TÉCNICAS DE ROTEAMENTO
ENGENHARIA DE TRÁFEGO E QUALIDADE DE SERVIÇO

Autor: Me. Gustavo de Lins e Horta
Revisor: Rafael Rehm

INICIAR

Introdução

A internet é formada por um conjunto de vários equipamentos como roteadores, servidores, computadores, entre outros. O volume de dados trafegado na rede aumenta diariamente a uma velocidade extraordinária. Vídeos, arquivos, mensagens de voz e texto são transmitidos diariamente por todo o planeta. O controle e o gerenciamento da qualidade são fundamentais para o funcionamento da internet, e por meio da engenharia de tráfego e de protocolos de sinalização e controle, a qualidade de serviço (QoS) na internet é implementada pelos provedores de internet. A segurança também é aspecto fundamental quando se fala em transmissão de dados confidenciais por meio da internet, sendo que o uso da VPN (*Virtual Private Network*) permite uma maior segurança de ponta a ponta na comunicação de dados pela internet. Já os protocolos PPPoE e PPPoA são utilizados pelas provedoras de internet para conectar seus clientes à rede de internet.

Engenharia de Tráfego

Segundo Tanenbaum e Wetherall (2011), a engenharia de tráfego está preocupada com a otimização do desempenho da rede e da internet. A engenharia de tráfego ainda soluciona o problema de alocar recursos com eficiência na rede, para que as restrições do usuário sejam atendidas e o benefício do operador seja maximizado. Pode ser realizado automaticamente ou através de intervenção manual dos operadores da rede. Foram desenvolvidos vários protocolos, algoritmos e serviços para a engenharia de tráfego.

reflita

Reflita

A internet é repleta de serviços, aplicações, protocolos e padrões diferentes. Você já pensou como esses padrões e protocolos são definidos? Quem define, regulamenta e gerencia esses padrões? Existe um órgão ou empresa responsável? Onde são publicados esses padrões? Quantos padrões existem? Reflita um pouco mais sobre esse assunto.

RSVP

O RSVP (*Resource Reservation Protocol*) é um dos primeiros protocolos significativos a configurar QoS sobre IP de ponta a ponta. O RSVP é um protocolo de sinalização que permite que as estações obtenham qualidades especiais de serviço para seus fluxos de dados de aplicativos. O RSVP reserva largura de banda para o aplicativo de rede e trabalha em conjunto com protocolos de roteamento e instala o equivalente a listas de acesso dinâmico ao longo das rotas que os protocolos de roteamento calculam. O RSVP opera na camada de transporte do modelo OSI (CISCO, 2003).

Conforme Tanenbaum e Wetherall (2011), o RSVP pode ser entendido como um conjunto de regras de comunicação que permite que canais ou caminhos na Internet sejam reservados para a transmissão multicast (uma fonte para muitos receptores) de vídeo e outras mensagens de alta largura de banda. O RSVP faz parte do modelo *Internet Integrated Service* (IIS), que garante o melhor

esforço possível, o serviço em tempo real e o compartilhamento de links controlado.

Segundo Cisco (2002), a filosofia básica de roteamento na Internet é o "melhor esforço", que atende a maioria dos usuários o suficiente, mas não é adequada para a transmissão contínua de fluxo necessária para programas de vídeo e áudio na Internet. Com o RSVP, as pessoas que desejam receber um "programa" específico da Internet (filme, programa de TV) podem reservar largura de banda pela Internet antes do programa e podem recebê-lo com uma taxa de dados mais alta e fluxo de dados mais confiável do que o habitual. Quando o programa for iniciado, ele será multicast para usuários específicos que tenham reservado prioridade de roteamento com antecedência. O RSVP também suporta transmissões unicast (uma fonte para um destino) e multifonte para um destino.

Funcionamento do RSVP

Conforme Cisco (2003), vamos supor que um programa de vídeo específico seja multicast em um determinado horário na segunda-feira à noite. Esperando recebê-lo, você envia uma solicitação de RSVP antes da transmissão (você precisará de um programa cliente especial, ou talvez o seu navegador inclua um) para alocar largura de banda e prioridade suficientes de agendamento de pacotes para o programa. Essa solicitação irá para o *gateway* da Internet mais próximo com um servidor RSVP. Ele determinará se você é elegível para ter essa reserva configurada e, em caso afirmativo, se a largura de banda suficiente lhe será reservada sem afetar as reservas anteriores.

Supondo que você possa fazer a reserva e ela seja inserida, o *gateway* encaminha a reserva para o próximo *gateway* em direção ao destino (ou origem do multicast). Dessa maneira, sua reserva é garantida até o destino.

Ainda segundo Cisco (2003), quando o multicast começa, os pacotes da fonte aceleram pela Internet em alta prioridade. À medida que os pacotes chegam a um *host de gateway* , são classificados e programados usando um conjunto de filas e, em alguns casos, temporizadores. Um pacote RSVP é muito flexível; pode variar em tamanho e no número de tipos e objetos de dados. Nos casos

em que os pacotes precisam viajar através de gateways que não suportam RSVP, eles podem ser "encapsulados" como pacotes comuns. O RSVP funciona com o IPv4 e o IPv6.

CSPF

Segundo Cisco (2003), o CSPF (*Constrained Shortest Path First*) é um algoritmo de roteamento de caminho mais curto que leva em consideração diversas restrições ao seu cálculo de roteamento. O uso do CSPF significa que um administrador de rede pode garantir que o algoritmo de roteamento SPF, por exemplo, considere apenas rotas capazes de suportar taxa de transferência de tráfego de 100 Mbps ou rotas com um atraso de ponta a ponta específico. Protocolos populares de roteamento de caminho mais curto, como OSPF (*Open Shortest Path First*) e IS-IS (*Sistema Intermediário para Sistema Intermediário*), foram ampliados para oferecer suporte ao roteamento baseado em restrições.

De acordo com Tanenbaum e Wetherall (2011) o CSPF precisa de três tipos de entradas:

- Informações sobre o estado do enlace da topologia;
- Atributos associados ao estado dos recursos de rede;
- Atributos administrativos necessários para oferecer suporte ao tráfego que atravessa o LSP (*Label Switched Path*) (por exemplo, requisitos de largura de banda, contagem máxima de saltos, requisitos de política administrativa).

Todos os nós candidatos e enlaces para um novo LSP são considerados. O CSPF rejeita todos os componentes do caminho que não atendem aos requisitos de rota (restrições). A saída do cálculo do CSPF é uma rota explícita que consiste em uma sequência de endereços LSR que fornece o caminho mais curto que atende às restrições.

Saiba mais

As RFCs (*Request for Comments*) ou pedidos de comentários são documentos técnicos criados pela IETF (*Internet Engineering Task Force*) que é a instituição responsável por especificar os padrões que serão utilizados na internet. O primeiro RFC foi publicado em 1972 e tratava do protocolo de controle de rede da ARPAnet. O RFC 2616 por exemplo trata do protocolo HTTP, já o RFC 959 trata do protocolo FTP. Saiba mais a respeito dos RFCs acessando a página da IETF a seguir.

ACESSAR

Controle de Banda

O controle de banda é essencial em uma rede de computadores e na internet. O controle de banda, por exemplo, é utilizado para evitar um congestionamento da rede, seja aumentando os recursos (aumento de enlace, memória e processamento dos roteadores), ou diminuindo a carga na rede (priorizando alguns serviços).

Segundo Tanenbaum e Wetherall (2011), o controle e gerenciamento da rede é importante por vários motivos:

- As redes de computadores estão se tornando fundamentais para as empresas e uma falha na rede significa perdas e custos para essas empresas;

- As redes estão cada vez maiores e mais complexas;
- As redes estão cada vez mais heterogêneas (vários serviços, equipamentos e fabricantes diferentes);
- As tecnologias das redes são cada vez mais complexas.

A Figura 4.1 exemplifica uma rede de computadores com os vários componentes que compõem essa rede.

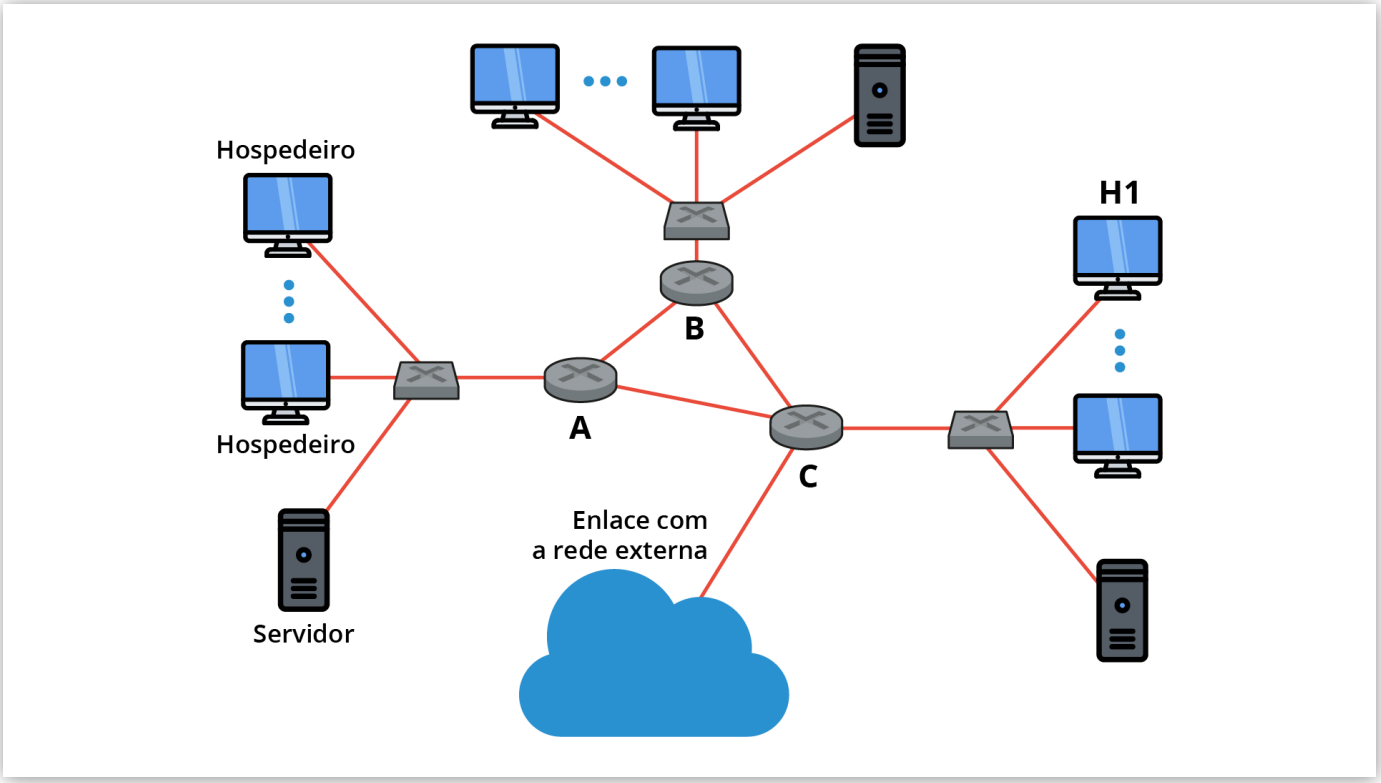


Figura 4.1 - Exemplo de uma rede de computadores
Fonte: Kurose (2014, p. 557).

SegundoCisco (2003), a falta de um controle de banda pode ocasionar um congestionamentoda rede, já que cada vez mais os serviços e aplicações consomem mais banda.Aplicações de realidade virtual, por exemplo, consomem largura de banda naordem de 100 Mbps.

Vamos Praticar

A engenharia de tráfego se preocupa com o desempenho da rede e da internet. Vários protocolos e serviços são utilizados para implementar a qualidade de serviço (QoS) nas redes de computadores e na internet. A engenharia de tráfego possui uma série de ferramentas e protocolos para melhorar o desempenho da rede. Qual protocolo permite que os hosts solicitem parâmetros de qualidade de serviço dos recursos da rede?

- **a)** MPLS.
- **b)** CAR.
- **c)** RTP.
- **d)** RSVP.
- **e)** OSPF.

Qualidade de Serviço

Segundo Tanenbaum e Wetherall (2011), a provisão da Qualidade de Serviço (QoS) na Internet atualmente depende de dois mecanismos: abordagens de escala de tempo de dados existentes para alocação de recursos que normalmente são restritas a mecanismos de controle de congestionamento compatíveis com TCP; e negociação de SLA (*Service Level Agreement*) entre os operadores de rede, que normalmente ocorre muito lentamente.

É necessária uma abordagem mais flexível para resolver esses dois problemas. Em primeiro lugar, a engenharia de tráfego deve ser considerada em várias escalas de tempo: dados, controle e gerenciamento. Em segundo lugar, é necessário um mecanismo para permitir a especificação e comparação de muitos tipos de tráfego diferentes. Por fim, esse mecanismo deve oferecer aos usuários incentivos para que se comportem 'de verdade' ao especificar suas restrições à rede para ajudar a reduzir os custos de gerenciamento e policiamento.

DIFFSERV

Segundo Cisco (2003), o DIFFSERV (*Differentiated Services*) ou serviços diferenciados é uma abordagem alternativa para fornecer QoS na Internet. Em vez de basear-se na ideia de reserva de recursos por período, ela assume que muita diferenciação de serviço maior será satisfatória, dada a natureza abundante da largura de banda no futuro. Usando DSCP (*Differentiated Services Code Point*) como identificação, são definidos PHBs (*Per Hop Behaviours*) ou comportamentos por salto, que permitem que os roteadores ofereçam diferentes níveis de serviço aos pacotes que ostentam DSCPs diferentes.

Os PHBs padronizados são mapeados nos DSCPs pela IETF (*Internet Engineering Task Force*) e atualmente consistem no melhor esforço, encaminhamento acelerado, baixa latência, instabilidade baixa, serviço de baixa perda e encaminhamento garantido, um serviço solicitado de baixa perda. PHBs experimentais também podem existir, mas não é garantido que sejam suportados. Operadores diferentes podem implementar os PHBs de maneira diferente, a única condição é que os PHBs padronizados sejam representados por seus DSCPs obrigatórios. O tráfego entre operadores será gerenciado por meio de SLAs, com promoção e rebaixamento de tráfego entre PHBs permitidos para atender aos SLAs especificados.

praticar

Vamos Praticar

O Diffserv ou serviços diferenciados é uma maneira de fornecer QoS (Qualidade de Serviço) para o tráfego de dados na internet. O que torna o modelo DiffServ mais escalável que o modelo IntServ? Avalie as afirmações a seguir.

i. O DiffServ utiliza QoS por agregado em vez de QoS por fluxo.

ii. O DiffServ utiliza sinalização de salto por salto, que permite que o DiffServ seja escalado para um número maior de fluxos de aplicativos.
iii. O DiffServ é capaz de implementar o controle de admissão localmente nos roteadores ou ser transferido para um servidor de políticas central usando o protocolo COPS.
iv. Os roteadores DiffServ não são obrigados a rastrear as informações de estado de cada fluxo individual.

Está correto o que se afirma em:

- **a)** I e IV, apenas.
- **b)** I e II, apenas.
- **c)** II e III, apenas.
- **d)** II e IV, apenas.
- **e)** III e IV, apenas.

VPN PPP

Segundo Paquet (2003), as VPNs (*Virtual Private Network*) permitem que usuário remotos se conectem com a infraestrutura interna ou extranets corporativas de qualquer lugar e em qualquer momento, melhorando a produtividade e reduzindo os custos. A Figura 4.2 apresenta um exemplo de uma VPN.

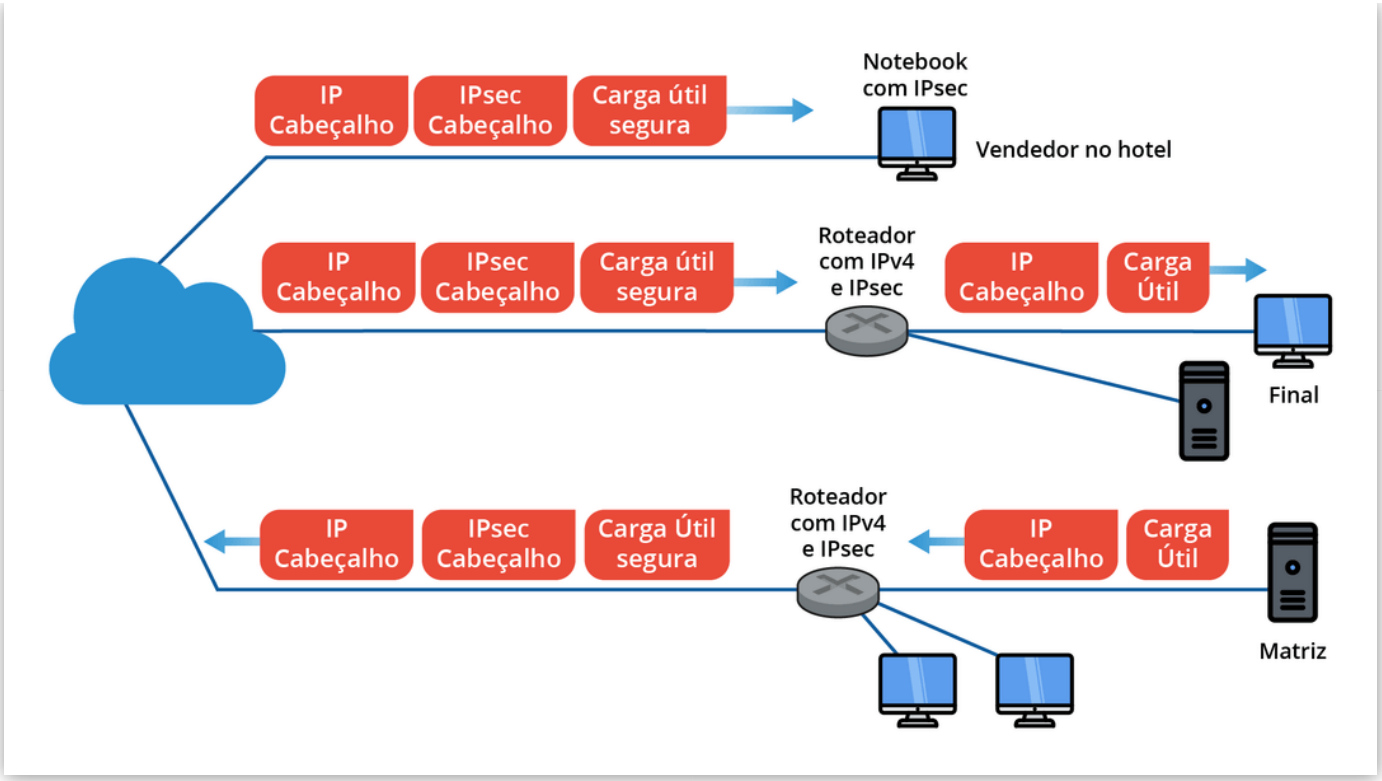


Figura 4.2 - VPN

Fonte: Kurose (2014, p. 529).

Ainda segundo Paquet (2003), uma VPN simula uma rede privada em uma estrutura compartilhada como a internet. Um elemento principal da VPN é o L2TP (*Layer 2 Tunneling Protocol*), uma extensão do protocolo PPP (*Point-to-Point*).

PPTP

O protocolo PPTP (*Point-to-Point Tunneling Protocol*) é um conjunto de regras de comunicação que governam a implementação segura de redes privadas virtuais (VPN), que permitem às organizações um método de estender suas próprias redes privadas pela Internet pública via "túneis".

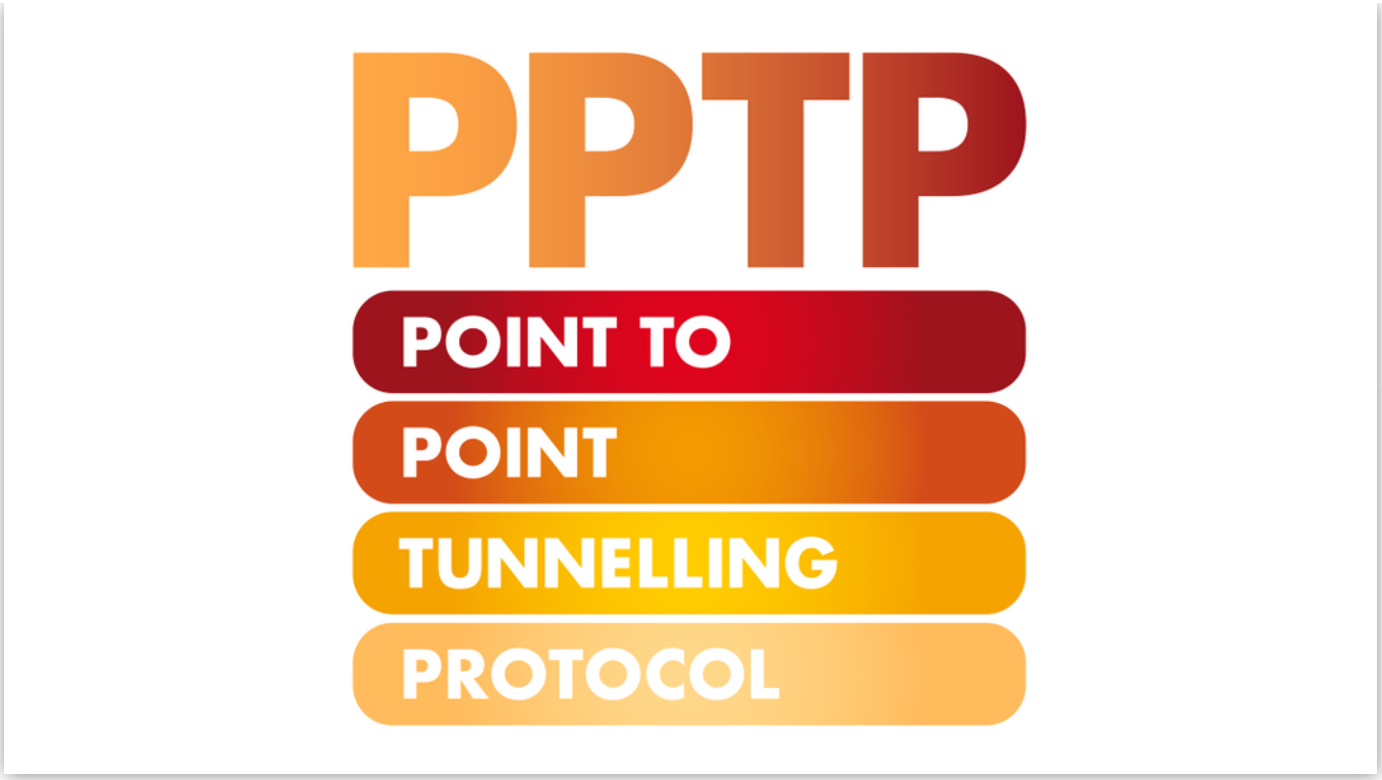


Figura 4.3 - PPTP - Protocolo de Tunelamento Ponto a Ponto
Fonte: dizanna / 123RF.

Ao usar o PPTP, uma grande organização com escritórios distribuídos pode criar uma grande rede local (LAN) - essencialmente uma VPN - usando a infraestrutura de uma ampla área de rede (WAN), como a rede de um provedor de serviços de Internet público (ISP) ou telecom. Isso é mais econômico do que estabelecer uma infraestrutura de rede nessas distâncias.

Segundo Tanenbaum e Wetherall (2011), o PPTP permite a criação de uma rota segura de transferência de dados de um cliente remoto para um servidor em uma rede corporativa privada, através da criação de uma VPN em redes baseadas em TCP/IP, como a Internet. Ele permite que usuários remotos acessem redes corporativas com segurança pela Internet, como se o cliente estivesse fisicamente presente na rede corporativa.

O PPTP é uma extensão do protocolo ponto a ponto já usado na Internet, e a Microsoft e seus parceiros o propuseram como padrão. Juntamente com a proposta da Cisco do Protocolo de encapsulamento da camada 2, essas propostas podem se tornar a base para o próximo padrão da IETF (*Internet Engineering Task Force*).

O PPTP oferece as seguintes vantagens:

- Custos de transmissão mais baixos: nenhum serviço adicional usado, além da Internet.
- Menores custos de hardware: permite que as placas e modems ISDN sejam separados dos servidores RAS, o que resulta em menos dispositivos para compra e gerenciamento.
- Baixa sobrecarga administrativa: os administradores gerenciam apenas o servidor de acesso remoto (RAS) e as contas de usuário, em vez de gerenciar diferentes configurações de hardware.
- Segurança aprimorada: a conexão PPTP é criptografada e protegida pela Internet e funciona com outros protocolos de rede, como IP, *Internetwork Packet Exchange* (IPX) e NetBEOS *Extended User Interface* (NetBEUI).

L2TP

De acordo com Tanenbaum e Wetherall (2011), o L2TP (*Layer 2 Tunneling Protocol*) é uma extensão do protocolo de encapsulamento ponto a ponto (PPTP). É a fusão de dois protocolos, um da Microsoft (PPTP) e outro da Cisco. O L2TP economiza o custo de discagem e as despesas gerais para qualquer usuário disposto a se conectar remotamente com o escritório do site. O L2TP é conhecido como Protocolo de Discagem Virtual devido ao serviço da extensão de Protocolo Ponto a Ponto (PPP) na Internet.

Figura 4.4 - L2TP
Fonte: Timur Arbaev / 123RF.

O protocolo L2TP é um protocolo de rede de computadores usado por provedores de serviços da Internet (ISPs) para permitir operações de rede virtual privada (VPN). O L2TP é semelhante ao *Data Link Layer Protocol* no modelo de referência OSI, mas na verdade é um protocolo de camada de sessão.

Conforme Paquet (2003), uma porta UDP (*User Datagram Protocol*) é usada para comunicação L2TP. Como ele não fornece segurança para dados, como criptografia e confidencialidade, um protocolo de criptografia como o IPsec (*Internet Protocol security*) é frequentemente usado com o L2TP.

As vantagens do L2TP incluem:

- Alta segurança de dados é fornecida para aplicativos críticos;
- A criptografia de alto nível é usada para que informações críticas estejam sempre seguras e permaneçam pessoais;
- Ele fornece conectividade excelente e eficiente;
- É econômico e não possui custos indiretos após a implementação;
- É confiável, escalável, rápido e flexível;

- É o melhor padrão do setor para o setor corporativo;
- Possui a melhor política de autorização para usuários com autenticação VPN.

praticar

Vamos Praticar

Uma VPN (*Virtual Private Network*) protege a rede privada, usando criptografia e outros mecanismos de segurança para garantir que apenas usuários autorizados possam acessar a rede e que os dados não possam ser interceptados. Esse tipo de rede é projetado para fornecer um túnel seguro e criptografado no qual se transmitam os dados entre o usuário remoto e a rede da empresa. Qual dos seguintes protocolos fornece a criptografia real usada na VPN?

- **a)** HTTPS.
- **b)** SSH.
- **c)** PPP
- **d)** TLS.
- **e)** PPTP.

PPPoE e PPPoA

Conforme Paquet (2003), o PPPoE (*Point-to-Point Protocol over Ethernet*) e PPPoA (*Point-to-Point Protocol over ATM*) são dois protocolos alternativos para conectar ao provedor de internet (ISP). Alguns ISPs suportam apenas um ou outro, mas muitos suportam ambos. O PPPoA é um pouco mais rápido que o PPPoE, pois o PPPoA possui 8 bytes a menos de sobrecarga em cada pacote de 1500 bytes.

O uso do PPPoA evita o problema da *Maximum Transfer Unit* (MTU). O efeito das MTUs incompatíveis é que as páginas aleatórias da Web podem não ser totalmente carregadas, as transferências de arquivos e os downloads de e-mail também parecem congelar. O MTU para PPPoA é de 1500 bytes, enquanto o MTU para PPPoE é de 1492 bytes devido à sobrecarga de 8 bytes incorrida por esse protocolo.

Segundo Tanenbaum e Wetherall (2011), o PPPoE é um tipo de protocolo de rede que encapsula quadros PPP dentro dos quadros Ethernet. Basicamente, o PPPoE é configurado como uma conexão ponto a ponto entre duas portas Ethernet. Esse protocolo é normalmente usado nos pacotes mais baixos do ISP, já que o PPPoE é frequentemente usado para funcionar com uma taxa de

transferência de largura de banda mais baixa.

Ainda segundo Tanenbaum e Wetherall (2011), o protocolo PPPoA também é um protocolo de rede, mas dessa vez é para encapsular quadros dentro do AAL5 ou da camada de adaptação ATM 5. ATM significa Modo de transferência assíncrona, um tipo de comutação usando a multiplexação por divisão de tempo de forma assíncrona.

O Quadro 4.1 apresenta as características do PPPoE e do PPPoA.

Características	**PPPoE**	**PPPoA**
Encapsulamento	Encapsula quadros PPP dentro dos quadros Ethernet.	Encapsula quadros dentro de AAAL5.
Pacotes	É frequentemente usado em pacotes mais baixos.	É frequentemente usado em pacotes corporativos.
Utilização	É mais utilizado que o PPPoA.	É menos utilizado que o PPPoE.
Velocidade	Mais lento que o PPPoA.	Mais rápido que o PPPoE.

Quadro 4.1 - PPPoE e PPPoA
Fonte: Elaborado pelo autor.

praticar

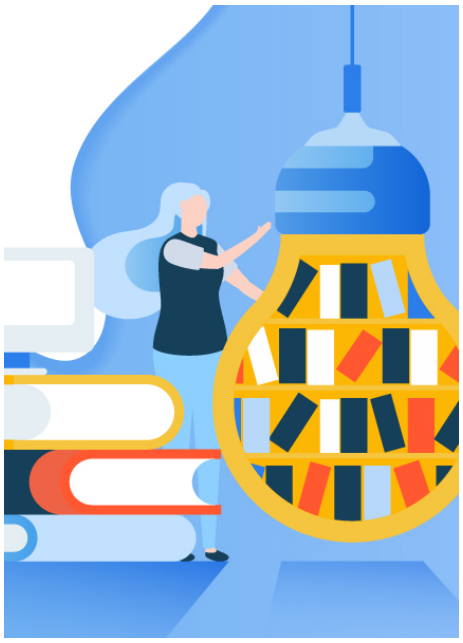
Vamos Praticar

O PPPoE (*Point-to-Point Protocol over Ethernet*) é projetado para gerenciar como os dados são transmitidos por redes Ethernet (redes a cabo) e permite que uma conexão de servidor único seja dividida entre vários clientes, usando Ethernet. Durante qual fase do PPPoE é realizada a autenticação PPP?

- **a)** Fase 1.
- **b)** A fase de descoberta ativa.
- **c)** A fase de PPP.
- **d)** Fase 2.
- **e)** A fase de autenticação.

indicações

Material Complementar



LIVRO

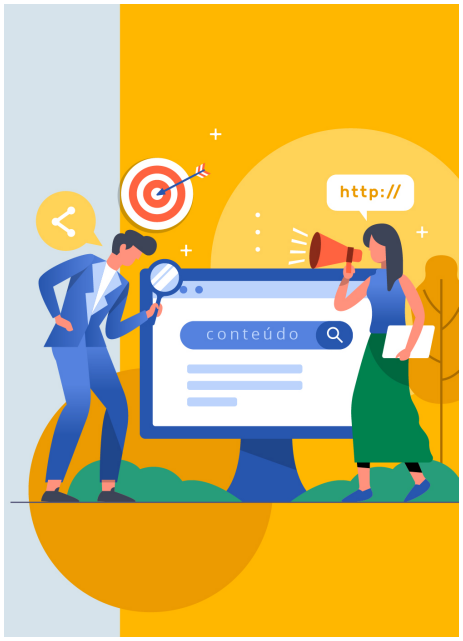
Qualidade de Serviço em Redes de Computadores

Editora : LTC

Autor : Edison de Queiroz Albuquerque

ISBN : 9788535272321

Comentário : Esse livro aborda conceito de QoS para os novos serviços e aplicações na internet, como a voz sobre IP (VoIP) e vídeos interativos. Várias técnicas são apresentadas para implementar o QoS nas redes de computadores. Um livro atual e de fácil leitura apresenta conceitos importantes para quem deseja atuar na área.



WEB

Cisco Packet Tracer - Configuração Básica de Roteadores

Ano : 2015

Comentário : Nessa primeira aula você verá como realizar a configuração básica de um roteador no Cisco Packet Tracer.

Para conhecer mais sobre o filme, acesse o trailer a seguir.

ASSISTA

conclusão

Conclusão

A qualidade de serviço (QoS) é fundamental para que a internet e as redes de computadores apresentem um bom desempenho e sejam capazes de oferecer os mais diversos serviços. Os mecanismos de gerenciamento de tráfego são ferramentas importantes para otimizar o desempenho das redes e da internet. Para aumentar a segurança dos dados trafegados pela internet, as VPNs (*Virtual Private Network*) são um recurso cada vez mais utilizado por empresas e usuários para aumentar a segurança da comunicação de dados da origem até o destino. Os provedores de internet, por sua vez, disponibilizam vários protocolos de comunicação para conectar seus clientes à internet, como por exemplo os protocolos PPPoE (*Point-to-Point Protocol over Ethernet*) e PPPoA (*Point-to-Point Protocol over ATM*), muito utilizados pelos provedores de internet para conectar seus clientes à internet.

referências

Referências Bibliográficas

CISCO. **Diagnosticando Redes** : Cisco Internetwork Troubleshooting. São Paulo: Pearson, 2002.

CISCO. **Guia de Certificação do CCIE Roteamento e Comutação Exame** . [S.l]: Cisco Press, 2003.

CISCO Networking Academy. **Cisco Packet Tracer** . [2020]. Disponível em: https://www.netacad.com/pt-br/courses/packet-tracer . Acesso em: 3 dez. 2019.

KUROSE, J. F.; ROSS, K. W. **Redes de Computadores e a Internet** - Uma Abordagem Top-Down. 6. ed. São Paulo: Pearson, 2014.

PAQUET, C. **Construindo Redes Cisco de Acesso Remoto** . São Paulo: Pearson Education do Brasil, 2003.

TANENBAUM, A. S.; WETHERALL, D. **Redes de Computadores** . 5. ed. São Paulo: Pearson, 2011.