Glossário de termo do Switches

Objetivo

Este artigo contém a lista de termo usada na fundação, configurando, e pesquisando defeitos o Switches da empresa de pequeno porte de Cisco.

Dispositivos aplicáveis

Sx200 Series

Sx250 Series

Sx300 Series

Sx350 Series

Série SG300X

Sx500 Series

Série Sx550X

Lista de termo

suplicante do 802.1X — O suplicante é um dos três papéis no padrão de IEEE do 802.1X. O 802.1X foi desenvolvido para fornecer a Segurança na camada 2 do modelo osi. É composto dos seguintes componentes: Suplicante, autenticador, e Authentication Server. Um suplicante é o cliente ou o software que conectam a uma rede de modo que possa alcançar recursos nessa rede. Precisa de fornecer credenciais ou Certificados para obter parte de um endereço IP de Um ou Mais Servidores Cisco ICM NT e para ser essa rede particular. Um suplicante não pode ter o acesso aos recursos de rede até que esteja autenticado.

ACL — Um Access Control List (ACL) é filtros de tráfego de uma lista de rede e ações correlacionadas usados para melhorar a Segurança. Obstrui ou permite que os usuários alcancem recursos específicos. Um ACL contém os anfitriões que são permitidos ou acesso negado ao dispositivo de rede. O roteador ou o interruptor examinam cada pacote para determinar se enviar ou deixar cair o pacote, com base nos critérios especificados dentro das Listas de acesso. Os critérios da lista de acesso podiam ser o endereço de origem do tráfego, o endereço de destino do tráfego, o protocolo de camada superior, ou a outra informação.

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

sobre o Switches que permite que aprenda dinamicamente sobre o tráfego multicast. O IGMP Snooping é uma característica que permita que um switch de rede escute a conversação IGMP entre anfitriões e Roteadores. O IGMP Snooping executa um mecanismo de filtração que seja permitido no roteador de enviar o tráfego multicast de um grupo somente às portas que se junte ao grupo. Assim com IGMP Snooping, o tráfego na rede é reduzido e o realce no desempenho dos anfitriões atrás do roteador é possível. Os Multicast podem ser filtrados dos links que não os precisam.

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 de redes de computador, incluindo o Internet.

IPv6 — O IPv6 é um sistema de endereçamento do 128-bit usado para identificar um dispositivo em uma rede. É o sucessor ao IPv4 e à maioria de versão recente do sistema de endereçamento usado nas redes de computador. O IPv6 está sendo desenrolado atualmente em todo o mundo. Um endereço do IPv6 é representado em oito campos dos números hexadecimais, cada campo que contém 16 bit. Um endereço do IPv6 é dividido em duas porções, cada parte composta de 64 bit. A primeira parte que são o endereço de rede, e a segunda parte o endereço de host.

Flap do link — O flap do link é uma situação em que uma interface física no interruptor vai continuamente para cima e para baixo, três ou mais cronometra um segundo para a duração pelo menos dos segundos 10. A causa comum é relacionada geralmente ao cabo ruim, unsupported, ou não padronizado ou ao Form Fatora pequeno Pluggable (SFP), ou relacionado a outro questões de sincronização do link. A causa para o não sincronismo de link pode ser intermitente ou permanente.

ACL com base em MAC — Media Access Control (MAC) - o Access Control List baseado (ACL) é uma lista de endereços MAC de origem. Se um pacote está vindo de um ponto de acesso Wireless a uma porta de rede de área local (LAN) ou vice versa, este dispositivo verificará se o endereço MAC de origem do pacote combina qualquer entrada nesta lista e verifica as regras ACL contra o índice do quadro. Usa então os resultados combinados ao permit or deny este pacote. Contudo, os pacotes do LAN à porta de LAN não serão verificados.

Espião MLD — O Multicast é a técnica da camada de rede que transmite pacotes de dados de um host aos anfitriões selecionados em um grupo. Na camada mais baixa, o interruptor transmite o tráfego multicast em todas as portas, mesmo se somente um host quer o receber. A espião da descoberta do ouvinte do Multicast (MLD) é usada para enviar o tráfego do Multicast IPv6 somente aos host desejados. Quando a espião MLD é permitida no interruptor, detecta as mensagens MLD trocadas entre o roteador do IPv6 e os anfitriões do Multicast anexados na relação. Então mantém uma tabela que restrinja o tráfego do Multicast IPv6 e encaminhar-la dinamicamente 2 aquelas portas que querem a receber.

MSTP — O protocolo multiple spanning-tree (MSTP) é um protocolo que crie Spanning Tree múltiplas (exemplos) para o Each Virtual LAN (VLAN) em uma única rede física. Isto permite cada VLAN ter uma topologia configurada do bridge-raiz e da transmissão. Isto reduz o número do bridge protocol data units (BPDU) através da rede e reduz o esforço nas unidades de processamento central (CPU) dos dispositivos de rede.

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

Segurança de portas — Configurar a Segurança de portas é uma maneira de aumentar a segurança de rede. Pode ser configurado em um grupo específico da agregação da porta ou do link (RETARDAÇÃO). UMA RETARDAÇÃO combina interfaces individuais em um único enlace lógico, que forneça uma largura de banda agregada de até oito enlaces físicos. Você pode limitar ou permitir o acesso aos usuários diferentes em um port/LAG dado. A Segurança de portas pode igualmente ser usada com dinamicamente instruído e endereços MAC estáticos para limitar o tráfego de ingresso de uma porta.

VLAN com base nos protocolos — Os grupos com base nos protocolos podem ser definidos e limitado a uma porta; consequentemente, cada pacote que origina dos grupos de protocolo é atribuído ao VLAN configurado na página. O VLAN com base nos protocolos divide a rede física em grupos vlan lógicos para cada protocolo exigido. No pacote de entrada, o quadro é verificado e a sociedade de VLAN pode ser determinada com base no tipo de protocolo. Os grupos com base nos protocolos ao mapeamento VLAN ajudam a traçar um grupo de protocolo a uma porta única.

QoS — O Qualidade de Serviço (QoS) permite que você dê a prioridade ao tráfego para aplicativos diferentes, usuários ou fluxos de dados. Pode igualmente ser usado para garantir o desempenho a um nível especificado, assim, afetando Qualidade de Serviço do cliente. QoS é afetado geralmente pelos seguintes fatores: tremor, latência, e perda de pacotes.

Servidor Radius — O Remote Authentication Dial-In User Service (RADIUS) é um mecanismo da autenticação para que os dispositivos conectem e usem um serviço de rede. É usado para a autenticação centralizada, a autorização, e os propósitos de contabilidade. Um servidor Radius regula o acesso à rede verificando a identidade dos usuários através das credenciais do início de uma sessão incorporadas. Por exemplo, uma rede pública do Wi-fi é instalada em um campus de universidade. Somente aqueles estudantes que têm a senha podem alcançar estas redes. O servidor Radius verifica as senhas incorporadas pelos usuários e concede ou nega o acesso como apropriado.

RSTP — O protocolo rapid spanning-tree (RSTP) é um realce do STP. O RSTP fornece uma convergência de Spanning Tree mais rápida após uma alteração de topologia. O STP pode tomar 30 aos segundos dos 50 pés para responder a uma alteração de topologia quando o RSTP responder dentro de três vezes o tempo de hello configurado. O RSTP é para trás compatível com STP.

SNMP — O Simple Network Management Protocol (SNMP) é um padrão de rede para armazenar e compartilhar da informação sobre dispositivos de rede. O SNMP facilita o Gerenciamento de redes, o Troubleshooting, e a manutenção.

Medir - árvore — o Spanning Tree Protocol (STP) é um protocolo de rede usado em uma rede de área local (LAN). A finalidade do STP é assegurar uma topologia sem loop para um

LAN. O STP remove os laços com um algoritmo que garanta que há somente um caminho ativo entre dois dispositivos de rede. O STP assegura-se de que o tráfego tome o caminho mais curto possível dentro da rede. O STP pode igualmente automaticamente re-permitir caminhos redundantes como trajetos alternativos se um caminho ativo falha.

Servidor SSL — O secure sockets layer (SSL) é um protocolo usado principalmente para o Gerenciamento de segurança no Internet. Usa uma camada do programa que seja ficada situada entre o HTTP e as camadas TCP. Para a autenticação, o SSL usa os Certificados que digitalmente são assinados e limitados à chave pública para identificar o proprietário da chave privada. Esta autenticação ajuda durante a época da conexão. Com o uso do SSL, os Certificados são trocados nos blocos durante o processo de autenticação que estão no formato descrito no padrão X.509 do ITU-T. Então pela autoridade de certificação que é uma autoridade externo, os Certificados X.509 são emitidos que são assinados digitalmente.

Agregação do Syslog — Um serviço de SYSLOG aceita simplesmente mensagens, e armazena-as nos arquivos ou imprime-os de acordo com um arquivo de configuração simples. A agregação do Syslog significa que diversos mensagens do syslog do mesmo tipo não aparecerão na tela cada vez que um exemplo ocorre. Permitir a agregação de registro permite que você filtre os mensagens de sistema que você receberá por um período de tempo específico. Recolhe alguns mensagens do syslog do mesmo tipo assim que não aparecerão quando ocorrem, mas apareceriam um pouco em um intervalo especificado.

TACACS+ — O Terminal Access Controller Access Control System (TACACS+) é um protocolo de proprietário de Cisco que seja usado para a aplicação da segurança avançada fornecendo a authentication e autorização através do nome de usuário e senha. Para configurar um server TACACS+, o usuário deve ter o acesso do privilégio 15, que fornece o acesso de usuário a todas as características de configuração do interruptor. Algum Switches pode atuar como um cliente TACACS+, onde todos os usuários conectados possam ser autenticados e autorizado na rede através de um server corretamente configurado TACACS+. IPv4 dos suportes TACACS+ somente.

Servidor TFTP — Um server do Trivial File Transfer Protocol (TFTP) é um server que seja usado para transferir automaticamente arquivos da configuração e da bota entre dispositivos em um LAN. O protocolo é simples que permite o uso da memória baixa; contudo, esta simplicidade igualmente permite que o protocolo seja comprometido facilmente. Por este motivo, o TFTP é usado raramente com o Internet.

VLAN — Uma rede de área local virtual (VLAN) é uma rede comutada que seja segmentada logicamente pela função, pela área, ou pelo aplicativo, sem consideração aos locais físicos dos usuários. Os VLAN são um grupo de anfitriões ou as portas que possam ser ficados situados em qualquer lugar em uma rede mas para comunicar-se como se estão no mesmo segmento físico. Os VLAN ajudam a simplificar o Gerenciamento de redes deixando o mover um dispositivo para um VLAN novo sem mudar nenhumas conexões física.