MATERIAL DIDÁTICO COMPLETO: REDES DE COMPUTADORES

MÓDULO 2 – ROTEADORES E SWITCHES

INTRODUÇÃO AOS DISPOSITIVOS DE INTERCONEXÃO DE REDES

Os roteadores e switches são os pilares fundamentais sobre os quais toda infraestrutura de rede se sustenta. Enquanto os serviços de rede, explorados no módulo anterior, fornecem funcionalidades e recursos aos usuários, são os roteadores e switches que possibilitam a comunicação básica entre dispositivos, o encaminhamento de dados através de múltiplos caminhos e a construção de arquiteturas de rede escaláveis e eficientes. Compreender profundamente esses dispositivos significa ir além de simplesmente saber conectá-los fisicamente — é necessário entender como processam informações, tomam decisões de encaminhamento, gerenciam tráfego e se integram à arquitetura global da rede.

Em uma rede de computadores, a informação não viaja magicamente de um ponto a outro. Ela precisa ser transportada através de enlaces físicos (cabos de cobre, fibra óptica, ondas de rádio) e processada por dispositivos intermediários que determinam o melhor caminho para cada pacote de dados. Roteadores e switches desempenham papéis distintos mas complementares nesse processo: switches operam primariamente na camada de enlace (camada 2 do modelo OSI), conectando dispositivos dentro de uma mesma rede local e utilizando endereços MAC para encaminhar quadros; roteadores operam na camada de rede (camada 3), conectando diferentes redes e utilizando endereços IP para rotear pacotes através de múltiplos saltos até seus destinos finais.

A distinção entre essas camadas de operação não é meramente acadêmica — ela determina fundamentalmente como cada dispositivo funciona, quais informações utiliza para tomar decisões, quais tipos de problemas pode resolver e quais limitações possui. Um switch não pode, por si só, conectar duas redes com endereçamentos IP diferentes; um roteador, embora capaz de rotear entre redes, seria ineficiente e excessivamente caro se usado para conectar dezenas de computadores em um mesmo escritório. Por isso, redes modernas utilizam ambos os tipos de dispositivos, cada um desempenhando a função para a qual foi otimizado.

Neste módulo, exploraremos em profundidade os conceitos fundamentais de roteadores e switches, suas diferenças práticas, seu funcionamento interno, comandos básicos de configuração e os aspectos práticos de administração e manutenção em ambientes reais. O objetivo é construir um conhecimento sólido que permita não apenas operar esses dispositivos, mas compreender suas decisões, diagnosticar problemas e projetar topologias de rede eficientes e confiáveis.

CONCEITOS FUNDAMENTAIS DE SWITCHES

Um switch é um dispositivo de rede que opera principalmente na camada 2 do modelo OSI (camada de enlace de dados), sendo responsável por conectar múltiplos dispositivos em uma

rede local (LAN - Local Area Network) e encaminhar quadros (frames) de dados entre eles. A função primária de um switch é aprender quais dispositivos estão conectados a cada uma de suas portas e utilizar esse conhecimento para encaminhar tráfego de forma inteligente, enviando dados apenas para a porta onde o destinatário está conectado, em vez de transmitir para todas as portas como faziam os antigos hubs.

Para compreender como um switch funciona, é fundamental entender o conceito de endereço MAC (Media Access Control). Cada placa de rede fabricada no mundo possui um endereço MAC único, um identificador de 48 bits geralmente representado em formato hexadecimal (por exemplo, 00:1A:2B:3C:4D:5E). Esse endereço é gravado no hardware da placa de rede durante a fabricação e identifica unicamente aquele dispositivo na camada de enlace. Quando dispositivos comunicam-se dentro de uma rede local, os quadros Ethernet que transportam os dados incluem o endereço MAC de origem e o endereço MAC de destino nos cabeçalhos.

Quando um switch é ligado pela primeira vez, ele não possui conhecimento sobre quais dispositivos estão conectados a quais portas. Sua tabela de endereços MAC (também chamada de CAM table - Content Addressable Memory table) está vazia. À medida que dispositivos começam a transmitir dados, o switch observa cada quadro que chega, examinando o endereço MAC de origem. O switch então registra esse endereço MAC associado à porta física por onde o quadro chegou. Este processo é chamado de aprendizado de endereços MAC.

Quando o switch precisa encaminhar um quadro, ele consulta sua tabela de endereços MAC procurando pelo endereço MAC de destino. Se o endereço de destino for encontrado na tabela, o switch sabe exatamente em qual porta o dispositivo destinatário está conectado e encaminha o quadro apenas através daquela porta. Este comportamento é chamado de comutação (switching) e é muito mais eficiente que a difusão indiscriminada realizada por hubs, pois reduz colisões, melhora desempenho e aumenta a segurança, já que dispositivos não recebem tráfego destinado a outros.

Se o endereço MAC de destino não estiver na tabela (porque o switch ainda não aprendeu onde aquele dispositivo está, ou porque a entrada expirou), o switch realiza uma operação chamada flooding: ele encaminha o quadro através de todas as portas, exceto aquela por onde o quadro chegou. Quando o destinatário responder, o switch aprenderá sua localização e futuras comunicações serão encaminhadas diretamente. As entradas na tabela MAC possuem um tempo de vida (aging time), geralmente de 5 minutos, após o qual são removidas se não houver tráfego associado. Isso permite que a tabela se adapte a mudanças na rede, como dispositivos sendo movidos de uma porta para outra.

Switches modernos são capazes de operar em modo full-duplex, permitindo que dados sejam transmitidos e recebidos simultaneamente em cada porta, dobrando efetivamente a largura de banda utilizável. Cada porta funciona como um domínio de colisão separado, eliminando colisões dentro da rede comutada. Isso representa uma melhoria dramática em relação aos hubs, que operavam em half-duplex e compartilhavam toda a largura de banda entre todos os dispositivos conectados, criando um único grande domínio de colisão.

Além da comutação básica de quadros, switches oferecem funcionalidades avançadas essenciais para redes corporativas. A capacidade de criar VLANs (Virtual Local Area Networks) permite que um único switch físico seja segmentado logicamente em múltiplas redes virtuais isoladas. Dispositivos em VLANs diferentes não podem comunicar-se diretamente através do switch, mesmo estando fisicamente conectados ao mesmo equipamento. Isso proporciona segurança

(isolando departamentos sensíveis), organização (agrupando logicamente recursos relacionados) e eficiência (reduzindo broadcasts desnecessários).

VLANs são identificadas por números (VLAN IDs) que variam de 1 a 4094. A VLAN 1 é a VLAN padrão e geralmente é utilizada para gerenciamento. Portas de switch podem ser configuradas como access ports, pertencendo a uma única VLAN e conectando dispositivos finais (computadores, impressoras), ou como trunk ports, que transportam tráfego de múltiplas VLANs simultaneamente, sendo utilizadas para interconectar switches ou conectar switches a roteadores. Trunks utilizam um protocolo de marcação (tagging) chamado 802.1Q, que adiciona uma tag de 4 bytes aos quadros Ethernet identificando a qual VLAN cada quadro pertence.

Spanning Tree Protocol (STP) é outra funcionalidade crítica em switches. Em redes com redundância (múltiplos caminhos entre switches para garantir disponibilidade em caso de falhas), podem surgir loops de comutação, onde quadros circulam indefinidamente pela rede, causando tempestades de broadcast que saturam todos os enlaces e paralisam a rede. STP previne loops calculando uma topologia em árvore sem loops, bloqueando portas redundantes que criariam caminhos circulares. Se um enlace principal falha, STP recalcula a topologia e ativa portas anteriormente bloqueadas, restaurando conectividade. Variações mais modernas como RSTP (Rapid Spanning Tree Protocol) e MSTP (Multiple Spanning Tree Protocol) oferecem convergência mais rápida e suporte a múltiplas instâncias STP para diferentes VLANs.

Switches podem implementar qualidade de serviço (QoS) na camada 2, utilizando o campo de prioridade presente na tag 802.1Q (CoS - Class of Service) para priorizar tráfego. Isso permite que switches identifiquem e priorizem pacotes de VoIP ou videoconferência, garantindo baixa latência mesmo em momentos de congestionamento.

Segurança em switches inclui funcionalidades como port security, que limita o número de endereços MAC permitidos em uma porta e pode desabilitar automaticamente portas onde dispositivos não autorizados são detectados. DHCP snooping protege contra servidores DHCP não autorizados, construindo uma tabela de bindings confiáveis entre endereços MAC, endereços IP e portas. Dynamic ARP Inspection (DAI) valida pacotes ARP contra essa tabela, prevenindo ataques de envenenamento ARP.

Switches gerenciáveis permitem configuração, monitoramento e controle via interfaces CLI (Command Line Interface), web ou protocolos como SNMP. Switches não gerenciáveis (também chamados de plug-and-play) funcionam automaticamente sem configuração, sendo adequados para ambientes domésticos ou pequenas redes onde funcionalidades avançadas não são necessárias.

O desempenho de um switch é medido por métricas como taxa de encaminhamento (forwarding rate), medida em pacotes por segundo (pps), latência de comutação (switching latency), medida em microssegundos, e capacidade de comutação (switching capacity), medida em Gbps. Switches de alta performance utilizam hardware especializado (ASICs - Application-Specific Integrated Circuits) para processar quadros em velocidade de linha (line rate), garantindo que todo o tráfego seja encaminhado sem atrasos ou perdas.

CONCEITOS FUNDAMENTAIS DE ROTEADORES

Enquanto switches conectam dispositivos dentro de uma mesma rede local, roteadores conectam redes diferentes, operando na camada 3 do modelo OSI (camada de rede). O papel fundamental de um roteador é receber pacotes IP, determinar o melhor caminho para encaminhá-los através de múltiplas redes até seus destinos finais e, então, repassá-los para o próximo salto (next hop) nesse caminho. Roteadores são, portanto, os dispositivos que constroem a Internet e interconectam as milhares de redes que a compõem.

Para entender como roteadores funcionam, precisamos compreender o conceito de endereçamento IP. Diferentemente dos endereços MAC, que identificam placas de rede específicas independentemente de localização, endereços IP são hierárquicos e estruturados, refletindo a topologia da rede. Um endereço IPv4 consiste em 32 bits, geralmente representados como quatro octetos decimais separados por pontos (por exemplo, 192.168.1.50). Redes IP são identificadas por prefixos de rede, onde os bits mais significativos identificam a rede e os bits menos significativos identificam hosts individuais dentro daquela rede.

Máscaras de sub-rede (subnet masks) definem essa divisão entre porção de rede e porção de host. Uma máscara como 255.255.255.0 (ou /24 em notação CIDR) indica que os primeiros 24 bits identificam a rede e os últimos 8 bits identificam hosts. Dois dispositivos com endereços na mesma rede (mesma porção de rede) podem comunicar-se diretamente através de switches. Dispositivos em redes diferentes precisam de um roteador como intermediário.

Quando um pacote IP chega a um roteador, o dispositivo examina o endereço IP de destino e consulta sua tabela de roteamento (routing table). A tabela de roteamento contém informações sobre redes conhecidas e como alcançá-las. Cada entrada na tabela especifica uma rede de destino (definida por endereço e máscara), uma interface de saída (através de qual porta física o pacote deve ser encaminhado) e, frequentemente, o endereço do próximo roteador no caminho (gateway ou next hop).

O processo de consulta à tabela de roteamento utiliza o princípio da correspondência mais específica (longest prefix match). Se múltiplas entradas correspondem ao endereço de destino, o roteador seleciona a entrada com o prefixo mais longo (mais específico). Por exemplo, se a tabela contém entradas para 192.168.0.0/16 e 192.168.1.0/24, um pacote destinado a 192.168.1.100 será roteado usando a entrada /24, pois é mais específica. Se nenhuma correspondência for encontrada, o roteador pode utilizar uma rota padrão (default route), geralmente apontando para outro roteador que tem maior conhecimento da rede (como o roteador do provedor de Internet).

As entradas na tabela de roteamento podem ser de diferentes tipos. Rotas conectadas (connected routes) representam redes diretamente conectadas às interfaces do roteador — o roteador conhece essas redes porque possui interfaces nelas. Rotas estáticas são configuradas manualmente pelo administrador, especificando explicitamente como alcançar determinadas redes. Rotas dinâmicas são aprendidas através de protocolos de roteamento dinâmico, onde roteadores trocam informações sobre redes conhecidas, atualizando automaticamente suas tabelas conforme a topologia muda.

Protocolos de roteamento dinâmico como RIP (Routing Information Protocol), OSPF (Open Shortest Path First) e BGP (Border Gateway Protocol) permitem que roteadores construam e mantenham tabelas de roteamento automaticamente. RIP é um protocolo antigo e simples, adequado para redes pequenas, que utiliza contagem de saltos como métrica. OSPF é mais sofisticado, utiliza algoritmos de estado de enlace (link-state) e considera múltiplas métricas como largura de banda e atraso para calcular os melhores caminhos. BGP é o protocolo utilizado entre

sistemas autônomos (AS) na Internet, sendo extremamente robusto e escalável, capaz de gerenciar tabelas com centenas de milhares de rotas.

Quando o roteador determina a interface de saída e o próximo salto, ele precisa encapsular o pacote IP em um novo quadro de camada 2 apropriado para a tecnologia de rede da interface de saída (Ethernet, PPP, Frame Relay, etc.). Se a interface de saída é Ethernet, o roteador precisa descobrir o endereço MAC do próximo salto. Para isso, utiliza ARP (Address Resolution Protocol), enviando uma requisição ARP perguntando "quem possui o endereço IP X?" O dispositivo com aquele IP responde informando seu endereço MAC, permitindo que o roteador construa o quadro Ethernet adequado.

Cada vez que um pacote atravessa um roteador, o campo TTL (Time To Live) no cabeçalho IP é decrementado. TTL começa com um valor inicial (geralmente 64 ou 128) e é reduzido em 1 a cada salto. Se TTL chega a zero, o pacote é descartado, prevenindo que pacotes circulem indefinidamente na rede devido a loops de roteamento. O roteador que descarta um pacote por TTL expirado envia uma mensagem ICMP Time Exceeded de volta ao remetente, informando que o destino não foi alcançado.

Roteadores também executam fragmentação de pacotes quando necessário. Diferentes tecnologias de rede possuem diferentes MTUs (Maximum Transmission Units), que especificam o tamanho máximo de quadro que pode ser transmitido. Ethernet, por exemplo, tem MTU de 1500 bytes. Se um roteador recebe um pacote IP maior que o MTU da interface de saída, e o pacote permite fragmentação (flag Don't Fragment não está definida), o roteador divide o pacote em fragmentos menores, cada um com seu próprio cabeçalho IP. O destinatário final é responsável por remontar os fragmentos no pacote original.

Funcionalidades avançadas em roteadores incluem NAT (explorado no módulo anterior), firewalls integrados, suporte a VPN, QoS para priorização de tráfego entre redes, e capacidade de executar ACLs para controlar fluxos de tráfego. Roteadores modernos de alto desempenho utilizam hardware especializado e múltiplos processadores para encaminhar milhões de pacotes por segundo, essencial para backbones de Internet e datacenters.

A administração de roteadores envolve configuração de interfaces, definição de endereços IP e máscaras, configuração de rotas estáticas ou protocolos de roteamento dinâmico, implementação de políticas de segurança e monitoramento de desempenho. Roteadores mantêm estatísticas detalhadas sobre tráfego, erros, descartes e utilização de recursos, acessíveis via CLI, SNMP ou interfaces de gerenciamento.

DIFERENÇAS PRÁTICAS ENTRE ROTEADORES E SWITCHES

Embora roteadores e switches sejam frequentemente mencionados em conjunto e compartilhem algumas funcionalidades em dispositivos modernos (switches de camada 3, por exemplo, podem rotear), as diferenças fundamentais entre eles permanecem importantes para compreender quando e como utilizar cada um.

A principal diferença reside na camada do modelo OSI em que operam e nos tipos de endereços que utilizam para tomar decisões. Switches operam na camada 2, utilizando endereços MAC para encaminhar quadros dentro de uma rede local. Roteadores operam na camada 3, utilizando

endereços IP para rotear pacotes entre redes distintas. Esta diferença fundamental determina suas capacidades e limitações.

Switches são otimizados para conectar muitos dispositivos em uma mesma rede local com altíssimo desempenho e baixo custo por porta. Um switch corporativo pode ter 24, 48 ou até 96 portas, permitindo conectar centenas de dispositivos com latências de microssegundos. A comutação de quadros é realizada em hardware (ASICs), permitindo taxas de encaminhamento próximas da velocidade teórica dos enlaces (line rate). Switches são, portanto, a escolha natural para construir redes locais dentro de escritórios, andares de edifícios, datacenters ou campus universitários.

Roteadores, por outro lado, possuem menos portas (tipicamente de 2 a 8 em roteadores corporativos), mas cada porta pode conectar-se a uma rede diferente — redes locais, links WAN, circuitos dedicados, conexões de Internet. Roteadores tomam decisões mais complexas, consultando tabelas de roteamento extensas, aplicando políticas de segurança, executando NAT, implementando QoS e lidando com múltiplos protocolos de roteamento. Esse processamento adicional introduz maior latência (milissegundos em vez de microssegundos), mas permite funcionalidades que switches de camada 2 não podem oferecer.

Uma diferença prática importante é que switches não segmentam domínios de broadcast. Broadcasts enviados por um dispositivo são encaminhados por switches para todos os outros dispositivos na mesma VLAN, podendo causar congestionamento em redes grandes. Roteadores não encaminham broadcasts — eles segmentam domínios de broadcast. Cada rede conectada a um roteador forma seu próprio domínio de broadcast, isolado dos demais. Isso melhora eficiência e escalabilidade em redes de grande porte.

Switches de camada 3 (também chamados de multilayer switches) combinam funcionalidades de switches e roteadores, sendo capazes de comutar tráfego na camada 2 e rotear entre VLANs na camada 3, tudo em hardware de alta velocidade. São amplamente utilizados em datacenters e campus networks, onde é necessário conectar muitos dispositivos (função de switch) e rotear tráfego entre múltiplas VLANs ou sub-redes (função de roteador) com desempenho máximo. No entanto, switches de camada 3 geralmente não oferecem todas as funcionalidades de roteadores dedicados, como suporte a múltiplos protocolos WAN, capacidades avançadas de VPN ou integração com serviços de segurança complexos.

Do ponto de vista de custo, switches são significativamente mais baratos por porta que roteadores, pois seus requisitos de processamento são menores. Um switch de 48 portas Gigabit Ethernet gerenciável pode custar algumas centenas de dólares, enquanto um roteador corporativo com capacidades avançadas pode custar milhares.

Quanto à topologia de rede, switches são utilizados em arquitetura estrela, onde dispositivos finais conectam-se a switches, que por sua vez podem conectar-se hierarquicamente a switches de distribuição e núcleo. Roteadores conectam essas redes locais à Internet, a filiais remotas ou a outras redes externas, formando a camada de borda (edge) da rede.

Em resumo, switches constroem redes locais eficientes e de alto desempenho, conectando dispositivos finais. Roteadores interconectam essas redes locais, formando redes mais amplas, aplicando políticas de segurança, controlando fluxos de tráfego e conectando a organização ao mundo externo. Uma infraestrutura de rede bem projetada utiliza ambos adequadamente, aproveitando as forças de cada dispositivo.

FUNCIONAMENTO INTERNO: ENCAMINHAMENTO, COMUTAÇÃO E TABELAS

Compreender o funcionamento interno de roteadores e switches é essencial para diagnosticar problemas, otimizar desempenho e tomar decisões arquiteturais informadas. Apesar de suas diferenças, ambos compartilham princípios fundamentais de operação: receber dados, consultar tabelas de decisão, determinar a melhor ação e encaminhar os dados apropriadamente.

Funcionamento Interno de Switches

Quando um quadro Ethernet chega a uma porta de switch, o dispositivo realiza uma sequência de operações em velocidade extremamente alta, geralmente em microssegundos. Primeiro, o switch recebe o quadro completamente e verifica sua integridade através do FCS (Frame Check Sequence), um campo de detecção de erros no final do quadro. Se o quadro estiver corrompido, é descartado silenciosamente.

Assumindo que o quadro está íntegro, o switch extrai o endereço MAC de origem e realiza o processo de aprendizado: verifica se esse endereço MAC já está em sua tabela CAM associado àquela porta. Se não estiver, adiciona uma nova entrada. Se estiver associado a uma porta diferente, atualiza a entrada (indicando que o dispositivo foi movido). Se já estiver correto, apenas atualiza o timestamp da entrada, reiniciando o contador de aging.

Em seguida, o switch extrai o endereço MAC de destino e consulta a tabela CAM. Se encontrar uma correspondência, identifica a porta de saída. Se a porta de saída for a mesma porta de entrada (o destinatário está no mesmo segmento que o remetente), o switch descarta o quadro (não há necessidade de encaminhá-lo). Se a porta de saída for diferente, o switch encaminha o quadro apenas através daquela porta. Se não encontrar correspondência (endereço desconhecido), realiza flooding, enviando o quadro por todas as portas exceto a de entrada.

No contexto de VLANs, o switch também verifica a que VLAN a porta de entrada pertence e só encaminha o quadro para portas que fazem parte da mesma VLAN. Em trunk ports, o switch adiciona ou remove tags 802.1Q conforme necessário.

Switches utilizam diferentes métodos de comutação. Store-and-forward recebe o quadro completo, verifica erros e só então encaminha — mais lento mas mais confiável. Cut-through começa a encaminhar o quadro assim que lê o endereço MAC de destino, sem aguardar o quadro completo — mais rápido mas pode propagar quadros com erros. Fragment-free é um meio-termo, aguardando os primeiros 64 bytes (onde a maioria dos erros ocorre) antes de encaminhar.

Funcionamento Interno de Roteadores

Quando um pacote IP chega a uma interface de roteador, o dispositivo realiza um processo mais complexo. Primeiro, o roteador remove o cabeçalho de camada 2 (Ethernet, por exemplo), expondo o pacote IP. Verifica o checksum do cabeçalho IP para garantir integridade. Se o checksum estiver incorreto, o pacote é descartado.

O roteador verifica o campo TTL. Se TTL for 1, decrementa para 0 e descarta o pacote, enviando uma mensagem ICMP Time Exceeded ao remetente. Se TTL for maior que 1, decrementa o valor.

Em seguida, o roteador examina o endereço IP de destino e realiza a busca na tabela de roteamento. Usa o algoritmo de longest prefix match para encontrar a rota mais específica que corresponde ao destino. A entrada selecionada especifica a interface de saída e, possivelmente, o endereço IP do next hop (próximo roteador).

Se a interface de saída está diretamente conectada à rede de destino (rota conectada), o roteador entrega o pacote diretamente ao host final. Caso contrário, encaminha ao próximo roteador. Para construir o quadro de camada 2 para a interface de saída, o roteador precisa do endereço MAC do destinatário (se entrega direta) ou do next hop (se encaminhamento para outro roteador).

O roteador consulta sua tabela ARP, procurando o endereço MAC correspondente ao IP de destino ou next hop. Se encontrar, utiliza esse MAC. Se não encontrar, enfileira o pacote temporariamente e envia uma requisição ARP para descobrir o endereço MAC. Quando recebe a resposta ARP, atualiza sua tabela ARP e processa os pacotes enfileirados.

Com o endereço MAC disponível, o roteador constrói um novo quadro de camada 2, inserindo o pacote IP como carga útil. O endereço MAC de origem do quadro é o endereço MAC da interface de saída do roteador. O endereço MAC de destino é o do próximo salto ou destinatário final. Finalmente, o roteador transmite o quadro através da interface de saída.

Tabelas e Estruturas de Dados

Tanto switches quanto roteadores dependem de estruturas de dados eficientes para tomar decisões rapidamente. Tabelas CAM em switches utilizam memória associativa (content-addressable memory) que permite buscar endereços MAC em tempo constante, independentemente do tamanho da tabela. Isso é crucial para manter desempenho em velocidade de linha.

Tabelas de roteamento em roteadores podem conter milhares ou até milhões de entradas (em roteadores de Internet). Algoritmos eficientes como árvores de prefixos (tries) ou estruturas de busca acelerada por hardware permitem consultas rápidas. Roteadores de alto desempenho armazenam cópias da tabela de roteamento em memória de alta velocidade próxima aos processadores de encaminhamento, minimizando latência.

Tabelas ARP associam endereços IP a endereços MAC, sendo dinâmicas e atualizadas conforme dispositivos comunicam-se. Entradas ARP possuem tempo de vida limitado (geralmente minutos), expirando se não forem utilizadas, forçando redescoberta e permitindo adaptação a mudanças.

COMANDOS BÁSICOS E CONCEITOS DE CONFIGURAÇÃO

Configurar roteadores e switches exige familiaridade com suas interfaces de administração, geralmente baseadas em CLI (Command Line Interface). Embora diferentes fabricantes (Cisco, Juniper, HP, Huawei, etc.) possuam sintaxes e comandos específicos, os conceitos subjacentes são universais. Para fins didáticos, utilizaremos exemplos baseados em sintaxe Cisco IOS (Internetwork Operating System), amplamente utilizada e considerada padrão de facto na indústria.

Acesso e Modos de Configuração

O acesso inicial a um switch ou roteador geralmente ocorre via console serial (cabo conectado diretamente ao dispositivo) ou, se já configurado, via SSH (Secure Shell) ou Telnet através da rede. Ao conectar-se, o administrador é recebido pelo modo usuário (user EXEC mode), indicado pelo prompt `>`, onde pode executar comandos básicos de visualização mas não alterar configurações.

Para realizar configurações, é necessário entrar no modo privilegiado (privileged EXEC mode), digitando o comando `enable`. O prompt muda para `#`, indicando acesso privilegiado. Neste modo, é possível visualizar toda a configuração, executar comandos de diagnóstico e entrar no modo de configuração.

O modo de configuração global (global configuration mode) é acessado com o comando `configure terminal` (ou `conf t`). O prompt muda para `(config)#`. Neste modo, comandos afetam a configuração global do dispositivo. A partir daqui, pode-se entrar em modos de configuração específicos, como configuração de interface, configuração de roteamento ou configuração de linha.

Configuração Básica de Switch

Um exemplo de configuração inicial de switch incluiria:

Definir hostname (nome do dispositivo):

```
(config)# hostname Switch-Matriz
```

Configurar senhas de acesso:

```
(config)# enable secret senha_secreta
(config)# line console 0
(config-line)# password senha_console
(config-line)# login
```

Configurar endereço IP de gerenciamento (VLAN de gerenciamento):

```
(config)# interface vlan 1
(config-if)# ip address 192.168.1.10 255.255.255.0
(config-if)# no shutdown
(config)# ip default-gateway 192.168.1.1
```

Criar e configurar VLANs:

```
(config)# vlan 10
(config-vlan)# name Administrativo
(config)# vlan 20
(config-vlan)# name Producao
```

Atribuir portas a VLANs:

```
(config)# interface range fastethernet 0/1-10
(config-if-range)# switchport mode access
(config-if-range)# switchport access vlan 10
(config)# interface range fastethernet 0/11-20
(config-if-range)# switchport mode access
(config-if-range)# switchport access vlan 20
```

Configurar trunk (porta que transporta múltiplas VLANs):

```
(config)# interface gigabitethernet 0/1
(config-if)# switchport mode trunk
(config-if)# switchport trunk allowed vlan 10,20
```

Habilitar Spanning Tree Protocol:

```
(config)# spanning-tree mode rapid-pvst
```

Salvar configuração:

```
# copy running-config startup-config
```

Configuração Básica de Roteador

Configurar hostname e senhas:

```
(config)# hostname Roteador-Principal
(config)# enable secret senha_secreta
```

Configurar interfaces com endereços IP:

```
(config)# interface gigabitethernet 0/0
(config-if)# description Interface conectada a LAN interna
(config-if)# ip address 192.168.1.1 255.255.255.0
(config-if)# no shutdown

(config)# interface gigabitethernet 0/1
(config-if)# description Interface conectada a Internet
(config-if)# ip address 200.100.50.2 255.255.255.252
(config-if)# no shutdown
```

Configurar rota estática padrão:

```
(config)# ip route 0.0.0.0 0.0.0.0 200.100.50.1
```

Configurar NAT:

```
(config)# access-list 1 permit 192.168.1.0 0.0.0.255
(config)# ip nat inside source list 1 interface gigabitethernet 0/1 overload
(config)# interface gigabitethernet 0/0
(config-if)# ip nat inside
(config)# interface gigabitethernet 0/1
(config-if)# ip nat outside
```

Configurar roteamento dinâmico (OSPF):

```
(config)# router ospf 1
(config-router)# network 192.168.1.0 0.0.0.255 area 0
```

Comandos de Verificação e Diagnóstico

Visualizar tabela MAC do switch:

```
# show mac address-table
```

Visualizar configuração de VLANs:

```
# show vlan brief
```

Visualizar status de interfaces:

```
# show interfaces status
# show ip interface brief
```

Visualizar tabela de roteamento:

```
# show ip route
```

Visualizar tabela ARP:

```
# show arp
```

Testar conectividade:

```
# ping 8.8.8.8
# traceroute 8.8.8.8
```

Visualizar estatísticas de interface:

```
# show interfaces gigabitethernet 0/0
```

Visualizar logs do sistema:

```
# show logging
```

Esses comandos fornecem visibilidade sobre o estado operacional dos dispositivos, essencial para diagnóstico de problemas e verificação de configurações.

ADMINISTRAÇÃO E MANUTENÇÃO EM REDES REAIS

A administração eficaz de roteadores e switches em ambientes de produção vai muito além da configuração inicial. Envolve monitoramento contínuo, manutenção preventiva, atualização de firmware, gerenciamento de configurações, implementação de políticas de segurança e resposta rápida a incidentes.

Monitoramento e Visibilidade

Monitorar a saúde e desempenho dos dispositivos de rede é fundamental para detectar problemas antes que impactem usuários e para planejar expansões. Sistemas de monitoramento baseados em SNMP (Simple Network Management Protocol) consultam periodicamente dispositivos de

rede, coletando métricas como utilização de CPU, utilização de memória, tráfego em interfaces (bytes/pacotes enviados e recebidos), erros, descartes e estado operacional de interfaces.

Ferramentas como Zabbix, Nagios, PRTG ou SolarWinds permitem centralizar monitoramento, criar dashboards visualizando o estado da rede em tempo real, configurar alertas para condições anormais (interface down, utilização acima de limite, erros crescentes) e gerar relatórios históricos para análise de tendências.

Syslog é um protocolo utilizado por roteadores e switches para enviar logs de eventos a um servidor centralizado. Eventos como mudanças de estado de interface, falhas de autenticação, detecção de loops STP, ou violações de ACL são registrados. Analisar logs centralizados permite identificar padrões, investigar incidentes de segurança e auditar ações administrativas.

Gerenciamento de Configurações

Manter controle rigoroso das configurações de dispositivos é essencial. Configurações devem ser documentadas, versionadas e armazenadas em local seguro. Ferramentas de gerenciamento de configuração permitem fazer backup automático de configurações regularmente, comparar versões (identificando mudanças), e restaurar configurações rapidamente em caso de falhas.

Mudanças em configurações devem seguir processos controlados: planejamento (documentar o que será alterado e por quê), teste em ambiente de desenvolvimento ou homologação quando possível, implementação em janela de manutenção apropriada, e validação pós-mudança (verificar que a alteração funcionou e não causou efeitos colaterais). Mudanças emergenciais devem ser documentadas retroativamente.

Atualizações de Firmware

Fabricantes de equipamentos de rede lançam regularmente atualizações de firmware (sistema operacional dos dispositivos) corrigindo vulnerabilidades de segurança, bugs e adicionando funcionalidades. Manter firmware atualizado é importante para segurança e estabilidade, mas atualizações também podem introduzir novos bugs e incompatibilidades.

Antes de atualizar firmware em produção, é prudente testar a nova versão em ambiente de laboratório, revisar notas de lançamento (release notes) identificando mudanças e problemas conhecidos, e planejar rollback (reversão) caso algo falhe. Atualizações devem ser realizadas em janelas de manutenção, com comunicação prévia aos usuários.

Segurança Física e Lógica

Os dispositivos de rede devem estar fisicamente seguros, em salas de TI com acesso restrito, prevenindo manipulação não autorizada, roubo ou danos. Logicamente, acesso administrativo deve ser protegido: senhas fortes e únicas, mudanças regulares de senhas, uso de autenticação centralizada (RADIUS, TACACS+) integrando com sistemas corporativos, e desabilitação de protocolos inseguros como Telnet (substituído por SSH) e SNMP v1/v2c (substituído por SNMP v3 com criptografia).

Desabilitar serviços e portas não utilizadas reduz a superfície de ataque. Implementar ACLs restringindo acesso administrativo apenas de redes ou dispositivos autorizados. Habilitar logging de comandos executados (command logging) para auditoria.

Redundância e Alta Disponibilidade

Redes corporativas críticas não podem tolerar pontos únicos de falha. Implementar redundância em dispositivos de rede garante que falhas de hardware ou enlaces não causem interrupções. Técnicas incluem:

- **Redundância de hardware**: switches empilhados (stacking), onde múltiplos switches físicos funcionam como um único switch lógico, compartilhando configuração e plano de controle. Se um switch falha, os demais continuam operando.

- **Redundância de enlaces**: múltiplos cabos conectando switches, com STP bloqueando caminhos redundantes em operação normal mas ativando-os automaticamente em caso de falha do caminho principal. Protocolos como LACP (Link Aggregation Control Protocol) permitem agregar múltiplos enlaces físicos em um enlace lógico, aumentando a largura de banda e resiliência.

- **Roteadores redundantes**: protocolos como HSRP (Hot Standby Router Protocol), VRRP (Virtual Router Redundancy Protocol) ou GLBP (Gateway Load Balancing Protocol) permitem que múltiplos roteadores funcionem como gateway padrão, compartilhando um endereço IP virtual. Se o roteador ativo falha, outro assume automaticamente, com interrupção mínima.

Dimensionamento e Planejamento de Capacidade

Monitoramento contínuo de utilização de recursos (tráfego, CPU, memória) permite identificar tendências de crescimento e planejar expansões antes que gargalos impactem o desempenho. Se a utilização de uma interface consistentemente ultrapassa 70-80% da capacidade, é hora de considerar upgrade (por exemplo, de Gigabit para 10 Gigabit) ou balanceamento de carga.

Crescimento no número de usuários ou dispositivos pode exigir adição de switches, ampliação de VLANs ou segmentação adicional. Planejamento de capacidade evita surpresas e permite orçamentar recursos adequadamente.

Diagnóstico e Resolução de Problemas

Quando problemas ocorrem, metodologia sistemática de "troubleshooting " é essencial. Dividir o modelo OSI em camadas ajuda a isolar o problema:

- **Camada 1 (Física)**: cabos danificados, conectores soltos, transceivers defeituosos. Verificar LEDs de link, testar cabos, trocar hardware suspeito.

- **Camada 2 (Enlace)**: loops STP, VLAN incorretas, tabelas MAC cheias. Comandos como `show spanning-tree`, `show vlan`, `show mac address-table` ajudam diagnosticar.

- **Camada 3 (Rede)**: rotas faltando, máscaras de sub-rede incorretas, gateways configurados errados. `show ip route`, `ping`, `traceroute` são ferramentas essenciais.

Documentar topologias de rede, diagramas lógicos e físicos, manter inventário atualizado de dispositivos e configurações, e treinar equipe regularmente são práticas que facilitam a manutenção e reduzem tempo de resolução de problemas.
