Glossário de termos dos switches

Objetivo

Este artigo contém a lista de termos usados na instalação, configuração e solução de problemas dos Switches Cisco Small Business.

Dispositivos aplicáveis

Série Sx200

Sx250 Series

Sx300 Series

Sx350 Series

Série SG300X

Sx500 Series

Sx550X Series

Lista de termos

Solicitante 802.1X — O solicitante é uma das três funções no Padrão IEEE 802.1X. O 802.1X foi desenvolvido para fornecer segurança na Camada 2 do Modelo OSI. Ele é composto pelos seguintes componentes: suplicante, autenticador e servidor de autenticação. Um suplicante é o cliente ou software que se conecta a uma rede para que possa acessar recursos nessa rede. Ele precisa fornecer credenciais ou certificados para obter um endereço IP e fazer parte dessa rede específica. Um Requerente não pode ter acesso aos recursos da rede até que tenha sido autenticado.

ACL — Uma lista de controle de acesso (ACL) é uma lista de filtros de tráfego de rede e ações correlacionadas usadas para melhorar a segurança. Bloqueia ou permite que os usuários acessem recursos específicos. Uma ACL contém os hosts com acesso permitido ou negado ao dispositivo de rede. O roteador ou switch examina cada pacote para determinar se deve encaminhá-lo ou descartá-lo, com base nos critérios especificados nas listas de acesso. Os critérios da lista de acesso podem ser o endereço origem do tráfego, o endereço destino do tráfego, o protocolo da camada superior ou outras informações.

Snooping IGMP — O Internet Group Management Protocol (IGMP) é um protocolo que opera

em switches que permite que eles aprendam dinamicamente sobre o tráfego multicast. O rastreamento de IGMP é um recurso que permite que um switch de rede ouça a conversação de IGMP entre hosts e roteadores. O rastreamento de IGMP executa um mecanismo de filtragem que é habilitado no roteador para encaminhar o tráfego de multicast de um grupo somente para as portas que se uniram ao grupo. Assim, com a espionagem de IGMP, o tráfego na rede é reduzido e o aprimoramento no desempenho dos hosts atrás do roteador é possível. Os multicasts podem ser filtrados a partir dos links que não precisam deles.

IPv4 — O IPv4 é um sistema de endereçamento de 32 bits usado para identificar um dispositivo em uma rede. É o sistema de endereçamento usado na maioria das redes de computadores, incluindo a Internet.

IPv6 — O IPv6 é um sistema de endereçamento de 128 bits usado para identificar um dispositivo em uma rede. É o sucessor do IPv4 e a versão mais recente do sistema de endereçamento usado em redes de computadores. O IPv6 está sendo implantado em todo o mundo. Um endereço IPv6 é representado em oito campos de números hexadecimais, cada campo contendo 16 bits. Um endereço IPv6 é dividido em duas partes, cada parte composta de 64 bits. A primeira parte é o endereço de rede e a segunda é o endereço do host.

Link Flap — Link flap é uma situação em que uma interface física no switch fica continuamente ativa e inativa, três ou mais vezes por segundo durante pelo menos 10 segundos. A causa comum geralmente está relacionada a cabos defeituosos, não suportados ou fora do padrão ou SFP (Small Form-Fator Pluggable), ou relacionados a outros problemas de sincronização de link. A causa da oscilação de link pode ser intermitente ou permanente.

ACL baseada em MAC — A Lista de Controle de Acesso (ACL) baseada no Controle de Acesso ao Meio (MAC - Media Access Control) é uma lista de endereços MAC origem. Se um pacote estiver vindo de um ponto de acesso sem fio para uma porta de rede local (LAN) ou vice-versa, esse dispositivo verificará se o endereço MAC origem do pacote corresponde a qualquer entrada nessa lista e verificará as regras de ACL em relação ao conteúdo do quadro. Em seguida, ele usa os resultados correspondentes para permitir ou negar esse pacote. No entanto, os pacotes de LAN para porta LAN não serão verificados.

Rastreamento de MLD — O multicast é a técnica da camada de rede que transmite pacotes de dados de um host para os hosts selecionados em um grupo. Na camada inferior, o switch envia o tráfego multicast por broadcast em todas as portas, mesmo que apenas um host queira recebê-lo. A espionagem de Multicast Listener Discovery (MLD) é usada para encaminhar o tráfego de multicast IPv6 somente para o(s) host(s) desejado(s). Quando o rastreamento de MLD é habilitado no switch, ele detecta as mensagens de MLD trocadas entre o roteador IPv6 e os hosts multicast conectados à interface. Em seguida, ele mantém uma tabela que restringe o tráfego multicast IPv6 e o encaminha dinamicamente para as portas que desejam recebê-lo.

MSTP — O MSTP (Multiple Spanning Tree Protocol) é um protocolo que cria várias spanning trees (instâncias) para cada LAN Virtual (VLAN) em uma única rede física. Isso permite que cada VLAN tenha uma bridge raiz configurada e uma topologia de encaminhamento. Isso reduz o número de BPDUs (Bridge Protocol Data Units, unidades de dados de protocolo de ligação) na rede e reduz o estresse nas CPUs (Central Processing Units, unidades de processamento central) dos dispositivos de rede.

Espelhamento de porta/VLAN — O espelhamento é um método usado para monitorar o tráfego de rede. Com o espelhamento de porta ou VLAN, cópias de pacotes de entrada e saída nas portas (portas de origem) de um dispositivo de rede são encaminhadas para outra porta (porta de destino) onde os pacotes são estudados. Isso é usado como uma ferramenta de diagnóstico pelo administrador da rede.

Segurança de porta — Configurar a segurança de porta é uma forma de aumentar a segurança da rede. Ele pode ser configurado em uma porta específica ou em um LAG (Link Aggregation Group). Um LAG combina interfaces individuais em um único link lógico, que fornece uma largura de banda agregada de até oito links físicos. Você pode limitar ou permitir o acesso a diferentes usuários em uma determinada porta/LAG. A segurança de porta também pode ser usada com endereços MAC estáticos e aprendidos dinamicamente para limitar o tráfego de entrada de uma porta.

VLAN baseada em protocolo — Os grupos baseados em protocolo podem ser definidos e vinculados a uma porta; portanto, cada pacote originário dos grupos de protocolo é atribuído à VLAN configurada na página. A VLAN baseada em protocolo divide a rede física em grupos de VLAN lógicos para cada protocolo necessário. No pacote de entrada, o quadro é verificado e a participação na VLAN pode ser determinada com base no tipo de protocolo. O mapeamento de grupos baseados em protocolo para VLAN ajuda a mapear um grupo de protocolo para uma única porta.

QoS — A qualidade de serviço (QoS) permite priorizar o tráfego para diferentes aplicativos, usuários ou fluxos de dados. Ele também pode ser usado para garantir o desempenho em um nível especificado, afetando, assim, a qualidade do serviço do cliente. A QoS é geralmente afetada pelos seguintes fatores: instabilidade, latência e perda de pacotes.

Servidor RADIUS — O Remote Authentication Dial-In User Service (RADIUS) é um mecanismo de autenticação para dispositivos se conectarem e usarem um serviço de rede. Ele é usado para fins de autenticação, autorização e contabilidade centralizados. Um servidor RADIUS regula o acesso à rede verificando a identidade dos usuários através das credenciais de login inseridas. Por exemplo, uma rede Wi-Fi pública é instalada em um campus universitário. Somente os alunos que tiverem a senha poderão acessar essas redes. O servidor RADIUS verifica as senhas inseridas pelos usuários e concede ou nega o acesso conforme apropriado.

RSTP — O Rapid Spanning Tree Protocol (RSTP) é um aprimoramento do STP. O RSTP fornece uma convergência de spanning tree mais rápida após uma alteração de topologia. O STP pode levar de 30 a 50 segundos para responder a uma alteração de topologia, enquanto o RSTP responde dentro de três vezes o tempo de Hello configurado. O RSTP é retrocompatível com o STP.

SNMP — O SNMP (Simple Network Management Protocol) é um padrão de rede para armazenar e compartilhar informações sobre dispositivos de rede. O SNMP facilita o gerenciamento, a solução de problemas e a manutenção da rede.

Spanning Tree — O Spanning Tree Protocol (STP) é um protocolo de rede usado em uma rede local (LAN). A finalidade do STP é garantir uma topologia sem loops para uma LAN. O

STP remove loops através de um algoritmo que garante que haja apenas um caminho ativo entre dois dispositivos de rede. O STP garante que o tráfego siga o caminho mais curto possível dentro da rede. O STP também pode reativar automaticamente caminhos redundantes como caminhos de backup se um caminho ativo falhar.

Servidor SSL — O Secure Sockets Layer (SSL) é um protocolo usado principalmente para gerenciamento de segurança na Internet. Ele usa uma camada de programa localizada entre as camadas HTTP e TCP. Para autenticação, o SSL usa certificados assinados digitalmente e associados à chave pública para identificar o proprietário da chave privada. Essa autenticação ajuda durante o tempo de conexão. Através do uso de SSL, os certificados são trocados em blocos durante o processo de autenticação, que estão no formato descrito no padrão ITU-T X.509. Depois, pela autoridade de certificação, que é uma autoridade externa, são emitidos certificados X.509 que são assinados digitalmente.

Agregação de Syslog — Um serviço de Syslog simplesmente aceita mensagens e as armazena em arquivos ou as imprime de acordo com um arquivo de configuração simples. Agregação de syslog significa que várias mensagens de syslog do mesmo tipo não serão exibidas na tela toda vez que uma instância ocorrer. A ativação da agregação de logs permite filtrar as mensagens do sistema que você receberá por um período específico. Ele coleta algumas mensagens de syslog do mesmo tipo para que elas não apareçam quando ocorrerem, mas em vez disso apareçam em um intervalo especificado.

TACACS+ — O Terminal Access Controller Access Control System (TACACS+) é um protocolo proprietário da Cisco que é usado para a implementação de segurança avançada, fornecendo autenticação e autorização através de nome de usuário e senha. Para configurar um servidor TACACS+, o usuário deve ter o privilégio de acesso 15, que fornece ao usuário acesso a todos os recursos de configuração do switch. Alguns switches podem atuar como um cliente TACACS+, onde todos os usuários conectados podem ser autenticados e autorizados na rede através de um servidor TACACS+ configurado corretamente. O TACACS+ suporta apenas IPv4.

Servidor TFTP — Um servidor TFTP (Trivial File Transfer Protocol) é um servidor usado para transferir automaticamente arquivos de configuração e inicialização entre dispositivos em uma LAN. O protocolo é simples, o que permite o uso de pouca memória; no entanto, essa simplicidade também permite que o protocolo seja facilmente comprometido. Por esse motivo, o TFTP raramente é usado com a Internet.

VLAN — Uma rede local virtual (VLAN) é uma rede comutada que é logicamente segmentada por função, área ou aplicativo, independentemente das localizações físicas dos usuários. As VLANs são um grupo de hosts ou portas que podem estar localizados em qualquer lugar de uma rede, mas se comunicam como se estivessem no mesmo segmento físico. As VLANs ajudam a simplificar o gerenciamento de rede, permitindo que você mova um dispositivo para uma nova VLAN sem alterar nenhuma conexão física.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.