Utilização de VLAN para segmentação de rede em universidade

Pereira, Diego Cesar

Resumo **- Com a evolução da tecnologia e seus meios de comunicações, observa-se que o número de dispositivos eletrônicos interligados a redes locais e a rede mundial de computadores é crescente e volumosa. O ambiente de trabalho em empresas de modo geral se tornou totalmente conectado, setores estão automatizados e interligados a uma rede de computadores gerando e recebendo informações. O tema abordado foca em contextualizar e informar o leitor sobre a importância do controle de tráfego de dados em uma rede local, garantindo a entrega e o recebimento dos dados com eficiência e segurança aos destinatários, sem a interferência de outras conexões internas não autorizadas e consequentemente conexões externas. A utilização de VLANs (redes locais virtuais) tem como proposito a segmentação logica da rede tornando-a independente da topologia física, garantindo uma redução de custo e controle de tráfego broadcast resultando em uma rede de fácil gerenciamento e maior segurança.**

Palavras-chave **- Iot, broadcast, switch, segurança da informação.**

Abstract **- With the evolution of technology and its means of communications, noted that the number of electronic devices connected to local networks and the world wide network of computers is increasing and voluminous. The work environment in companies in general has become fully connected, sectors are automated and interconnected to a computer network generating and receiving information. The theme addressed focuses on contextualizing and informing the reader about the importance of controlling data traffic in a local area network, ensuring that data is delivered and received efficiently and safely to the recipients without the interference of other unauthorized internal connections and consequently connections. The use of virtual local area networks (VLANs) is aimed at the logical segmentation of the network making it independent of the physical topology, ensuring a cost reduction and control of broadcast traffic resulting in a network of easy management and greater security.**

Keywords **- Iot, broadcast, switch, information security.**

I. INTRODUÇÃO

MEIOS corporativos e universidades estão modernizando seus processos internos para aumentar a qualidade da entrega final afim de gerar ganhos de produtividade. Para garantir a entrega de serviços de maneira rápida e eficaz são utilizados computadores interligados dentro de uma rede local comunicando com servidores e diversos dispositivos, que por sua vez processam inúmeros sistemas gerenciando as atividades e demanda de cada setor.

Na última década, presenciamos um crescente número de dispositivos conectados as redes de comunicações e consequentemente o aumento de conexões da rede local das organizações. A troca de informações de sistemas e serviços destes dispositivos compartilhados em uma mesma rede tem como consequência a geração de alto tráfego dentro da rede, podendo ocasionar uma lentidão na comunicação entre os dispositivos e até mesmo a indisponibilidade destes serviços e sistemas, trazendo complexidade no gerenciamento e incredibilidade para a rede.

A evolução de equipamentos gerenciadores de redes nos últimos anos, possibilitou um melhor gerenciamento das redes tornando-as mais eficientes e seguras. Os switches que interligam a rede de maneira a manter os dispositivos conectados e comunicando o tempo todo, tratam do recebimento e entrega de pacotes de dados em toda rede.

Neste sentido, objetiva-se com este trabalho apresentar os benefícios da utilização de VLAN para segmentar a rede de uma universidade de maneira lógica, criando redes locais virtuais (VLANs) dentro de um ambiente de rede física. Para determinar acessos específicos de dispositivos pertencentes a diferentes setores e blocos, afim de garantir a integridade e entrega de dados contribuindo para o melhor desempenho e segurança na rede.

II. A REDE CONECTADA POR SWITCHES

Partindo da comunicação dos antigos hubs de repetição que irradiam por todas as portas um frame recebido de um dispositivo, podendo ocasionar colisões no barramento da rede local se o número de dispositivos e tráfego forem altos. Estes foram substituídos pelos switches, com função de segmentar a rede local separando-a em vários segmentos com domínios de colisão separados. Este processo é feito pela filtração de frames Ethernet pelo endereço MAC, direcionando apenas os frames direcionados para um determinado segmento (BARROS 2013). O switch recebe um frame e o endereço MAC de destino, se seu endereço consta na tabela de endereços MAC ele é enviado somente para a porta do seguimento à na qual está ligado. Caso o endereço MAC de destino não conste na tabela, este frame é enviado a todas as portas do segmento ligados ao switch. Podendo assim sobrecarregar a rede gerando frames do tipo broadcast que circulam por todos os segmentos da rede.

Para controla o volume de conexões TCP/IP (principal protocolo de comunicação de dispositivos de uma rede) evitando a propagação destes frames broadcast na rede, surgiram os switches segmentadores lógicos criando redes virtuais locais (VLANs) em seu domínio.

Os switches ethernet estão classificados da seguinte maneira.

A. Switches não gerenciados

Os switches desta categoria são os mais simples, como indicado no nome, eles não podem ser gerenciados, não podem ter modificações nas suas configurações. São indicados para

Diego Cesar Pereira, Universidade Uberaba (UNIUBE), Uberaba, Minas Gerais, Brasil, diegocesar.engcomp@gmail.com

interligação de uma rede pequena e simples onde o objetivo é apenas expansão de uma rede como a de sua casa ou escritório. São switches de baixo custo que oferecem conectividade plug-and-play como mostrado na Fig. 1, possuem comutação Fast Ethernet e os mais atuais são conexão Gigabit com recursos importante como Power over Ethernet (PoE) fornecendo energia para telefones IP, pontos de acesso e outros dispositivos.

Figura 1. Switches ethernet não gerenciados.

Fonte: https://www.cisco.com/c/pt_br/products/switches

B. Switches ethernet inteligentes

Os switches desta categoria oferecem gerenciamento básicos, são indicados para infraestruturas menores e redes de baixa complexidade. Possui interface para modificações na sua segurança e qualidade de serviços (QoS), suportam recursos como o roteamento estático da camada 3, listas de controle de acessos (ACLs) e o Power over Ethernet Plus (PoE +). São switches com desempenho, confiabilidade, eficiência energética e além disso, permitem segmentar a rede de maneira lógica, em grupos de trabalho por VLANs, com número menor de VLAN e e hosts conectados. (CISCO, 2018)

C. Switches ethernet gerenciáveis

Os switches gerenciáveis são projetados para oferecerem maior escalabilidade, melhor desempenho com altos níveis de segurança e qualidade de serviços (QoS) baseados e fluxo, são indicados para infraestruturas maiores em meios corporativos como em centro de serviços compartilhados (CSC), universidades. Permite segmentação da rede, com grande número de VLANs, hosts, rotas IP, ACLs. (CISCO, 2018)

Os switches de camada 2 alterna os quadros usando apenas informações da camada 2 (endereço MAC de destino), as comunicações dos hosts só podem ser feitas dentro da mesma VLAN e sub-rede, necessitando de um roteador.

Os switches da camada 3 têm a capacidade de alternar os switches da camada 2 usando o endereço MAC de destino, mas também a capacidade de encaminhar usando informações da camada 3 (endereço IP de destino), não há necessidade de um roteador separado, ele é embutido no switch e é mais rápido na troca de pacotes do que um roteador tradicional.

Figura 2. Switches ethernet Cisco gerenciáveis e switches inteligentes.

Fonte: https://www.cisco.com/c/pt_br/products/switches

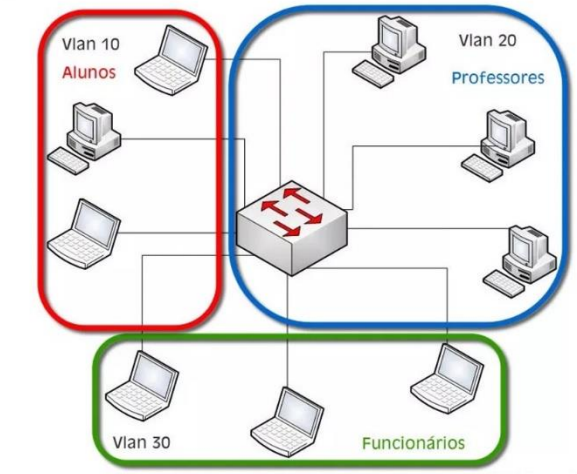
III. SEGMENTAÇÃO DA REDE POR VLANS

Como já tratado anteriormente, as VLANs segmentam a rede física de maneira lógica, definindo encapsulamentos dentro da rede para tratar os frames de broadcast que circulam naquele determinado segmento, sem que possam ser encaminhados para toda rede ou uma outra VLAN criada pelo administrador da rede na interface de gerenciamento do switch.

A segmentação feita pelos switches para controlar os broadcasts que circulam no domínio, de acordo com Lindeberg Barros (2013, p.222)

> Normalmente o broadcast só é bloqueado pelo roteador, que não transmite mensagens a outras portas (cada porta do roteador é um domínio de broadcast), porém existem switches que possuem uma facilidade de configuração das VLANs, e dividem a rede em diferentes domínios de broadcast. A vantagem desse procedimento é que se diminui o tráfego da rede pela contenção de mensagens broadcast antes transmitidas a todos os segmentos da rede locais (LAN), agora transmitidas apenas a uma parte ou grupo de estações ou dispositivos que compõem a VLAN

Figura 3. Dispositivos espalhados pela rede conectados a um switch agrupados em VLAN.



Fonte: http://www.blogporta80.com.br/2016/09/02/artigos-o-que-sao-vlan-e-vlan-trunk

A organização da rede mostrado na Fig.3 ilustra os dispositivos conectados à uma rede por um switch inteligente que tem a capacidade de segmentar a rede em níveis lógicos. Cada VLAN é um domínio de broadcast, mensagens de broadcast de uma VLAN não passam para outra VLAN. Assim é permitido configuração de grupos de estações de determinados setores, ou de acordo com o perfil de usuários em cada VLAN. O grupo de funcionários da VLAN do administrativo de uma universidade não se comunica com os dispositivos de alunos e professores conectados na rede, como

também a VLAN de alunos não se comunica com as VLANS de funcionários e professores.

A necessidade da implementação de VLAN em uma rede de uma universidade se dá pelo conjunto de altos e diversos volumes de informações transitando dentro da rede. Setores administrativos não necessariamente precisam estar em uma mesma rede de alunos e professores, onde o objetivo de utilização da rede é totalmente diferente. Da mesma maneira setores dentro do administrativo não precisam se comunicarem a rede dos outros setores com objetivos opostos, o financeiro não precisa se comunicar com a reitoria, da mesma forma que os recursos humanos não necessitam comunicar com a rede da biblioteca.

A definição para utilização da VLAN para segmentar a rede segundo Leonardo Haffermann (2009, p.4)

> Em determinada organização um setor pode pertencer a uma VLAN diferente do restante da organização a fim de proteger informações sigilosas. Em outra situação um setor que gera muito tráfego de rede pode fazer parte de outra VLAN a fim de melhorar o desempenho da rede de modo geral.
> A segurança é uma das características que mais é levada em conta quando se implementa VLAN, permitindo que dispositivos localizados em diferentes segmentos físicos e em uma mesma VLAN possam se comunicar sem que dispositivos fisicamente vizinhos e tenham acesso. Os pacotes transmitidos são normalmente entregues somente ao endereço de destino dificultando a interceptação dos mesmos. Quando se trata de tráfego entre VLANs, os pacotes são submetidos a um roteador, que possui diversas funcionalidades de filtragem, segurança e prioridade, antes de chegarem a seu suposto destino, criando assim domínios de segurança para acesso a recursos da rede.

IV. CARACTERISTICAS E TIPO DE VLANS

As VLANs podem ser configuradas de diversas formas, entre elas a configuração baseado no nível de protocolo, normalmente por IP, mas também configurado baseando no endereço MAC do dispositivo, ou até configurado por uma porta específica do switch.

A classificação dessas VLANs definida em estática ou dinâmica, independentes da topologia física da rede. As VLANs estáticas têm como característica à sua configuração por portas podendo alocar uma porta permanente a uma ou mais VLANs. Uma sub-rede é então feita por uma lista dos números da porta. As VLANS dinâmicas, as sub-redes são feitas dos endereços MAC ou endereços IP que são mantidos num banco de dados. As portas dos switches são automaticamente configuradas com base nesse banco de dados. (BAUMIER, 2018)

Um switch com suporte para criação de VLANs suporta dois tipos de portas.

A. Portas de Acesso

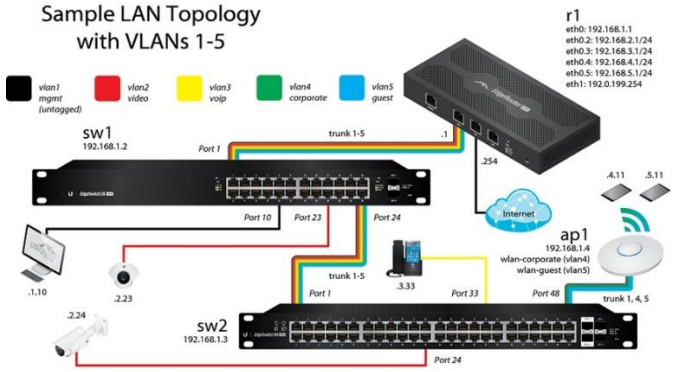
Definida por ligações de acesso permite associação de uma porta do switch a uma VLAN.

B. Portas Trunk

Definida por ligações partilhadas, permite associação de uma porta do switch a várias VLANs, podem ser usadas para interligação de switches e roteadores permitindo a passagem de trafego de várias VLANS naquela porta para escalabilidade da rede. Conforme (Barros, 2013) “em uma rede comutada um tronco é um link ponto-a-ponto que suporta várias VLANs.

É suportado apenas em switches com protocolos 802.1Q que é padrão do Instituto de Engenheiros Eletricistas e Eletrônicos (IEEE).

Figura 4. Topologia de uma rede utilizando VLAN trunk com protocolo IEEE 802.1Q

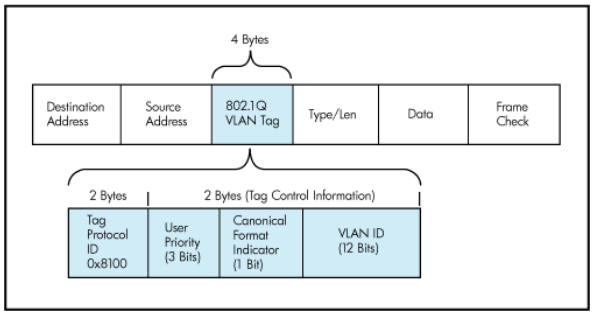


Fonte: goo.gl/qgwnrA

Com a utilização do protocolo 802.1Q através da VLAN trunk é possível utilizar apenas uma porta de cada switch para realizar conexões de VLANs entre os switches, assim fazendo com que as VLANs se comuniquem dentro da rede em switches alocados em espaços físicos diferentes.

A comunicação das VLANs entre os switches com protocolo 802.1Q independente do fabricante por ser utilizado em qualquer porta do switch que suporte o protocolo, mas geralmente são utilizados nas portas com maior capacidade de velocidade (Gigabit) onde é feita pelo método de marcação de cada frame ou quadro. A marcação é denominada VLAN tag adicionando ao quadro ethernet 4 bytes no frame original, composta dentro de seu quadro as VLANs ID (VID) que possuem 12 bits cada. Possibilitando 4096 VLANS.

Figura 5. Composição interna da VLAN tag



Fonte: https://osqa-ask.wireshark.org

V. DISCUSSÃO

O conceito e a utilização das VLANs em meios corporativos e universidades estão relacionados diretamente a uma redução de custos para o tratamento de mudanças constantes nos setores e usuários da rede. A VLAN irá resultar em uma maior capacidade de gerenciar redes dinâmicas e realizar economias substanciais. Normalmente, quando um usuário se move para uma sub-rede diferente, endereços IP devem ser atualizados manualmente na estação de trabalho. Esse processo de atualização pode consumir uma quantidade maior de tempo que poderia ser definido automaticamente pelo administrador que gerencia o switch da rede. A VLAN pode eliminar esse incômodo, ela não está vinculada a localização de uma estação de trabalho na rede, permitindo que as estações de trabalho mudem de local mantendo seus endereços IP originais e a associação de sub-rede.

Com a utilização das tecnologias incorporadas as redes como a da VLAN, há uma absorção de gastos relacionados ao gerenciamento de redes, podendo ser mais escalável às alterações de setores e seus usuários. No entanto, não é qualquer implementação que vai reduzir estes custos provocados pelas constantes mudanças no ambiente de uma universidade, cuidados devem ser tomados, não se deve apenas aplicar as VLANs na rede, mas também realizar uma análise minuciosa para certificar que a implementação não vai gerar uma maior demanda de administração de rede do que a própria rede necessita no seu atual cenário.

Uma configuração mais complexa e com maior ambição pela tecnologia apresentada nas VLANs é sua configuração definida em meio ao um grupo de trabalho virtual, definindo a VLAN de um setor específico para um grupo de usuários onde os acessos podem ser feitos em todo o ambiente do campus de uma universidade. Membros de um mesmo setor podem ter os mesmos acessos relacionados dentro da VLAN com os dados trafegados dentro do mesmo domínio sem a preocupação que sua rede sofra uma instabilidade de velocidade e segurança. Em tese o usuário se move pelas estações de trabalho dentro do ambiente de trabalho, mas seus acessos à rede ficam agrupados de maneira lógica.

Conforme tratado sobre a utilização da VLAN em relação ao custo operacional, a utilização de switches gerenciados de camada 3 contribuem para diminuir o custo de equipamentos que no passado eram totalmente necessários a rede, mas com a evolução da tecnologia dos switches, equipamento como roteadores deixaram de ser obrigatórios para o funcionamento da rede. Os switches de camada 3 tem em seu interior um roteamento realizado pelo conjunto aplicado de hardware e software, não sendo necessário que o tráfego de dados passe por um roteador físico da rede para alcançar seu endereço de destino.

A segurança é um dos fatores mais importantes na implementação das VLANs em uma infraestrutura de rede para uma universidade, pois garantem a integridade dos dados circulados, garantindo que os acessos de alunos, professores e ambiente administrativo não se cruzem ou se comuniquem. Os switches estão capacitados para criar firewalls podendo satisfazer os requisitos de segurança mais rigorosas e, assim, substituir grande parte da funcionalidade de roteadores nesta área. Podemos afirmar que o conjunto destas funcionalidades limita um único tráfego de broadcast em um segmento da VLAN de maneira que não ultrapasse para outra VLAN, e assim do mesmo modo para as diversas VLANs criadas dentro de uma rede física. Apesarem de as conexões estarem no mesmo switch físico a comunicação entre elas não é feita.

Assim uma das razões de se dividir a rede em VLANs é diminuir a quantidade de broadcasts que cada equipamento recebe. Um computador em uma rede de 1000 computadores vai receber o dobro de broadcast do que se ele estivesse em uma rede de 500 computadores. Assim se for dividido uma rede de 1000 equipamentos em duas VLANs de 500 máquinas, eu reduzo automaticamente para a metade a quantidade de pacotes de broadcasts (Lopes, 2012).

A limitação de dispositivos e estações de trabalho podem ser definidas por blocos do campus de uma universidade, isolando totalmente os blocos um dos outros mantendo somente a comunicação unitária de cada bloco com o servidor, então se em um bloco temos 20 salas de laboratórios de informática, podemos isolar essas 20 salas limitadas a aquele bloco sem que comunique com os demais. E ainda mais, podemos isolar unitariamente essas 20 salas dentro do bloco, onde pode-se isolar sala por sala, garantindo que a sala número 1 não vai se comunicar com as outras 19 salas dentro do bloco, e assim consequentemente para cada sala. Este gerenciamento utilizando as VLANs contribuirá para um melhor desempenho, controle no tráfego de dados e suas permissões como também a propagação dos broadcasts dentro do bloco. Interferindo diretamente na segurança dos usuários de cada sala, com este isolamento será garantido que se uma estação de trabalho for infectada por um vírus mesmo com todos os métodos e aplicações de última geração disponíveis atualmente, a propagação da infecção não afetará outras estações ou dispositivos conectados à rede do bloco.

As empresas também podem separar os servidores em uma VLAN separada, no entanto nesse caso é importante tem um roteador de alta performance para conectar a VLAN dos usuários até a VLAN dos servidores. Se o roteador não tiver uma excelente performance e uma baixa latência ele irá causar atrasos graves na rede que irão afetar os usuários. Nesses casos os switches L3 são essenciais (um switch L3 ou de camada 3 é um switch normal que tem dentro um roteador de alta performance) (Lopes, 2012).

Todavia, as VLANs são uma das melhores técnicas de segmentação para se obter um melhor gerenciamento da infraestrutura de rede de uma universidade, desde que seja adquirido equipamentos com funcionalidades e protocolos

corretos para a aplicação das configurações. Estes equipamentos também possuem funções de monitoramento de tráfego e comporta a ativação/desativação de portas permitindo que o administrador bloqueie portas que apresentem qualquer problema ou impedir que pessoas, inadvertidamente, conectem equipamentos em determinada rede virtual

VI. CONCLUSÃO

Segmentação da rede utilizando VLANs é a maneira mais eficaz para um melhor controle a nível de gerenciamento da infraestrutura de rede de uma universidade, contribuindo para escalabilidade, confiabilidade e disponibilidade da rede, tornado a rede sólida. A combinação dos equipamentos administradores de redes como os switches de camada 3 que são essenciais para o roteamento estático e qualidade de serviços, também como recursos abrangentes de economia de energia e por fim, fornecimento de energia para os diversos dispositivos conectados as suas portas (PoE).

Independência da topologia física torna a utilização da VLAN a melhor opção para o custo benefício da rede, criando novas VLANs sem a necessidade do remanejamento de equipamentos dentro da rede, aplicando regras para grupos de trabalho de trabalho, usuários, setores, blocos e salas dentro de um campus de uma universidade.

Segurança é a principal característica na aplicação das VLANs dentro de uma infraestrutura de rede, não permitindo que pacotes não rotulados cheguem à destinos incertos, isolando possíveis falhas dentro do segmento juntamente com a propagação de broadcasts e acessos indevidos dentro do servidor. Interfere diretamente no combate de crimes cibernéticos, isolando possíveis falhas e acessos dentro do segmento lógico, evitando o sequestro de dados de usuários, sistemas e servidores.

AGRADECIMENTOS

O autor agradece o apoio do professor da disciplina de TCC juntamente aos gestores de cursos e a instituição de ensino Universidade de Uberaba.

REFERÊNCIAS

TANENBAUM, Andrew S. Redes de Computadores. São Paulo: Pearson, 2011. 563 p.

MADEIRA, Frederico. VLAN. 2006. Disponível em: <http://www.madeira.eng.br/wiki/index.php?page=VLAN>. Acesso em: 30 set. 2018.

PINTO, Pedro. Redes – Sabe o que é uma VLAN?. 2010. Disponível em: <https://pplware.sapo.pt/tutoriais/networking/redes-sabe-o-que-uma-vlan/>. Acesso em: 4 set. 2018.

CARVALHO, José Eduardo Maluf de. Introdução a Redes de Micros. São Paulo: Makron Books, 1998.

ALBURQUERQUE, Fernando. TCP/IP – Internet: Protocolos e Tecnologia. Rio de Janeiro: Axcel Books, 2001.

MACÊDO, Diego. VLAN – Virtual Local Area Network. Disponível em: <http://Macêdo>. Acesso em: 16 ago. 2018.

PINTO, Pedro. Redes: Saiba o que é uma VLAN e aprenda a configurar. Disponível em: <https://pplware.sapo.pt/tutoriais/networking/redes-saiba-o-que-e-uma-vlan-e-aprenda-a-configurar/>. Acesso em: 05 set. 2018.

MORAES, Igor Monteiro. VLANs - Redes Locais Virtuais. Disponível em: <https://www.gta.ufrj.br/grad/02_2/vlans/index1.html>. Acesso em: 18 out. 2018.

HAFFERMANN, Leonardo. Segmentação de Redes com VLAN. Disponível em: <https://www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS08A/Leonardo%20Haffermann%20-%20Artigo.pdf>. Acesso em: 12 set. 2018.

NASCIMENTO, Marcelo Brenzink do. Entenda os Diferentes Tipos de Switch Ethernet. Disponível em: <http://www.dltec.com.br/blog/cisco/entenda-os-diferentes-tipos-de-switch-ethernet/>. Acesso em: 21 out. 2018.

VARADARAJAN, Suba. Virtual Local Area Networks. Disponível em: <https://www.cse.wustl.edu/~jain/cis788-97/ftp/virtual_lans/index.html>. Acesso em: 16 ago. 2018.

Switches. Disponível em: <https://www.baumier.com.br/index.php/cesta/switches>. Acesso em: 02 nov. 2018.

Configuring VLAN Trunking. Disponível em: <http://help.sonicwall.com/help/sw/eng/7631/7/2/0/content/Policies_Switching_VLANTrunking_Snwls.htm>. Acesso em: 25 set. 2018.

Switches Cisco. Disponível em: <https://www.cisco.com/c/en/us/products/switches>. Acesso em: 29 out. 2018.

Quais são as funções de um switch Ethernet Layer 2. Disponível em: <http://ptcomputador.com/Networking/ethernet/66133.html>. Acesso em: 10 out. 2018.