necessários 80 *hosts*, já na Madeira são 60. Neste caso da Madeira, partimos do endereço de rede 172.16.34.0/24 (número máximo de *hosts* possíveis nesta rede são 254). Para a correta implementação são necessários cálculos, que englobam o endereço da sub-rede e a respectiva máscara consequente do número de *hosts* mínimo ; depois de feitos devemos de atribuir o endereço do 1º*host* à sub-rede , o do último *host* e o endereço de *broadcast*. É opcional, mas convém começarmos na sub-rede com o maior número de *hosts* até à menor. Já na rede Açores, o *subnetting* foi feito baseando-se no endereço de rede 10.210.34.0/24 e é feito de forma análoga ao da Madeira.

Madeira

Sub-rede	Endereço da sub-rede	Máscara da sub-rede	End. 1ºhost	End.Último host	End.Broadcast
Atendimento	172.16.34.0	255.255.255.192	172.16.34.1	172.16.34.62	172.16.34.63
Wireless	172.16.34.64	255.255.255.192	172.16.34.65	172.16.34.126	172.16.34.127
IoT	172.16.34.128	255.255.255.240	172.16.34.129	172.16.34.142	172.16.34.143
Servidores	172.16.34.144	255.255.255.240	172.16.34.145	172.16.34.158	172.16.34.159
Printers	172.16.34.160	255.255.255.240	172.16.34.161	172.16.34.174	172.16.34.175
Management	172.16.34.176	255.255.255.248	172.16.34.177	172.16.34.182	172.16.34.183

Tabela das sub-redes na rede Madeira

Dispositivo	Interface	End.Ip	Máscara de sub-rede	Gateway padrão
NOS	Serial 1/2	89.180.24.41	255.255.255.252	N/A
NOS	Serial 1/0	142.140.5.76	255.255.255.252	N/A
NOS	Serial 1/1	62.33.5.42	255.255.255.252	N/A
NOS	Serial 1/3	89.231.109.142	255.255.255.252	N/A
FNC	Serial 1/0	89.231.109.141	255.255.255.252	N/A
FNC	Fa 0/0	172.16.34.1	255.255.255.192	N/A
FNC	Fa 0/0.10	172.16.34.161	255.255.255.240	N/A
FNC	Fa 0/0.15	172.16.34.129	255.255.255.240	N/A
FNC	Fa 0/0.55	172.16.34.1	255.255.255.192	N/A
FNC	Fa 0/0.90	172.16.34.65	255.255.255.192	N/A
FNC	Fa 0/0.130	172.16.34.145	255.255.255.240	N/A
FNC	Fa 0/0.500	172.16.34.177	255.255.255.248	N/A
FNC-AP1	Placa de Rede	172.16.34.66	255.255.255.192	172.16.34.65
FNC-DHCP	Placa de Rede	172.16.34.146	255.255.255.240	172.16.34.145
FNC-NTP	Placa de Rede	172.16.34.147	255.255.255.240	172.16.34.145
FNC-P1	Placa de Rede	172.16.34.162	255.255.255.240	172.16.34.161
FNC-P2	Placa de Rede	172.16.34.163	255.255.255.240	172.16.34.161
FNC-IOT1	Placa de Rede	172.16.34.130	255.255.255.240	172.16.34.129
FNC-IOT2	Placa de Rede	172.16.34.131	255.255.255.240	172.16.34.129
FNC-IOT3	Placa de Rede	172.16.34.132	255.255.255.240	172.16.34.129
FNC-IOT4	Placa de Rede	172.16.34.133	255.255.255.240	172.16.34.129
FNC-PC1	Placa de Rede	IP POR DHCP	MASCARA POR DHCP	172.16.34.1
FNC-PC2	Placa de Rede	IP POR DHCP	MASCARA POR DHCP	172.16.34.1
FNC-S1	Placa de Rede	172.16.34.178	255.255.255.248	172.16.34.177
FNC-S2	Placa de Rede	172.16.34.179	255.255.255.248	172.16.34.177
FNC-S3	Placa de Rede	172.16.34.180	255.255.255.248	172.16.34.177

Tabela de endereçamento da rede Madeira

Açores

Sub-rede	Endereço da sub-rede	Máscara da sub-rede	End. 1ºhost	End.Último host	End.Broadcast
Atendimento	10.210.34.0	255.255.255.128	10.210.34.1	10.210.34.126	10.210.34.127
IoT	10.210.34.128	255.255.255.192	10.210.34.129	10.210.34.190	10.210.34.191
Wireless	10.210.34.192	255.255.255.224	10.210.34.193	10.210.34.222	10.210.34.223
Servidores	10.210.34.224	255.255.255.240	10.210.34.225	10.210.34.238	10.210.34.239
Printers	10.210.34.240	255.255.255.248	10.210.34.241	10.210.34.246	10.210.34.247
Management	10.210.34.248	255.255.255.248	10.210.34.249	10.210.34.254	10.210.34.255

Tabela das sub-redes na rede Açores

Dispositivo	Interface	Endereço IP	Máscara de sub-rede	Gateway padrão
MEO	Serial 1/0	62.223.143.102	255.255.255.252	N/A
MEO	Serial 1/1	62.31.53.17	255.255.255.252	N/A
MEO	Serial 1/2	62.33.5.41	255.255.255.252	N/A
PLD	Fa 0/0	10.210.34.1	255.255.255.128	N/A
PLD	Serial 1/0	62.223.143.101	255.255.255.252	N/A
PLD	Fa 0/0.10	10.210.34.241	255.255.255.248	N/A
PLD	Fa 0/0.15	10.210.34.129	255.255.255.192	N/A
PLD	Fa 0/0.55	10.210.34.1	255.255.255.128	N/A
PLD	Fa 0/0.90	10.210.34.193	255.255.255.224	N/A
PLD	Fa 0/0.130	10.210.34.225	255.255.255.240	N/A
PLD	Fa 0/0.500	10.210.34.249	255.255.255.248	N/A
PLD-NTP	Placa de Rede	10.210.34.226	255.255.255.240	10.210.34.225
PLD-DHCP	Placa de Rede	10.210.34.227	255.255.255.240	10.210.34.225
PLD-DNS	Placa de Rede	10.210.34.228	255.255.255.240	10.210.34.225
PLD-WEB	Placa de Rede	10.210.34.229	255.255.255.240	10.210.34.225
PLD-PC1	Placa de Rede	IP POR DHCP	MASCARA POR DHCP	10.210.34.1
PLD-PC2	Placa de Rede	IP POR DHCP	MASCARA POR DHCP	10.210.34.1
PLD-S1	Placa de Rede	10.210.34.250	255.255.255.248	10.210.34.249
PLD-S2	Placa de Rede	10.210.34.251	255.255.255.248	10.210.34.249
PLD-S3	Placa de Rede	10.210.34.252	255.255.255.248	10.210.34.249
PLD-S4	Placa de Rede	10.210.34.253	255.255.255.248	10.210.34.249
PLD-S5	Placa de Rede	10.210.34.254	255.255.255.248	10.210.34.249
PLD-S6	Placa de Rede	-	255.255.255.248	10.210.34.249
PLD-P1	Placa de Rede	10.210.34.242	255.255.255.248	10.210.34.241
PLD-P2	Placa de Rede	10.210.34.243	255.255.255.248	10.210.34.241
PLD-P3	Placa de Rede	10.210.34.244	255.255.255.248	10.210.34.241
PLD-P4	Placa de Rede	10.210.34.245	255.255.255.248	10.210.34.241
PLD-AP1	Placa de Rede	10.210.34.194	255.255.255.224	10.210.34.193
PLD-AP2	Placa de Rede	10.210.34.195	255.255.255.224	10.210.34.193
PLD-AP3	Placa de Rede	10.210.34.196	255.255.255.224	10.210.34.193
PLD-AP4	Placa de Rede	10.210.34.197	255.255.255.224	10.210.34.193
PLD-IoT1	Placa de Rede	10.210.34.130	255.255.255.192	10.210.34.129
PLD-IoT2	Placa de Rede	10.210.34.131	255.255.255.192	10.210.34.129

Tabela de endereçamento da rede Açores

Sub-redes criadas com *Subnetting Standard*

Para a criação das sub-redes no Continente usou-se o *Subnetting Standard*, que consiste em implementar em todas as sub-redes o mesmo comprimento de prefixo. Neste caso usou-se o /27, partindo-se do endereço de base 10.34.0.0/24. Este processo é mais simples que o *VLSM*, pois todas as sub-redes têm a mesma máscara, logo o mesmo número de *hosts* disponíveis (30). Não é necessário alterar o comprimento da máscara, pois o número máximo de *hosts* numa sub-rede (*IoT*) desta rede são 24. Os cálculos são

simples, é só partir do primeiro endereço disponível (10.34.0.0/27) e irmos adicionando 32, k vezes (k são o número de sub-redes que queremos) , até obtermos o último endereço da última sub-rede. Não é preciso verificarmos qual sub-rede tem o maior número de *hosts*, pois a máscara é igual para todas. Depois de feitos os cálculos, adicionamos o endereço do 1º*host*, o endereço do último e o endereço de *broadcast*.

Continente

Sub-rede	Endereço da sub-rede	Máscara da sub-rede	End. 1ºhost	End.Último host	End.Broadcast
Wireless	10.34.0.0	255.255.255.224	10.34.0.1	10.34.0.30	10.34.0.31
Contabilidade	10.34.0.32	255.255.255.224	10.34.0.33	10.34.0.62	10.34.0.63
Atendimento	10.34.0.64	255.255.255.224	10.34.0.65	10.34.0.94	10.34.0.95
Printers	10.34.0.96	255.255.255.224	10.34.0.97	10.34.0.126	10.34.0.127
Management	10.34.0.128	255.255.255.224	10.34.0.129	10.34.0.158	10.34.0.159
IoT	10.34.0.160	255.255.255.224	10.34.0.161	10.34.0.190	10.34.0.191

Tabela das sub-redes na rede Continente

Dispositivo	Interface	End.ip	Máscara de sub-rede	Gateway padrão
VOD	Serial 1/2	23.1.51.4	255.255.255.252	N/A
VOD	Serial 1/0	143.128.31.42	255.255.255.252	N/A
VOD	Serial 1/1	142.140.5.78	255.255.255.252	N/A
SINES	Serial 1/0	143.128.31.41	255.255.255.252	N/A
SINES	Fa 0/0	10.34.0.1	255.255.255.224	N/A
SINES	Fa 0/0.10	10.34.0.97	255.255.255.224	N/A
SINES	Fa 0/0.15	10.34.0.161	255.255.255.224	N/A
SINES	Fa 0/0.55	10.34.0.65	255.255.255.224	N/A
SINES	Fa 0/0.90	10.34.0.1	255.255.255.224	N/A
SINES	Fa 0/0.130	10.34.0.33	255.255.255.224	N/A
SINES	Fa 0/0.500	10.34.0.129	255.255.255.224	N/A
POR-DNS	Placa de Rede	10.34.0.194	255.255.255.224	10.34.0.193
LIS-DNS	Placa de Rede	10.34.0.195	255.255.255.224	10.34.0.193
POR-IoT1	Placa de Rede	10.34.0.162	255.255.255.224	10.34.0.161
LIS-IoT1	Placa de Rede	10.34.0.163	255.255.255.224	10.34.0.161
LIS-IoT2	Placa de Rede	10.34.0.164	255.255.255.224	10.34.0.161
POR-AP1	Placa de Rede	10.34.0.2	255.255.255.224	10.34.0.1
LIS-AP1	Placa de Rede	10.34.0.3	255.255.255.224	10.34.0.1
LIS-P1	Placa de Rede	10.34.0.98	255.255.255.224	10.34.0.97
LIS-PC1	Placa de Rede	IP por DHCP	MASCARA por DHCP	10.34.0.65
POR-LT2	Placa de Rede	IP por DHCP	MASCARA por DHCP	10.34.0.65
LIS-LT1	Placa de Rede	IP por DHCP	MASCARA por DHCP	10.34.0.33
POR-PC2	Placa de Rede	IP por DHCP	MASCARA por DHCP	10.34.0.33
LIS-S1	Placa de Rede	10.34.0.130	255.255.255.224	10.34.0.129
POR-S1	Placa de Rede	10.34.0.131	255.255.255.224	10.34.0.129

Tabela de endereçamento da rede Continente

Problemas encontrados e possíveis soluções

Ao longo do desenvolvimento do projeto, fomos enfrentados com adversidades, quer do ponto de vista de implementação de alguma funcionalidade na aplicação *Cisco Packet Tracer*, quer pelo facto de no enunciado termos alguns problemas que poderão complicar o bom funcionamento das redes. Nesta secção iremos enumerar os vários problemas que tivemos, as suas soluções e as configurações que não conseguimos implementar.

Problema com a quantidade de *switches* e o número de *hosts* disponíveis na rede Açores

Na rede Açores, precisamos na sub-rede “Management” de 6 *hosts*, sendo que os dispositivos que pertencem a esta rede são os *Switches*. Não precisam de possuir um endereço *IP* para que funcionem de forma correta, pois pertencendo à camada de ligação

de dados do modelo OSI resolvem certos pedidos, por exemplo de protocolo *ICMP* , através do *MAC address* dos dispositivos que estão conectados às suas *interfaces*. A atribuição do *IP* nos *switches*, serve para que estes sejam acedidos remotamente para configuração ou visualização das suas características.

O problema é que por termos: só 6 *hosts*, um *default-gateway* pertencente à sub-rede (6 *hosts* - 1 *host* = 5), não podemos atribuir mais *hosts*, pois a máscara de sub-rede tem ser obrigatoriamente /29, pelo facto de devido a partirmos de um endereço base que tem capacidade máxima de 254 *hosts* e não podemos “esticar” mais a máscara, ficamos com um *switch* a não possuir a possibilidade de ser modificado remotamente. Uma alternativa seria aumentar a máscara base de rede. Por exemplo ,partirmos de um comprimento de prefixo de /23, assim obteríamos 510 *hosts*. Outra solução seria, se obrigatoriamente todos os *switches* tivessem de ser acedidos à distância, retirar o último *switch* (S6) e passar todos os seus dispositivos para S5. Porém não é muito eficiente, pois teríamos a gastar dinheiro e hardware desnecessariamente.

Problema na atribuição dos servidores *DNS* pelo protocolo *DHCP* no *router* da rede Continente.

Na rede Continente, quando foi configurado o protocolo *DHCP* no *router* , verificámos que houve uma adversidade que não conseguímos ultrapassar. Numa certa *POOL* criada, é preciso dar obrigatoriamente o servidor *DNS* correspondente. Nesta rede tínhamos dois servidores *DNS*, um em Lisboa e outro no Porto, então o óbvio seria quando estivéssemos no comando *router#(dhcp-config)*, configurarmos os dois servidores *DNS*. Porém, depois de várias alternativas que pensámos como: em vez de termos 2 servidores, termos só 1 que cobriria todo o Continente, porém não seria eficiente, pois estaríamos a desperdiçar algo que já estava implementado. A solução que encontrámos foi que não há solução, pois a própria aplicação não possui a alternativa de termos 2 servidores *DNS* numa só *POOL*. Decidimos que cada uma ficaria com um dos dois servidores, funcionando assim como pretendido.

Problema da não escalabilidade presente em algumas sub-redes nas redes Madeira e Continente

Nas redes Madeira e Continente, existem sub-redes que, com a máscara que foi implementada, ficam com poucos *hosts* disponíveis para uso. Isso pode, no futuro, originar problemas de escalabilidade. Por exemplo na rede Madeira, na sub-rede Atendimento, temos 62 *hosts* disponíveis. Como o *default-gateway* ocupa um desses *hosts*, ficamos com 61 *hosts* disponíveis. Para o que é pedido que são 60 *hosts* (*default-gateway* não está incluído) funciona, mas se quiséssemos inserir mais computadores , não conseguímos. Como nesta rede temos 254 *hosts* disponíveis (à partida ,pois devido ao número de sub-redes existentes, esse número diminui, devido a termos os endereços de cada sub-rede e os de *broadcast*) e só estarmos usando no total 168 *hosts*, poderíamos alongar as máscaras nas sub-redes que têm poucos *hosts* disponíveis, assim dá uma maior liberdade ao utilizador, para inserir nas sub-redes os respectivos dispositivos sem ter de se preocupar com o número máximo de equipamentos disponíveis.

Na rede Continente, devido ao facto de termos 6 redes necessárias e estarmos usando o *Subnetting Standard* , que nos impossibilita de ajustarmos o tamanho (*hosts*) de cada

sub-rede, não conseguiríamos fazer a extensão de cada sub-rede. Pois a próxima máscara seria /26, onde teríamos 62 hosts disponíveis. $62 \times 6 > 256$, logo como partimos de um endereço de rede fixa /24, ou implementávamos o *VLSM* nesta rede, ou não seria possível a sua extensão, que originaria a falta de escalabilidade.

Configurações que não conseguimos implementar

A configuração do relógio interno dos equipamentos de rede foi parcialmente feita com sucesso. Todos os *routers* possuem as horas, minutos e segundos, fornecidas por um servidor *NTP*. Decidimos que na rede Açores, para simular o contexto real, atrasou-se em 1 hora o relógio em relação ao da Madeira que tem o fuso horário mais comum, o mesmo do *Meridiano de Greenwich (GMT/UTC+0)*. Por isso, em todos os restantes *routers* optámos por este horário (Madeira). Porém não conseguimos implementar esta funcionalidade nos *switches* presentes nas redes, pois não conseguem fazer *ping* ao servidor *NTP* correspondente. Até tentámos verificar as conexões das *VLAN's* nas *interfaces* , as *sub-interfaces* no *router* ou o tipo de conexão entre os *switches*, mas não chegámos a obter êxito.

No que toca à *NAT Overload*, tentámos implementá-la usando as respectivas instruções inerentes. Só que na *access-list* que possui o endereço da rede e um *wildcard* que simboliza o número (intervalo) de endereços privados que vão ser traduzidos para endereços públicos quando saírem da rede, chegámos à conclusão depois de alguns testes que não seria este *wildcard*. Na nossa ideia seria 0.0.0.255, pois como temos só *hosts* referentes a uma rede com *IPs* que diferem no último *byte* de um endereço IPv4, pensámos que estaríamos a implementar de maneira certa. Quando fazímos *ping* num dispositivo de outra rede, o pedido *ICMP* era feito com sucesso até o dispositivo destino, só que quando este fazia o *reply* ficava “preso” no *router* do dispositivo origem. Tentámos verificar qual seria o problema mas não achámos a solução. Até considerámos a hipótese de termos configurado sem querer, a negação/proibição do protocolo *ICMP* entre redes. O que resolvemos fazer foi deixar a *NAT* praticamente finalizada, pois na nossa opinião o que falta é modificar o *wildcard* para funcionar perfeitamente e conseguirmos fazer *ping* noutro dispositivo de outra rede, com a *NAT* ativada.

Testes e Resultados

No decorrer do nosso trabalho, foram realizados vários testes para verificar se todas as funcionalidades estavam bem implementadas. Um dos mais usados foi o protocolo *ICMP*, que é responsável por verificar se existe conexão entre dois dispositivos diferentes na rede. Podemos executar esta funcionalidade de diferentes maneiras como : no dispositivo(computador) , aceder à linha de comandos e fazer o comando *ping* X, em que X é o *IP* do dispositivo que queremos comunicar. No caso dos *routers*, é possível fazer através do *CLI* e o processo é igual. Ou de maneira ainda mais rápida, a aplicação possui um atalho que é uma *PDU* (unidade de dados de protocolo) simples, de maneira intuitiva clicamos nos dois dispositivos a verificar, aparecendo se a conexão foi feita com sucesso ou se falhou(**fig.13**). Outro teste executado foi nas três redes, em que verificámos se os computadores estavam a receber pelo protocolo *DHCP*, os respectivos *IP* 's. Uma das dificuldades que tivemos a implementar o *DHCP* pelo servidor, foi inicialmente não termos configurado o comando *ip helper-address* X no *router* , em que X é o *IP* do servidor *DHCP*, estando sempre a falhar

quando metíamos a opção *DHCP* na configuração dos computadores. Quando isso acontecia era atribuído um *IP* automático, mas que não pertencia à rede (**fig.14**).

Outra dificuldade que surgiu foi implementar o tipo de *routing*. A meio do projeto, pensámos que poderíamos fazer a conexão entre as diferentes redes, só através das rotas padrão. Por exemplo em todos os *routers*, fizemos X rotas padrão , em que X é o número de *interfaces* presentes, usando a *AD* (distância administrativa) para seguir uma certa rota primeiramente e só depois seguir as outras (quando um certo caminho não dá sucesso, o próprio protocolo *ICMP* tenta resolver o problema escolhendo outra rota padrão do *router*) . Resultou em termos de *ping*, só que não era a forma pedida pelo enunciado, por isso tivemos de alterar para o protocolo *RIPv2*.

Para a confirmação de que podemos aceder a um *site* a partir de um computador, é necessário testar se para certo *URL*, há um *output* (página gerada). Para isso, tivemos de averiguar se no servidor *DNS*, o nome do domínio estava presente e se o *IP* do servidor *WEB* estava associado a este. Obviamente para o computador comunicar com o servidor *DNS*, é necessário primeiro ter um certo *IP*, máscara de rede, *default-gateway* e o *IP* do servidor *DNS* correto. Se tivermos todos estes aspectos, então o teste do *site* funcionará perfeitamente e visualizaremos a página *HTML*. Caso contrário, no *output* aparece esta mensagem de erro (**fig.15**).

No nosso caso para acedermos remotamente a um certo *router*, o fazemos através do protocolo *SSH*, que devido ao facto de termos gerado as chaves *SSH* e termos criados linhas virtuais, que permitem haver sessões abertas de conexão entre um dispositivo e o equipamento de rede, é possível haver essa conexão à distância. Uma maneira de evitarmos que certo utilizador tente aceder ao *router* de maneira maliciosa, por exemplo com ataques de *brute force* (tentar várias palavras passe até acertar na correta), devemos implementar o comando: *login block-for X attempts Y within Z*, prevenindo/enfraquecendo a força destes ataques (**fig. 16**).

No que toca à configuração dos *switches* para interconexão, garantimos que apenas as *VLANs* estritamente necessárias foram configuradas, com a finalidade de permitirem tráfego específico de cada sub-rede através dos *links trunk*. Isto permitiu minimizar o tráfego desnecessário e melhorar a segmentação da rede (**fig.10**). Foram realizados inúmeros testes entre dispositivos presentes na rede e conectados a diferentes *switches*. Os seus resultados foram de sucesso, comprovando a boa implementação desta funcionalidade.

Conclusão

Com a execução deste trabalho, foi possível compreender melhor como uma rede deve ser configurada e como funcionar com a aplicação *Cisco Packet Tracer*. Foram aplicadas/aprimoradas várias técnicas, como o endereçamento de todos os dispositivos na rede, utilizando *subnetting VLSM* e *Standard*, distribuindo de forma eficiente os *IPs* pelas sub-redes.

Para cada ligação entre dispositivos foi escolhido o melhor cabo, por exemplo, cabos *Serial* para conexões entre *routers* (rede *WAN*), e *FastEthernet* para ligações entre computadores e *switches* (rede *LAN*). Foi tido em conta o número de *hosts* pretendido em cada sub-rede, modulando (aumentando/ diminuindo o comprimento de prefixo) as máscaras para que este aspecto fosse respeitado.

A implementação das diferentes sub-redes foi feita, por exemplo, com a configuração de *sub-interfaces* num certo *router* (referenciando o *IP* do *default gateway* de cada sub-rede) , permitindo a comunicação entre dispositivos de sub-redes distintas. A execução das configurações básicas/complexas em todos os dispositivos de rede, serviu para que a rede ficasse mais credível e funcional, sendo possível aceder a um *site* a partir de qualquer computador, através da configuração eficiente do servidor *DNS* e *WEB*. Para um certo site ficar ainda mais realista, optámos por adicionar código *HTML/CSS*, em diversos ficheiros/páginas presentes nos servidores *WEB*.

Outra implementação crucial neste trabalho, foi a configuração do protocolo *DHCP* nos servidores respectivos (Açores, Madeira) e *router* (Continente), atribuindo dinamicamente endereços *IP*, em todos os computadores ; relacionou-se também as *interfaces* dos *switches* com as *VLANs* correspondentes e implementou-se a técnica de *NAT overload*, permitindo a tradução de endereços privados em públicos; configurou-se o *routing* dinâmico com o protocolo *RIPv2*, garantindo a comunicação entre dispositivos em redes distintas, entre outras funcionalidades já descritas previamente.

Como já mencionado, para a realização deste projeto foi utilizada a aplicação *Cisco Packet Tracer*, cuja *interface* intuitiva, aliada a dicas/vídeos de ajuda integrados e ao material disponibilizado pelos docentes (*slides* teóricos e fichas práticas), tornaram a implementação do trabalho mais acessível e menos difícil/exaustiva.

Anexos

Nas próximas páginas estão disponíveis todas as configurações gravadas (NVRAM) , de todos os equipamentos de rede e a topologia da rede.

Routers

Pld-Router

```

!#show running-config
Using 3530 bytes
!
version 15.1
no service timestamp log datetime msec
no service timestamps debug datetime msec
service password-encryption
security password-max-length 12
!
hostname PidRouter
login block-for 30 attempts 3 within 60
!
enable secret 5 $10$ERp0.RGLvme0@W1TKvGd8B/
!
!
!
no ip cef
no ipre ipre
!
!
username metadamin privilege 15 secret 5 $10$ERp0.RGLvme0@W1TKvGd8B/Console1
!
license udl pid CISCO2811/K9 sn FX10174LMS-
!
!
!
!
!
no ip domain-lookup
ip domain-name cam.gov.pt
!
spanning-tree mode pwt
!
!
!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
!
interface FastEthernet0/0.10
description interface que faz conexao dos dispositivos com vian id:10, com o PidRouter
encapsulation dot1Q 10
ip address 10.210.34.241 255.255.255.248
ip nat inside
!
interface FastEthernet0/0.15
description interface que faz a conexao dos dispositivos com vian id:15, com o PidRouter
encapsulation dot1Q 15
ip address 10.210.34.129 255.255.255.192
ip nat inside
!
interface FastEthernet0/0.55
description interface que faz a conexao dos dispositivos com vian id:55, com o PidRouter
encapsulation dot1Q 55
ip address 10.210.34.193 255.255.255.224
ip nat inside
!
interface FastEthernet0/0.90
description interface que faz a conexao dos dispositivos com vian id:90, com o PidRouter
encapsulation dot1Q 90
ip address 10.210.34.199 255.255.255.224
ip nat inside
!
interface FastEthernet0/0.130
description interface que faz a conexao dos dispositivos com vian id:130, com o PidRouter
encapsulation dot1Q 130
ip address 10.210.34.225 255.255.255.240
ip nat inside
!
interface FastEthernet0/0.500
description interface que faz a conexao dos dispositivos com vian id:500, com o PidRouter
encapsulation dot1Q 500
ip address 10.210.34.249 255.255.255.248
ip nat inside
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Serial1/0
description interface do tipo serial que faz a conexao do NeoRouter com o PidRouter
ip address 62.223.143.101 255.255.255.252
ip nat outside
!
interface Serial1/1
no ip address
clock rate 2000000
shutdown
!
interface Serial1/2
no ip address
clock rate 2000000
shutdown
!
interface Serial1/3
no ip address
clock rate 2000000
shutdown
!
interface Vlan1
no ip address
shutdown
!
router rip
version 2
passive-interface FastEthernet0/0
network 10.0.0.0
network 62.0.0.0
default-information originate
no auto-summary
!
ip nat inside source list 1 interface Serial1/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 62.223.143.102
ip flow-export version 9
!
ip access-list extended sl_def_acl
deny tcp any any eq telnet
deny tcp any any eq www
deny tcp any any eq 22
permit ip any any eq 22
access-list 1 permit host 10.210.34.0
banner motd "C
!! UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED !!
You must have explicit, authorized permission to access or configure this device.
Unauthorized attempts and actions to access or use this system may result in civil and/or
All activities performed on this device are logged and monitored."C
!
!
line con 0
exec-timeout 0 0
password 7 0802455D0A16261E0100803567F79747A666772C
login
transport input ssh
!
ntp server 10.210.34.226
!
end

!#show running-config

```

Fnc-Router

```

FncRouter#show startup-config
Using 3332 bytes
!
version 15.1
no service timestamp log datetime msec
no service timestamp debug datetime msec
service password-encryption
security passwords min-length 12
!
hostname FncRouter
!
login block-for 30 attempts 3 within 60
!
enable secret 5 $1$0mErRrSp0.rGLvw6cWWiTTkVdAB8/
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
username netadmin privilege 15 secret 5 $1$0mErRv1CkLMcTWwkFlCndll.
!
license udi pid CISCO2811/K9 sn FTX10178TQ-
!
!
!
!
!
!
no ip domain-lookup
ip domain-name cam.gov.pt
!
!
spanning-tree mode pwt
!
!
!
!
!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
!
interface FastEthernet0/0.10
description interface que faz a conexao dos dispositivos com vian id:10, com o FncRouter
encapsulation dot1Q 10
ip address 172.16.34.161 255.255.255.240
ip nat inside
!
interface FastEthernet0/0.15
description interface que faz a conexao dos dispositivos com vian id:15, com o FncRouter
encapsulation dot1Q 15
ip address 172.16.34.129 255.255.255.240
ip nat inside
!
interface FastEthernet0/0.55
description interface que faz a conexao dos dispositivos com vian id:55, com o FncRouter
encapsulation dot1Q 55
ip address 172.16.34.1 255.255.255.192
ip nat inside
ip address 172.16.34.146
ip nat inside
!
interface FastEthernet0/0.90
description interface que faz a conexao dos dispositivos com vian id:90, com o FncRouter
encapsulation dot1Q 90
ip address 172.16.34.68 255.255.255.192
ip nat inside
!
interface FastEthernet0/0.130
description interface que faz a conexao dos dispositivos com vian id:130, com o FncRouter
encapsulation dot1Q 130
ip address 172.16.34.145 255.255.255.240
ip nat inside
!
interface FastEthernet0/0.500
description interface que faz a conexao dos dispositivos com vian id:500, com o FncRouter
encapsulation dot1Q 800
ip address 172.16.34.177 255.255.255.248
ip nat inside
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Serial1/0
description interface do tipo serial que faz a conexao do NsRouter com o FncRouter
ip address 231.109.141 255.255.255.252
ip nat outside
clock rate 64000
!
interface Serial1/1
no ip address
clock rate 2000000
shutdown
!
interface Serial1/2
no ip address
clock rate 2000000
shutdown
!
interface Serial1/3
no ip address
clock rate 2000000
shutdown
!
interface Vlan1
no ip address
shutdown
!
router rip
version 2
passive-interface FastEthernet0/0
network 25.0.0.0
network 172.16.0.0
default-information originate
no auto-summary
!
ip nat inside source list 1 interface Serial1/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 88.231.109.142
!
ip flow-export version 9
!
ip access-list extended sl_def_acl
deny tcp any any eq telnet
deny tcp any any eq www
deny tcp any any eq 22
permit tcp any any eq 22
access-list 1 permit host 172.16.34.0
!
banner motd "C
! UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED !!
You must have explicit, authorized permission to access or configure this device.
Unauthorized attempts and actions to access or use this system may result in civil and/or criminal penalties.
All activities performed on this device are logged and monitored."C
!
!
line con 0
password 7 0802455D0A16261E010803567F79747A66651D
login
!
line aux 0
!
line vty 0 4
password 7 0802455D0A16261E010803567F79747A666772C
login local
transport input ssh
!
ntp server 172.16.34.147
!
end
FncRouter# |

```

Sines-Router

Meo-Router

```

MeoRouter#show startup-config
using 1888 bytes
!
version 15.1
no service timestamp log datetime msec
no service timestamp debug datetime msec
service password-encryption
security passwords min-length 12
!
hostname MeoRouter
!
!
enable secret 5 $1$meEr$Sp0.rGLvw6oWWiTTkVdABH/
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
username netadmin privilege 15 secret 5 $1$meEr$ViCkLMcTYWkf1Cndt11.
!
!
license udi pid CISCO2811/K9 sn FTX10171XG7-
!
!
!
!
!
!
no ip domain-lookup
ip domain-name cam.gov.pt
!
spanning-tree mode pvt
!
!
!
!
!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
shutdown
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Serial1/0
description interface do tipo serial que faz a conexao do PidRouter com o MeoRouter
ip address 62.223.143.102 255.255.255.252
clock rate 64000
!
interface Serial1/1
description interface do tipo serial que faz a conexao do MainRouter com o MeoRouter
ip address 62.31.53.17 255.255.255.252
clock rate 64000
!
interface Serial1/2
description interface do tipo serial que faz a conexao do MeoRouter com o NosRouter
ip address 62.33.5.41 255.255.255.252
!
interface Serial1/3
no ip address
clock rate 2000000
!
interface Vlan1
no ip address
!
router rip
version 2
network 62.0.0.0
no auto-summary
!
ip classless
!
ip flow-export version 9
!
!
!
banner motd "C
!! UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED !!
You must have explicit, authorized permission to access or configure this device.
Unauthorized attempts to access or use this system may result in civil and/or criminal penalties.
All activities performed on this device are logged and monitored."C
!
!
!
line con 0
password 7 0802455D0A16261E010803567F79747A66651D
login
!
line aux 0
!
line vty 0 4
password 7 0802455D0A16261E010803567F79717A6667772C5C
login local
transport input ssh
!
!
ntp server 10.210.34.226
!
end
MeoRouter#

```

Nos-Router

```

NosRouter#show startup-config
Building configuration
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
security passwords min-length 12
!
hostname NosRouter
!
!
enable secret 5 $1$meRrSp0.rGLvw6oWWITkVgABR/
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
username admin privilege 15 secret 5 $1$meRr$Y1OkIMcTYWwkJ1Cndt11.
!
!
license udi pid CISCO2811/K9 an FTX1017INON-
!
!
!
!
!
!
no ip domain-lookup
ip domain-name cam.gov.pt
!
!
!
spanning-tree mode pvrst
!
!
!
!
!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
shutdown
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Serial1/0
description interface do tipo serial que faz a conexão do VodRouter com o NosRouter
ip address 142.140.5.77 255.255.255.252
clock rate 64000
!
interface Serial1/1
description interface do tipo serial que faz a conexão do MeoRouter com o NosRouter
ip address 142.140.5.42 255.255.255.252
clock rate 64000
!
interface Serial1/2
description interface do tipo serial que faz a conexão do MainRouter com o NosRouter
ip address 89.180.24.41 255.255.255.252
clock rate 64000
!
interface Serial1/3
description interface do tipo serial que faz a conexão do FncRouter com o NosRouter
ip address 89.231.109.142 255.255.255.252
!
interface Vlan1
no ip address
shutdown
!
router rip
version 2
network 142.0.0.0
network 89.0.0.0
network 142.140.0.0
no auto-summary
!
ip classless
!
ip flow-export version 9
!
!
banner motd "C
!! UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED !!

You must have explicit, authorized permission to access or configure this device.
Unauthorized attempts and actions to access or use this system may result in civil and/or criminal penalties.
All activities performed on this device are logged and monitored."C
!
!
!
line con 0
password 7 0802455D0A1e261E010803567F79717A6667772C
login
!
line aux 0
!
line vty 0 4
password 7 0802455D0A1e261E010803567F79717A6667772C
login local
transport input ssh
!
ntp server 172.16.34.147
!
end

NosRouter#

```

Vod-Router

```

VodRouter#show startup-config
Using 1931 bytes
!
version 15.1
no service timestamp log datetime msec
no service timestamp debug datetime msec
service password-encryption
security passwords min-length 12
!
hostname VodRouter
!
!
enable secret 5 $1$0mErz$p0.rGLvw6cWWiTTkVdABM/
!
!
!
!
no ip cef
no ipv6 cef
!
!
username netadmin privilege 15 secret 5 $1$0mErz$YlCkLMcTYwkJ1Cond1l.
!
!
license udi pid CISCO2811/K9 an FTX1017TSRS-
!
!
!
!
!
no ip domain-lookup
ip domain-name cam.gov.pt
!
spanning-tree mode pvst
!
!
!
!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
shutdown
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Serial1/0
description interface do tipo serial que faz a conexao do SinesRouter com o VodRouter
ip address 143.128.31.42 255.255.255.252
!
interface Serial1/1
description interface do tipo serial que faz a conexao do NosRouter com o VodRouter
ip address 142.140.37.78 255.255.255.252
!
interface Serial1/2
description interface do tipo serial que faz a conexao do MainRouter com o VodRouter
ip address 23.1.31.3 255.255.255.252
clock rate 64000
!
interface Serial1/3
no ip address
clock rate 2000000
shutdown
!
interface Vlan1
no ip address
shutdown
!
router rip
version 2
network 23.0.0.0
network 143.129.0.0
network 143.129.0.0
no auto-summary
!
ip classless
!
ip flow-export version 9
!
!
banner modem "C
! UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED !!

You must have explicit, authorized permission to access or configure this device.
Unauthorized attempts and actions to access or use this system may result in civil and/or criminal penalties.
All activities performed on this device are logged and monitored."C
!
!
!
line con 0
password 7 0802455D0A16261E010803567F79747A66651D
login
!
line aux 0
!
line vty 0 4
password 7 0802455D0A16261E010803567F79717A6667772C
login local
transport input ssh
!
ntp server 172.16.34.147
!
end
VodRouter#

```

MainRouter

```

MainRouter#show startup-config
Using 2429 bytes
!
version 15.1
no service timestamp log datetime msec
no service timestamp debug datetime msec
service password-encryption
security passwords min-length 12
!
hostname MainRouter
!
login block-for 60 attempts 3 within 30
!
enable secret 5 $1$OmERr5p0.rGLvv6oWWiTTKvDABH/
!
!
!
!
ip cef
no ipv6 cef
!
!
!
username netadmin privilege 15 secret 5 $1$OmERr5RldxcZZEsITfIEtUyRaA50
!
!
!
license udi pid CISCO2811/K9 sn FTK10176UNK-
!
!
!
!
!
!
ip ssh version 2
no ip domain-lookup
ip domain-name cam.gov.pt
!
!
spanning-tree mode pvtst
!
!
!
!
!
!
interface FastEthernet0/0
description interface do tipo fastEthernet que faz a conexao do servidor cloudflare DNS com o MainRouter
ip address 1.1.1.12 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
description interface do tipo fastEthernet que faz a conexao do servidor web com o MainRouter
ip address 172.67.185.1 255.255.255.0
duplex auto
speed auto
!
interface Serial1/0
description interface do tipo serial que faz a conexao do NosRouter com o MainRouter
ip address 10.10.10.10 255.255.255.252
!
interface Serial1/1
description interface do tipo serial que faz a conexao do MeoRouter com o MainRouter
ip address 42.31.53.18 255.255.255.252
!
interface Serial1/2
description interface do tipo serial que faz a conexao do VodRouter com o MainRouter
ip address 23.1.1.16 255.255.255.252
!
interface Serial1/3
no ip address
clock rate 2000000
shutdown
!
interface Vlan1
no ip address
shutdown
!
router rip
version 2
passive-interface FastEthernet0/0
passive-interface FastEthernet0/1
network 1.0.0.0
network 23.0.0.0
network 42.0.0.0
network 69.0.0.0
network 172.67.0.0
no auto-summary
!
ip classless
!
ip flow-export version 9
!
ip access-list extended sl_def_acl
deny tcp any any eq telnet
deny tcp any any eq www
deny tcp any any eq 22
permit tcp any any eq 22
!
banner motd "C
!! UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED !!
You must have explicit, authorized permission to access or configure this device.
Unauthorized attempts and actions to access or use this system may result in civil and/or criminal penalties.
All activities performed on this device are logged and monitored."C
!
!
line con 0
password 7 0802455D0A16261E010803567F7974A66651D
login
!
line aux 0
!
line vty 0 4
password 7 0802455D0A16261E010803567F7971A6667772C
login local
transport input ssh
!
ntp server 172.16.34.147
!
end
MainRouter#

```

Switches

PId-S1 (Switch)

```

PIdS1#show startup-config
Using 3744 bytes
!
version 15.0
no service timestamp log datetime nsec
no service timestamp debug datetime nsec
service password-encryption
!
hostname PIdS1
!
enable secret 5 $1$MErRzSp0.rGLvv6oWW11TkVdABH/
!
!
ip domain-name cam.gov.pt
!
username netadmin secret 5 $1$MErRzSp0.rGLvv6oWW11TkVdABH/
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface Port-channel
switchport trunk allowed vlan 10,15,55,90,130
switchport mode trunk
!
interface FastEthernet0/1
description interface do tipo fastEthernet que faz a conexao do PId-WEB com o PId-S1
switchport access vlan 130
switchport mode access
!
interface FastEthernet0/3
description interface do tipo fastEthernet que faz a conexao do PId-DNS com o PId-S1
switchport access vlan 130
switchport mode access
!
interface FastEthernet0/4
description interface do tipo fastEthernet que faz a conexao do PId-NTP com o PId-S1
switchport access vlan 130
switchport mode access
!
interface FastEthernet0/5
description interface do tipo fastEthernet que faz a conexao do PId-PI com o PId-S1
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/6
description interface do tipo fastEthernet que faz a conexao do PIdRouter com o PId-S1
switchport trunk allowed vlan 10,15,55,90,130
switchport mode trunk
!
interface FastEthernet0/7
description interface do tipo fastEthernet que faz a conexao do PId-API com o PId-S1
switchport trunk allowed vlan 90
switchport mode access
!
interface FastEthernet0/8
description interface do tipo fastEthernet que faz a conexao do PId-S2 com o PId-S1. Serve para conectar dois switches. Existem duas conexoes iguais para casos de falha em alguma interface/conexao. Redundancia para a resolucao desse possivel problema.
switchport trunk allowed vlan 10,15,55,90,130
switchport mode trunk
channel-group 1 mode passive
!
interface FastEthernet0/9
description interface do tipo fastEthernet que faz a conexao do PId-S2 com o PId-S1. Serve para conectar dois switches. Existem duas conexoes iguais para casos de falha em alguma interface/conexao. Redundancia para a resolucao desse possivel problema.
switchport trunk allowed vlan 10,15,55,90,130
switchport mode trunk
channel-group 1 mode passive
!
interface FastEthernet0/10
shutdown
!
interface FastEthernet0/11
shutdown
!
interface FastEthernet0/12
shutdown
!
interface FastEthernet0/13
shutdown
!
interface FastEthernet0/14
shutdown
!
interface FastEthernet0/15
shutdown
!
interface FastEthernet0/16
shutdown
!
interface FastEthernet0/17
shutdown
!
interface FastEthernet0/18
shutdown
!
interface FastEthernet0/19
shutdown
!
interface FastEthernet0/20
shutdown
!
interface FastEthernet0/21
shutdown
!
interface FastEthernet0/22
shutdown
!
interface FastEthernet0/23
shutdown
!
interface FastEthernet0/24
shutdown
!
interface GigabitEthernet0/1
shutdown
!
interface GigabitEthernet0/2
shutdown
!
interface Vlan1
no ip address
!
interface Vlan500
ip address 10.210.34.250 255.255.255.248
ip default-gateway 10.210.34.249
!
banner motd "C
!! UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED !!
You must have explicit, authorized permission to access or configure this device.
Unauthorized attempts and actions to access or use this system may result in civil and/or criminal penalties.
All activities performed on this device are logged and monitored."C
!
!
line con 0
password 7 0802455D0A16261E010803567F797A66651D
login
!
line vty 0 4
password 7 0802455D0A16261E010803567F79717A6667772C
login local
transport input ssh
line vty 5 15
login
!
ntp server 10.210.34.226
!
end
PIdS1# +

```

Pls-S2 (Switch)

```

PlsS2#show start
PlsS2#show startup-config
Using 4766 bytes
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname PlsS2
!
enable secret 5 $1$0mErzSp0.rGLvw6c0W1TTkVdASH/
!
!
ip domain-name com.gov.pt
!
username netadmin secret 5 $1$0mErzSp1k1McTWWkfCcmd11.
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
  switchport trunk allowed vlan 10,15,55,90,130
  switchport mode trunk
!
interface Port-channel2
  switchport trunk allowed vlan 10,15,55,90,130
  switchport mode trunk
  interface Port-channel3
  switchport trunk allowed vlan 10,15,55,90,130
  switchport mode trunk
  interface FastEthernet0/1
  description Interface do tipo fastEthernet que faz a conexao do Pld-S1 com o Pld-S2. Serve para conectar dois switches. Existem duas conexoes iguais para casos de falha nalguma interface/conexao. Redundancia para a resolucao desse possivel problema.
  switchport trunk allowed vlan 10,15,55,90,130
  switchport mode trunk
  channel-group 1 mode passive
  interface FastEthernet0/2
  description Interface do tipo fastEthernet que faz a conexao do Pld-S3 com o Pld-S2. Serve para conectar dois switches. Existem duas conexoes iguais para casos de falha nalguma interface/conexao. Redundancia para a resolucao desse possivel problema.
  switchport trunk allowed vlan 10,15,55,90,130
  switchport mode trunk
  channel-group 1 mode passive
  interface FastEthernet0/3
  description Interface do tipo fastEthernet que faz a conexao do Pld-PC9 com o Pld-S2
  switchport access vlan 55
  switchport mode access
  interface FastEthernet0/4
  description Interface do tipo fastEthernet que faz a conexao do Pld-S1 com o Pld-S2. Serve para conectar dois switches. Existem duas conexoes iguais para casos de falha nalguma interface/conexao. Redundancia para a resolucao desse possivel problema.
  switchport trunk allowed vlan 10,15,55,90,130
  switchport mode trunk
  channel-group 1 mode passive
  interface FastEthernet0/5
  description Interface do tipo fastEthernet que faz a conexao do Pld-S2 com o Pld-S2
  switchport access vlan 10
  switchport mode access
  interface FastEthernet0/6
  description Interface do tipo fastEthernet que faz a conexao do Pld-AP2 com o Pld-S2
  switchport access vlan 90
  switchport mode access
  interface FastEthernet0/7
  description Interface do tipo fastEthernet que faz a conexao do Pld-S3 com o Pld-S2. Serve para conectar dois switches. Existem duas conexoes iguais para casos de falha nalguma interface/conexao. Redundancia para a resolucao desse possivel problema.
  switchport trunk allowed vlan 10,15,55,90,130
  switchport mode trunk
  channel-group 3 mode passive
  interface FastEthernet0/8
  shutdown
  interface FastEthernet0/9
  shutdown
  interface FastEthernet0/10
  description Interface do tipo fastEthernet que faz a conexao do Pld-S4 com o Pld-S2. Serve para conectar dois switches. Existem duas conexoes iguais para casos de falha nalguma interface/conexao. Redundancia para a resolucao desse possivel problema.
  switchport trunk allowed vlan 10,15,55,90,130
  switchport mode trunk
  channel-group 2 mode passive
  interface FastEthernet0/11
  shutdown
  interface FastEthernet0/12
  shutdown
  interface FastEthernet0/13
  shutdown
  interface FastEthernet0/14
  shutdown
  interface FastEthernet0/15
  shutdown
  interface FastEthernet0/16
  shutdown
  interface FastEthernet0/17
  shutdown
  interface FastEthernet0/18
  description Interface do tipo fastEthernet que faz a conexao do Pld-S4 com o Pld-S2. Serve para conectar dois switches. Existem duas conexoes iguais para casos de falha nalguma interface/conexao. Redundancia para a resolucao desse possivel problema.
  switchport trunk allowed vlan 10,15,55,90,130
  switchport mode trunk
  channel-group 2 mode passive
  interface FastEthernet0/19
  shutdown
  interface FastEthernet0/20
  shutdown
  interface FastEthernet0/21
  shutdown
  interface FastEthernet0/22
  shutdown
  interface FastEthernet0/23
  shutdown
  interface FastEthernet0/24
  shutdown
  interface GigabitEthernet0/1
  shutdown
  interface GigabitEthernet0/2
  shutdown
  interface Vlan500
  no ip address
  interface Vlan500
  ip address 10.210.34.251 255.255.255.248
  !
  ip default-gateway 10.210.34.249
  !
  banner motd ^C
  !! UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED !!
You must have explicit, authorized permission to access or configure this device.
Unauthorized attempts and actions to access or use this system may result in civil and/or criminal penalties.
All activities performed on this device are logged and monitored.^C
!
!
line con 0
password 7 0802455D0A16261E010803567F79747A66651D
login
line vty 0 4
password 7 0802455D0A16261E010803567F79747A66651D
login local
transport input ssh
line vty 5 15
login
!
ntp server 10.210.34.226
!
end
PlsS2#

```

Pld-S3 (Switch)

```

PldS3#show startup-config
Using 4239 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname PldS3
enable secret 5 $1$Erp0.rGlrw6oWw1TkvGABH/
!
ip domain-name cam.gov.pt
username metadmin secret 5 $1$Erp0ViCkln6TJWwKF1Cndtl1.
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface Port-channel3
switchport trunk allowed vlan 10,15,55,90,130
switchport mode trunk
!
interface Port-channel4
switchport trunk allowed vlan 10,15,55,90,130
switchport mode trunk
!
interface FastEthernet0/1
description interface do tipo fastEthernet que faz a conexao do Pld-S2 com o Pld-S3. Serve para conectar dois switches. Existem duas conexoes iguais para casos de falha nalguma interface/conexao. Redundancia para a resolucao desse possivel problema.
switchport trunk allowed vlan 10,15,55,90,130
switchport mode trunk
channel-group 1 mode passive
!
interface FastEthernet0/2
description interface do tipo fastEthernet que faz a conexao do Pld-S4 com o Pld-S3. Serve para conectar dois switches. Existem duas conexoes iguais para casos de falha nalguma interface/conexao. Redundancia para a resolucao desse possivel problema.
switchport trunk allowed vlan 10,15,55,90,130
switchport mode trunk
channel-group 2 mode passive
!
interface FastEthernet0/3
description interface do tipo fastEthernet que faz a conexao do Pld-S5 com o Pld-S3. Serve para conectar dois switches. Neste caso pode haver perda de informacao , porque nao ha redundancia.
switchport trunk allowed vlan 10,15,55,90,130
switchport mode trunk
!
interface FastEthernet0/4
description interface do tipo fastEthernet que faz a conexao do PC-PC4 com o Pld-S3
switchport access vlan 55
switchport mode access
!
interface FastEthernet0/5
description interface do tipo fastEthernet que faz a conexao do PC-PC5 com o Pld-S3
switchport access vlan 55
switchport mode access
!
interface FastEthernet0/6
description interface do tipo fastEthernet que faz a conexao do Pld-S2 com o Pld-S3. Serve para conectar dois switches. Existem duas conexoes iguais para casos de falha nalguma interface/conexao. Redundancia para a resolucao desse possivel problema.
switchport trunk allowed vlan 10,15,55,90,130
switchport mode trunk
channel-group 3 mode passive
!
interface FastEthernet0/7
description interface do tipo fastEthernet que faz a conexao do Pld-S4 com o Pld-S3. Serve para conectar dois switches. Existem duas conexoes iguais para casos de falha nalguma interface/conexao. Redundancia para a resolucao desse possivel problema.
switchport trunk allowed vlan 10,15,55,90,130
switchport mode trunk
channel-group 4 mode passive
!
interface FastEthernet0/8
description interface do tipo fastEthernet que faz a conexao do Pld-S5 com o Pld-S3
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/9
shutdown
!
interface FastEthernet0/10
shutdown
!
interface FastEthernet0/11
shutdown
!
interface FastEthernet0/12
shutdown
!
interface FastEthernet0/13
shutdown
!
interface FastEthernet0/14
shutdown
!
interface FastEthernet0/15
shutdown
!
interface FastEthernet0/16
shutdown
!
interface FastEthernet0/17
shutdown
!
interface FastEthernet0/18
shutdown
!
interface FastEthernet0/19
shutdown
!
interface FastEthernet0/20
shutdown
!
interface FastEthernet0/21
shutdown
!
interface FastEthernet0/22
shutdown
!
interface FastEthernet0/23
shutdown
!
interface FastEthernet0/24
shutdown
!
interface GigabitEthernet0/1
shutdown
!
interface GigabitEthernet0/2
shutdown
!
interface Vlan1
no ip address
!
interface Vlan500
ip address 10.210.34.252 255.255.255.248
ip default-gateway 10.210.34.249
banner motd ^C
!! UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED !!
You must have explicit, authorized permission to access or configure this device.
Unauthorized attempts and actions to access or use this system may result in civil and/or criminal penalties.
All activities performed on this device are logged and monitored.^C
!
!
line con 0
password 7 0802455D0A16261E010803567F7974A66651D
login
!
line vty 0 4
password 7 0802455D0A16261E010803567F7971A6667772C
login local
transport input ssh
line vty 5 15
login
!
!
ftp server 10.210.34.226
!
end
PldS3#

```

Pld-S4 (Switch)

```

PldS4# show startup-config
Using 4498 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname PldS4
!
enable secret 5 $1$0mErkRp0.rGLvw6oWW1TtKVGBRM/
!
!
ip domain-name cam.gov.pt
!
username netadmin secret 5 $1$0mErzViCkLMcTWvkF1Cmctl1.
!
!
spanning-tree mode pvrp
spanning-tree extend system-id
!
interface Port-channel1
switchport trunk allowed vlan 10,15,55,90,130
switchport mode trunk
!
interface Port-channel14
switchport trunk allowed vlan 10,15,55,90,130
switchport mode trunk
!
interface FastEthernet0/1
description interface do tipo fastEthernet que faz a conexao do Pld-S3 com o Pld-S4. Serve para conectar dois switches. Existem duas conexoes iguais para casos de falha nalguma interface/conexao. Redundancia para a resolucao desse possivel problema.
switchport trunk allowed vlan 10,15,55,90,130
switchport mode trunk
channel-group 4 mode passive
!
interface FastEthernet0/2
description interface do tipo fastEthernet que faz a conexao do Pld-S3 com o Pld-S4. Serve para conectar dois switches. Existem duas conexoes iguais para casos de falha nalguma interface/conexao. Redundancia para a resolucao desse possivel problema.
switchport trunk allowed vlan 10,15,55,90,130
switchport mode trunk
channel-group 4 mode passive
!
interface FastEthernet0/3
description interface do tipo fastEthernet que faz a conexao do Pld-P4 com o Pld-S4
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/4
description interface do tipo fastEthernet que faz a conexao do Pld-AP4 com o Pld-S4
switchport access vlan 90
switchport mode access
!
interface FastEthernet0/5
description interface do tipo fastEthernet que faz a conexao do Pld-PC1 com o Pld-S4
switchport access vlan 55
switchport mode access
!
interface FastEthernet0/6
description interface do tipo fastEthernet que faz a conexao do Pld-PC2 com o Pld-S4
switchport access vlan 55
switchport mode access
!
interface FastEthernet0/7
description interface do tipo fastEthernet que faz a conexao do Pld-PC3 com o Pld-S4
switchport access vlan 55
switchport mode access
!
interface FastEthernet0/8
description interface do tipo fastEthernet que faz a conexao do Pld-IoT2 com o Pld-S4
switchport access vlan 15
switchport mode access
!
interface FastEthernet0/9
description interface do tipo fastEthernet que faz a conexao do Pld-IoT1 com o Pld-S4
switchport access vlan 15
switchport mode access
!
interface FastEthernet0/10
description interface do tipo fastEthernet que faz a conexao do Pld-S2 com o Pld-S4. Serve para conectar dois switches. Existem duas conexoes iguais para casos de falha nalguma interface/conexao. Redundancia para a resolucao desse possivel problema.
switchport trunk allowed vlan 10,15,55,90,130
switchport mode trunk
channel-group 2 mode passive
!
interface FastEthernet0/11
shutdown
!
interface FastEthernet0/12
shutdown
!
interface FastEthernet0/13
shutdown
!
interface FastEthernet0/14
shutdown
!
interface FastEthernet0/15
shutdown
!
interface FastEthernet0/16
shutdown
!
interface FastEthernet0/17
shutdown
!
interface FastEthernet0/18
description interface do tipo fastEthernet que faz a conexao do Pld-S2 com o Pld-S4. Serve para conectar dois switches. Existem duas conexoes iguais para casos de falha nalguma interface/conexao. Redundancia para a resolucao desse possivel problema.
switchport trunk allowed vlan 10,15,55,90,130
switchport mode trunk
channel-group 2 mode passive
!
interface FastEthernet0/19
shutdown
!
interface FastEthernet0/20
shutdown
!
interface FastEthernet0/21
shutdown
!
interface FastEthernet0/22
shutdown
!
interface FastEthernet0/23
shutdown
!
interface FastEthernet0/24
shutdown
!
interface GigabitEthernet0/1
shutdown
!
interface GigabitEthernet0/2
shutdown
!
interface Vlan1
no ip address
!
interface Vlan500
ip address 10.210.34.253 255.255.255.249
ip default-gateway 10.210.34.249
!
banner motd "C
!! UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED !!
You must have explicit, authorized permission to access or configure this device.
Unauthorized attempts and actions to access or use this system may result in civil and/or criminal penalties.
All activities performed on this device are logged and monitored.^C
!
!
line con 0
password ? 080245SD0a16261E010803567F7974A66651D
login
!
line vty 0 4
password ? 080245SD0a16261E010803567F7971A6667772C
login local
transport input ssh
line vty 5 15
login
!
ntp server 10.210.34.226
!
end
PldS4# |

```

Pld-S5 (Switch)

```

PldSS#show startup-config
Using 3209 bytes
!
version 1.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname PldS5
!
enable secret 5 $1$6mERrp0.rGLvweoWWT1kVdABH/
!
!
ip domain-name can.gov.pt
username netadmin secret 5 $1$6mERr5V1ckLMoTYwkf1Cndt11.
!
!
spanning-tree mode pvrst
spanning-tree extend system-id
!
interface Port-channels1
switchport trunk allowed vlan 10,15,55,90,130
switchport mode trunk
!
interface FastEthernet0/1
description interface do tipo fastEthernet que faz a conexao do PLD-S5 com o Pld-S5. Serve para conectar dois switches. Neste caso pode haver perda de informacao , porque nao ha redundancia.
switchport trunk allowed vlan 10,15,55,90,130
switchport mode trunk
!
interface FastEthernet0/2
description interface do tipo fastEthernet que faz a conexao do PLD-S6 com o Pld-S5. Serve para conectar dois switches. Existem duas conexoes iguais para casos de falha em alguma interface/conexao. Redundancia para a resolucao desse possivel problema.
switchport trunk allowed vlan 10,15,55,90,130
switchport mode trunk
channel-group 5 mode passive
!
interface FastEthernet0/3
description interface do tipo fastEthernet que faz a conexao do PLD-PC8 com o Pld-S5
switchport access vlan 55
switchport mode access
!
interface FastEthernet0/4
description interface do tipo fastEthernet que faz a conexao do PLD-S6 com o Pld-S5. Serve para conectar dois switches. Existem duas conexoes iguais para casos de falha em alguma interface/conexao. Redundancia para a resolucao desse possivel problema.
switchport trunk allowed vlan 10,15,55,90,130
switchport mode trunk
channel-group 5 mode passive
!
interface FastEthernet0/5
shutdown
!
interface FastEthernet0/6
shutdown
!
interface FastEthernet0/7
shutdown
!
interface FastEthernet0/8
shutdown
!
interface FastEthernet0/9
shutdown
!
interface FastEthernet0/10
shutdown
!
interface FastEthernet0/11
shutdown
!
interface FastEthernet0/12
shutdown
!
interface FastEthernet0/13
shutdown
!
interface FastEthernet0/14
shutdown
!
interface FastEthernet0/15
shutdown
!
interface FastEthernet0/16
shutdown
!
interface FastEthernet0/17
shutdown
!
interface FastEthernet0/18
shutdown
!
interface FastEthernet0/19
shutdown
!
interface FastEthernet0/20
shutdown
!
interface FastEthernet0/21
shutdown
!
interface FastEthernet0/22
shutdown
!
interface FastEthernet0/23
shutdown
!
interface FastEthernet0/24
shutdown
!
interface GigabitEthernet0/1
shutdown
!
interface GigabitEthernet0/2
shutdown
!
interface Vlan1
no ip address
!
interface Vlan500
ip address 10.210.34.254 255.255.255.248
ip default-gateway 10.210.34.249
banner motd "C
!! UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED !!
You must have explicit, authorized permission to access or configure this device.
Unauthorized attempts and actions to access or use this system may result in civil and/or criminal penalties.
All activities performed on this device are logged and monitored."C
!
!
line con 0
password 7 0$02455D0A1e261E010803567F79747A66651D
!
line vty 0 4
password 7 0$02455D0A1e261E010803567F79717A6667772C
login local
transport input ssh
line vty 5 15
login
!
!
ntp server 10.210.34.226
!
end
PldS5#  |

```

PlD-S6 (Switch)

```

PlD-S6#show startup-config
Using 3157 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname PlD-S6
!
enable secret 5 $1$mcERr5p0.rGLvw6oWWiTtxVdAB/
!
!
ip domain-name cam.gov.pt
username netadmin secret 5 $1$mcERr5Y1ckIMcTYWwKfCndtl1.
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface Port-channel1
switchport trunk allowed vlan 10,15,55,90,130
switchport mode trunk
!
description interface do tipo fastEthernet que faz a conexao do PlD-35 com o PlD-S6. Serve para conectar dois switches. Existem duas conexoes iguais para casos de falha nalguma interface/conexao. Redundancia para a resolucao de possivel problema
switchport trunk allowed vlan 10,15,55,90,130
switchport mode trunk
channel-group 5 mode active
!
interface FastEthernet0/2
description interface do tipo fastEthernet que faz a conexao do PlD-AP3 com o PlD-S6
switchport access vlan 90
switchport mode access
!
interface FastEthernet0/3
description interface do tipo fastEthernet que faz a conexao do PlD-PC6 com o PlD-S6
switchport access vlan 55
switchport mode access
!
interface FastEthernet0/4
description interface do tipo fastEthernet que faz a conexao do PlD-PC7 com o PlD-S6
switchport access vlan 55
switchport mode access
!
description interface do tipo fastEthernet que faz a conexao do PlD-35 com o PlD-S6. Serve para conectar dois switches. Existem duas conexoes iguais para casos de falha nalguma interface/conexao. Redundancia para a resolucao de possivel problema
switchport trunk allowed vlan 10,15,55,90,130
switchport mode trunk
channel-group 5 mode active
!
interface FastEthernet0/6
shutdown
!
interface FastEthernet0/7
shutdown
!
interface FastEthernet0/8
shutdown
!
interface FastEthernet0/9
shutdown
!
interface FastEthernet0/10
shutdown
!
interface FastEthernet0/11
shutdown
!
interface FastEthernet0/12
shutdown
!
interface FastEthernet0/13
shutdown
!
interface FastEthernet0/14
shutdown
!
interface FastEthernet0/15
shutdown
!
interface FastEthernet0/16
shutdown
!
interface FastEthernet0/17
shutdown
!
interface FastEthernet0/18
shutdown
!
interface FastEthernet0/19
shutdown
!
interface FastEthernet0/20
shutdown
!
interface FastEthernet0/21
shutdown
!
interface FastEthernet0/22
shutdown
!
interface FastEthernet0/23
shutdown
!
interface FastEthernet0/24
shutdown
!
interface GigabitEthernet0/1
shutdown
!
interface GigabitEthernet0/2
shutdown
!
interface Vlan1
no ip address
shutdown
!
ip default-gateway 10.210.34.249
!
banner motd "C
!! UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED !!
You must have explicit, authorized permission to access or configure this device.
Unauthorized attempts and actions to access or use this system may result in civil and/or criminal penalties.
All activities performed on this device are logged and monitored."C
!
!
line con 0
password 7 080245SD0A16261E010803567F79747A6667772C
login
!
line vty 0 4
password 7 080245SD0A16261E010803567F79747A6667772C
login local
transport input ssh
line vty 5 15
login
!
!
ntp server 10.210.34.226
!
end
PlD-S6#

```

Fnc-S1 (Switch)

```

FncS1#show startup-config
!
Using 2833 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname FncS1
!
enable secret 5 $1$0mErRifp0.rGLvv6oWWITIKVdABH/
!
!
ip domain-name cam.gov.pt
username netadmin secret 5 $1$0mErzYiCkIMoTYWwKF1Cndt11.
!
!
spanning-tree mode pvtst
spanning-tree extend system-id
!
interface FastEthernet0/1
description interface do tipo fastEthernet que faz a conexao do Fnc-S2 com o Fnc-S1. Serve para conectar dois switches. Neste caso pode haver perda de informacao , porque nao ha redundancia.
switchport trunk allowed vlan 10,15,55,90,130
switchport mode trunk
!
interface FastEthernet0/2
description interface do tipo fastEthernet que faz a conexao do FncRouter com o Fnc-S1
switchport trunk allowed vlan 10,15,55,90,130
switchport mode trunk
!
interface FastEthernet0/3
description interface do tipo fastEthernet que faz a conexao do Fnc-PC1 com o Fnc-S1
switchport access vlan 55
switchport mode access
!
interface FastEthernet0/4
description interface do tipo fastEthernet que faz a conexao do Fnc-PC2 com o Fnc-S1
switchport access vlan 55
switchport mode access
!
interface FastEthernet0/5
description interface do tipo fastEthernet que faz a conexao do Fnc-AP1 com o Fnc-S1
switchport access vlan 90
switchport mode access
!
interface FastEthernet0/6
shutdown
!
interface FastEthernet0/7
shutdown
!
interface FastEthernet0/8
shutdown
!
interface FastEthernet0/9
shutdown
!
interface FastEthernet0/10
shutdown
!
interface FastEthernet0/11
shutdown
!
interface FastEthernet0/12
shutdown
!
interface FastEthernet0/13
shutdown
!
interface FastEthernet0/14
shutdown
!
interface FastEthernet0/15
shutdown
!
interface FastEthernet0/16
shutdown
!
interface FastEthernet0/17
shutdown
!
interface FastEthernet0/18
shutdown
!
interface FastEthernet0/19
shutdown
!
interface FastEthernet0/20
shutdown
!
interface FastEthernet0/21
shutdown
!
interface FastEthernet0/22
shutdown
!
interface FastEthernet0/23
shutdown
!
interface FastEthernet0/24
shutdown
!
interface GigabitEthernet0/1
shutdown
!
interface GigabitEthernet0/2
shutdown
!
interface Vlan900
no ip address
!
interface Vlan500
ip address 172.16.34.178 255.255.255.248
!
ip default-gateway 172.16.34.177
!
banner motd "C
!! UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED !!

You must have explicit, authorized permission to access or configure this device.
Unauthorized attempts and actions to access or use this system may result in civil and/or criminal penalties.
All activities performed on this device are logged and monitored."C
!
!
line con 0
password 7 0802455D0A16261E010803567F7974A66651D
login
!
line vty 0 4
password 7 0802455D0A16261E010803567F79717A6667772C
login local
transport input ssh
line vty 5 15
login
!
ntp server 172.16.34.147
!
end
!
FncS1#

```

Fnc-S2 (Switch)

```

FncS2#show startup-config
Using 3322 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname FncS2
!
enable secret 5 $1$MER0$0.rGLvw6WWiTTkVdABH/
!
!
!
ip domain-name cam.gov.pt
!
username netadmin secret 5 $1$MER0$V1CKLMcTVwvxF1Cmnd11.
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
description interface do tipo fastEthernet que faz a conexao do Fnc-IoT2 com o Fnc-S2
switchport access vlan 15
switchport mode access
!
interface FastEthernet0/2
description interface do tipo fastEthernet que faz a conexao do Fnc-IoT1 com o Fnc-S2
switchport access vlan 15
switchport mode access
!
interface FastEthernet0/3
description interface do tipo fastEthernet que faz a conexao do Fnc-NTF com o Fnc-S2
switchport access vlan 130
switchport mode access
!
interface FastEthernet0/4
description interface do tipo fastEthernet que faz a conexao do Fnc-DHCP com o Fnc-S2
switchport access vlan 130
switchport mode access
!
interface FastEthernet0/5
description interface do tipo fastEthernet que faz a conexao do Fnc-P1 com o Fnc-S2
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/6
description interface do tipo fastEthernet que faz a conexao do Fnc-S1 com o Fnc-S2. Serve para conectar dois switches. Neste caso pode haver perda de informacao , porque nao ha redundancia.
switchport trunk allowed vlan 10,15,55,90,130
switchport mode trunk
!
interface FastEthernet0/7
description interface do tipo fastEthernet que faz a conexao do Fnc-S3 com o Fnc-S2. Serve para conectar dois switches. Neste caso pode haver perda de informacao , porque nao ha redundancia.
switchport trunk allowed vlan 10,15,55,90,130
switchport mode trunk
!
interface FastEthernet0/8
description interface do tipo fastEthernet que faz a conexao do Fnc-PC3 com o Fnc-S2
switchport access vlan 55
switchport mode access
!
interface FastEthernet0/9
shutdown
!
interface FastEthernet0/10
shutdown
!
interface FastEthernet0/11
shutdown
!
interface FastEthernet0/12
shutdown
!
interface FastEthernet0/13
shutdown
!
interface FastEthernet0/14
shutdown
!
interface FastEthernet0/15
shutdown
!
interface FastEthernet0/16
shutdown
!
interface FastEthernet0/17
shutdown
!
interface FastEthernet0/18
shutdown
!
interface FastEthernet0/19
shutdown
!
interface FastEthernet0/20
shutdown
!
interface FastEthernet0/21
shutdown
!
interface FastEthernet0/22
shutdown
!
interface FastEthernet0/23
shutdown
!
interface FastEthernet0/24
shutdown
!
interface GigabitEthernet0/1
shutdown
!
interface GigabitEthernet0/2
shutdown
!
interface Vlan1
no ip address
!
interface Vlan500
ip address 172.16.34.179 255.255.255.248
ip default-gateway 172.16.34.177
!
banner motd ^C
! UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED !!
You must have explicit, authorized permission to access or configure this device.
Unauthorized attempts and actions to access or use this system may result in civil and/or criminal penalties.
All activities performed on this device are logged and monitored.^C
!
!
line con 0
password 7 0802455D0A16261E010803567F79747A66651D
login
!
line vty 0 4
password 7 0802455D0A16261E010803567F79747A666772C
login local
transport input ssh
line vty 5 15
login
!
!
ntp server 172.16.34.147
!
end
FncS2#

```

Fnc-S3 (Switch)

```

FncS3#show startup-config
Using 2817 bytes
!
version 15.0
no service timestamp log datetime msec
no service timestamp debug datetime msec
service password-encryption
!
hostname FncS3
!
enable secret 5 $1$9mERz$V1CkLMcTiWwkfICndt1.
!
!
ip domain-name cam.gov.pt
!
username netadmin secret 5 $1$9mERz$V1CkLMcTiWwkfICndt1.
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
description interface do tipo fastEthernet que faz a conexao do Fnc-32 com o Fnc-33. Serve para conectar dois switches. Neste caso pode haver perda de informacao , porque nao ha redundancia.
switchport trunk allowed vlan 10,14,55,90,130
switchport mode trunk
!
interface FastEthernet0/2
description interface do tipo fastEthernet que faz a conexao do Fnc-PC4 com o Fnc-33.
switchport access vlan 55
switchport mode access
!
interface FastEthernet0/3
description interface do tipo fastEthernet que faz a conexao do Fnc-92 com o Fnc-33.
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/4
description interface do tipo fastEthernet que faz a conexao do Fnc-IoT3 com o Fnc-33.
switchport access vlan 15
switchport mode access
!
interface FastEthernet0/5
description interface do tipo fastEthernet que faz a conexao do Fnc-IoT4 com o Fnc-33.
switchport access vlan 15
switchport mode access
!
interface FastEthernet0/6
shutdown
!
interface FastEthernet0/7
shutdown
!
interface FastEthernet0/8
shutdown
!
interface FastEthernet0/9
shutdown
!
interface FastEthernet0/10
shutdown
!
interface FastEthernet0/11
shutdown
!
interface FastEthernet0/12
shutdown
!
interface FastEthernet0/13
shutdown
!
interface FastEthernet0/14
shutdown
!
interface FastEthernet0/15
shutdown
!
interface FastEthernet0/16
shutdown
!
interface FastEthernet0/17
shutdown
!
interface FastEthernet0/18
shutdown
!
interface FastEthernet0/19
shutdown
!
interface FastEthernet0/20
shutdown
!
interface FastEthernet0/21
shutdown
!
interface FastEthernet0/22
shutdown
!
interface FastEthernet0/23
shutdown
!
interface FastEthernet0/24
shutdown
!
interface GigabitEthernet0/1
shutdown
!
interface GigabitEthernet0/2
shutdown
!
interface Vlan1
no ip address
!
interface Vlan500
ip address 172.16.34.180 255.255.255.248
!
ip default-gateway 172.16.34.177
!
banner motd "C
!! UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED !!

You must have explicit, authorized permission to access or configure this device.
Unauthorized attempts and actions to access or use this system may result in civil and/or criminal penalties.
All activities performed on this device are logged and monitored."C
!
!
line con 0
password 7 0802455D0A16261E010803567F79747A66651D
login
!
line vty 0 4
password 7 0802455D0A16261E010803567F79717A6667772C
login local
line vty 5 15
login
!
!
ntp server 172.16.34.147
!
end
FncS3#

```

Lis-S1 (Switch)

```

LisS1#show startup-config
Using 3364 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname LisS1
!
enable secret 5 $1$0mERr0p0.rGLvweoNWTkVdASH/
!
!
ip domain-name cam.gov.pt
!
username netadmin secret 5 $1$0mERr0p0.rGLvweoNWTkVdASH/
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface Port-channel
description LACP trunk to POR-S1
switchport trunk allowed vlan 10,15,55,90,130
switchport mode trunk
!
interface FastEthernet0/0
description interface do tipo fastEthernet que faz a conexao do SinesRouter com o Lis-S1
switchport trunk allowed vlan 10,15,55,90,130
switchport mode trunk
!
interface FastEthernet0/2
description interface do tipo fastEthernet que faz a conexao do Lis-IoT1 com o Lis-S1
switchport access vlan 15
switchport mode access
!
interface FastEthernet0/3
description interface do tipo fastEthernet que faz a conexao do Lis-IoT2 com o Lis-S1
switchport access vlan 15
switchport mode access
!
interface FastEthernet0/4
description interface do tipo fastEthernet que faz a conexao do Lis-P1 com o Lis-S1
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/5
description interface do tipo fastEthernet que faz a conexao do Server0 com o Lis-S1
switchport access vlan 130
switchport mode access
!
interface FastEthernet0/6
description interface do tipo fastEthernet que faz a conexao do Lis-PC1 com o Lis-S1
switchport access vlan 130
switchport mode access
!
interface FastEthernet0/7
description Link to POR-S1 via LACP
switchport trunk allowed vlan 10,15,55,90,130
switchport mode trunk
channel-group 1 mode passive
!
interface FastEthernet0/8
description interface do tipo fastEthernet que faz a conexao do Lis-S1 via LACP
switchport trunk allowed vlan 10,15,55,90,130
switchport mode trunk
channel-group 1 mode passive
!
interface FastEthernet0/9
description interface do tipo fastEthernet que faz a conexao do Lis-API com o Lis-S1
switchport access vlan 90
switchport mode access
!
interface FastEthernet0/10
switchport access vlan 55
switchport mode access
!
interface FastEthernet0/11
shutdown
!
interface FastEthernet0/12
shutdown
!
interface FastEthernet0/13
shutdown
!
interface FastEthernet0/14
shutdown
!
interface FastEthernet0/15
shutdown
!
interface FastEthernet0/16
shutdown
!
interface FastEthernet0/17
shutdown
!
interface FastEthernet0/18
shutdown
!
interface FastEthernet0/19
shutdown
!
interface FastEthernet0/20
shutdown
!
interface FastEthernet0/21
shutdown
!
interface FastEthernet0/22
shutdown
!
interface FastEthernet0/23
shutdown
!
interface FastEthernet0/24
shutdown
!
interface GigabitEthernet0/1
shutdown
!
interface Vlan1
no ip address
!
interface Vlan500
ip address 10.34.0.130 255.255.255.224
ip default-gateway 10.34.0.129
!
banner motd "C
!! UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED !!

You must have explicit, authorized permission to access or configure this device.
Unauthorized attempts and actions to access or use this system may result in civil and/or criminal penalties.
All activities performed on this device are logged and monitored."C
!
!
line con 0
password 7 0802455D0a16261E010803567F79747A66651D
login
!
line vty 0 4
password 7 0802455D0a16261E010803567F79717A6667772C
login
transport input ssh
line vty 5 15
login
!
!
end

LisS1#

```

Por-S1 (Switch)

```

PorS1#show startup-config
Using 2559 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname PorS1
!
enable secret 5 $1$6ERxRsp0.rGLvw6oWTTkVdABH/
!
!
ip domain-name cam.gov.pt
!
username netadmin secret 5 $1$6ERxSY1CkLMcTYWwF1Cndt1.
!
!
spanning-tree mode pwt
spanning-tree extend system-id
!
interface Port-channel
  description LACP trunk to LIS-S1
  switchport trunk allowed vlan 10,15,55,90,130
  switchport mode trunk
!
interface FastEthernet0/1
  description Link to LIS-S1 via LACP
  switchport trunk allowed vlan 10,15,55,90,130
  switchport mode trunk
  channel-group 1 mode passive
!
interface FastEthernet0/2
  description Link to LIS-S1 via LACP
  switchport trunk allowed vlan 10,15,55,90,130
  switchport mode trunk
  channel-group 1 mode passive
!
interface FastEthernet0/3
  description interface do tipo fastEthernet que faz a conexao do Por-DNS com o POR-S1
  switchport access vlan 130
  switchport mode access
!
interface FastEthernet0/4
  description interface do tipo fastEthernet que faz a conexao do Por-EC2 com o POR-S1
  switchport access vlan 55
  switchport mode access
!
interface FastEthernet0/5
  description interface do tipo fastEthernet que faz a conexao do Por-IoT1 com o POR-S1
  switchport access vlan 15
  switchport mode access
!
interface FastEthernet0/6
  description interface do tipo fastEthernet que faz a conexao do Por-API com o POR-S1
  switchport access vlan 90
  switchport mode access
!
interface FastEthernet0/7
  switchport access vlan 130
  switchport mode access
!
interface FastEthernet0/8
  shutdown
!
interface FastEthernet0/9
  shutdown
!
interface FastEthernet0/10
  shutdown
!
interface FastEthernet0/11
  shutdown
!
interface FastEthernet0/12
  shutdown
!
interface FastEthernet0/13
  shutdown
!
interface FastEthernet0/14
  shutdown
!
interface FastEthernet0/15
  shutdown
!
interface FastEthernet0/16
  shutdown
!
interface FastEthernet0/17
  shutdown
!
interface FastEthernet0/18
  shutdown
!
interface FastEthernet0/19
  shutdown
!
interface FastEthernet0/20
  shutdown
!
interface FastEthernet0/21
  shutdown
!
interface FastEthernet0/22
  shutdown
!
interface FastEthernet0/23
  shutdown
!
interface FastEthernet0/24
  shutdown
!
interface GigabitEthernet0/1
  shutdown
!
interface GigabitEthernet0/2
  shutdown
!
interface Vlan1
  no ip address
!
interface Vlan500
  ip address 10.34.0.131 255.255.255.224
  ip default-gateway 10.34.0.129
!
banner motd "C
!! UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED !!
You must have explicit, authorized permission to access or configure this device.
Unauthorized attempts and actions to access or use this system may result in civil and/or criminal penalties.
All activities performed on this device are logged and monitored."C
!
!
line con 0
password 7 0802455D0A16261E010803567F79747A66651D
login
!
line vty 0 4
password 7 0802455D0A16261E010803567F79717A6667772C
login local
transport input ssh
line vty 5 15
login
!
!
end
PorS1# 

```

Topologia da Rede

