Universidade Atlântica

Infra-estruturas de rede num *campus* universitário

Projecto final de licenciatura 2007

Gestão de Sistemas e Tecnologias de Informação

Rui Manuel Costa de Aires nº20030740

Docente Coordenadora: Eng. Filipa Taborda Ferreira

Índice

Tabela de Figuras

1. Introdução

No passado, uma rede informática era usada simplesmente para obter conectividade entre computadores, mas hoje em dia assume um papel crítico para o trabalho, para permitir o uso de novas aplicações, para melhorar a produtividade e fornecer uma multiplicidade de serviços. Aplicações para trabalho colaborativo em tempo-real e ferramentas de comunicação como por exemplo: voz sobre IP, vídeo sobre IP, e e-learning, oferecem uma oportunidade para as organizações se destacarem no campo da produtividade. As redes sem fios expandem os espaços de trabalho permitindo o acesso à informação para além dos computadores de secretária. Contudo, esta crescente expansão que assenta no uso e dependência da rede levanta alguns desafios.

Da mesma forma que as organizações dão passos no sentido de melhorar a sua produtividade no geral, também devem encontrar formas de proteger a rede e a informação que nela é transmitida, ao mesmo tempo que asseguram a sua disponibilidade e os seus recursos. Servindo de base a todos os sistemas, a rede deve estar preparada não só para as necessidades actuais como também deve estar preparada para escalar à medida das mudanças que são esperadas no futuro.

Este trabalho faz parte de um projecto que está dividido em duas partes que por sua vez constituíram dois trabalhos finais de curso. O projecto, no global, consiste num estudo de solução para a estrutura tecnológica e serviços colaborativos num campus universitário.

O problema tratado neste trabalho centra-se na infra-estrutura de rede sendo que, tendo em conta a conjuntura, irá integrar com outra componente que tratará toda a área de sistemas. O objectivo do estudo é o planeamento da rede activa com maior detalhe nas áreas de switching, routing e wireless. Além destas, ainda serão focadas as áreas da gestão da qualidade de serviço e segurança embora de uma forma bastante sucinta por serem temas que só por si dariam matéria para dois novos projectos.

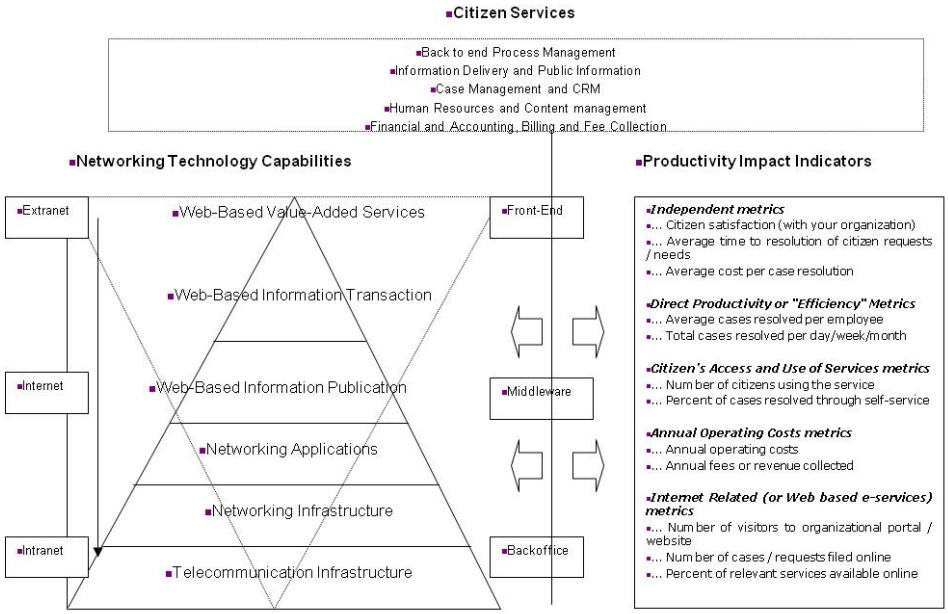


Figura 1, Análise Estratégica das Infra-estruturas [SII-GSC]

A figura 1 reflecte o posicionamento do âmbito deste trabalho no segundo e terceiro nível, ou seja imediatamente a seguir às infra-estruturas disponibilizadas pelos operadores. O quarto e quinto níveis já se referem ao âmbito do projecto de sistemas.

Neste sentido, o presente trabalho divide-se em duas partes. O objectivo da primeira parte é clarificar conceitos que se traduzem nas melhores práticas para na segunda parte os aplicar na construção da solução com a arquitectura proposta tendo em conta as regulamentações e os objectivos estudados neste trabalho.

Para o dimensionamento da infra-estrutura consideraram-se como pressupostos os seguintes princípios:

Acessos e Conectividades Seguras: Garantir de forma segura o acesso aos serviços de rede desde os equipamentos com e sem fios existentes nas diversas localizações dentro do campus. Proteger os dados e o tráfego de rede contra ameaças internas e externas. Controlar o acesso aos recursos com base na identificação do utilizador. Alcançar a conformidade em termos regulatórios tendo em vista proteger os registos e identidade dentro do campus.

Continuidade Operacional: Alcançar níveis de alta disponibilidade em dados, aplicações e serviços disponibilizados na rede. Minimizar os custos associados à indisponibilidade de rede. Alcançar ou exceder a regulação existente nas áreas de recuperação de desastres e replicação de dados.

Garantia da Entrega de Serviços e Aplicações: Fornecer uma entrega consistente dos serviços e aplicações em toda a rede independentemente da localização do utilizador. Prioritizar a entrega com base no conteúdo e aplicação. Optimizar a produtividade de todos os utilizadores.

Gestão Automatizada: Utilizar políticas, diagnósticos, e o *provisioning* com vista a automatizar o processo de monitorização e gestão para manter a infra-estrutura de rede. Minimizar a necessidade de verificações e intervenções manuais.

Consolidação e utilização da Infra-Estrutura: Maximizar a utilização dos componentes de rede através da consolidação, segmentação e fornecimento dinâmico de acções com vista a proteger o investimento e baixar os custos de operação. Incorporar a virtualização da infra-estrutura para reduzir a necessidade de redundância física mantendo a redundância funcional.

Convergência de Comunicações e Trabalho Colaborativo em Tempo-Real: Dinamizar a integração de dados voz e vídeo na rede para garantir as necessidades de telefonia, mensagens unificadas e conteúdos multimédia para conferência. Dinamizar a interacção de utilizadores e a possibilidade de partilharem conteúdos, aplicações e ferramentas em qualquer altura e em qualquer lugar.

2. Conceitos

A abordagem aos conceitos apresentados visa enquadrar o posterior dimensionamento, apresentando-se os principais modelos de rede, e o significado de *routing* & *switching* numa rede de transporte de dados, bem como a importância da qualidade de serviço e segurança para a fiabilidade da rede. Introduzem-se também os fundamentos das comunicações wireless e o que deve ser tido em conta numa rede wireless.

2.1. Modelos de rede

Existem vários modelos, passa-se a uma breve apresentação dos dois modelos que mais se adequam ao problema: O DoD model (DoD, Department of Defense), também conhecido como *Internet reference model* ou como *TCP/IP model* e o *OSI reference model*.

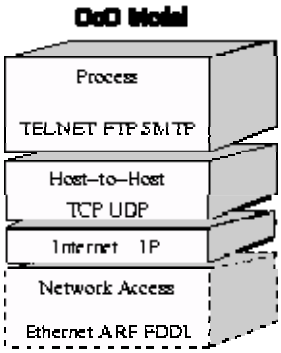


Figura 2, Modelo DoD [freesoft.org]

O modelo DoD ou TCP/IP é constituído por quatro camadas sendo a quarta camada, camada de processo ou aplicações, a camada onde operam protocolos como o SMTP, FTP, SSH e HTTP entre outros. A terceira camada garante a comunicação *host-to-host* ou seja o transporte. É aqui que se processa o controlo de fluxos e onde existem os protocolos de ligação como o TCP, sendo o principal objectivo criar e manter ligações activas garantindo que os pacotes são de facto recebidos. Descendo para a segunda camada, chegamos à camada internet onde se definem os endereços IP e os diversos mecanismos que permitem aos pacotes navegar de um endereço IP para outro. A primeira camada corresponde ao nível físico onde existem os equipamentos que garantem as comunicações, que vão desde os cabos até à sinalização usada por esses equipamentos.

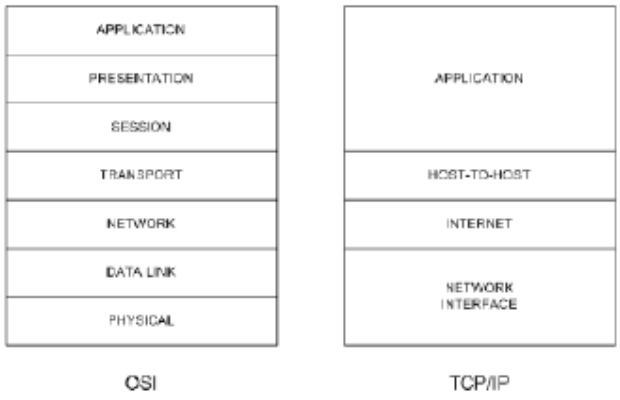


Figura 3, Modelo OSI comparado com o TCP/IP model. [Cisco]

Os protocolos que concretizam cada um dos níveis nos diferentes modelos são diferentes e cobrem um ou mais níveis. O modelo DoD caracterizado pelos protocolos TCP e IP cobre os níveis 3 e 4 do modelo OSI. O TCP (protocolo de nível 4 do modelo OSI) é um protocolo de transporte orientado à conexão. Utiliza números sequenciais e mensagens de confirmação de entrega, o TCP pode fornecer uma nota de envio com informação sobre os pacotes transmitidos para o destino. Quando a informação se perder em trânsito, o TCP pode retransmitir essa informação até que seja entregue com sucesso.

Veja-se na figura 3 a distribuição de alguns importantes protocolos pelas diferentes camadas do modelo OSI.

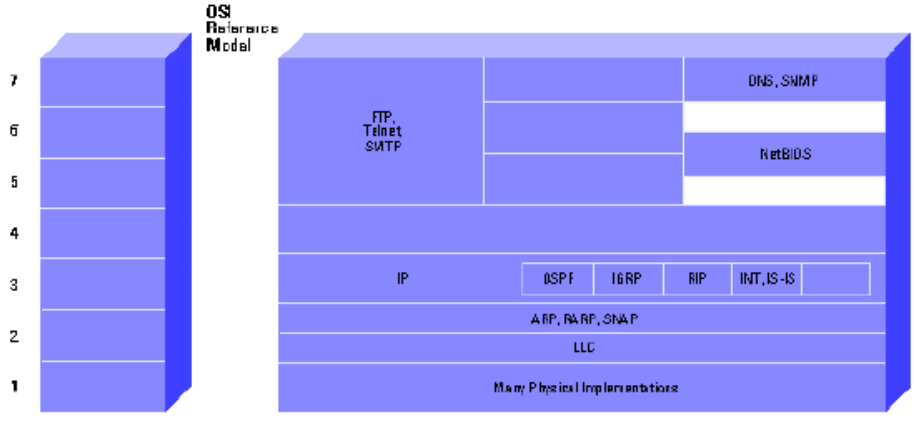


Figura 4, Protocolos importantes referidos às camadas do modelo OSI. [Cisco]

Os protocolos que compõem as várias camadas correspondem a sucessivos encapsulamentos/desencapsulamentos da informação. Os pormenores sobre esta operação estão disponíveis no Anexo A.

É igualmente no nível 4 do modelo OSI que se verifica a transferência de informação entre sistemas, ou comunicação *end-to-end*. Descendo para o nível 3, onde é efectuado o *routing*, a informação passa a ter a forma de pacote. Continuando para o nível 2, onde é efectuado o *switching*, a informação é organizada em tramas. Finalmente no nível 1 a informação é reduzida a bits que serão transmitidos sob a forma de impulsos eléctricos, sinal de rádio ou luz. O modelo OSI, por ser mais detalhado e objectivo vai servir como ponto de referência ao longo deste ponto em diante.

2.2. Switching

O *switching* é uma operação vital na construção de uma rede. Deve ser tido em consideração não só como um simples meio veicular informação mas como membro de um sistema inteligente. Um *switch* permite operacionalizar o *switching* e diversas funcionalidades até aos utilizadores finais.

2.2.1. Funções de Switching e Bridging

Os Switches operam no nível 2 do modelo OSI e devido à sua arquitectura de alta velocidade e ao elevado numero de portas que disponibilizam tornam-se mais eficientes que as tradicionais *bridges*.

O papel dos *Switches* e *Bridges Ethernet* é aumentar a largura de banda disponível possibilitando reduzir o número de equipamentos para cada segmento de rede. Conseguem também tomar decisões inteligentes examinando os MAC addresses de origem e destino das tramas emitidas por cada equipamento procedendo à filtragem.

Um switch faz a sua gestão recorrendo a uma base de dados própria onde recolhe informações que aprende da rede. Um switch tipicamente de *Access Layer* pode suportar mais de 8000 registos. Quando um switch é inicializado, a sua MAC address table está vazia, e a partir desse momento ele vai aprender o que se passa na rede e rapidamente vai construir a sua própria representação topográfica para começar a tomar decisões sobre o que ele conhece ou não para encaminhar ou filtrar as tramas.

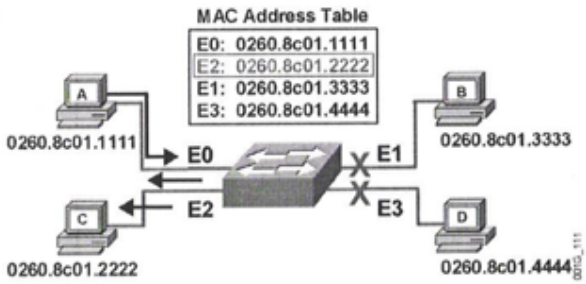


Figura 5, Esquema de filtragem de tramas [Cisco]

2.2.2. Identificar problemas que ocorrem em topologias redundantes

As topologias redundantes de *switching* e *bridging* eliminam a possibilidade de um único ponto de falha se tornar numa indisponibilidade total ou parcial da rede. No entanto há problemas que surgem com este tipo de topologia.

As *Broadcast storms*, acontecem quando não existem mecanismos que evitem a existência de *loop's* provocando uma transmissão repetida de informação.

Outro problema clássico deste tipo de topologia são as transmissões múltiplas. Por exemplo, uma máquina X envia um *unicast* para o router Y, uma cópia é recebida pela pelo circuito 1. Mais ou menos ao mesmo tempo, outra cópia da mesma frame é recebida pelo switch A; quando o switch A examinar o endereço de destino, vai verificar que não tem nenhuma entrada na sua MAC address table para o router Y, então o switch faz o flooding da frame, ou seja, encaminha-a a todas as suas portas excepto a porta por onde a recebeu; quando o switch B recebe a cópia da frame vinda do switch A pelo circuito 2, o switch B também vai tomar a decisão de encaminhar a cópia da frame ao circuito 1 se não existir na sua MAC address table nenhuma entrada para o router Y.

Um terceiro problema que pode ocorrer é a instabilidade das MAC *address table*. Por exemplo, um switch B insere uma entrada na sua base de dados mapeamento um MAC address de uma máquina X na porta 0, e se essa porta 0 está ligada ao circuito 1. Mais tarde, quando a cópia da frame transmitida pelo switch A chega à porta 1 do switch B, o switch B retira a sua primeira entrada e actualiza uma nova entrada incorrectamente mapeia a máquina X à porta 1 que liga ao circuito 2. Dependendo da arquitectura interna do switch em questão, ele pode não funcionar bem com estas rápidas mudanças na sua MAC address table.

2.2.3. Métodos de *switching*

Existem três métodos de transmissão de tramas, cada um deles com diferentes objectivos: No método "store and forward", o switch recebe a frame na totalidade e só depois o encaminha. Lê os endereços de origem e destino, faz uma verificação de redundância cíclica (CRC), aplica os filtros relevantes e finalmente encaminha a frame. Se o CRC for negativo, a frame é

descartada. Este processo origina maior ou menor latência consoante a dimensão da frame. No método "Cut-throught", o switch verifica imediatamente o endereço de destino e encaminha a *frame*. Isto faz com que a latência diminua significativamente quando comparado com o método "store and forward". O atraso, neste método, mantém-se constante independentemente do tamanho da frame contudo o switch não interromperá a transmissão de uma frame que contenha erros. O terceiro método é o "Fragment-free", onde o switch vai ler os primeiros 64 bytes da frame, que é o tamanho mínimo de uma frame Ethernet, antes de tomar uma decisão. Normalmente, as colisões ocorrem nestes primeiros 64 bytes da frame, e quando isso acontece é criado um fragmento, que no fundo é uma frame com menos de 64 bytes. Voltando ao inicio, quando o switch lê os primeiros 64 bytes pode filtrar imediatamente essas colisões, ou tramas fragmentados. Este método tem uma latência superior ao Cut-throught, que enviaria a frame desde que o endereço de destino exista, mas por outro lado reduz a transmissão de informação desnecessária tornando-se uma solução bastante eficiente.

2.2.4. O protocolo Spanning Tree

O STP foi originalmente desenvolvido pela *Digital Equipment Corporation*. O algoritmo da DEC foi mais tarde revisto pelo *committee IEEE 802* e publicada a sua especificação *IEEE 802.1d*. O propósito deste protocolo é manter uma topologia de rede livre de *loop's*. Isto é conseguido quando um *switch* reconhece um *loop* na topologia e bloqueia de forma lógica uma ou mais portas redundantes automaticamente.

A operação funciona com base num modelo hierárquico onde existem quatro componentes: uma *root bridge* por rede; uma *root port* por cada *bridge não-root*; uma *designated port* por cada segmento, e as *nondesignated ports* que são as que ficam em *stand-by*. São utilizados dois conceitos, o *bridge ID* (BID) e o *path cost*.

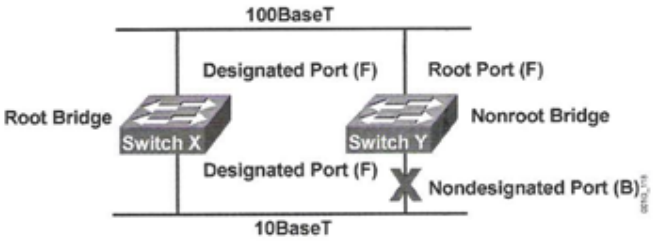


Figura 6, Filtragem de tramas [Cisco]

Os três passos que são efectuados quando o STP é instanciado são:

- A eleição da *root bridge*, única numa determinada rede, e onde todas as portas nos diversos segmentos são *designated ports* e por isso podem enviar e receber tráfego. Na figura 5, o switch X é eleito como *root bridge*.

- O segundo passo, é a selecção da root port na *bridge* não-root. Para tal, o STP determina o caminho com o custo mais baixo para a *root bridge* sendo que o custo no STP é calculado pela largura de banda acumulada. Neste exemplo será o circuito Fast Ethernet 100BaseT.

- Finalmente é seleccionada a *designated port* em cada segmento. A *designated port* é seccionada na *bridge* com o mais baixo custo para a *root bridge*. Na figura 5, a *designated port* para ambos os segmentos é a *root bridge* porque a *root bridge* e está ligada directamente aos dois segmentos. A porta *Ethernet 10BaseT* no *switch* Y é uma *nondesignated* port porque só pode existir uma *designated port* por segmento. Estas portas estão normalmente bloqueadas de forma lógica para quebrar o *loop* na topologia. Quando uma porta se encontra neste estado, ela não transmite tráfego mas consegue ainda receber informações sobre o estado da topologia (BPDU's) para se necessário entrar imediatamente em serviço. Por defeito demora 20 segundos, o correspondente a 10 BPDU's falhados.

O *Rapid Spanning Tree Protocol*, RSTP, especificado pelo *IEEE 802.1w*, sucede ao *STP IEEE 802.1d*, mantendo-se no entanto compatível com o STP. O RSTP define novos papéis adicionais às portas, o papel alternate e o papel *backup*. A rápida transição é a característica mais importante introduzida no IEEE 802.1w. Até à chegada do RSTP, o algoritmo aguardava passivamente que a rede convergisse antes de transitar o estado da porta para *forwarding*. O RSTP confirma activamente que a porta pode mudar para *forwarding* sem ter que confiar num contador.

2.2.5. O papel das VLANs no *switching*

Uma VLAN representa um "*broadcast domain"* ou por outras palavras uma rede lógica também conhecida por *subnet*. Enquanto os "*colision domains"* se resumem ao âmbito de um *HUB* ou ao âmbito de cada porta de switch, um broadcast domain é todo o espaço onde pode ser ouvido um broadcast emitido por uma máquina. Apenas os equipamentos de terceiro nível do modelo OSI podem separar broadcast domains, por exemplo um router.

Sendo um switch um equipamento tipicamente de segundo nível, permite segmentar várias redes lógicas num equipamento ou em vários equipamentos. Assim, podemos desenhar várias *VLAN's* segmentando

diversas máquinas por funções independentemente da sua localização física, adicionando desta forma um nível adicional de segurança.

Imaginando um edifício com vários pisos, com um switch por cada piso, é possível ter um grupo de máquinas isoladas entre si embora dispersas por cada piso, é por todos os pisos. Por exemplo, podemos distribuir as máquinas de um determinado departamento por todos os pisos do edifício, todas elas no mesmo *broadcast domain*, sem que todas as outras máquinas que estão ao lado possam comunicar directamente. Para além da questão de se incrementar um nível de segurança, esta tecnologia permite optimizar o desempenho da rede ao reduzir a dimensão dos *broadcast domains*. As *VLAN's* podem incluir máquinas de um ou vários edifícios podendo mesmo estender-se pelas WAN's.

Para interligar os vários *switches* que suportarão todas estas *VLAN's*, são utilizadas configurações especiais de portas que tem como missão transportar todas as *VLAN's* de forma estanque entre *switches*. Estas portas são conhecidas por *Trunks* sendo o protocolo *IEEE 802.1q* o mais utilizado na interligação de múltiplos *switches*.

Quando as redes começam a ter dimensões consideráveis, torna-se difícil e até imprudente gerir manualmente todas as implementações de *VLAN's*. Para resolver esse problema existe o *VLAN Trunking Protocol* (VTP). O VTP é um protocolo de nível dois do modelo OSI, que mantém a consistência das configurações de *VLAN's* gerindo todas as adições, eliminações ou mudanças de nome das *VLAN's* ao longo de toda a rede. É então criado um domínio VTP constituído por uma rede de switches interligados entre si, onde existem três tipos de papeis que podem desempenhar, *Server*, *Client* ou *Transparent*. Tipicamente num campus universitário, utilizar-se-á um ou dois servers consoante exista redundância lógica ou física sendo todos os outros clientes.

2.3. Routing

Routing é normalmente efectuado por equipamento dedicado denominado de *router.* A sua principal função é encaminhar a informação em forma de pacotes, de máquina em máquina até ao destino, envolvendo um processo de selecção do melhor caminho possível.

2.3.1. Determinação de rotas IP/Protocolos de *Routing*

Um *router* é tipicamente um equipamento de terceiro nível do modelo OSI, e necessita de cinco condições para exercer a sua função:

- Conhecer o endereço de destino

- Identificar as fontes a partir das quais ele pode aprender

- Descobrir possíveis rotas para um determinado destino

- Seleccionar a melhor rota

- Manter e verificar toda a informação de routing

Existem apenas duas formas de um router aprender informação, ou é inserida manualmente pelo administrador de rede ou a informação é recolhida através do processo dinâmico de routing que está a correr nos routers. Com esta informação podem ser geradas dois tipos de rotas, as estáticas onde o administrador de rede deve actualizar manualmente uma determinada entrada estática sempre que ocorre alguma alteração topológica, mantendo no entanto um controlo muito preciso do que pretende. Por outro lado as rotas dinâmicas onde o administrador de rede configura um routing protocol que vai determinar as rotas. Neste caso, o router aprende e mantém as rotas para os diversos destinos trocando informações com outros routers ao longo de toda a rede.

Os protocolos de routing dividem-se em dois tipos:

- *Interior Gateway Protocols* (IGP's), estes protocolos são utilizados para trocar informação de routing dentro de um sistema autónomo. RIPv1, RIPv2, IGRP, EIGRP e OSPF são exemplos de IGP's.

- *Exterior Gateway Protocols* (EGP's), Utilizados para interligar sistemas autonomos. O protocolo *Border Gateway Protocol* (BGP) é o mais utilizado em todo o mundo.

Um *AS* (*autonomous system*) é um conjunto de redes sob a mesma administração que partilham a mesma estratégia de routing. Dentro de um *AS*, os protocolos são classificados como estando em conformidade com um dos seguintes algoritmos:

- *Distance vector*: determina a direcção (vector) e distancia (hops) para cada ligação ao longo de toda a rede.

- *Link state*: o link state, também conhecido como shortest path first (SPF), cria uma abstracção da topologia de toda a rede com que ele mantém comunicações.

Não existe um algoritmo melhor que se aplique em todas as redes, porque todos os protocolos fornecem informações de forma diferenciada.

O *Inter-VLAN routing* ocorre entre *broadcast domains* através de um equipamento de nível três do modelo OSI. Num ambiente de VLAN os tramas são transmitidos apenas entre portas contidas no mesmo broadcast domain, particionando e separando o tráfego no nível dois do modelo OSI. Logo a comunicação entre *VLAN's* não pode ocorrer sem um equipamento de terceiro nível como por exemplo um router.

O Anexo B contém informação uma descrição de cada um dos Interior Gateway Protocols.

2.3.2. VLSM - Gestão de endereçamento

Para assegurar uma correcta utilização deste recurso escasso que são os IP's disponíveis para atribuir a equipamentos, existe uma técnica que permite optimizar a gestão de endereçamento, o VLSM.

Benefícios das VLSM – As *Variable-Length Subnet Mask* permitem a inclusão de mais de uma subnet mask numa rede e subnetar endereços de rede já subnetados. As VLSM apresentam as seguintes vantagens:

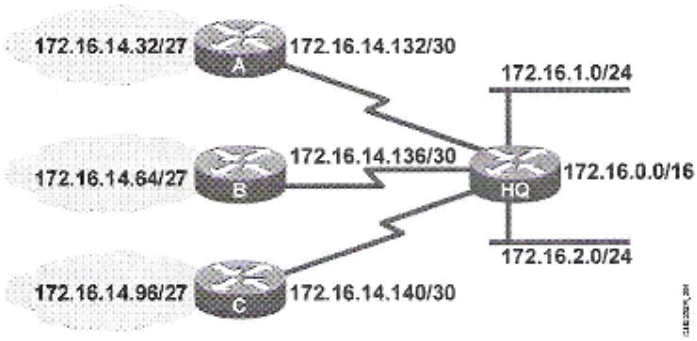


Figura 7, VLSM- *Variable Lenght Subnet Mask* [Cisco]

- Uso mais eficiente dos endereços IP, ou seja, sem utilizar o VLSM as organizações teriam que implementar uma única *subnet mask* gastando uma Classe inteira A, B ou C. Por exemplo, da divisão da rede 172.16.0.0/16 em sub-redes utilizando a mascara /24, resultam, entre outras, a sub-rede 172.16.14.0/24 que por sua vez ainda se divide em sub-redes ainda mais pequenas que vão da 172.16.14.0/27 até 172.16.14.224/27. Como podemos observar na figura 6, uma destas sub-redes, a 172.16.14.128/27, está ainda dividida em redes ainda mais pequenas, as /30 que disponibilizam apenas dois IP's e são normalmente aplicadas em ligações ponto a ponto.

- Maior capacidade para utilizar a sumarização de rotas, o VLSM permite criar mais níveis hierárquicos com base num plano de endereçamento e assim optimizar a sumarização das rotas. Por exemplo, a sub-rede 172.16.14.0/24, na figura 6, sumariza todos os endereços acima da sub-rede 172.16.14.0 incluindo todos da sub-rede 172.16.14.0/27 e 172.16.14.128/30.

- Isolamento das alterações topológicas vindas de outros routers, é outra das vantagens de usar sumarização de rotas em redes grandes e complexas. Por exemplo, se o circuito específico da sub-rede 172.16.27.0/24 avariar e começar a ir abaixo e voltar à normalidade

repetidamente, a sumarização de rotas não sofre alterações. Nenhum router externo a este domínio precisará de alterar as suas informações de routing devido a este problema.

2.4. Qualidade de Serviço (QoS)

QoS, é a capacidade de uma rede fornecer melhores serviços a um conjunto de utilizadores em detrimento de outro conjunto de utilizadores, aplicações ou ambos. O principal objectivo é conseguir transmitir dados, voz e vídeo de forma consistente, previsível e rápida.

O QoS, é utilizado para diminuir o *jitter*, *delay*, e perda de informação para aplicações onde o tempo de resposta é determinante ou a aplicações que são críticas para o bom funcionamento da organização.

Figura 7, QoS

http://www.cisco.com/warp/public/732/Tech/qos/docs/qos_graphic_cco2.swf

Esta matéria é tão vasta que seria possível efectuar um trabalho inteiro apenas dedicado a este tema. O objectivo de o incluir aqui é apenas fazer uma pequena introdução ao tema.

Existem três modelos para implementar QoS numa rede:

- o modelo Best-effort, que não aplica QoS aos pacotes, e é utilizado quando a importância de como ou quando chegam os pacotes ao seu destino não é importante.

- o modelo Integrated Services (IntServ), garante uma muito alta qualidade de serviço aos pacotes. Essencialmente, as aplicações indicam à rede que requerem um detreminado QoS para um certo período de tempo e que essa largura de banda deve ser reservada. Com *IntServ,* os pacotes a entrega de pacotes é garantida, no entanto o uso deste modelo limita fortemente a escalabilidade da rede.

- o modelo Differentiated Services (DiffServ), fornece uma escalabilidade optimizada e flexível ao implementar QoS porque divide o tráfego em classes que as máquinas conseguem interpretar. Desta forma, quando as máquinas reconhecem as classes de tráfego, fornecem diferentes níveis de QoS para diferentes classes.

2.5. Wireless Lan

Em terminologia de redes, wireless é o termo utilizado para descrever as redes onde não existem ligações físicas entre o emissor e o receptor, mas sim ligações por rádio frequencia ou microndas.

2.5.1. Diferenças entre IEEE 802.11 e IEEE 802.3

As redes locais (LANs) tradicionais condicionam os utilizadores a um local específico e não oferecem mobilidade sem intervenção técnica. As Wireless LANs são um complemento ou substituição das redes LAN. Ambas se definem nas camadas um e dois do modelo OSI, usam MAC addresses, e permitem utilizar as mesmas aplicações e protocolos.

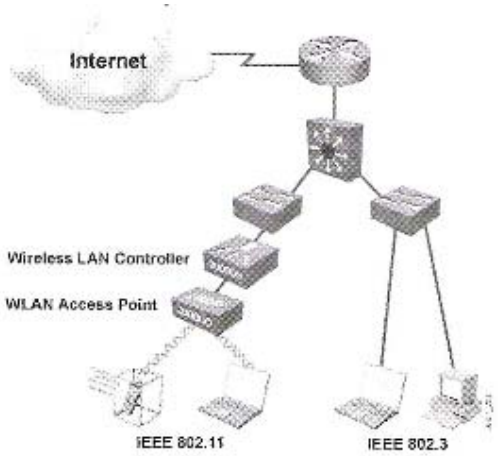


Figura 8, IEEE 802.11 e IEEE 802.3 [Cisco]

As WLAN têm por base a tecnologia CSMA/CA (Carrier Sense Multiple Access com Collision Avoidance) que não se deve confundir com CSMA/CD (Collision Detection) que é a tecnologia utilizada nas LAN's Ethernet. A detecção de colisões não é possível em redes sem fios porque a máquina emissora não pode receber ao mesmo tempo que transmite, e por isso mesmo não pode detectar uma colisão. As redes sem fios 802.11 tentam evitar colisões em vez de tomar uma acção depois de terem acontecido, como acontece nas redes 802.3 (Ethernet).

As redes sem fios implementam a funcionalidade DCF (Distributed Coordination Function) para evitar colisões recorrendo a técnicas como a

detecção de rádio frequência, espaços entre tramas, e temporizadores de espera aleatórios.

2.5.2. A necessidade de QoS na WLAN

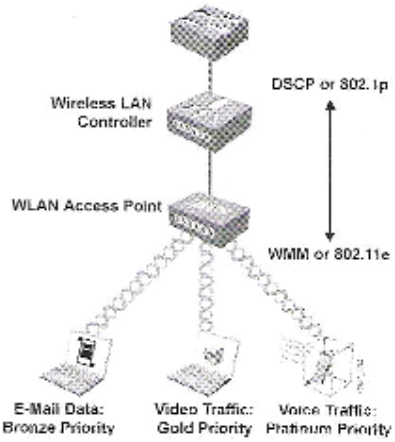


Figura 9, Extensão de QoS à WLAN [Cisco]

A extensão do QoS ao 802.11 permite transmissões de rádio frequência com mais qualidade e consistência para voz e vídeo. As implementações de QoS nas LAN utilizam frequentemente o DSCP (Diffentiated Services Code Point) ao nível tres do modelo OSI, ou o 802.1p ao nível dois do modelo OSI com o objectivo de assegurar prioridades. Contudo, em ambientes partilhados de rádio frequência não existem essas técnicas. O IEEE tem muitas extensões das redes sem fios 802.11, incluindo QoS definido pelo 802.11e, que está nesta altura em estado draft.

Para acelerar a adopção do QoS no mercado 802.11, a aliança Wi-Fi, lançou o standard Wi-Fi Multimedia (WMM). O WMM é um subconjunto do *802.11e* e reduz oito níveis de prioridade a quatro categorias de acesso. Este QoS permite a tradução do 802.1p ou DSCP para as apropriadas técnicas de rádio frequência dando ao tráfego de alta prioridade maiores probabilidades de transmissão rádio frequência que ao tráfego de baixa prioridade.

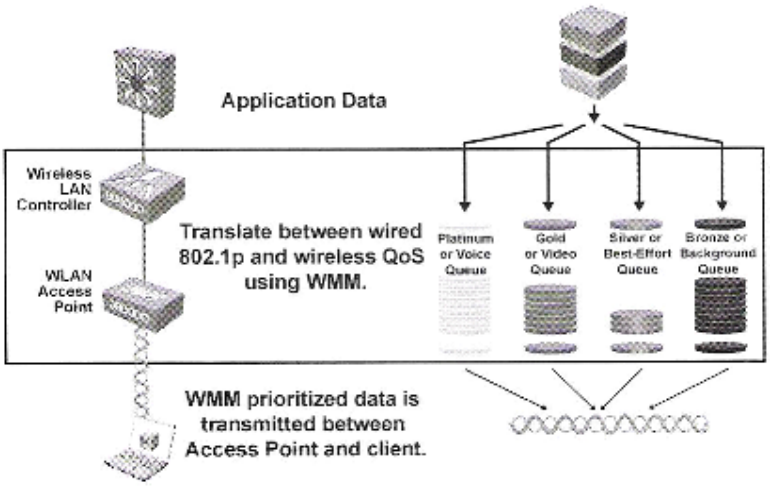


Figura 10, Filas de espera de QoS em WLAN. [Cisco]

O método de prioritização de tráfego WWM introduz quatro categorias de acesso. A categoria *Platinum* ou voz tem prioridade máxima. A categoria *Gold* ou vídeo, a categoria *Silver* ou *Best-Effort* e a categoria *Bronze* ou *Background*. Estas categorias foram desenhadas para corresponder às prioridades 802.1p ou DSCP e facilitar a operacionalidade das políticas de gestão de QoS. Todos os pacotes não pertencentes a uma destas categorias serão categorizados por defeito como *Best-Effort*. A relação destas quatro categorias quando comparadas com os oito níveis de prioridade do 802.11e são, para voz nível 6 ou 7, para vídeo nível 4 ou 5, para Background nível 1 ou 2 e para Best effort 0 ou 3, sendo que o o 0 ou 3 permitem prioritizar acima ou abaixo do *Backgound*.

2.6. Segurança

Existem duas premissas que com o tempo tendem a cair no esquecimento e a gerar falhas de segurança: a inconsistência e a complexidade.

A aproximação mais exacta à segurança é criar uma solução integrada que combine equipamentos de infra-estrutura com soluções de segurança integrada, equipamentos de segurança dotados de inteligência nativa e politicas de segurança num sistema de segurança colaborativo e adaptativo. Desta forma reduz-se a complexidade e garante-se uma maior harmonização de funcionalidades.

Os três conceitos aqui em questão são: a integração, onde cada elemento na rede actuará como um ponto de defesa recorrendo às tecnologias inerentes às operações de segurança contidas nesses mesmos equipamentos. O conceito colaborativo consiste no facto que os vários componentes de rede trabalham em conjunto fornecendo novos meios de protecção. A segurança está envolvida entre emissor/receptor, elementos de rede e aplicação das políticas. Por exemplo, a admissão de máquinas na rede está reservada às políticas de segurança que são aplicadas pelos equipamentos de rede como os switches e routers. Por último, o conceito adaptativo inova ao incorporar automaticamente comportamentos quando reconhece novos tipos de ameaça à medida que vão aparecendo. A capacidade de alerta entre equipamentos com inteligência ao nível da gestão de rede, melhora efectivamente o nível de segurança e permite uma resposta pró-activa a novas ameaças.

3. Caso de Estudo

O contexto actual do Campus Universitário fictício que servirá de caso de estudo, passa por uma necessidade de renovação tecnológica quer ao nível de redes quer ao nível de sistemas informáticos.

O Campus está implementado numa vasta área geográfica constituída por um património secular de diversos edifícios, jardins, museu e espaços públicos. Neste conjunto de edifícios e terrenos, são acomodados diversos pólos deste Campus onde existe necessidade de comunicação.

A nova solução terá que dar resposta às necessidades actuais e futuras, à semelhança do que já existe em Campus Universitários mais desenvolvidos.

Aproveitando as sinergias desta implementação, e tendo em atenção os espaços públicos que ficarão por inerência cobertos por esta infra-estrutura, será possível aproveitar parte desta rede para outros fins no âmbito das redes sem fios. De facto, depois de estarem garantidas as redes dos professores, alunos, e outras redes académicas como por exemplo a E-U, será ainda possível gerir sem dificuldades outras sub-redes como por exemplo uma rede municipal pública, ou serviços para operadores de internet. Como contrapartida do serviço público oferecido é assim possível, do ponto de vista financeiro, rentabilizar esta infra-estrutura recorrendo a investidores externos como a CMO e alguns operadores de internet potencialmente interessados.

Estabelecendo que vai ser possível reaproveitar na totalidade toda a rede passiva, permite assim reduzir um custo significativo ao projecto. Por outro lado, no que diz respeito à rede activa e por se encontrar obsoleta, será mais vantajoso não considerar a integração dos componentes existentes uma vez que iria comprometer a integridade do novo projecto e por outro lado, o seu valor comercial gerado numa operação *trade-in* será muito mais útil para abater os custos do projecto.

A nova infra-estrutura deverá ter em conta o crescimento físico e também a evolução tecnológica, bem como o numero de alunos e/ou edifícios. As suas capacidades serão nos primeiros anos amplamente suficientes para todas as necessidades previstas e deverá estar assegurada uma boa margem de capacidade de crescimento e renovação tecnológica.

Tendo em conta o ritmo crescente da evolução tecnológica, a nova solução deverá ser constituída na totalidade por equipamentos que suportarão actualizações tecnológicas de forma a mater a sua operacionalidade durante o máximo tempo possível.

Quanto às novas tecnologias, perspectiva-se que o espírito da tele-presença se generalize, que as comunicações sobre IP se banalizem à semelhança do que hoje acontece com a rede GSM. Tendo em conta esta perspectiva, os consumos crescentes de largura de banda e a sua gestão estarão considerados desde já, garantindo esta normal evolução.

Feito o enquadramento ao caso de estudo segue-se o levantamento específico das necessidades na óptica da segurança, disponibilidade, produtividade comunicações e mobilidade e é apresentada a proposta de arquitectura de solução que traduz o dimensionamento conforme os requisitos.

3.1. Levantamento de necessidades

3.1.1. Segurança

A falta de segurança informática é mais do que uma simples desconformidade numa organização. Os ataques praticados actualmente podem provocar a paragem completa de uma rede ou permitir fuga de informação e com isso causar prejuízos por vezes difíceis de quantificar.

Para alcançar as necessidades de segurança que se exigem na rede de um *campus,* é necessário implementar uma solução que garanta funcionalidades de protecção embebidas em toda a extensão da rede de forma a proteger, prevenir e actuar autonomamente numa situação de ataque. Além disso, deve permitir controlar quem tem acesso à rede e o que pode ou não fazer com esse mesmo acesso. Para tal essa solução deve integrar opções tecnológicas como *firewall, intrusion detection system* (IDS), anti-vírus, authentication, authorization, accounting (AAA), filtragem de sites e 802.1x.

Com estes pressupostos deverá estar garantida a segurança à entrada do *campus,* no seu interior e também nos utilizadores finais protegendo-os proactivamente contra infecções e ataques. Deverá ser igualmente garantida a identidade bem como a inviolabilidade das comunicações.

3.1.2. Disponibilidade

A disponibilidade dos recursos na altura exacta em que são requisitados é um factor decisivo para o sucesso de uma rede. Com o crescente aumento da dependência dos recursos oferecidos pela rede de um *campus,* torna-se cada vez mais inaceitável qualquer quebra de serviço.

Deverá ser acautelada qualquer quebra de serviço resultante de brechas relacionadas com segurança, falhas de energia ou mesmo intervenções planeadas para actualização ou configurações de sistema.

3.1.3. Produtividade

Outro desafio não menos importante é o aumento significativo dos níveis de produtividade dos utilizadores finais da rede de um *campus*. Para tal, a rede deverá estar preparada para receber a implementação de aplicações que automatizem os processos de trabalho ligados às funções críticas que se desenvolvem no dia-a-dia. O alinhar destes processos vai permitir aos utilizadores responder à informação a partir dessas mesmas aplicações e com isso ter um efeito positivo nos seus objectivos pessoais.

3.1.4. Comunicações IP

Os ambientes de trabalho mudam frequentemente e com isso trazem novos desafios às organizações no sentido de virtualizar os recursos, dar resposta ao crescimento de tráfego nas comunicações e manter a capacidade de trabalhar com agilidade. Para colmatar estas necessidades será necessário adoptar uma solução que contemple telefonia IP, para utilizar o IP como meio primário de comunicação; centro de contactos IP, para adicionar serviços de contacto inteligentes que permitam o trabalho colaborativo em tempo real; Vídeo conferencia e transmissão de vídeo em tempo real, para permitir a entrega de eventos em tempo real em toda a rede; e comunicações unificadas, ou seja a combinação de ferramentas de produtividade pessoal como *messaging* e regras baseadas em routeamento de mensagens.

3.1.5. Mobilidade

A crescente necessidade de melhorar a produtividade não admite quebras durante a permanência no *campus*. Quer se esteja à secretária, no auditório, no bar ou mesmo no jardim, os utilizadores necessitam de acesso à totalidade dos seus recursos., incluindo telefonia IP e vídeo conferencia bem como serviços de dados como o e-mail, calendários ou bases de dados.

Como resposta a esta necessidade, o *campus* deverá estar dotado de uma infra-estrutura sem fios que permita comunicações rádio frequência seguras e cifradas ao longo de toda a sua área útil.

3.2. Arquitectura proposta / Dimensionamento

Sendo esta solução efectuada com equipamentos Cisco Systems, foi seguido um planeamento hierárquico em três camadas conceptuais: o *Core Layer*, o *Distribution Layer* e o *Access Layer.*

3.2.1. Core Layer

O Centro de Processamento de Dados (CPD) será o local seleccionado para albergar os sistemas críticos da nova arquitectura. Este local deverá ter condições especiais e acesso físico muito limitado. Entre as condições especiais estão a climatização apropriada e recomendada pelos fabricantes, fontes de energia ininterrupta, meios de extinção de incêndio e gestão de acessos.

Os critérios que levaram à escolha desta solução foram a adequação da capacidade de processamento por um lado, a capacidade de redundância e a escalabilidade tendo em conta que o factor custo é ainda mais determinante num ambiente não industrial. Assim, e para garantir o máximo aproveitamento do equipamento principal do *Core Layer* do *campus*, foi seleccionado um único equipamento modular que agrega todas as funcionalidades requeridas ao mesmo tempo que garante a redundância necessária sem recorrer à duplicação de unidades.

Este equipamento modular garante a redundância necessária por ser constituído por duas unidades em todas as suas componentes activas, ou seja, nos alimentadores de energia, nos CPU's, e nas cartas de conectores. A única parte não duplicada é o próprio chassis que por ser uma unidade passiva não é tão susceptível de sofrer uma avaria como as restantes onde predominam componentes electrónicos. Desta forma reduzem-se de forma considerável os pontos únicos de falha, conseguindo-se um equipamento com um elevado grau de fiabilidade.

Para garantir a compatibilidade em todos os componentes seleccionados foi utilizada uma ferramenta da Cisco Systems denominada *Cisco Configuration Tool* na configuração do equipamento.

Product	Description	Quantity
(1) WS-C4507R	Catalyst 4500 Chassis (7-Slot),fan, no p/s, Red Sup Capable	1
(2) PWR-C45-1400AC	Catalyst 4500 1400W AC Power Supply (Data Only)	1
(3) PWR-C45-1400AC/2	Catalyst 4500 1400W AC Power Supply Redundant(Data Only)	1
(4) CAB-7513ACE	AC POWER CORD (EUROPE)	2
(5) WS-X4516-10GE	Catalyst 4500 Supervisor V-10GE, 2x10GE (X2) and 4x1GE (SFP)	1
(6) WS-X4516-10GE/2	Catalyst 45xxR Supervisor V-10GE, 2x10GE (X2) or 4x1GE (SFP)	1
(7) S4KL3EK9-12225EWA	Cisco IOS ENHNCD L3 C4500 SUP4/5,3DES(OSPF,EIGRP,IS-IS)	1

```
(8) WS-X4424-GB-RJ45    Catalyst 4000 24-port 10/100/1000 Module (RJ45)            2
(9) WS-X4448-GB-SFP     Catalyst 4500 48-Port 1000Base-X (SFPs Optional)           2
(10) GLC-LH-SM           GE SFP, LC connector LX/LH transceiver                    8
(11) GLC-SX-MM           GE SFP, LC connector SX transceiver                      48
(12) X2-10GB-CX4         10GBASE-CX4 X2 Module                                     2
```

Para descrever um pouco melhor esta configuração foram enumerados todos os componentes de 1 a 12. Nos pontos 1 a 4, trata-se do chassis devidamente equipado com ventilação, alimentadores e cablagem eléctrica. Os pontos 5 e 6 são os CPU's do sistema, conhecidos neste caso por *Supervisor* de quinta geração. Estes *supervisor's* estão equipados com conectores de alto débito para garantir ligações a equipamentos modulares na *server farm* à velocidade de duas vezes 10 Gbps. O ponto 7 refere-se ao software que estas unidades vão correr. Neste caso será um IOS com capacidade de cifragem 3DES e capacidade para correr três dos mais importantes *routing protocols* incluindo o OSPF que é o mais popular dos protocolos não proprietários e por isso mesmo garante a interligação do campus com qualquer outro sistema independentemente da sua arquitectura. O ponto 8 refere-se às cartas Ethernet que servirão várias redes incluindo a *server-farm, DMZ's,* e outras que se justifiquem dentro da limitação em distância que o cobre permite, ou seja, 100 metros. O ponto 9 vem colmatar esta limitação da distância com as cartas de fibra óptica que são utilizadas igualmente nos equipamentos que utilizem este tipo de *media* nomeadamente os equipamentos do *Distribution Layer* e alguns equipamentos específicos existentes nas *server-farm, DMZ's* e em todos os pontos com distancias superiores a 100 metros. Os pontos 10 e 11 referem os interfaces que serão instalados nas cartas anteriores dividindo-se em dois tipos de fibra óptica, a MMF e a SMF. A MMF é a fibra tipicamente utilizada dentro do *campus* e a SMF a mais utilizada nas interligações na ordem dos vários KM. Estes conectores permitem a interligação directa em banda larga do *campus* com outras instituições. O ponto 12 refere-se aos conectores de 10 Gbps que serão instalados nos *supervisor's.*

O sistema operativo deste equipamento (IOS) permite implementar as funções básicas de *firewall* no que diz respeito à filtragem de tráfego ao permitir ou negar as comunicações consoante a sua origem, destino e tipo de tráfego. Esta será a primeira camada de protecção que externamente será complementada com outro tipo de protecção ao nível dos utilizadores e aplicações garantido por outro firewall que estará a correr em ambiente *Intel*, nomeadamente *ISA Server*, e/ou outros que se venham a eleger como por exemplo *Checkpoint FW1*. Tal como no capítulo do QoS, a implementação de segurança de um *campus,* por ser tão extensa, poderá ser objecto de outro estudo mais aprofundado.

No que diz respeito ao objectivo deste trabalho, e à implementação de *routing* e *switching*, este equipamento será responsável por centralizar a gestão de *VLAN's* pela sua função de *VTP server*.

Quanto ao conjunto de problemas e soluções típicas do *Core Layer*, destacam-se como problemas o eficiente balanceamento de carga, a disponibilidade constante da rede, ligações de alto débito e ligações redundantes. Como resposta a estes problemas implementar-se-ão funcionalidades ou tecnologias como OSPF, túneis EtherChannel, Gigabit Ethernet e 10 GbE.

3.2.2. Distribution Layer

O *Distribution Layer* é responsável por agregar todas as ligações provenientes do *Access Layer* e garantir a melhor gestão do tráfego que recebe do *Core Layer* bem como evitar que o tráfego proveniente de diferentes àreas do *Access Layer* seja desnecessariamente processado no *Core Layer*.

Quanto ao conjunto de problemas e soluções típicas do *Distribution Layer*, destacam-se como problemas a detecção de *loop's*, *default gateways* redundantes, balanceamento de carga, gestão topológica, disponibilidade constante da rede e redundantes. Como resposta a estes problemas implementar-se-ão funcionalidades ou tecnologias como *Spanning Tree*, *Gateway Load Balancing Protocol* (GLBP) e túneis *EtherChannel*.

Esta camada conceptual é geralmente eliminada em termos físicos quando as dimensões das redes assim o justificam. Tendo em conta o binómio custo e perspectiva de crescimento, não se justifica a sua implementação física neste caso de estudo optando-se antes pela sua virtualização. Neste caso, como o equipamento principal do *Core Layer* tem capacidade de processamento intra-modular, é possível gerir parte das comunicações das diferentes àreas do *Access Layer* sem solicitar o processamento dos *supervisor's.*

3.2.3. Access Layer:

Embora a gestão de endereçamento e segmentação seja gerida no *Core Layer*, estas são estendidas pelos diversos *trunk's* 802.1Q até ao Access Layer onde os utilizadores finais as vão utilizar. As zonas de trabalho ou *subnet's* serão definidas por função independentemente da sua localização física e virtualizadas em *VLAN's*. Por exemplo, a VLAN Professores será disponibilizada nas salas de aulas, salas de professores e também na rede wireless através de um processo de autenticação que apenas autorize os Professores. Nas mesmas salas de aulas, e rede wireless será disponibilizada outra *VLAN* para os alunos, com outro processo de autenticação. Da mesma forma se poderá tratar a *VLAN* administrativa e outras que se venham a verificar necessárias.

O processo de autenticação será constituído por um conjunto de métodos que começam nos pontos de acesso pelas funções de *Port Security,* até à validação do conjunto username/password na *Active Directory* por MS-CHAP-V2 em paralelo com a validação dot1x onde um certificado digital pessoal emitido automaticamente pela infra-estrutura *PKI será atribuído* a cada utilizador. Esta infra-estrutura terá a capacidade de revogar a qualquer momento qualquer certificado emitido a cada utilizador por motivos de segurança. As revalidações dos certificados serão automáticas pelo período que for definido, cessando automaticamente na data pretendida. A atribuição da *VLAN* correspondente ao tipo de utilizador depende do *template* de autenticação correspondente. Um professor depois de se autenticar terá acesso à *VLAN* Professores, da mesma forma que os alunos depois de autenticados apenas terão acesso à *VLAN* Alunos. Desta forma qualquer máquina que se ligue num ponto de rede activo no *campus* será sempre alvo de um processo de autenticação, onde se não cumprir cumulativamente todos os requisitos de acesso que forem definidos será apenas disponibilizada uma *VLAN* para convidados com acesso limitado a determinados recursos como por exemplo uma parte restrita da intranet.

Este tipo de autenticação é igualmente aplicado na rede wireless onde a selecção das respectivas *VLAN's* se processa de forma similar. Nesta rede as *VLAN's* encontram-se agregadas aos diversos SSID's de forma a isolar completamente os recursos entre *VLAN's* conforme já acontece na rede fixa. Para gerir todos os pontos de acesso da infra-estrutura wireless, será utilizado um controlador wireless da série 4440 (Cisco 4400 Series Wireless Lan Controllers) que tratará de forma automática todos os

aspectos relacionados com a gestão da transmissão de rádio, como por exemplo a racionalização de canais de transmissão, e *roamming* entre pontos de acesso de forma transparente para os utilizadores. Este controlador tem capacidade para gerir até 100 *access point's wireless*, o que é suficiente para dar cobertura total ao *campus*.

Quanto à selecção de equipamento neste caso de estudo, serão utilizadas n unidades de acesso da série *Catalyst Express 500 Cisco Systems*, até estarem supridos todos os utilizadores. Estas unidades recebem 2 ligações em fibra óptica Gigabit Ethernet da camada superior e garantem o acesso a grupos de 24 utilizadores, tendo 4 destas portas a capacidade de fornecer PoE o que na prática possibilita a integração de pontos de acesso wireles, telefonia IP, cameras de vídeo e outros equipamentos que requeiram alimentação. Além desta importante funcionalidade, esta gama permite utilizar todas as tecnologias anteriormente referidas sendo as mais importantes o RSTP, VTP, QoS, Etherchannel, e SPAN.

Este dimensionamento de 2 Gbps full duplex para cada grupo de 24 utilizadores a 10/100 Mbps é bastante equilibrada e permite alcançar os objectivos de performance que se exigem num *campus* com todos os serviços que foram anteriormente referidos.

Quanto ao conjunto de problemas e soluções típicas do *Access Layer*, destacam-se como problemas a detecção de equipamentos não autorizados, pontos únicos de falha, ligações redundantes e prevenção de loop's. Como resposta a estes problemas implementar-se-ão funcionalidades ou tecnologias como BPDU/Root Guard, componentes Dual Modular, Stateful Switchover (SSO), *Spanning Tree* e as funções integradas de segurança referidas no parágrafo anterior.

4. Conclusão

No desenvolvimento deste trabalho houve uma preocupação de que o levantamento teórico desse um enquadramento à ponderação para a escolha da solução. A selecção dos equipamentos foi elaborada tendo em conta, por um lado, a robustez e performance que se exige de um *campus universitário* e, por outro, a facilidade de administração e actualização tecnológica da infra-estrutura sem esquecer a escalabilidade e segurança.

Tendo presente que um *campus* universitário não é um ambiente industrial foi dada especial atenção à componente custo *versus* operacionalidade para criar a base de uma infra-estrutura com capacidade de evolução especialmente na área da segurança. Para alcançar este pressuposto a solução passou por centralizar a solução numa única máquina modular central que satisfizesse todas as capacidades que se impunham neste estudo. Esta máquina modular central estende todas as funcionalidades importantes até aos utilizadores finais pelas suas múltiplas ligações aos equipamentos de acesso.

Este investimento representa um passo importante por servir de base não só à plataforma de servidores, por permitir rentabilizar os recursos no seu máximo aproveitamento, como também para servir eficientemente os utilizadores que beneficiam de novas condições no que diz respeito às mais diversas implementações que se venham a considerar úteis no futuro.

5. Glossário

Termo	Significado
3DES	Triple Data Encryption Standard é um padrão de criptografia baseado no algoritmo de criptografia DES desenvolvido pela IBM em 1974 e adoptado como padrão em 1977.
AAA	AAA é uma referência aos protocolos relacionados com os procedimentos de autenticação, autorização e acompanhamento do uso de recursos pelos utilizadores (accounting).
(W) AP	Wireless Access Point, é um equipamento que permite a interligação sem fios de outros equipamentos entre si formando uma rede.
BPDU	Bridge Protocol Data Units, são tramas especiais que contêm a identificação das bridges e outras informações relacionadas com o *Spanning Tree Protocol.*
Bridge ID (BID)	BID é um campo contido num pacote BPDU. Tem 8 bytes de comprimento sendo que os primeiros 2 bytes se referem à prioridade e os últimos 6 bytes o Mac address fornecido pelo switch.
Bridge	Uma Bridge é um equipamento que interliga vários segmentos de rede. Operam no nível 2 do modelo OSI e utilizam o método bridging.
Bridging	Bridging é uma técnica de encaminhamento de informação que ao contrário do routing não assume a localização de um endereço de rede em particular. Depende do broadcasting para localizar equipamentos desconhecidos.
Broadcasting	Broadcasting refere-se à transmissão de tramas que serão recebidas conceptualmente em todos os destinatários contidos nessa mesma rede.
Broadcast storm	Broadcast storm, é a acumulação de tráfego broadcast numa determinada rede até um ponto de congestão onde não é possível estabelecer novas comunicações e onde as existentes possam ser afectadas.
Checkpoint FW1	É uma reconhecida solução de firewall que utiliza uma tecnologia adaptativa de inspecção inteligente de tráfego.
DMZ	É a abreviação de demilitarized zone (em português, zona desmilitarizada), sendo a área de rede que permanece entre a rede

	interna de uma organização e uma rede externa, em geral a internet.
EtherChannel	Permite a agregação incremental de conjuntos de circuitos num único interface no sentido de criar circuitos de alta capacidade de transmissão e redundância.
Ethernet	é uma tecnologia de interligação para redes locais - Local Area Networks (LAN) - define o meio de transmissão para a camada física, e formato de tramas e protocolos para a camada de controle de acesso ao meio (Media Access Control - MAC) do modelo OSI. A Ethernet foi padronizada pelo IEEE como 802.3 e partir dos anos 90, tem vindo a ser a tecnologia de LAN mais utilizada e tem tomado grande parte do espaço de outros padrões de rede como Token Ring, FDDI e ARCNET.
Firewall	Firewall é o nome dado ao dispositivo de uma rede de computadores que tem por função regular o tráfego de rede entre redes distintas e impedir a transmissão e/ou recepção de dados nocivos ou não autorizados de uma rede a outra.
FTP	FTP significa File Transfer Protocol (Protocolo de Transferência de Arquivos), e é uma forma bastante rápida e versátil de transferir ficheiros.
HTTP	é a sigla em língua inglesa de HyperText Transfer Protocol (Protocolo de Transferência de Hipertexto), um protocolo da camada de Aplicação do modelo OSI utilizado para transferência de dados na rede mundial de computadores, a World Wide Web. Também transfere dados de hiper-mídia (imagens, sons e textos).
HUB	é um equipamento que interliga diversas máquinas (computadores) que pode ligar externamente redes TAN, LAN, MAN e WAN sendo indicado para redes com poucos terminais de rede, pois não comporta um grande volume de tráfego devido à sua metodologia de trabalho por broadcast, que envia a mesma informação dentro de uma rede para todas as máquinas interligadas. Devido a isto, a sua aplicação a uma rede maior é desaconselhada.
IDS	intrusion detection system (IDS) é um equipamento que detecta manipulações não desejadas dirigidas a sistemas informáticos. Estas manipulações resultam de ataques efectuados propositadamente. Um IDS é utilizado para detectar tráfego malicioso que não pode ser detectado por um firewall convencional.
IEEE	Instituto de Engenheiros Eléctricos e Electrónicos ou IEEE (pronuncia-se I-3-E, ou, conforme a pronúncia inglesa, eye-triple-e) é uma organização profissional sem fins lucrativos, fundada nos Estados Unidos.

IOS	Cisco IOS (originalmente Internetwork Operating System) é o software utilizado na maioria dos equipamentos Cisco Systems. O IOS é um conjunto de funções de routing, switching, internetworking and telecommunications integradas num sistema operative multi-tarefa. O primeiro IOS foi programado por William Yeager.
IP	Internet Protocol (IP) é um protocolo orientado à ligação utilizado para comunicação de dados através de uma rede comutada. É um protocolo do nível 3 do modelo OSI e é encapsulado num protocolo de nível 2 como por exemplo Ethernet. O IP fornece a possibilidade de comunicar através de um endereço global único entre computadores.
ISA Server	Microsoft Internet Security and Acceleration Server (ISA Server) é descrito pelaMicrosoft como uma "integrated edge security gateway". Tendo por base o Microsoft Proxy Server, o ISA is é um produto de segurança e firewall que assenta no sistema operativo Microsoft Windows.
MAC address	Media Access Control address (MAC address) ou Ethernet Hardware Address (EHA) ou *hardware address* ou *adapter address* é um endereço, teoricamente único e inalterável, atribuído a todos os adaptadores de rede.
Roamming	É o termo utilizado nas telecomunicações sem fios que se refere à extensão da conectividade a uma localização diferente da localização onde o serviço foi inicialmente registado. Este termo tem origem nas redes GSM (Global System for Mobile Communications Association).
Router	É um equipamento que determina o melhor caminho para fazer circular dados entre diferentes redes, ligando as próprias redes entre si.
Routing	É o processo de selecção de rotas através das quais será encaminhado o tráfego. O *routing* é efectuado em muitos tipos de redes incluindo a rede telefónica, a internet e redes de transporte.
Server-farm	Uma *server farm* é um conjunto de servidores estrategicamente agrupados para ultrapassar a capacidade de máquinas isoladas. Normalmente as *server farms* tem máquinas primárias e de backup atribuídas a uma única tarefa de forma a que se uma máquina falhar não ocorra quebra de serviço.
SMTP	Simple Mail Transfer Protocol (SMTP) é o standard para transmissão de e-mail pela Internet. O SMTP é definido no RFC 821 (STD 10).
SSH	Secure Shell ou SSH é um protocolo de rede que permite trocar informação por um canal seguro entre dois computadores. A cifragem permite a confidencialidade e integridade dos dados ao utilizar

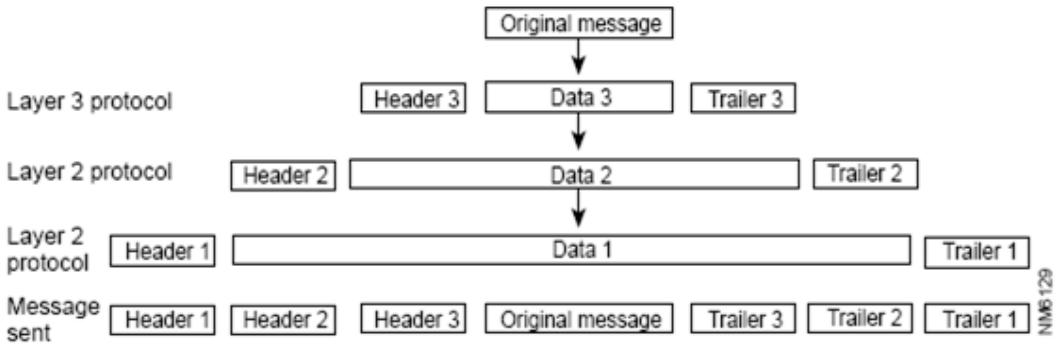
	criptografia de chave-publica para autenticar o computador remoto e permitir a autenticação do utilizador.
TCP	Transmission Control Protocol (TCP) é um dos principais protocolos do *Internet protocol suite*, conhecido por TCP/IP. Ao utilizar TCP, as aplicações que correm numa rede endereçada podem criar ligações entre si e através delas trocar dados. Ao contrário do protocolo IP, o TCP garante a entrega da informação entre o emissor e o receptor e distingue as múltiplas ligações utilizadas em simultâneo por diversas aplicações a correr no mesmo computador.
Unicast	Unicast é o envio de informação para um único endereço. Deriva da palavra broadcast, sendo o seu extreme oposto.
WiFi	Abreviatura para "wireless fidelity" é uma tecnologia de interligação entre dispositivos sem fios, utilizando o protocolo IEEE 802.11.

6. Anexo A

Encapsulamento de informação

A informação que vai sendo processada dentro de uma camada é passada para o nível superior até completar a transmissão. Cada camada adiciona informação de controlo à informação a transmitir propriamente dita. Esta informação de controlo chama-se header e/ou trrailer porque é colocada à frente ou atrás da informação a ser transmitida. A informação é então passada à camada superior. Durante o processo de transmissão dá-se então o encapsulamento.

Figura 4 **Encapsulation of Data for Network Delivery**



Quando a informação é recebida, acontece o inverso. Cada camada retira o seu header antes de passar a informação para a camada inferior. À medida que a informação vai descendo as camadas, vão sendo retirados os headers e/ou trailers, a este processo dá-se o nome de desencapsulamento.

7. Anexo B

Protocolos de routing (IGP's)

RIP- O routing information protocol foi desenvolvido pela Xerox Corp. No princípio dos anos 80. É actualmente utilizado em muitas redes pequenas, mas tem serias limitações quando usado em redes de maior dimensão. Por exemplo, o RIP limita o numero de hops a 16, entre duas máquinas. É também bastante lento a convergir, ou seja demora bastante tempo para que as alterações de rede sejam conhecidas por todos os routers envolvidos. Por fim, o RIP determina as suas rotas apenas analisando o número de hops entre duas máquinas, sendo que esta técnica ignora as diferentes larguras de banda em cada circuito, os níveis de utilização e todas as outras métricas que são importantes para escolher a melhor rota. É por este motivo que muitas organizações que cresceram para redes de grande dimensão estão a migrar para protocolos mais sofisticados.

IGRP- este protocolo foi igualmente criado no inicio dos anos 80 pela Cisco Systems, que foi a primeira companhia a resolver os problemas do RIP. O IGRP determina a melhor rota analisando a largura de banda e o delay dos diversos circuitos onde está ligado. Converge mais rápido que o RIP e não está limitado por contagem de hops. Como resultado destes e outros melhoramentos sobre o RIP, o IGRP implementou-se em muitas das maiores e mais complexas topologias em todo o mundo.

EIGRP- a Cisco melhorou o seu IGRP para dar resposta às redes cada vez maiores e às redes de alta disponibilidade. Esta versão melhorada combina a facilidade de utilização dos tradicionais *distance vector protocols* com as rápidas capacidade dos novos *link state protocols.* O *Enhanced IGRP* consome significativamente menos largura de banda que o IGRP porque tem a capacidade de trocar apenas a informação de routing que foi efectivamente alterada. O Enhanced IGRP consegue igualmente gerir informação de routing AppleTalk e Novell IPX, além do IP routing.

OSPF – este protocolo foi desenvolvido pela Internet Engineering Task Force (IETF) para substituição do RIP. O OSPF é baseado no trabalho iniciado por John McQuillan nos finais dos anos 70 tendo sido continuado pela Radia Perlman e pela DEC nos anos 80. É um protocolo utilizado industrialmente por todos os grandes fabricantes de equipamentos de

networking. É um protocolo link-state, que suporta routing hierárquico dentro de um AS e pode ser dividido em áreas. Cada área é constituída tipicamente uma ou mais subnets relacionadas entre si e todas a áreas vão ligar a uma área principal chamada backbone área.

8. Bibliografia

- www.cisco.com

- **Jeff Doyle**

  Routing TCP/IP, Volume I (CCIE Professional Development)
  Cisco Press.

- **Jeff Doyle and Jennifer Carroll**

  Routing TCP/IP, Volume II (CCIE Professional Development)
  Cisco Press.

- **Peterson, L. and Davie, B.**

  Computer Networks: A Systems Approach, second edition
  Morgan Kaufmann Publishers. 2000.

- **Bassam Halabi**

  Internet Routing Architectures (2nd Edition)
  Cisco Press.

- **John T. Moy**

  OSPF: Anatomy of an Internet Routing Protocol
  Addison-Wesley, February 1998.

- **James Boney**

  Cisco IOS In a Nutshell
  O'Reilly 2002.

- **Tony Kenyon**

  Data Networks, Routing, Security, and Performance Optimization
  Digital Press, 2002, ISBN: 1-55558-271-0

- **Andrew S. Tanenbaum**

  Computer Networks, Fourth Edition
  Prentice-Hall.

- **James Kurose and Keith Ross**

  Computer Networking, A Top-Down Approach Featuring the Internet, Second Edition
  Addison-Wesley, 2003, ISBN: 0-321-17644-8.

- **William Stallings**

  Computer Networking with Internet Protocols and Technology
  Pearson, Prentice Hall, 2004, ISBN: 0-13-191155-4