UNIVERSIDADE BEIRA INTERIOR

LICENCIATURA EM ENGENHARIA INFORMÁTICA

ADMINISTRAÇÃO DE SISTEMAS EM REDE

TRABALHO PRÁTICO

Data de Distribuição: 2023/05/07;

Data e Hora Limite para Entrega da Resolução: 2023/05/28, 23h59m

A resolução do Trabalho deve ser submetida através do Moodle

Penalização por cada dia de atraso na entrega: 0,5 valores

OBSERVAÇÕES

- É permitida a consulta de livros, artigos e sites da Internet. Indique as fontes de onde retirar informação.
- As situações de plágio que forem detetadas são penalizadas com a atribuição da classificação de 0 valores ao Trabalho.
- Trabalhos iguais ou muito semelhantes serão ambos penalizados com classificação de 0 valores.
- O projeto é desenvolvido por um grupo de no máximo 2 alunos;

---

1. INTRODUÇÃO E OBJETIVOS

O projeto final de Administração de Sistemas em Rede tem como objetivo avaliar a capacidade de os alunos aplicarem os conhecimentos adquiridos ao longo do semestre num projeto que simula um cenário real. O projeto terá de ser implementado no simulador ***Cisco Packet Tracer***.

Para conseguirem implementar com sucesso este projeto, os alunos terão de estar familiarizados com os seguintes conceitos relacionados com redes de comunicação: (i) cablagem – características e limitações; (ii) redes estruturadas; (iii) topologias físicas e lógicas; (iv) tecnologias de rede (Ethernet principalmente); (v) endereçamento IPv4, IPv6 e sub-redes; (vi) configurações de PCs, servidores, routers, sensores e outros dispositivos de rede; (vii) encaminhamento estático e dinâmico (RIP); (viii) protocolos ARP, IPv4, IPv6, ICMP, UDP, TCP, DHCP, DNS, TFTP, HTTP, FTP, POP3, SMTP e Telnet; (ix) listas de controlo de acesso (ACLs).

Pretende-se que após a realização do projeto os alunos estejam aptos a projetar, dimensionar, configurar e administrar uma rede de dados estruturada num ambiente de edifícios inteligentes (smart building), onde o conceito da Internet das coisas (IoT) é fundamental.

Com base na solução apresentada serão quantificados os seguintes aspetos de avaliação dos alunos:

- compreensão dos conhecimentos lecionados nesta UC e aplicação desses conhecimentos a cenários de projeto reais;
- capacidade de autoestudo (principalmente nos tópicos relacionados com ACLs e IoT);
- criatividade e concretização;
- capacidade de resolução de problemas complexos em tempo útil;
- capacidade de demonstrar perante terceiros o conhecimento adquirido nesta Unidade Curricular;
- capacidade de trabalhar em grupo.

2. DESCRIÇÃO DO CENÁRIO DO PROJETO

a) O grupo é responsável por configurar a rede de comunicações da XPTOtec, uma nova empresa que se sediou na Covilhã. A empresa é de base tecnológica e fornece serviços inovadores para cidades inteligentes (smart cities), desenvolvendo hardware e software aplicado à Internet das Coisas (IoT). Prevê-se que a curto prazo a empresa possa duplicar os seus 120 funcionários atuais;

b) A rede de comunicações da XPTOtec está dividida por 3 edifícios de três andares cada, separados geograficamente por uma distância de 200 metros. O Edifício 1 (XPTOtec_Oriente) é onde se encontram os serviços administrativos, o atendimento ao publico e os serviços de IT. O Edifício 2 (XPTOtec_Nascente) é onde se localizam os laboratórios de desenvolvimento e o Edifício 3 (XPTOtec_Leste) é onde se localiza o armazém e se realizam os testes de controlo de qualidade das soluções de IoT antes da sua comercialização pela XPTOtec;

c) O grupo é responsável por configurar não só a rede de comunicações dos três edifícios como também aspetos de smart building, garantindo que os edifícios refletem a filosofia da empresa;

d) A interligação das redes dos diferentes edifícios é feita através da funcionalidade '*multiuser connection*' disponibilizada no simulador. Isto significa que a cada edifício corresponde um

ficheiro de simulação independente. Os três ficheiros de simulação são depois interligados através da funcionalidade '*multiuser connection*';

e) A ligação à Internet é efetuada obrigatoriamente através da rede do edifício XPTOtec_Oriente;

Como preparação do projeto, o grupo deve estudar:

- quantas tomadas de rede devem ser implementadas em cada um dos pisos e nos 3 edifícios no total;
- a localização dos distribuidores de piso, de edifício e de campus;
- a quantidade de bastidores (verticais, parede) a usar em cada planta;
- a topologia de rede da empresa (como interligar os 3 edifícios);
- a topologia de rede a usar em cada edifício (como interligar dispositivos no mesmo edifício);
- determinar o tipo de cablagem a usar em cada edifício e entre edifícios.

3. TRABALHO A REALIZAR

a) Enviar um e-mail (até ao final do dia 12 de Maio de 2023) ao docente com o nome e endereço de e-mail dos 2 elementos do grupo.

b) O grupo é responsável por escolher as plantas dos vários pisos dos 3 edifícios da empresa XPTOtec.

- Podem ser usadas plantas em 3D;
- As plantas poderão ser criadas pelos alunos;
- As plantas não carecem de aprovação por parte do docente da disciplina, no entanto os alunos devem evitar a utilização de plantas semelhantes;
- As plantas devem refletir a natureza/propósito do edifício (ver próxima secção) e salvaguardar espaço para o número de trabalhadores da empresa (com possibilidade de crescimento a curto prazo);
- Deve-se considerar que os trabalhadores da empresa se encontram igualmente distribuídos por cada um dos edifícios.

c) Cada grupo, no seu ficheiro de simulação, deve usar o 'ambiente de trabalho físico' (*Physical Workspace*), para importar as plantas de cada piso e identificar a localização física dos equipamentos simulados (bastidores, PCs, servidores, switches, routers, sensores, objetos, etc.). Os 3 pisos podem ser representados usando a funcionalidade (*new building*), em que cada '*buiding*' representa um piso.

d) Cada grupo deve instalar e configurar os vários equipamentos nos respetivos ficheiros de simulação, por forma a implementar as funcionalidades descritas nas secções seguintes;

e) O grupo deve interligar os 3 ficheiros de simulação através de 'nuvens *multiuser*' para testar e resolver eventuais problemas que advenham de má configuração no cenário final;

f) O grupo deve submeter o trabalho via Moodle até às 23:59 de dia 28 de maio de 2023 contendo:

- Um slide (PDF) com a vista sumária dos 3 edifícios/pisos e das redes usadas em cada edifício/piso. O slide deve indicar ainda o número total de tomadas de rede por piso;
- Os 3 ficheiros de simulação;
- As plantas dos edifícios (em formato JPG ou PNG).

4. ITENS A CONSIDERAR PARA A IMPLEMENTAÇÃO DO PROJETO NOS FICHEIROS DE SIMULAÇÃO

a) A escolha da cablagem, equipamentos e interfaces a usar fica a cargo do aluno, salvaguardando que esta escolha permite a implementação das funcionalidades requeridas. O aluno deve estar preparado para justificar as suas escolhas;

b) Acerca dos routers:

- A configuração dos routers tem de incluir obrigatoriamente: acesso por Telnet, descrições para as interfaces, passwords e banners de acesso;
- O protocolo de encaminhamento a usar é o RIP;

- Podem ser usadas rotas estáticas onde aplicável. O grupo deve estar preparado para justificar as suas escolhas.

c) Acerca dos switches, hubs e pontos de acesso sem fios, a escolha é deixada ao critério do grupo.

d) Os serviços de rede a implementar nos edifícios são:

Edifício 1 – XPTOtec_Oriente	Servidor de e-mail	Contém contas de e-mail para os funcionários do edifício (pelo menos dois funcionários).
	Servidor HTTP	Contém página web da empresa e links para as páginas web dos outros 2 edifícios (ver mais abaixo).
	Servidor DNS	Contém configuração que permite a correta a resolução de nomes DNS de todos os dispositivos relevantes da empresa XPTOtec (incluindo a Internet e dispositivos dos outros edifícios). Este servidor é autoritário para o domínio DNS da empresa.
	Servidor(es) DHCP	Deverão ser usados servidores DHCP por forma a providenciar configuração de rede automática a dispositivos que o solicitem.
	Servidor TFTP	Contém *backup* de ficheiros de configuração de todos os routers da empresa.
	Servidor de Registo IoT	Servidor de registo usado para monitorizar todas as aplicações de IoT deste edifício.

Edifício 2 – XPTOtec_Nascente	Servidor de e-mail	Contém contas de e-mail para os funcionários do edifício (pelo menos dois funcionários). O subdomínio DNS deve ser diferente dos outros dois edifícios.
	Servidor HTTP	Contém página web associada ao trabalho que se faz neste edifício. Inclui obrigatoriamente uma hiperligação para a página da empresa.

	Servidor FTP	Contém contas de FTP personalizadas para pelo menos 2 utilizadores. Deve constar no servidor FTP um ficheiro de texto onde consta o nome e número dos alunos do grupo.
	Servidor(es) DHCP	Deverão ser usados servidores DHCP por forma a providenciar configuração de rede automática a dispositivos que o solicitem.
	Servidor de Registo IoT	Servidor de registo usado para monitorizar todas as aplicações de IoT deste edifício.

Edifício 3 – XPTOtec_Leste	Servidor de e-mail	Contém contas de e-mail para os funcionários do edifício (pelo menos dois funcionários). O subdomínio DNS deve ser diferente dos outros dois edifícios.
	Servidor HTTP	Contém página web associada ao trabalho que se faz neste edifício. Inclui obrigatoriamente uma hiperligação para a página da empresa.
	Servidor FTP	Contém contas de FTP personalizadas para pelo menos 2 utilizadores. Deve constar no servidor FTP um ficheiro de texto onde consta a data e hora de apresentação.
	Servidor(es) DHCP	Deverão ser usados servidores DHCP por forma a providenciar configuração de rede automática a dispositivos que o solicitem.
	Servidor de Registo IoT	Servidor de registo usado para monitorizar todas as aplicações de IoT deste edifício.

e) Após a receção das gamas de endereçamento a usar, o grupo deve respeitar as normas e boas regras para a utilização dos endereços IP;
   - Existe 1 PC específico por edifício que é atribuído ao administrador da rede (IP estático).

f) Dispositivos da rede XPTOtec conseguem aceder à Internet (simulada pelos servidores "www.google.com", "www.minhaubi.org" e servidor DNS Root).

Algumas notas:

- Não é necessário implementar todos os equipamentos que seriam usados num cenário real. Em ambiente de simulação apenas se deverão implementar os equipamentos imprescindíveis para se observar o correto funcionamento do projeto.
- Outros itens a considerar e que não estejam aqui referidos terão de ser escolhidos pelo aluno e devidamente fundamentados.

5. SUPORTE A IPV6

a) Nos 3 edifícios considera-se que todos os dispositivos para além do protocolo IPv4 também suportam IPv6. Neste sentido é esperado que haja comunicação IPv6 entre todos os dispositivos (incluindo servidores) da empresa e também com a Internet;

b) Aplicações relacionadas com IoT também devem estar configuradas com IPv6.

6. FUNCIONALIDADES DE EDIFÍCIO INTELIGENTE

Todos os edifícios da empresa são considerados edifícios inteligentes (*smart buildings*). Todos os dispositivos/sensores/objetos relacionados com IoT deverão operar em redes IP privadas, separadas da rede de dados da XPTOtec. Várias funcionalidades devem ser implementadas e testadas num único edifício:

a) Os edifícios possuem refrigeração e aquecimento de ar automático. A temperatura de cada edifício deve ser definida pelo utilizador e visualizada num display, no Servidor de Registo IoT e/ou tablet/smartphone.

b) Os edifícios possuem detetores de incêndio. As regras a aplicar são:

- Se for detetado um incêndio, é ativada uma sirene, uma luz de alarme e os dispersores de água;

- Quando a água atingir volumes superiores a 7cm de altura são ativados os ralos para extração de água;
- Se forem detetados níveis de CO2 superiores a 50%, são abertas as janelas. Se o nível de CO2 ultrapassar os 65% é ativada a extração de ar forçada (ventoinhas). Quando o nível de CO2 retomar a valores inferiores a 30% são fechadas as janelas e desligada a extração forçada.
- Os valores de CO2 devem ser visualizados num display e no Servidor de Registo IoT.

c) Todos os edifícios têm zonas de acesso restrito com portas controladas eletronicamente, por RFID e feixes laser. As regras a aplicar são:

- Existem portas que se encontram bloqueadas e que podem ser abertas por RFID. Caso se use um RFID inválido a porta não deve abrir e deverá ser ativada uma sirene de alarme.
- Existem zonas em que as passagens são controladas por feixes laser (exemplo, alarmes ativos durante o período noturno). Caso seja detetada uma presença deverá ser ativada uma sirene e enviado um e-mail ao responsável pelo serviço de segurança.
- Os acessos por RFID e os estados das portas podem ser visualizados no Servidor de Registo IoT.

d) Os jardins da empresa estão iluminados com candeeiros inteligentes, alimentados por baterias, carregadas por painéis solares fotovoltaicos instalados nos edifícios. Os candeeiros são ligados automaticamente quando escurece.

e) Outras funcionalidades poderão ser incluídas pelo grupo, por forma a tornar o projeto mais real.

7. POLÍTICAS DE SEGURANÇA

Esta secção apenas se aplica a dispositivos IPv4 (PCs, servidores e routers).

ALERTA-SE QUE A CONFIGURAÇÃO DAS LISTAS DE CONTROLO DE ACESSO (ACLs) SOLICITADAS NESTA SECÇÃO PODEM INTERFERIR COM AS CONFIGURAÇÕES EFETUADAS ANTERIORMENTE PELO QUE SE ACONSELHA A QUE SE GRAVE UMA VERSÃO DO PROJETO SEM O USO DE ACLs.

O grupo será avaliado apenas numa versão do projeto, com ou sem ACLs, a escolha é do grupo. Não apresentar ACLs implica perder 2,75 valores.

a) Deverá ser proibido o acesso de qualquer computador da empresa ao servidor www.minhaubi.org que se situa na Internet;

b) O acesso por Telnet aos routers é apenas permitido aos 3 PCs do Administrador;

c) O acesso às redes associadas a IoT apenas deverá ser permitido aos 3 PCs do Administrador;

d) Os servidores HTTP, DNS e E-MAIL apenas permitem acesso por ICMP (permitem *ping*) e pelo respetivo protocolo (exemplo, o servidor HTTP apenas será acedido por ICMP e por HTTP, não podendo ser acedido por qualquer outro tipo de protocolo);

e) Os servidores TFTP, FTP não podem ser acedidos a partir da Internet;

f) Os 3 PCs do administrador podem aceder à Internet sem restrições;

g) Os PCs da empresa acedem à Internet apenas por ICMP e por HTTP.

h) Restantes comunicações (não referidas aqui) que não sejam imprescindíveis para o bom funcionamento da rede devem ser negadas.