Olá professor e caros colegas.

Considerando que uma loja é composta por mais de um departamento, segue minha singela sugestão:

Cabeamento

Considero que a questão do cabeamento CAT5E OU CAT6 dependerá do fluxo de trabalho dessa loja, pois se o fluxo é alto, com certeza precisa de uma transmissão de dados mais rápida.

Diante disso, considerando um fluxo alto, adotarei um cabeamento CAT6 na camada de enlace da rede e fibra óptica monomodo, com um link dedicado de 100Mbs.

ATIVOS DE REDE

4 Switches 2960 CISCO L2 gerenciáveis

2 Switchs Cisco 3960 L3 gerenciáreis

2 Roteadores Cisco 2811 gerenciáveis

1 Access Point Cisco (wifi para os clientes)

1 No-break 2.200 va (umas 7 horas)

1 pach panel furukawa

4 baterias automotivas adaptadas (umas 24 horas)

1 hack com porta e chave

1 máquina servidor para gerenciamento da rede

1 máquina para atuar como servidor (FTP, e-mail, Proxy, DHCP e Impressão)

Cabo UTP CAT6 (para camada de enlace)

Fibra Óptica Monomodo (para camada de rede)

Topologia

Uma rede deve possuir redundância, ser escalável e ser tolerante à falhas.

Diante disso, a meu ver a topologia estrela estendida é a melhor opção, pois a falta de conexão em host, não afetará outros, como no barramento, e poderá ser facilmente escalável, uma limitação de um anel.

Configurações

Muito se fala sobre a rede em si, mas é necessário pensar, principalmente, na segurança.

Função dos Switchs

Switchs estão localizados na camada 2 do Modelo OSI, camada de enlace. São responsáveis pela comutação da rede local, LAN.

Por quê 4 Switchs ?

Uma rede deve possuir redundância, ser tolerante a falhas e escalável.
Com 4 Switchs é possível dividir todos os hosts em partes iguais, e ainda configurar cada vlan que seja necessária. Exemplo:

Switch 1 L2

10 máquinas, 4 impressoras de rede, 1 fiscal, VLAN DP Comercial

Switch 2 L2

10 máquinas, 4 impressoras de rede, 1 fiscal VLAN DP Estoque

Protocolo STP (spanning-tree-protocol)

No documento em anexo demonstro a redundância da rede com a utilização dos 4 Switchs.
Veja que os Switchs estão ligados um ao outro a fim de que se um falhar os hosts do Switch que falhou possam continuar a se comunicar na rede através da interface que liga um Switch ao outro, que chamamos de porta tronco.
Contudo, esse tipo de topologia pode causar um loop de camada 2 na rede devido a uma provável tempestade de broadcast e para evitar isso habilitamos o STP nos Switch. (no cisco já vem habilitado por padrão).

Etherchannel

Como adotei uma rede redundante, logo posso otimizar minha largura de banda, configurando o protocolo Etherchannel. Assim, é criada uma interface virtual que une duas interfaces, que a princípio dividiriam um link. Logo, um link dividido, é visto como somente um, aumentando a largura de banda e descongestionando a rede.

Switchs L3

Os Switchs de camada 3 são chamados assim porque possuem funções de roteamento, isso não quer dizer que consigam se comunicar com redes externas, apenas que podem rotear quadros ethernet entre VLANS e sub-redes.

Em Switchs L2 podemos habilitar portas tronco, mas ao adicionarmos um L3 em nossa rede, poderemos aumentar a taxa de transferência de dados, pois ele possui buffer para comutação de quadros muito grandes e uma cpu mais rápida.

Veja que coloco 2 L3 em minha topologia, ou seja, redundância, tolerância a falhas e escalabilidade.

Segurança

Com switchs gerenciáveis podemos aumentar muito a segurança de nossa rede. Seguem algumas possibilidades:

Criar Sub-redes e Vlans

Como serão 20 computadores e, na maioria das vezes, distribuídos entre os departamentos, cada departamento poderia ser separado por sub-redes, e posteriormente em VLANS, a fim de diminuir os domínios de broadcast e otimizar transmissão de dados. Isso possibilita também o bloqueio de acesso não autorizado de um departamento a documentos de outro que não são disponibilizados a todos. (eu adotaria apenas VLANS)

Servidores

Criar Serviço de DHCP

O DHCP (Dinamic Host Configuration Protocol) distribui endereços IP automaticamente entre os hosts (equipamentos) da rede.

Criar um servidor DHCP é importante pois além de evitar que toda vez que trocarmos um equipamento, ou ele sofrer uma pane, termos que inserir um endereço IP manualmente, aumenta a segurança, pois um roteador cisco por padrão tem o serviço DHCP habilitado, mas sua

capacidade computacional diante de um servidor é insignificante. Logo, diante de um ataque GRATUITOUS ARP, por exemplo, o servidor terá mais recursos para resistir ao ataque até que algo possa ser feito.

Configurar Servidor de Diretório

Com a utilização da máquina servidor, podemos cadastrar usuários e senhas e determinar a quais recursos eles poderão ter acesso e bloquear os demais.

Configurar Servidor de Impressão

Com a utilização da máquina servidor, podemos configurar um servidor de impressão, separados em vlans para uso dos departamentos e para uso comercial da loja.

Configurar um Servidor de Proxy

A produtividade sempre será o foco de uma empresa, não importa o seu porte.

Por isso, ao configurarmos um Servidor Proxy, poderemos limitar o acesso dos funcionários a sites que nada tem a ver com o trabalho.

Configurar um Servidor de Arquivos FTP

O FTP (file transfer protocol) é um protocolo para transferência de arquivos seguro e confiável.

Como a loja possui muitos documentos sensíveis (notas fiscais, documentos de clientes, funcionários, etc) é interessante configurar um servidor para tal serviço, a fim de aumentar a segurança, concentrando esses documentos e restringindo o acesso a determinadas pastas.

Máquina de Gerenciamento

Como sistema operacional adotaria o sistema operacional Ubuntu-Server, pois em questão de segurança, estabilidade e velocidade, não vi um que o superasse.

Software Wireshark e Zabbix para monitoramento.

Hydra e nmap para procurar falhas na rede.

Por fim, para evitar incompatibilidades com sistemas microsoft, bastaria utilizar o Software Samba.

Roteadores

Os roteadores são responsáveis pela comunicação com outras redes.

Por padrão os roteadores CISCO já vem com muitas configurações habilitadas, mas vamos citá-las a fim ter um trabalho mais completo.

Ao configurarmos os roteadores poderíamos adicionar rotas estáticas para nossa loja, tendo em vista o serviço é rotineiro. Isso aumentaria muito a segurança, pois uma mudança no tráfego seria facilmente descoberta.

No entanto, correríamos o perigo do trabalho manual em redes, e perder milhares de reais em vendas por alguma falha eventual, além de ser praticamente impraticável com acesso à internet.

Diante disso, como utilizarei dois roteadores, um para comunicação externa, um em modo bridge redundância, e um Access Point, é aconselhável habilitar os protocolos, quais sejam, a depender da necessidade RIP, OSPF e BGP.

RIP, OSPF OU BGP?

Resumindo como funciona um roteador.

O R1 conversa com o R2, R3, R4….. E procura saber qual o melhor caminho para enviar um pacote.

Os outros roteadores enviam para R1 suas tabelas roteamento, eles trocam algumas figurinhas, cada um faz seus cálculos e decidem através de um algoritmo complexo qual o melhor caminho.

Com o **RIP** (Routing Information Protocol) e roteador analisa o caminho mais curto, mas imagine que é um google maps em desenvolvimento, ele não verifica se esse caminho está congestionado e comunicação do pacote pode ser lenta.

O **OSPF** não busca o caminho mais, mas sim o caminho mais rápido! É o Maps! O roteador habilitado com o OSPF manda um hello, isso mesmo, um hello para os outros roteadores para que eles forneçam suas tabelas e analisa por qual rede devera enviar seu pacote para que ele chegue mais rápido.

Além disso, o OSPF pode enviar esse pacote por diferentes redes, a fim de diminuir o peso do pacote, logo, ele chega mais rápido!

BGP é um protocolo utilizado por grandes redes, conhecidas como Sistemas Autônomos. Não entrarei em detalhes, mas saiba que se quiser ter um sistema autônomo vai precisar desembolsar alguns milhões. Ele utiliza muitos critérios para determinar a rota como, local, tamanho do pacote, origem, destino. Ele não fica tagarelando com outros roteadores. Só atualiza sua tabela quando necessário.

Para entender melhor: Você tem o seu roteador, que te conecta a internet, e utiliza o OSPF nele por exemplo, O BGP é utilizado no roteador da própria Internet, entende, a grande rede, ARPANET gafanhoto! Temos dois tipos o IBGP e o EBGP, interno e externo, mas não entrarei em detalhes.

Configuração de Firewall

Quando se fala em investimento em firewall alguns dizem que é perda de tempo até sofrer o primeiro ataque.

Implementar um bom Firewall é de uma importância, e não estou falando do Firewall do Windows.

É uma solução cara, mas indispensável.

Link Dedicado

Como se trata de um comércio, não é possível dividir largura de banda com outros cliente, então é interessante contratar um link dedicado.

O que é um link dedicado?

Quando você contrata 100Mps (mais conhecido como 100 megas) para sua residência, na verdade você está contratando uma banda larga que será utilizada por outros clientes, e se todos decidirem acessar a internet de uma vez para assistir a “ Casa do Dragão” na HBO, numa TV 4k, provavelmente sua conexão vai travar, dependendo do porte do seu provedor, pois dividem a mesma banda, que é bem maior que os seus 100 Mbps, mas ainda assim, você a divide.

Exemplo, o bom exemplo:

Você contratou 200Mbps, seu vizinho 100Mps, a banda larga do seu provedor é de 300 Mps, agora imagine que você está jogando online no seu supercomputador que tem uma placa de rede de 250Mps, em dado momento você utiliza 200 Mps e seu vizinho liga a Neflix, o celular e o notebook, consumindo os 100 dele. Seu jogo, vai travar e você vai perder, sua taxa de transferência real vai para uns 30 Mps.

Agora, link dedicado.

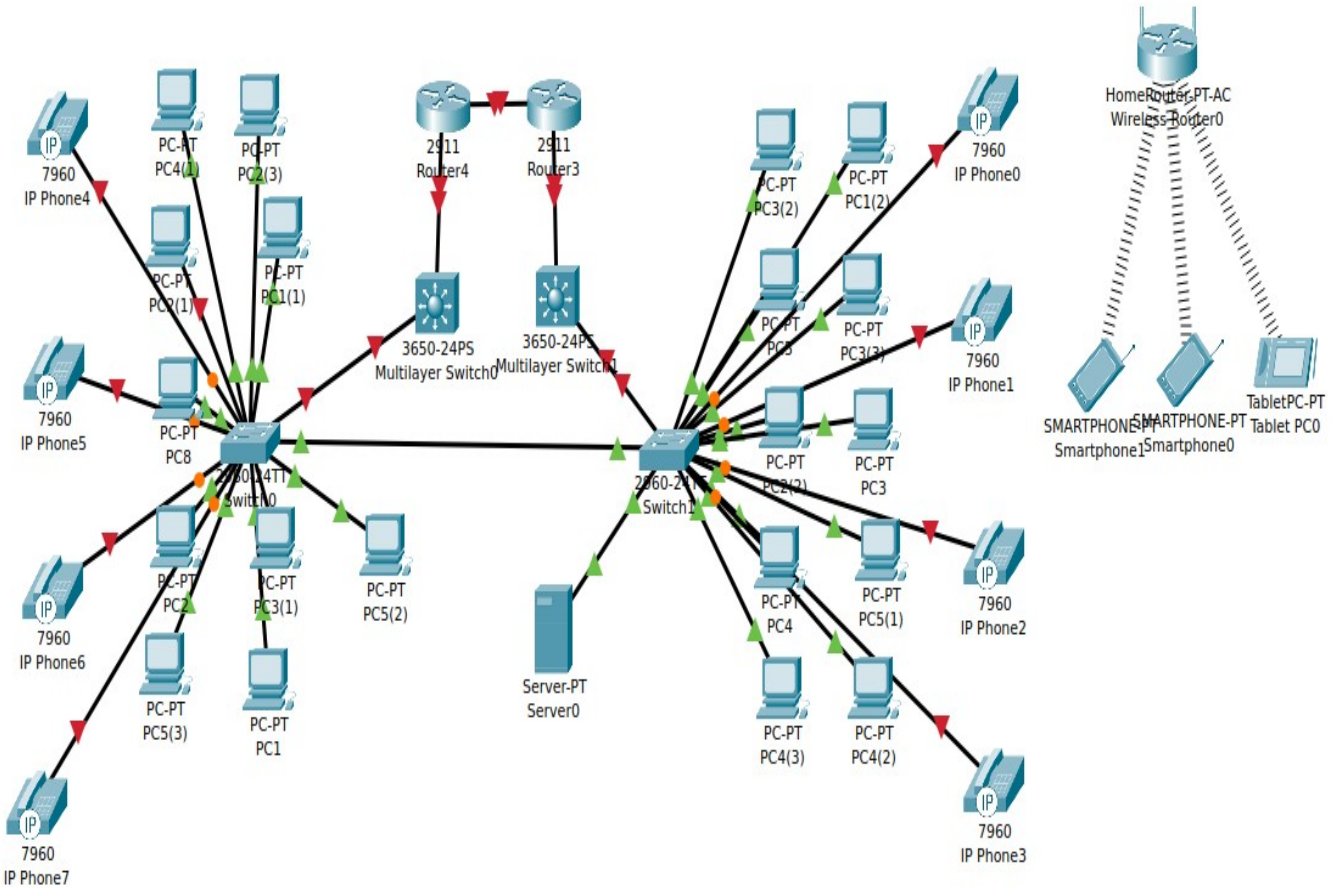
Ao contratar um link dedicado, a banda largar é só sua. Isso, não tem divisão. São 100 Mps só para você usar. Outra coisa, são 100 Mbps de velocidade de Download e Upload! Comunicação Assíncrona !
Espere, espere aí, antes de cancelar seu plano e pedir um link dedicado: custa em média 4 vezes mais. Sorry….rsrrs

Logo, uma loja não tem como dividir banda, precisa de uma canal exclusivo.

Telefones voip

Adicionei telefonia VOIP à rede, pois um departamento terá que se comunicar com outro, além da comunicação com fornecedores, etc.
A única observação é que é obrigatória a configuração de uma VLAN exclusiva para VOIP.

Conclusão
Como se trata de um fórum, dispensei a formalidade acadêmica, para poder explicar de uma forma mais lúdica alguns conceitos. Espero ter adicionado algo ao conhecimento dos colegas com essa singela contribuição.


HomeRouter-PT-AC
Wireless Router0
2911
Router4
2911
Router3
3650-24PS
Multilayer Switch0
3650-24PS
Multilayer Switch1
2960-24TT
Switch0
2960-24TT
Switch1
Server-PT
Server0
7960
IP Phone0
7960
IP Phone1
7960
IP Phone2
7960
IP Phone3
7960
IP Phone4
7960
IP Phone5
7960
IP Phone6
7960
IP Phone7
SMARTPHONE-PT
Smartphone1
SMARTPHONE-PT
Smartphone0
TabletPC-PT
Tablet PC0
PC-PT
PC8
PC-PT
PC1
PC-PT
PC1(1)
PC-PT
PC1(2)
PC-PT
PC2
PC-PT
PC2(1)
PC-PT
PC2(2)
PC-PT
PC2(3)
PC-PT
PC3
PC-PT
PC3(1)
PC-PT
PC3(2)
PC-PT
PC3(3)
PC-PT
PC4
PC-PT
PC4(1)
PC-PT
PC4(2)
PC-PT
PC4(3)
PC-PT
PC5(1)
PC-PT
PC5(2)
PC-PT
PC5(3)