**Introdução**

11.0.1

**Por que devo cursar este módulo?**

A infra-estrutura de rede define a forma como os dispositivos são conectados entre si para alcançar comunicações de ponta a ponta. Assim como há muitos tamanhos de redes, há também muitas maneiras de construir uma infraestrutura. No entanto, existem alguns projetos padrão que o setor de rede recomenda alcançar redes que estão disponíveis e seguras.

Este módulo abrange o funcionamento básico das infra-estruturas de rede, incluindo redes com e sem fios.

11.0.2

**O que vou aprender neste módulo?**

**Título do módulo:** Dispositivos de comunicação de rede

**Objetivo do módulo:** Explicar como os dispositivos de rede permitem a comunicação de rede com e sem fio.

| **Título do Tópico** | **Objetivo do Tópico** |
| --- | --- |
| Dispositivos de Rede | Explicar como os dispositivos de rede viabilizam a comunicação de rede. |
| Comunicações sem fio | Explicar como os dispositivos sem fio viabilizam a comunicação de rede. |

# Dispositivos de Rede

11.1.1

## Dispositivos Finais

Os dispositivos de rede com os quais as pessoas estão mais familiarizadas são dispositivos finais. Para distinguir um dispositivo final de outro, cada dispositivo final em uma rede tem um endereço. Quando um dispositivo final inicia a comunicação, ele usa o endereço do dispositivo final de destino para especificar onde entregar a mensagem.

Um dispositivo final é a origem ou o destino de uma mensagem transmitida pela rede.

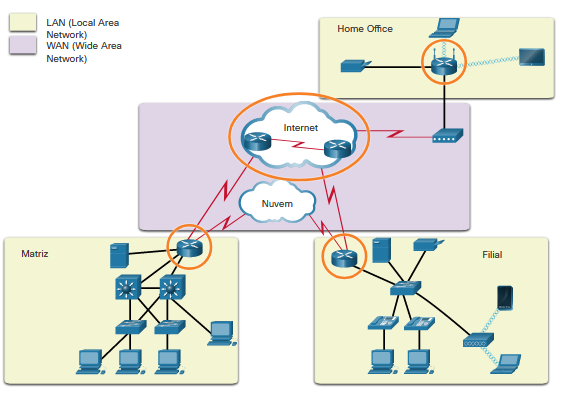
11.1.3

## Roteadores

Os roteadores são dispositivos que operam na camada de rede OSI (Camada 3). Conforme mostrado na figura, os roteadores são usados para interconectar sites remotos. Eles usam o processo de roteamento para encaminhar pacotes de dados entre redes. O processo de roteamento usa tabelas de roteamento de rede, protocolos e algoritmos para determinar o caminho mais eficiente para encaminhar um pacote IP. Os roteadores coletam informações de roteamento e atualizam outros roteadores sobre alterações na rede. Os roteadores aumentam a escalabilidade das redes segmentando domínios de transmissão.

A imagem mostra quatro caixas, uma na parte superior do gráfico rotulado Home Office e contendo um roteador sem fio, uma impressora conectada por uma linha que representa uma conexão com fio, um tablet sem fio e um laptop sem fio. Uma linha conecta o roteador sem fio a um modem a cabo, que se conecta à segunda caixa chamada WAN, contendo uma nuvem chamada Internet e outra nuvem chamada Nuvem. Há duas caixas na parte inferior do gráfico, uma rotulada como Central e uma rotulada como Branch. Ambas as caixas contêm ícones de roteador conectados à Nuvem e à Internet com mídia WAN mostrada como raios vermelhos. Na caixa Central, há dois ícones de switch multicamadas, conectados a dois switches LAN. Há um servidor conectado diretamente ao roteador e quatro computadores conectados aos switches. Na caixa rotulada Branch, há seis dispositivos finais conectados a um ícone de switch. Os seis dispositivos são um servidor, uma impressora, dois telefones IP e dois computadores. Também está ligado ao comutador LAN um ponto de acesso sem fios. Um tablet sem fio e um laptop sem fio são mostrados conectando ao ponto de acesso sem fio.

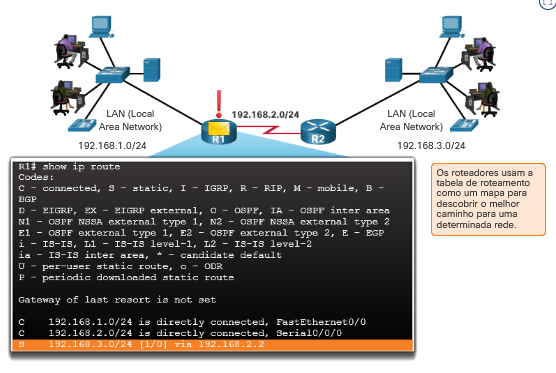
### A conexão do roteador

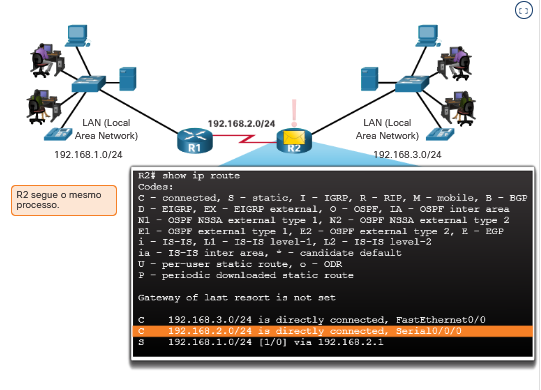


Os roteadores têm duas funções principais: determinação de caminho e encaminhamento de pacotes. Para executar a determinação do caminho, cada roteador constrói e mantém uma tabela de roteamento que é um banco de dados de redes conhecidas e como alcançá-las. A tabela de roteamento pode ser criada manualmente e conter rotas estáticas ou pode ser construída usando um protocolo de roteamento dinâmico.

O encaminhamento de pacotes é realizado usando uma função de comutação. A comutação é o processo usado por um roteador para aceitar um pacote em uma interface e encaminhá-lo para outra interface. Uma responsabilidade primária da função de comutação é encapsular os pacotes no tipo de quadro de enlace de dados apropriado para o enlace de dados de saída.

Reproduza a animação dos roteadores R1 e R2 recebendo um pacote de uma rede e encaminhando o pacote para a rede de destino.





Depois que o roteador determinar a interface de saída utilizando a função de determinação do caminho, ele deverá encapsular o pacote no quadro de enlace de dados da interface de saída.

O que um roteador faz com um pacote recebido de uma rede e destinado a outra rede? O roteador executa as três etapas principais seguintes:

1. Ele desencapsula o cabeçalho e o trailer do quadro da Camada 2 para expor o pacote da Camada 3.

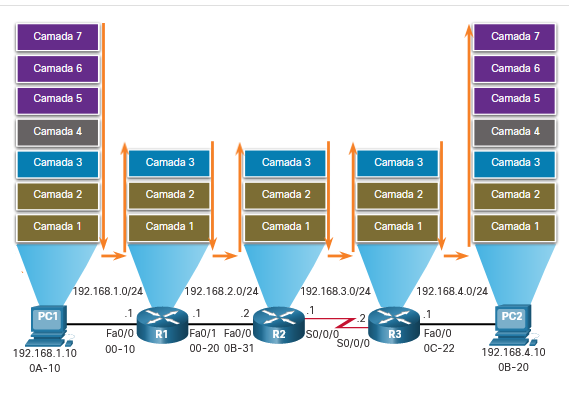
2. Ele examina o endereço IP de destino do pacote IP para encontrar o melhor caminho na tabela de roteamento.

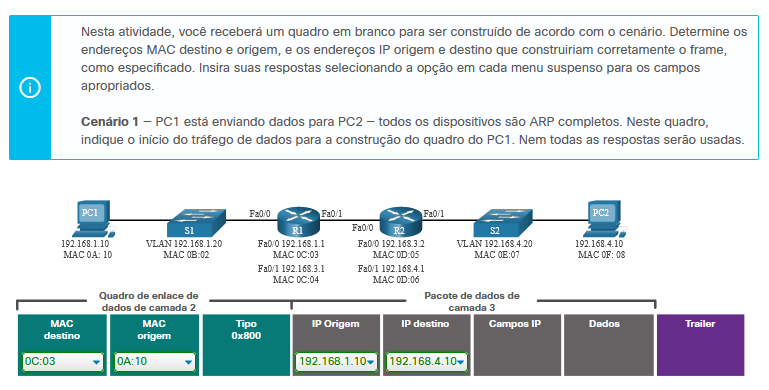
3. Se o roteador encontrar um caminho para o destino, ele encapsula o pacote da Camada 3 em um novo quadro da Camada 2 e encaminha esse quadro pela interface de saída.

Conforme mostrado na figura, os dispositivos têm endereços IPv4 da Camada 3, enquanto as interfaces Ethernet têm endereços de enlace de dados da Camada 2. Os endereços MAC são encurtados para simplificar a ilustração. Por exemplo, o PC1 é configurado com um endereço IPv4 192.168.1.10 e um endereço MAC de exemplo de 0A-10. À medida que um pacote vai do dispositivo origem para o dispositivo destino, os endereços IP de Camada 3 não são alterados. Isso ocorre porque a PDU da Camada 3 não se altera. No entanto, os endereços de enlace de dados da Camada 2 mudam em cada roteador no caminho para o destino, à medida que o pacote é desencapsulado e reencapsulado em um novo quadro da Camada 2.

Gráfico intitulado Encapsulamento e Desencapsulamento de pacotes. Na imagem estão cinco colunas mostradas lado a lado. A coluna 1 contém as sete camadas do modelo OSI, rotuladas Camada 1, Camada 2 etc. As colunas 2, 3 e 4 contêm três camadas rotuladas Camada 1, Camada 2 e Camada 3. A quinta coluna no lado direito da imagem, contém as sete camadas do modelo OSI. Na parte inferior da Coluna 1, há um ícone chamado PC1, com um endereço IPv4 de 192.168.1.10. Ele é conectado por uma linha a um ícone de roteador rotulado R1 localizado abaixo da coluna 2. O roteador R1 é mostrado com duas interfaces FastEthernet. A interface conectada ao PC1 é rotulada como FA0/0, 00-10 e .1 Acima do link entre PC1 e R1 está o endereço de rede IP 192.168.1.0/24. O roteador R1 é conectado por uma linha ao roteador R2, que é mostrado abaixo da coluna 3. A interface no roteador R1 que se conecta ao R2 é rotulada como Fa0/1, 00-20 e .1. O Roteador R2 é mostrado com uma Interface Fastee uma interface WAN serial. A Interface FastEque se conecta ao R1 é rotulada como Fa0/0, 0B-31 e .2. Acima do link entre R1 e R2 está o endereço de rede IP 192.168.2.0/24. O roteador R2 se conecta por meio de um link serial representado por um raio vermelho. ao roteador R3, localizado abaixo da coluna 4. A interface no roteador R2 que se conecta a R3 é identificada como S0 / 0/0 e .2. Acima do link entre R2 e R3 está o endereço de rede IP 192.168.3.0/24. O roteador R3 é mostrado com uma interface WAN serial e uma interface FastEthernet. A interface serial no roteador R3 é identificada como S0 / 0/0 e .2. A interface FastEthernet no roteador R3 se conecta ao PC2, localizada abaixo da coluna 5. A interface FastEthernet no roteador R3 é identificada como Fa0 / 0, OC-22 e .1. Acima do link entre o roteador R3 e PC2 está o endereço de rede IP 192.168.4.0. PC2 está rotulado 192.168.4.10 e 0B-20.

### Pacotes de encapsulamento e desencapsulamento





11.1.5

**Processo de decisão de encaminhamento de pacotes**

Agora que o roteador determinou o melhor caminho para um pacote com base na correspondência mais longa, ele deve determinar como encapsular o pacote e encaminhá-lo para a interface de saída correta.

A figura explica como um roteador determina o melhor caminho a ser usado para encaminhar um pacote.

A figura mostra como um roteador primeiro determina o melhor caminho e, em seguida, encaminha o pacote. Existem 5 etapas representadas com estas etapas:

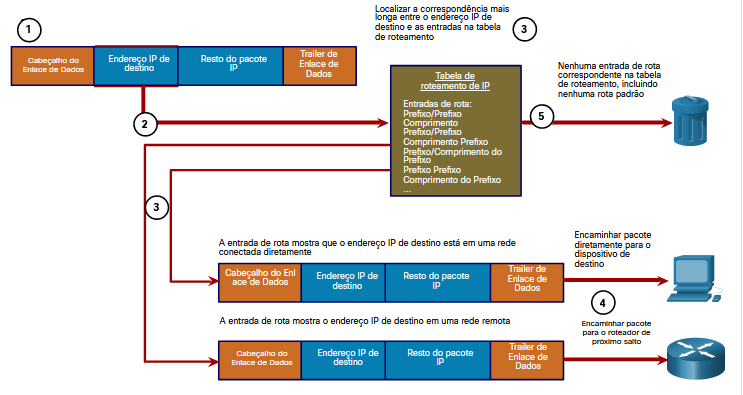
1. O quadro de enlace de dados com um pacote IP encapsulado chega na interface de entrada.

2. O roteador examina o endereço IP de destino no cabeçalho do pacote e consulta sua tabela de roteamento IP.

3. O roteador localiza o prefixo correspondente mais longo na tabela de roteamento.

4. O roteador encapsula o pacote em um quadro de enlace de dados e o encaminha para fora da interface de saída. O destino pode ser um dispositivo conectado à rede ou um roteador de próximo salto.

5. No entanto, se não houver nenhuma entrada de rota correspondente, o pacote será descartado.



...

As etapas a seguir descrevem o processo de encaminhamento de pacotes mostrado na figura:

1. O quadro de enlace de dados com um pacote IP encapsulado chega na interface de entrada.
2. O roteador examina o endereço IP de destino no cabeçalho do pacote e consulta sua tabela de roteamento IP.
3. O roteador localiza o prefixo correspondente mais longo na tabela de roteamento.
4. O roteador encapsula o pacote em um quadro de enlace de dados e o encaminha para fora da interface de saída. O destino pode ser um dispositivo conectado à rede ou um roteador de próximo salto.
5. No entanto, se não houver nenhuma entrada de rota correspondente, o pacote será descartado.

**Encaminha o pacote para um dispositivo em uma rede conectada diretamente**

Se a entrada de rota indicar que a interface de saída é uma rede conectada diretamente, isso significa que o endereço IP de destino do pacote pertence a um dispositivo na rede diretamente conectada. Portanto, o pacote pode ser encaminhado diretamente para o dispositivo de destino. O dispositivo de destino geralmente é um dispositivo final em uma LAN Ethernet, o que significa que o pacote deve ser encapsulado em um quadro Ethernet.

Para encapsular o pacote no quadro Ethernet, o roteador precisa determinar o endereço MAC de destino associado ao endereço IP de destino do pacote. O processo varia com base em se o pacote é um pacote IPv4 ou IPv6:

* **Pacote IPv4** - O roteador verifica sua tabela ARP para o endereço IPv4 de destino e um endereço MAC Ethernet associado. Se não houver correspondência, o roteador enviará uma Solicitação ARP. O dispositivo de destino retornará uma resposta ARP com seu endereço MAC. O roteador agora pode encaminhar o pacote IPv4 em um quadro Ethernet com o endereço MAC de destino apropriado.
* **Pacote IPv6** - O roteador verifica seu cache vizinho para o endereço IPv6 de destino e um endereço MAC Ethernet associado. Se não houver correspondência, o roteador enviará uma mensagem ICMPv6 Neighbor Solicitation (NS). O dispositivo de destino retornará uma mensagem de anúncio de vizinho (NA) ICMPv6 com seu endereço MAC. O roteador agora pode encaminhar o pacote IPv6 em um quadro Ethernet com o endereço MAC de destino apropriado.

**Encaminha o pacote para um roteador Next-Hop**

Se a entrada de rota indicar que o endereço IP de destino está em uma rede remota, isso significa que o endereço IP de destino do pacote pertence a um dispositivo na rede que não está conectado diretamente. Portanto, o pacote deve ser encaminhado para outro roteador, especificamente um roteador de próximo salto. O endereço do próximo salto é indicado na entrada da rota.

Se o roteador de encaminhamento e o roteador de próximo salto estiverem em uma rede Ethernet, ocorrerá um processo semelhante (ARP e ICMPv6 Neighbor Discovery) para determinar o endereço MAC de destino do pacote, conforme descrito anteriormente. A diferença é que o roteador procurará o endereço IP do roteador próximo salto em sua tabela ARP ou cache vizinho, em vez do endereço IP de destino do pacote.

**Observação**: Este processo irá variar para outros tipos de redes da Camada 2.

**Elimina o pacote - Nenhuma correspondência na tabela de roteamento**

Se não houver correspondência entre o endereço IP de destino e um prefixo na tabela de roteamento, e se não houver rota padrão, o pacote será descartado.

11.1.6

## Informação de Roteamento

A tabela de roteamento de um roteador armazena as seguintes informações:

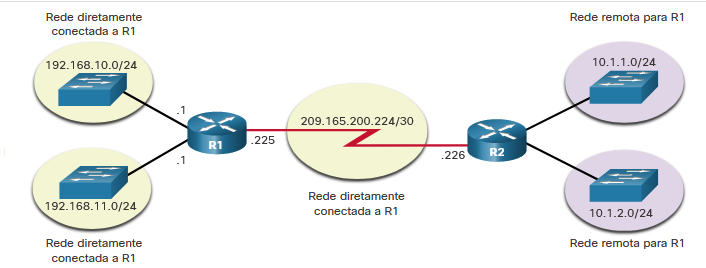
* **Rotas conectadas diretamente** - essas rotas vêm das interfaces ativas do roteador. Os roteadores adicionam uma rota diretamente conectada quando uma interface está configurada com um endereço IP e está ativada.
* **Rotas remotas** - são redes remotas conectadas a outros roteadores. As rotas para essas redes podem ser configuradas estaticamente ou ser dinamicamente aprendidas através de protocolos de roteamento dinâmico.

Especificamente, uma tabela de roteamento é um arquivo de dados na RAM que é usado para armazenar informações sobre redes diretamente conectadas e remotas. A tabela de roteamento contém a rede ou associações do próximo salto. Essas associações informam ao roteador que um determinado destino pode ser acessado de modo ideal com o envio do pacote a um roteador específico que representa o próximo salto no caminho até o destino final. A associação do próximo salto também pode ser a interface de saída para o próximo destino.

A figura identifica as redes diretamente conectadas e as redes remotas do roteador R1.

A figura é rotulada como rotas de rede remotas e conectadas diretamente. A imagem mostra cinco ovais, dois no lado esquerdo, dois no lado direito e um no meio. Os dois ovais à esquerda contêm um ícone de switch LAN. O oval superior esquerdo é rotulado: rede diretamente conectada ao R1, com o endereço IP 192.168.10.0/24. Uma linha conecta o ícone do switch LAN a um ícone de roteador rotulado como R1. R1 é mostrado como tendo duas interfaces FastEe uma interface serial. A interface no R1 é rotulada como .1. O oval inferior esquerdo é rotulado: a rede conecta-se diretamente ao R1 com o endereço IP de 192.168.11.0/24. Uma linha conecta o ícone do switch LAN ao roteador R1. Dentro do oval médio, o roteador R1 é conectado ao roteador R2 com uma conexão serial wan, representada como um raio vermelho. A interface serial no R1 é rotulada como .225 e a interface serial conectada no R2 é rotulada como .226. Acima da conexão entre R1 e R2 está o endereço de rede IP 209.165.200.224/30. Abaixo do oval médio está um rótulo que diz: rede diretamente conectada ao R1. Os dois ovais do lado direito contêm um ícone de switch LAN. O oval superior direito é rotulado: Remoto de rede para R1 e o endereço IP 10.1.1.0/24. O oval inferior direito é rotulado Network remote to R1 e o endereço IP 10.1.2.0/24.

### Rotas para Redes Diretamente Conectadas e Remotas



As entradas de rede de destino na tabela de roteamento podem ser adicionadas de várias maneiras:

* **Interfaces de rota local** - Adicionadas quando uma interface está configurada e ativa. Esta entrada só é exibida no IOS 15 ou mais recente para rotas IPv4 e em todas as versões do IOS para rotas IPv6.
* **Interfaces diretamente conectadas** - Adicionadas à tabela de roteamento quando uma interface está configurada e ativa.
* **Rotas estáticas** - Adicionadas quando uma rota é configurada manualmente e a interface de saída está ativa.
* **Protocolo de roteamento dinâmico** - Adicionado quando protocolos de roteamento que aprendem dinamicamente sobre a rede, como EIGRP ou OSPF, são implementados e redes são identificadas.

Protocolos de roteamento dinâmico trocam informações de acessibilidade de rede entre roteadores e se adaptam dinamicamente às alterações de rede. Cada protocolo de roteamento usa algoritmos de roteamento para determinar os melhores caminhos entre diferentes segmentos na rede e atualiza tabelas de roteamento com esses caminhos.

Os protocolos de roteamento dinâmico foram usados em redes desde o final da década de 80. Um dos primeiros protocolos de roteamento foi o RIP. RIPv1 foi lançado em 1988. Como as redes evoluíram e se tornaram mais complexas, surgiram novos protocolos de roteamento. O protocolo RIP foi atualizado para RIPv2 para acomodar o crescimento no ambiente de rede. No entanto, o RIPv2 ainda não é escalável nas implementações de redes maiores atuais. Para atender às necessidades de redes maiores foram desenvolvidos dois protocolos de roteamento avançados: OSPF (Open Shortest Path First) e IS-IS (Intermediate System-to-Intermediate System). A Cisco desenvolveu o IGRP (Interior Gateway Routing Protocol) e EIGRP (enhanced IGRP), que também é escalável nas implementações de redes maiores.

Além disso, há a necessidade de conectar diferentes redes interconectadas e de proporcionar roteamento entre elas. O Border Gateway Protocol (BGP) agora é usado entre provedores de serviços de Internet (ISPs). O BGP também é usado entre ISPs e seus grandes clientes privados para trocar informações de roteamento.

A tabela classifica os protocolos. Os roteadores configurados com esses protocolos enviarão mensagens periodicamente para outros roteadores. Como analista de segurança cibernética, você verá essas mensagens em vários logs e capturas de pacotes.

| **Protocolo** | **Protocolos de Gateway Interno** | | | | **Protocolos do Gateway Externo** |
| --- | --- | --- | --- | --- | --- |
|  | **Vetor de distância** | | **Estado do Link** | | **Vetor de Caminho** |
| IPv4 | RIPv2 | EIGRP | OSPFv2 | IS-IS | BGP-4 |
| IPv6 | RIPng | EIGRP para IPv6 | OSPFv3 | IS-IS para IPv6 | BGP-MP |

11.1.7

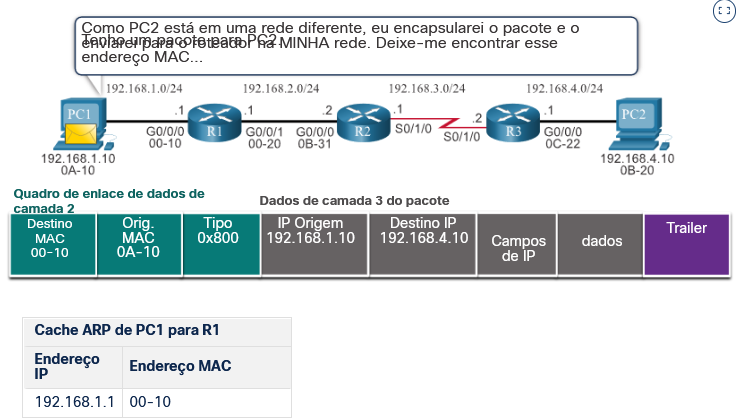
## Encaminhamento de ponta a ponta

A principal responsabilidade da função de encaminhamento de pacotes é encapsular pacotes no tipo de quadro de vínculo de dados apropriado para a interface de saída. Por exemplo, o formato de quadro de enlace de dados para um link serial pode ser o protocolo PPP (Point-to-Point), o protocolo HDLC (High-Level Data Link Control) ou algum outro protocolo de Camada 2.

**PC1 Envia pacote para PC2**

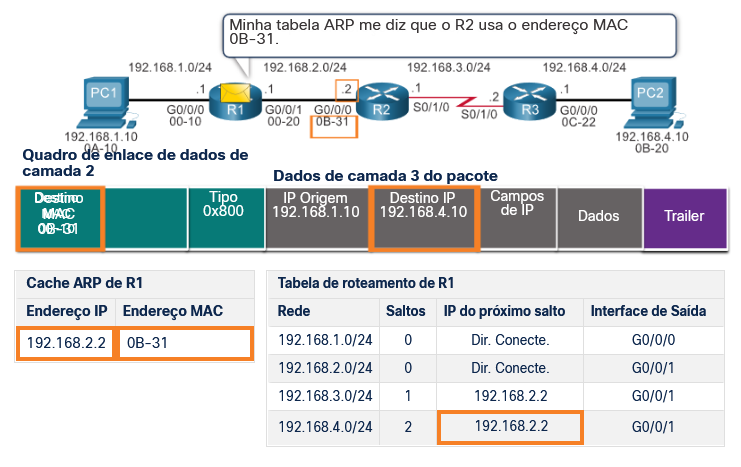
Na primeira animação, PC1 envia um pacote para PC2. Como o PC2 está em uma rede diferente, o PC1 encaminhará o pacote para seu gateway padrão. O PC1 procurará em seu cache ARP o endereço MAC do gateway padrão e adicionará as informações de quadro indicadas.

**Observação:** Se uma entrada ARP não existir na tabela ARP para o gateway padrão de 192.168.1.1, PC1 enviará uma solicitação ARP. O roteador R1 então retornaria uma resposta ARP com seu endereço MAC.



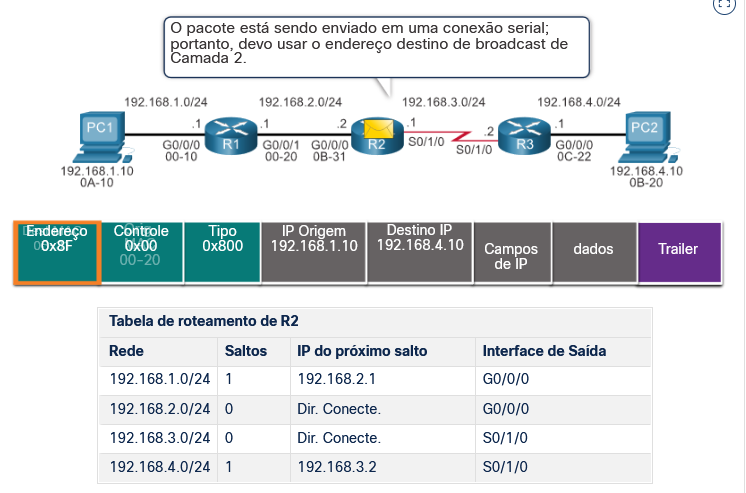
**R1 encaminha o pacote a PC2**

R1 agora encaminha o pacote para PC2. Como a interface de saída está em uma rede Ethernet, o R1 deve resolver o endereço IPv4 do próximo salto com um endereço MAC de destino usando sua tabela ARP. Se uma entrada ARP não existir na tabela ARP para a interface do próximo salto de 192.168.2.2, o R1 enviará uma solicitação ARP. R2 retornaria uma resposta ARP.



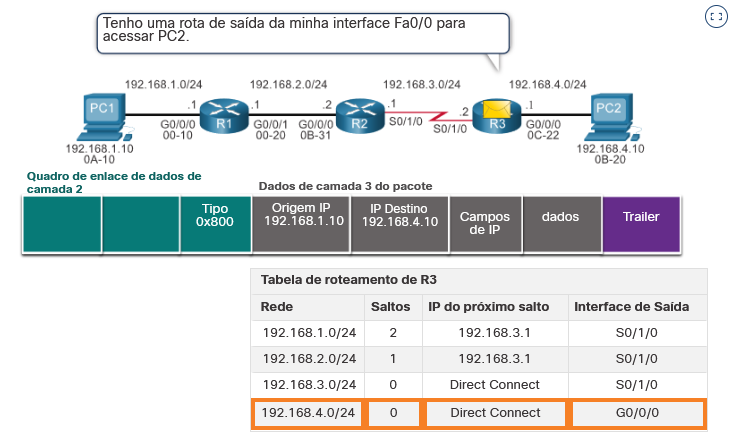
**R2 encaminha o pacote para R3**

R2 agora encaminha o pacote para R3. Como a interface de saída não é uma rede Ethernet, R2 não precisa resolver o endereço IPv4 do próximo salto com um endereço MAC destino. Quando a interface é uma conexão serial ponto-a-ponto (P2P), o roteador encapsula o pacote IPv4 no formato apropriado de quadro de enlace de dados usado pela interface de saída (HDLC, PPP etc.). Como não há endereços MAC nas interfaces seriais, R2 define o endereço destino de enlace de dados para um equivalente de um broadcast.



**R3 encaminha o pacote a PC2**

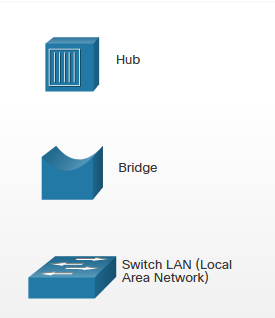
R3 agora encaminha o pacote para PC2. Como o endereço IPv4 de destino está em uma rede Ethernet diretamente conectada, o R3 deve resolver o endereço IPv4 de destino do pacote com o endereço MAC associado. Se a entrada não estiver na tabela ARP, o R3 enviará uma solicitação ARP de sua interface FastEthernet 0/0. O PC2 retornaria uma resposta ARP com seu endereço MAC.



11.1.9

## Hubs, Bridges, LAN Switches

Os ícones de topologia para hubs, pontes e switches LAN são mostrados na figura.



Um hub Ethernet atua como um repetidor de várias portas que recebe um sinal elétrico de entrada (dados) em uma porta. Em seguida, encaminha imediatamente um sinal regenerado para todas as outras portas. Os hubs usam processamento de camada física para encaminhar dados. They do not look at the source and destination MAC address of the Ethernet frame. Os hubs conectam a rede a uma topologia em estrela com o hub como ponto de conexão central. Quando dois ou mais dispositivos finais conectados a um hub enviam dados ao mesmo tempo, ocorre uma colisão elétrica, corrompendo os sinais. Todos os dispositivos conectados a um hub pertencem ao mesmo domínio de colisão. Apenas um dispositivo pode transmitir tráfego em um determinado momento em um domínio de colisão. Se ocorrer uma colisão, os dispositivos finais usam a lógica CSMA/CD para evitar a transmissão até que a rede fique sem tráfego. Devido ao baixo custo e à superioridade da comutação Ethernet, os hubs raramente são usados hoje.

As pontes têm duas interfaces e estão conectadas entre hubs para dividir a rede em vários domínios de colisão. Cada domínio de colisão pode ter apenas um remetente de cada vez. As colisões são isoladas pela ponte para um único segmento e não afetam dispositivos em outros segmentos. Assim como um switch, uma ponte toma decisões de encaminhamento com base em endereços MAC Ethernet. As pontes raramente são usadas em redes modernas.

Switches LAN são essencialmente pontes multiportas que conectam dispositivos a uma topologia em estrela. Assim como pontes, os switches segmentam uma LAN em domínios de colisão separados, um para cada porta de switch. Um switch toma decisões de encaminhamento com base em endereços MAC Ethernet. A figura mostra a série Cisco de switches 2960-X que são comumente usados para conectar dispositivos finais em uma LAN.

11.1.10

## Operação de Switch

Os switches usam endereços MAC para direcionar as comunicações de rede através do switch, para a porta apropriada e em direção ao destino. Um switch é composto de circuitos integrados e de um software que controla os caminhos dos dados através do switch. Para que um switch saiba qual porta usar para transmitir um quadro, primeiro ele deve saber quais dispositivos existem nas portas. Conforme o switch aprende a relação das portas com os dispositivos, ele constrói uma tabela chamada tabela de endereços MAC ou tabela de memória endereçável de conteúdo (CAM). A CAM é um tipo especial de memória usado em aplicativos de pesquisa em alta velocidade.

Os switches LAN determinam como lidar com quadros de dados de entrada mantendo a tabela de endereços MAC. Um switch constrói sua tabela de endereços MAC registrando o endereço MAC de cada dispositivo conectado a cada uma de suas portas. O switch usa as informações da tabela de endereços MAC para enviar frames destinados a um dispositivo específico pela porta à qual o dispositivo está conectado.

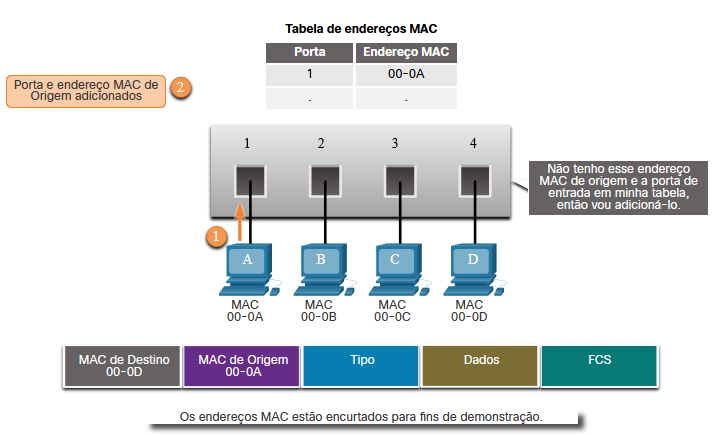
O processo de duas etapas a seguir é executado em todos os quadros Ethernet que entram em um switch.

**1\. Aprendizagem – Exame do Endereço MAC de Origem**

Cada quadro que entra em um switch é verificado para novas informações de endereço MAC que podem precisar ser aprendidas. Ele faz isso examinando o endereço MAC de origem do quadro e o número da porta onde o quadro entrou no switch. Se o endereço MAC de origem não estiver na tabela, ele será adicionado à tabela de endereços MAC junto com o número da porta de entrada, conforme mostrado na figura. Se o endereço MAC de origem não existir na tabela, o switch atualizará o cronômetro de atualização para essa entrada. Por padrão, a maioria dos switches Ethernet mantém uma entrada na tabela por cinco minutos.

A imagem é intitulada Aprender: Examine o endereço MAC de origem. A imagem contém três seções. Na seção inferior da imagem há uma representação de um quadro Ethernet. Os componentes do quadro da esquerda para a direita são: MAC de destino 00-0D, MAC de origem 00-0A, Tipo, Dados e FCS. Há uma isenção de responsabilidade na parte inferior que diz: os endereços MAC são encurtados para fins de demonstração. A seção do meio contém uma representação de um switch Ethernet com quatro portas rotuladas de 1 a 4. Há PCs mostrados conectados a cada porta, os PCs são rotulados PC-A MAC 00-0A, PC-B MAC 00-0B, PC-C MAC 00-0C e PC-D MAC 00-0D. Acima de PC-A há uma seta, rotulada 1, apontando do PC-A para a porta 1, Ao lado do switch há uma caixa de texto que diz: Eu não tenho esse endereço MAC souurce e a porta de entrada na minha tabela, então eu vou adicioná-lo. Na seção superior há uma tabela de duas colunas intitulada Tabela de Endereços MAC. As colunas na tabela são rotuladas como Porta e Endereço MAC. Ao lado da tabela de endereços MAC há uma caixa de texto rotulada 2, A caixa de texto diz: Porta e endereço MAC de origem adicionado. A primeira linha da tabela de endereços MAC possui a porta 1 e o endereço MAC 00-0A.

### Aprendizagem: Exame do Endereço MAC de Origem



A B C D 1 2 3 4 2

1

MAC  
00-0AMAC  
00-0BMAC  
00-0CMAC  
00-0D

|  |  |
| --- | --- |
| **Tabela de endereços MAC** | |
| **Porta** | **Endereço MAC** |
| 1 | 00-0A |
| . | . |

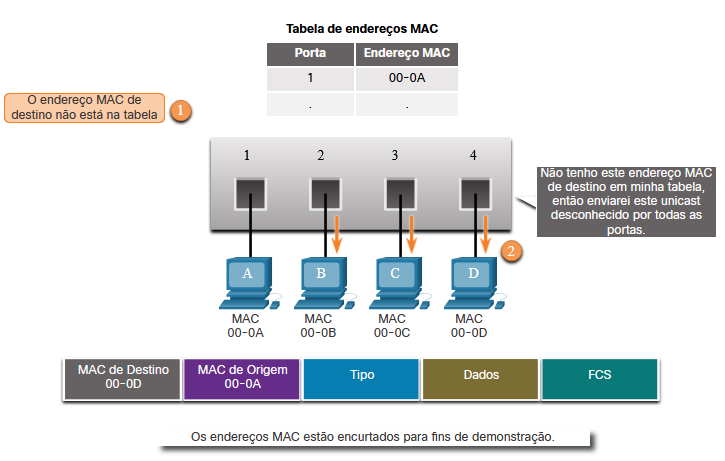
MAC de Destino  
00-0DMAC de Origem  
00-0APorta e endereço MAC de Origem adicionadosOs endereços MAC estão encurtados para fins de demonstração.TipoDadosFCSNão tenho esse endereço MAC de origem e a porta de entrada em minha tabela, então vou adicioná-lo.

**Observação:** se o endereço MAC de origem existe na tabela, mas em outra porta, o switch trata como uma nova entrada. A entrada é substituída usando o mesmo endereço MAC, mas com o número de porta mais atual. **2\. Encaminhamento – Exame do Endereço MAC de Destino**

Se o endereço MAC de destino for um endereço unicast, o switch procurará uma correspondência entre o endereço MAC de destino do quadro e uma entrada em sua tabela de endereços MAC. Se o endereço MAC de destino estiver na tabela, ele encaminhará o quadro pela porta especificada. Se o endereço MAC de destino não estiver na tabela, o switch encaminhará o quadro por todas as portas, exceto a porta de entrada, conforme mostrado na figura. Isso é chamado de unicast desconhecido.

A imagem é intitulada Encaminhamento: Examinando o endereço MAC de destino. A imagem contém três seções. Na seção inferior da imagem há uma representação de um quadro Ethernet. Os componentes do quadro da esquerda para a direita são: MAC de destino 00-0D, MAC de origem 00-0A, Tipo, Dados e FCS. Há uma isenção de responsabilidade na parte inferior que diz: os endereços MAC são encurtados para fins de demonstração. Na seção superior há uma tabela de duas colunas intitulada Tabela de Endereços MAC. As colunas na tabela são rotuladas como Porta e Endereço MAC. Ao lado da tabela de endereços MAC há uma caixa de texto rotulada 1. A caixa de texto diz: O endereço MAC de destino não está na tabela. A única linha na tabela de endereços MAC possui a porta 1 e o endereço MAC 00-0A. A seção do meio contém uma representação de um switch Ethernet com quatro portas rotuladas de 1 a 4. Há PCs mostrados conectados a cada porta, os PCs são rotulados PC-A MAC 00-0A, PC-B MAC 00-0B, PC-C MAC 00-0C e PC-D MAC 00-0D. Acima de PC-B, PC-C e PC-D são setas apontando para baixo de suas respectivas portas. Ao lado do switch, há uma caixa de texto que diz: Eu não tenho esse endereço MAC de destino em minha tabela, então enviarei esse unicast desconhecido por todas as portas.

### Encaminhamento: Examinando o endereço MAC de destino

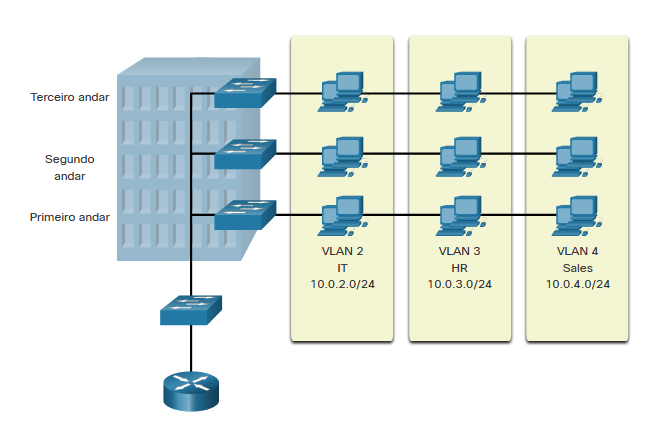


**Observação:** se o endereço MAC de destino for um endereço de broadcast ou multicast, o quadro será enviado por todas as portas, exceto a de entrada.

11.1.12

## VLANs

Dentro de uma rede comutada, as VLANs fornecem segmentação e flexibilidade organizacional. As VLANs oferecem uma maneira de agrupar dispositivos dentro de uma LAN. Um grupo de dispositivos em uma VLAN se comunica como se estivessem conectados ao mesmo segmento de rede. As VLANs são baseadas em conexões lógicas, em vez de conexões físicas.



As VLANs permitem que um administrador segmente redes com base em fatores como função, equipe de projeto ou aplicativo, sem levar em conta a localização física do usuário ou dispositivo, conforme mostrado na figura. Os dispositivos em uma VLAN atuam como se estivessem em sua própria rede independente, mesmo que compartilhem uma infraestrutura comum com outras VLANs. Qualquer porta do switch pode pertencer a uma VLAN. Pacotes de unicast, broadcast e multicast são encaminhados e inundados apenas para dispositivos finais na VLAN onde os pacotes são fornecidos. Cada VLAN é considerada uma rede lógica separada. Os pacotes destinados aos dispositivos que não pertencem a VLANs devem ser roteados por um dispositivo que permita roteamento.

Uma VLAN é um domínio de broadcast que pode abranger vários segmentos de LAN físicos. As VLANs melhoram o desempenho da rede, separando grandes domínios de transmissão em domínios menores. Se um dispositivo em uma VLAN envia um quadro Ethernet de transmissão, todos os dispositivos na VLAN recebem o quadro, mas os dispositivos em outras VLANs não.

As VLANs também impedem que usuários em VLANs diferentes espiem o tráfego uns dos outros. Por exemplo, mesmo que o RH e as Vendas estejam conectados ao mesmo switch na figura, o switch não encaminhará o tráfego entre as VLANs de RH e de Vendas. Isso permite que um roteador ou outro dispositivo use listas de controle de acesso para permitir ou negar o tráfego. As listas de acesso são discutidas com mais detalhes posteriormente neste capítulo. Por enquanto, lembre-se de que as VLANs podem ajudar a limitar a quantidade de visibilidade de dados em suas LANs.

11.1.13

## STP

Redundância de rede é primordial para a manutenção da confiabilidade da rede. Diversos links físicos entre dispositivos propiciam caminhos redundantes. A rede poderá continuar a operar quando um único link ou porta tiver falhado. Links redundantes também podem compartilhar a carga de tráfego e aumentar a capacidade.

Vários caminhos precisam ser gerenciados de modo que os loops de Camada 2 não sejam criados. Os melhores caminhos são selecionados e um caminho alternativo fica prontamente disponível se o caminho principal falhar. O Spanning Tree Protocol é usado para manter um caminho livre de loop na rede da Camada 2, a qualquer momento.

A redundância aumenta a disponibilidade da topologia de rede, protegendo-a de um único ponto de falha, como um cabo ou um switch com falha na rede. Quando a redundância física é introduzida em um projeto, ocorrem loops e quadros duplicados. Os loops e quadros duplicados têm consequências graves para uma rede comutada. O STP foi desenvolvido para resolver esses problemas.

O STP garante que há apenas um caminho lógico entre todos os destinos da rede, bloqueando intencionalmente os caminhos redundantes que podem causar um loop. Uma porta é considerada bloqueada quando os dados do usuário são impedidos de entrar ou de sair daquela porta. Isso não inclui os quadros da unidade de dados de protocolo de bridge (BPDU) que são usados pelo STP para evitar loops. Bloquear os caminhos redundantes é fundamental para evitar loops na rede. Os caminhos físicos ainda existirão para fornecer redundância, mas esses caminhos ficarão desativados para evitar que ocorram loops. Se o caminho for necessário em algum momento para compensar uma falha no cabo ou switch de rede, o STP recalculará os caminhos e desbloqueará as portas necessárias para permitir que o caminho redundante torne-se ativo.

11.1.14

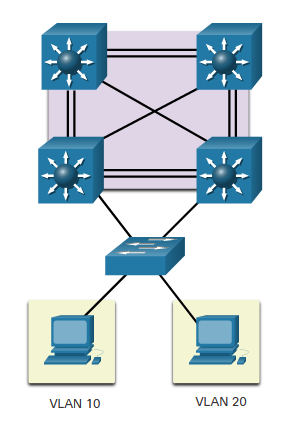
**Comutação Multilayer**

Switches multicamadas (também conhecidos como switches de Camada 3) não apenas executam switching de Camada 2, mas também quadros de encaminhamento baseados em informações de Camadas 3 e 4. Todos os switches multicamadas Cisco Catalyst suportam os seguintes tipos de interfaces da Camada 3:

* **Porta roteada** - Uma interface pura de Camada 3 semelhante a uma interface física em um roteador Cisco IOS.
* **Interface virtual do switch (SVI)** - Uma interface de VLAN virtual para o roteamento entre VLANs. Em outras palavras SVIs são as interfaces de VLAN roteadas virtuais.

**Portas roteadas**

Uma porta roteada é uma porta física que atua de forma semelhante a uma interface em um roteador, conforme mostrado na figura. Diferentemente de uma porta de acesso, uma porta roteada não está associada a uma VLAN. Uma porta roteada se comporta como uma interface de roteador regular. Além disso, como a funcionalidade de Camada 2 foi removida, os protocolos de Camada 2, como o STP, não funcionam em uma interface roteada. Entretanto, alguns protocolos, como LACP e EtherChannel, funcionam na Camada 3. Diferentemente dos roteadores Cisco IOS, as portas roteadas em um switch Cisco IOS não suportam subinterfaces.

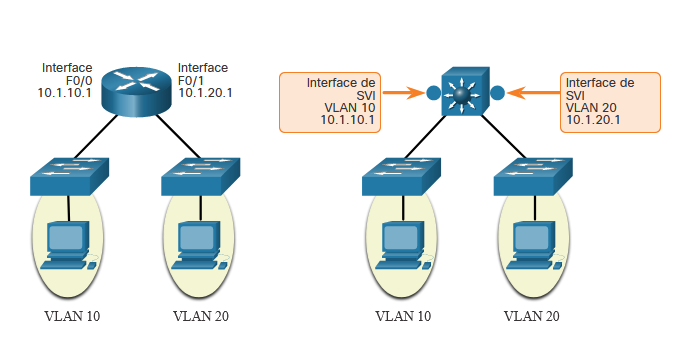


**Interfaces virtuais do switch**

Uma SVI é uma interface virtual configurada em um switch multicamada, como mostrado na figura. Ao contrário dos switches básicos de Camada 2 discutidos acima, um switch multicamada pode ter vários SVIs. Uma SVI pode ser criada para qualquer VLAN que exista no switch. Uma SVI é considerada virtual porque não há uma porta física dedicada à interface. Ela pode executar as mesmas funções para a VLAN que uma interface de roteador e pode ser configurada de forma similar a uma interface do roteador (isto é, endereço IP, ACLs de entrada/saída etc,). A SVI para a VLAN fornece o processamento de Camada 3 para pacotes para ou de todas as portas de switch associadas a essa VLAN.

A imagem é intitulada Interface virtual do switch. A imagem mostra dois diagramas de rede, lado a lado. No primeiro diagrama, há um ícone representando um roteador com duas interfaces FastEthernet. Uma interface é rotulada Interface F0/0, 10.1.10.1. A segunda interface é rotulada Interface F0/1, 10.1.20.1. Abaixo do roteador estão dois ícones representando switches LAN Ethernet. Há uma linha de cada switch conectando-o ao roteador. Abaixo dos dois switches estão dois ovais amarelos, um rotulado como VLAN 10 e o outro com VLAN 20. Dentro de cada oval amarelo há um PC com uma linha conectando-o a um dos switches LAN. O segundo diagrama é o mesmo que o primeiro diagrama, exceto que o ícone do roteador foi substituído por um ícone de switch multicamadas. Em ambos os lados do ícone de switch multicamada, há caixas de texto conectadas por setas ao switch multicamada. Na caixa à esquerda está o texto: Interface SVI, VLAN 10, 10.1.10.1. Na caixa de texto à direita está o texto: Interface SVI, VLAN 20, 10.1.20.1.

### Interface virtual do switch



# Comunicações sem fio

11.2.2

## LANs sem fio versus com fio

As WLANs usam Freqüências de Rádio (RF) em vez de cabos na camada física e na subcamada MAC da camada de enlace de dados. As WLANs compartilham uma origem semelhante com as LANs Ethernet. O IEEE adotou o portfólio 802 LAN/MAN de padrões de arquitetura de rede de computadores. Os dois grupos de trabalho dominantes 802 são 802.3 Ethernet, que definiu Ethernet para LANs com fio, e 802.11 que definiu Ethernet para WLANs. Existem diferenças importantes entre os dois.

As WLANs também diferem das LANs com fio da seguinte forma:

* As WLANs conectam clientes à rede por meio de um ponto de acesso sem fio (AP) ou roteador sem fio, em vez de um switch Ethernet.
* As WLANs conectam dispositivos móveis que geralmente são alimentados por bateria, em vez de dispositivos LAN conectados. As placas de rede sem fio tendem a reduzir a duração da bateria de um dispositivo móvel.
* WLANs suportam hosts que disputam acesso na mídia de RF (bandas de frequência). O 802.11 prescreve a prevenção de colisões (CSMA/CA) em vez de detecção de colisões (CSMA/CD) para acesso à mídia para evitar colisões proativamente dentro da mídia.
* As WLANs usam um formato de quadro diferente das LANs Ethernet com fio. As WLANs exigem informações adicionais no cabeçalho da Camada 2 do quadro.
* As WLANs levantam mais problemas de privacidade porque as frequências de rádio podem chegar fora das instalações.

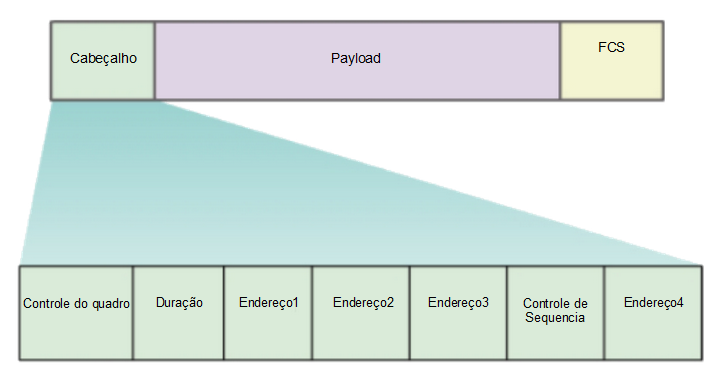
A tabela resume as diferenças entre LANs sem fio e com fio.

| **Característica** | **802.11 LAN sem fio** | **802.3 LANs Ethernet com fio** |
| --- | --- | --- |
| **Camada física** | Radiofrequência (RF) | cabos físicos |
| **Acesso à mídia** | prevenção de colisão | detecção de colisão |
| **Disponibilidade** | qualquer pessoa com uma placa de rede sem fio ao alcance de um ponto de acesso | conexão de cabo físico necessária |
| **Interferência de sinal** | sim | mínima |
| **Regulamentações** | diferentes regulamentos por país | O padrão IEEE dita |

11.2.3

**Estutura do quadro 802.11**

Lembre-se de que todos os quadros da camada 2 consistem em uma seção de cabeçalho, carga útil e sequência de verificação de quadro (FCS - Frame Check Sequence). O formato de quadro 802.11 é semelhante ao formato de quadro Ethernet, exceto pelo fato de conter mais campos, conforme mostrado na figura.



Todos os quadros sem fio 802.11 contêm os seguintes campos:

* **Controle do quadro** - Isso identifica o tipo de quadro sem fio e contém subcampos para versão do protocolo, tipo de quadro, tipo de endereço, gerenciamento de energia e configurações de segurança.
* **Duração** - Isso é normalmente usado para indicar a duração restante necessária para receber a próxima transmissão de quadro.
* **Endereço1** - Geralmente, contém o endereço MAC do dispositivo sem fio ou AP de recebimento.
* **Endereço2** - Geralmente, contém o endereço MAC do dispositivo sem fio transmissor ou ponto de acesso
* **Endereço3** - Às vezes, isso contém o endereço MAC do destino, como a interface do roteador (gateway padrão) à qual o ponto de acesso está conectado.
* **Controle de sequencia** - Ele contém informações para controlar o seqüenciamento e os quadros fragmentados.
* **Endereço4** - Isso geralmente está ausente porque é usado apenas no modo ad hoc.
* **Payload** - Este contém os dados para transmissão.
* **FCS** - Isso é usado para controle de erro da camada 2.

11.2.4

## CSMA/CA

As WLANs são configurações de mídia compartilhada half-duplex. Half-duplex significa que apenas um cliente pode transmitir ou receber a qualquer momento. Mídia compartilhada significa que todos os clientes sem fio podem transmitir e receber no mesmo canal de rádio. Isso cria um problema porque um cliente sem fio não pode ouvir enquanto está enviando, o que torna impossível detectar uma colisão.

Para resolver esse problema, as WLANs usam o acesso múltiplo com detecção de operadora com prevenção de colisão (CSMA / CA) como o método para determinar como e quando enviar dados na rede. Um cliente sem fio faz o seguinte:

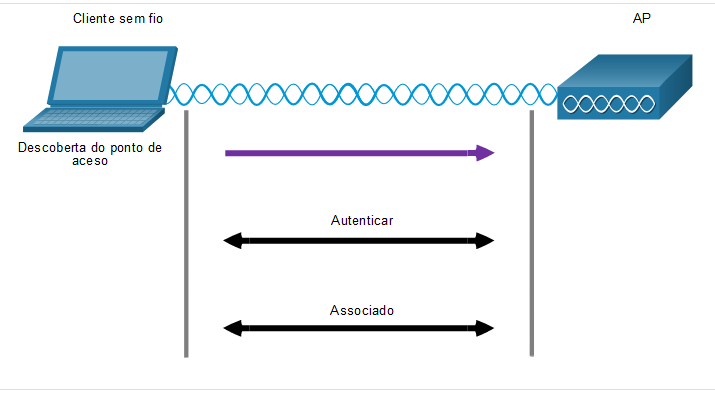
1. Ouve o canal para ver se ele está ocioso, o que significa que nenhum outro tráfego está atualmente no canal. O canal também é chamado de portadora.
2. Envia uma mensagem pronta para enviar (RTS) para o ponto de acesso para solicitar acesso dedicado à rede.
3. Recebe uma mensagem clara para enviar (CTS) do ponto de acesso que concede acesso ao envio.
4. Se o cliente sem fio não receber uma mensagem CTS, ele aguardará um período aleatório antes de reiniciar o processo.
5. Depois de receber o CTS, ele transmite os dados.
6. Todas as transmissões são confirmadas. Se um cliente sem fio não receber uma confirmação, ele assume uma colisão e reinicia o processo.

11.2.5

## Associação de cliente sem fio e ponto de acesso

Para que os dispositivos sem fio se comuniquem através de uma rede, eles devem primeiro se associar a um Ponto de acesso ou roteador sem fio. Uma parte importante do processo 802.11 é descobrir uma WLAN e subsequentemente conectar-se a ela. Os dispositivos sem fio concluem o seguinte processo de três estágios, conforme mostrado na figura:

* Descobrir um ponto de acesso sem fio
* Autenticar-se no ponto de acesso
* Associar-se ao ponto de acesso



Para ter uma associação bem-sucedida, um cliente sem fio e um ponto de acesso devem concordar com parâmetros específicos. Os parâmetros devem ser configurados no ponto de acesso e subseqüentemente no cliente para permitir a negociação de uma associação bem-sucedida.

* **SSID** - O nome SSID aparece na lista de redes sem fio disponíveis em um cliente. Em organizações maiores que usam várias VLANs para segmentar o tráfego, cada SSID é mapeado para uma VLAN. Dependendo da configuração da rede, vários pontos de acesso em uma rede podem compartilhar um SSID comum.
* **Senha** - Isso é necessário no cliente sem fio para se autenticar no ponto de acesso.
* **Modo de rede** - refere-se aos padrões de WLAN 802.11a/b/g/n/ac/ad. Os pontos de acesso e roteadores sem fio podem operar no modo misto, o que significa que eles podem oferecer suporte simultâneo a clientes que se conectam por vários padrões.
* **Modo de segurança** - Isso se refere às configurações de parâmetros de segurança, como WEP, WPA ou WPA2. Sempre habilite o nível de segurança mais alto suportado.
* **Configurações do canal** - Refere-se às bandas de frequência usadas para transmitir dados sem fio. Os roteadores sem fio e os APs podem verificar os canais de frequência de rádio e selecionar automaticamente uma configuração de canal apropriada. O canal também pode ser configurado manualmente se houver interferência com outro ponto de acesso ou dispositivo sem fio.

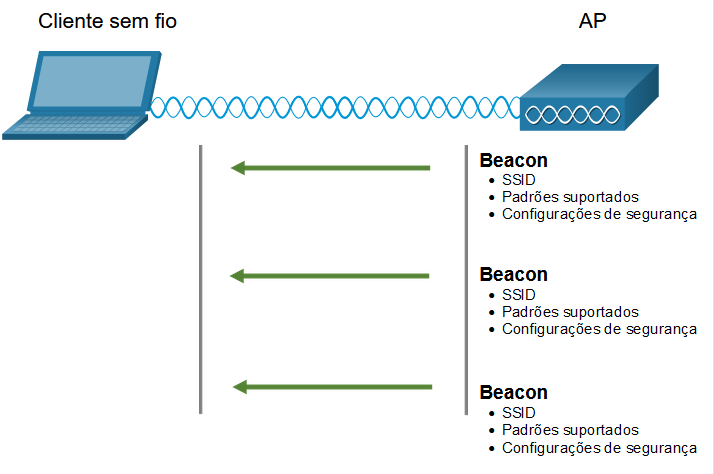
11.2.6

**Modo de descoberta passiva e ativa**

Os dispositivos sem fio devem descobrir e conectar-se a um ponto de acesso ou roteador sem fio. Os clientes sem fio se conectam ao ponto de acesso usando um processo de verificação (verificação). Este processo pode ser passivo ou ativo.

Modo passivo

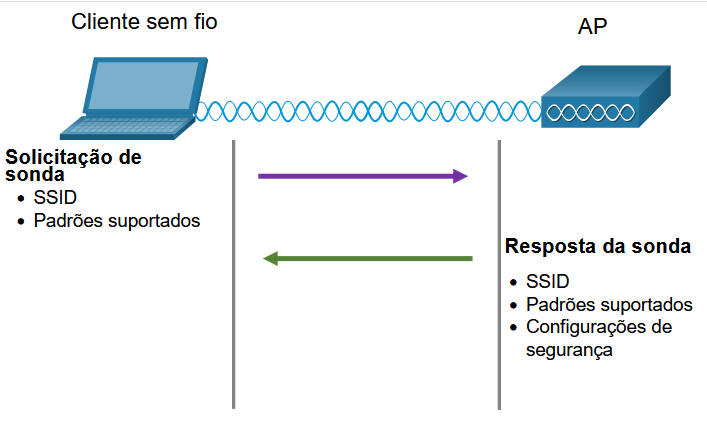
No modo passivo, o ponto de acesso anuncia abertamente seu serviço enviando periodicamente quadros de beacon de transmissão contendo o SSID, padrões suportados e configurações de segurança. O objetivo principal do beacon é permitir que os clientes sem fio aprendam quais redes e pontos de acesso estão disponíveis em uma determinada área. Isso permite que os clientes sem fio escolham qual rede e ponto de acesso usar.



Modo ativo

No modo ativo, os clientes sem fio devem saber o nome do SSID. O cliente sem fio inicia o processo transmitindo um quadro de solicitação de análise em vários canais. A solicitação de análise inclui o nome SSID e os padrões suportados. Os pontos de acesso configurados com o SSID enviarão uma resposta do probe que inclui o SSID, os padrões suportados e as configurações de segurança. O modo ativo pode ser necessário se um ponto de acesso ou roteador sem fio estiver configurado para não transmitir quadros de beacon.

Um cliente sem fio também pode enviar uma solicitação de análise sem um nome SSID para descobrir redes WLAN próximas. Os pontos de acesso configurados para transmitir quadros de beacon responderiam ao cliente sem fio com uma resposta do probe e forneceriam o nome SSID. Os pontos de acesso com o recurso SSID de transmissão desativado não respondem.



Quais são dois eventos que podem ocorrer na Etapa 1 (Descoberta) do processo de associação cliente e AP? (Escolha duas.)

Ouvir quadros de beacon para encontrar SSIDs WLAN (modo passivo)

Enviar uma solicitação de teste para o AP com ou sem um SSID conhecido (modo ativo)

Quais são dois eventos que podem ocorrer na Etapa 2 (Autenticação) do processo de associação cliente e AP? (Escolha duas.)

Concordar com o AP para compartilhar a autenticação aberta

Iniciar o processo de autenticação de chave compartilhada

Quais são os três eventos que podem ocorrer na Etapa 3 (Associação) do cliente e processo de associação AP? (Escolha três.)

Receber o endereço MAC do AP (BSSID)

Enviar o endereço MAC do cliente para AP

Receber o identificador de associação da AP (AID)

11.2.8

**Dispositivos sem fio - AP, LWAP e WLC**

Uma implementação comum de dados sem fio permite que dispositivos se conectem sem fio por meio de uma LAN. Em geral, uma LAN sem fio requer pontos de acesso sem fio e clientes que tenham NICs sem fio. Os roteadores sem fio domésticos e de pequenas empresas integram as funções de um roteador, comutador e ponto de acesso em um dispositivo, conforme mostrado na figura. Observe que em redes pequenas, o roteador sem fio pode ser o único AP porque apenas uma área pequena requer cobertura sem fio. Em redes maiores, pode haver muitos APs.

Todas as funções de controle e gerenciamento dos APs em uma rede podem ser centralizadas em um Wireless LAN Controller (WLC). Ao usar uma WLC, os APs não atuam mais de forma autônoma, mas atuam como APs leves (LWAPs). Os LWAPs apenas encaminham dados entre a LAN sem fio e a WLC. Todas as funções de gerenciamento, como definição de SSIDs e autenticação, são conduzidas na WLC centralizada, em vez de em cada AP individual. Um grande benefício da centralização das funções de gerenciamento de AP na WLC é a configuração simplificada e o monitoramento de vários pontos de acesso, entre muitos outros benefícios.

Qual dispositivo deve se conectar a outro dispositivo para obter acesso à rede?

Dispositivos finais

Qual dispositivo conecta clientes sem fio à rede?

Ponto de acesso sem fio (WAP)

Qual dispositivo usa endereços MAC para determinar a porta de saída?

Switch

# Resumo de dispositivos de comunicação de rede

11.3.1

## O que aprendi neste módulo?

**Dispositivos de Rede**

Neste módulo, você aprendeu que os dispositivos finais conectados a uma LAN se conectam a outras LANs usando uma interrede de dispositivos intermediários, como roteadores e switches.

Os roteadores são dispositivos de camada de rede (ou seja, Camada 3) e usam o processo de roteamento para encaminhar pacotes de dados entre redes ou sub-redes. Os roteadores fornecem:

* Determinação de caminho — O roteador cria uma tabela de roteamento contendo uma lista de todas as rotas de rede conectadas diretamente e remotas conhecidas e como alcançá-las. As informações na tabela de roteamento são configuradas manualmente usando rotas estáticas ou descobertas dinamicamente usando um protocolo de roteamento dinâmico (por exemplo, RIP, OSPF, EIGRP, BGP.) O processamento da decisão de encaminhamento de pacotes é baseado na correspondência mais longa e determina como encapsular o pacote e encaminhá-lo para a interface de saída correta.
* Serviços de encaminhamento de pacotes — Os pacotes de entrada passam pelo processo de determinação de caminho para identificar a interface de saída. O roteador então fornece uma função de comutação encapsulando o pacote de saída no tipo de quadro de enlace de dados apropriado e encaminhando-o para fora da interface de saída.

Os switches segmentam uma LAN em domínios de colisão separados, um para cada porta de switch. Um switch toma decisões de encaminhamento com base nos endereços MAC Ethernet contidos no quadro Ethernet. O switch usa o endereço de origem do quadro para saber mais sobre novos endereços MAC e o endereço MAC de destino para identificar a porta de saída para encaminhar o quadro. Os switches suportam a criação de VLANs (ou seja, domínios de transmissão lógicos) para melhorar o desempenho e a segurança da rede. Para redundância, os switches geralmente são interconectados para fornecer caminhos alternativos que podem causar problemas de loop da Camada 2. Os switches são configurados com o STP (Spanning Tree Protocol) para manter um caminho de Camada 2 sem loop bloqueando intencionalmente caminhos redundantes que podem causar um loop.

Switches multicamadas (também conhecidos como switches de Camada 3) não apenas executam switching de Camada 2, mas também quadros de encaminhamento baseados em informações de Camadas 3 e 4. Um switch multicamada Cisco Catalyst suporta portas roteadas e interfaces virtuais de switch (SVIs).

**Comunicações sem fio**

Os dispositivos de rede sem fio se conectam a um ponto de acesso (AP) ou WLC (Wireless LAN Controller) processando o padrão 802.11. O formato de quadro 802.11 é semelhante ao formato de quadro Ethernet, exceto que contém campos adicionais. Os dispositivos WLAN usam o acesso múltiplo com detecção de portadora com prevenção de colisão (CSMA / CA) como método para determinar como e quando enviar dados na rede. Para se conectar à WLAN, os dispositivos sem fio concluem um processo de três estágios para descobrir um AP sem fio, autenticar com o AP e associar com o AP.

Os APs podem ser configurados de forma autônoma (individualmente) ou usando uma WLC para simplificar a configuração e o monitoramento de vários pontos de acesso.

Para qual modo de descoberta um AP gerará mais tráfego em uma WLAN?

Modo passivo

Tópico 11.2.0 - Os dois modos de descoberta são passivos e ativos. Ao operar no modo passivo, um AP gerará mais tráfego à medida que transmite continuamente quadros de beacon para clientes potenciais. No modo ativo, o cliente inicia o processo de descoberta em vez do AP. O modo misto refere-se às configurações do modo de rede e o modo aberto refere-se às configurações de parâmetros de segurança.

Qual parâmetro é comumente usado para identificar um nome de rede sem fio quando um AP sem fio está sendo configurado?

SSID

Tópico 11.2.0 - O SSID é usado para nomear uma rede sem fio. Este parâmetro é necessário para que um cliente sem fio se conecte a um ponto de acesso sem fio.

Quais são os dois protocolos considerados protocolos de roteamento do vetor de distância? (Escolha duas.)

EIGRP

RIP

Tópico 11.1.0 - RIP e EIGRP são considerados protocolos de roteamento vetorial de distância. OSPF e ISIS são protocolos de roteamento link-state. BGP é um protocolo de roteamento de vetor de caminho.

Qual informação um switch Ethernet examina e usa para criar sua tabela de endereços?

Endereço MAC origem

Tópico 11.1.0 - Um switch Ethernet examina o endereço MAC de origem de um quadro de entrada. Se o endereço MAC de origem não estiver na tabela de endereços MAC, o switch irá adicioná-lo à tabela com a porta Ethernet de entrada associada.

Qual cabeçalho de camada OSI é reescrito com novas informações de endereçamento por um roteador ao encaminhar entre segmentos de LAN?

Camada 2

Tópico 11.1.0 - Quando um roteador encaminha o tráfego entre segmentos de LAN, ele encapsula o quadro da Camada 2 para determinar o caminho da Camada 3. Depois que o caminho da Camada 3 for determinado, o roteador encapsula o pacote da Camada 3 em um novo quadro da Camada 2 com novas informações de endereçamento da Camada 2 para o segmento de LAN de destino.

Em que camada do modelo OSI os roteadores operam?

Camada 3

Tópico 11.1.0 - Os roteadores operam na Camada 3 do modelo OSI e encaminham pacotes entre redes lógicas.

Qual parâmetro sem fio se refere às bandas de frequência usadas para transmitir dados para um ponto de acesso sem fio?

Configuração de canal

Tópico 11.2.0 - Um ponto de acesso pode ser configurado manualmente para uma banda de frequência ou canal específico para evitar interferência com outros dispositivos sem fio na área.

Qual é a função de um dispositivo intermediário em uma rede?

Determina o caminho e direciona dados ao longo do caminho até o destino final

Topic 11.1.0 - Os processos em execução nos dispositivos de rede intermediários desempenham funções como a regeneração e a retransmissão de sinais de dados, mantendo informações sobre quais caminhos existem pela rede e pela rede interna, direcionando dados por caminhos alternativos quando houver uma falha de link e permitindo ou negando o fluxo de dados, com base em configurações de segurança.

Que informações um switch Ethernet examina e usa para encaminhar um quadro?

Endereço MAC destino

Tópico 11.1.0 - Um switch é um dispositivo de Camada 2 que usa endereços MAC de origem para criar uma tabela de endereços MAC (uma tabela CAM) e endereços MAC de destino para encaminhar quadros.

Qual dispositivo pode controlar e gerenciar um grande número de APs corporativos?

WLC

Tópico 11.2.0 - Um controlador de LAN sem fio (WLC) pode ser configurado para gerenciar vários pontos de acesso leves (LWAPs). Na WLC, um administrador de rede pode configurar SSIDs, segurança, endereçamento IP e outros parâmetros de rede sem fio em um ambiente de gerenciamento centralizado.

Quais são as duas funções normalmente desempenhadas por um roteador sem fio usado em uma casa ou empresa de pequeno porte? (Escolha duas.)

Ponto de acesso

Switch Ethernet

Tópico 11.2.0 - Além de sua função de roteador, um roteador sem fio SOHO típico atua como um ponto de acesso sem fio e um comutador Ethernet. RADIUS authentication is provided by an external server. O WLAN controler é usado em implantações corporativas para gerenciar grupos de pontos de acesso leves. Um repetidor é um dispositivo que aprimora um sinal recebido e o retransmite.

Qual tecnologia é usada para evitar loops da Camada 2?

STP (Spanning Tree Protocol)

Tópico 11.1.0 - O STP (Spanning Tree Protocol) está habilitado em switches para impedir que loops de Camada 2 se formem quando há caminhos físicos redundantes.

Que termo descreve corretamente o método de roteamento entre VLANs da SVI?

A SVI é necessária para cada VLAN

Tópico 11.1.0 - Para criar o roteamento SVI entre VLANs em um switch da Camada 3, a VLAN deve existir no banco de dados e o SVI deve ser criado explicitamente. A única exceção é a VLAN1, criada por padrão.

Como os designs de endereçamento de IP são afetados por implementações de VLAN?

Cada VLAN Precisa ter um endereço de rede diferente

Tópico 11.1.0 - Cada VLAN requer seu próprio número de rede, endereço de broadcast e endereços IP válidos porque cada VLAN é uma rede separada. Os esquemas de endereçamento de IP são frequentemente projetados integrando os números da VLAN

12.0.1

## Por que devo cursar este módulo?

Com as muitas ameaças à segurança da rede, como as redes podem ser projetadas para proteger recursos de dados e garantir que os serviços de rede sejam fornecidos conforme necessário? A infra-estrutura de segurança de rede define a forma como os dispositivos são conectados entre si para obter comunicações seguras de ponta a ponta. Assim como existem muitos tamanhos de redes, há também muitas maneiras de construir uma infraestrutura de rede segura. No entanto, existem alguns designs padrão que a indústria de rede recomenda que sejam alcançadas redes que estejam disponíveis e sejam seguras. Este capítulo abrange o funcionamento básico das infra-estruturas de rede, os vários dispositivos de segurança da rede e os serviços de segurança utilizados para monitorizar e manter a transmissão segura e eficiente de dados.

12.0.2

## O que vou aprender neste módulo?

**Título do Módulo:** Infraestrutura de segurança de rede

**Objetivo do Módulo**: Explicar como os dispositivos e serviços são usados para aumentar a segurança da rede.

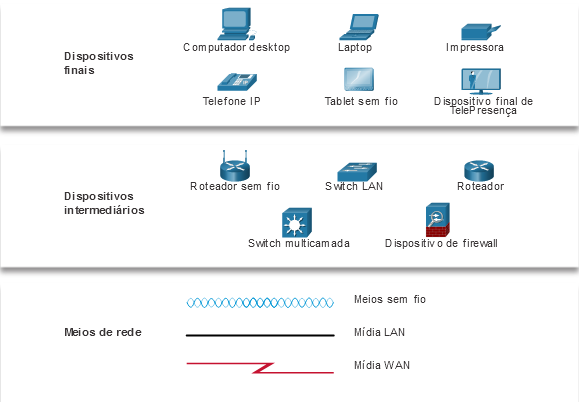
| **Título do Tópico** | **Objetivo do Tópico** |
| --- | --- |
| Topologias de rede | Explicar como os projetos de rede influenciam o fluxo de tráfego pela rede. |
| Dispositivos de segurança | Explicar como os dispositivos especializados são usados para aprimorar a segurança da rede. |
| Serviços de segurança | Explicar como os serviços de rede melhoram a segurança da rede. |

# Topologias de rede

12.1.1

## Representações de Rede

Arquitetos e administradores de rede devem ser capazes de mostrar como suas redes serão. Eles precisam ser capazes de ver facilmente quais componentes se conectam a outros componentes, onde eles serão localizados e como eles serão conectados. Os diagramas de redes geralmente usam símbolos, como os mostrados na figura, para representar os diferentes dispositivos e conexões que compõem uma rede.



A imagem mostra símbolos usados em diagramas de rede. At the top are the following end devices: desktop computer, laptop, printer, IP phone, wireless tablet, and TelePresence endpoint. No meio, estão os seguintes dispositivos intermediários: roteador sem fio, switch LAN, roteador, switch multicamada e dispositivo de firewall. Na parte inferior estão as seguintes mídias de rede: ondas azuis representando mídia sem fio, uma linha preta sólida representando mídia LAN e um parafuso de iluminação vermelho representando mídia WAN.

**Dispositivos finais**Computador desktopLaptopImpressoraTelefone IPTablet sem fioDispositivo final de TelePresença**Dispositivos intermediários**Roteador sem fioSwitch LANRoteadorSwitch multicamadaDispositivo de firewall**Meios de rede**Meios sem fioMídia LANMídia WAN

Um diagrama fornece uma maneira fácil de entender como os dispositivos se conectam em uma rede grande. Esse tipo de “fotografia” de uma rede é conhecido como um diagrama de topologia. A capacidade de reconhecer as representações lógicas dos componentes físicos de rede é crucial para se permitir visualizar a organização e a operação de uma rede.

Além dessas representações, é utilizada terminologia especializada para descrever como cada um desses dispositivos e mídias se conectam:

* **Placa de interface de rede (NIC)** - Uma NIC conecta fisicamente o dispositivo final à rede.
* **Porta física** - Um conector ou tomada em um dispositivo de rede onde a mídia se conecta a um dispositivo final ou outro dispositivo de rede.
* **Interface** - Portas especializadas em um dispositivo de rede que se conectam a redes individuais. Como os roteadores conectam redes, as portas em um roteador são chamadas de interfaces de rede.

**Observação**: Os termos porta e interface são freqüentemente usados alternadamente.

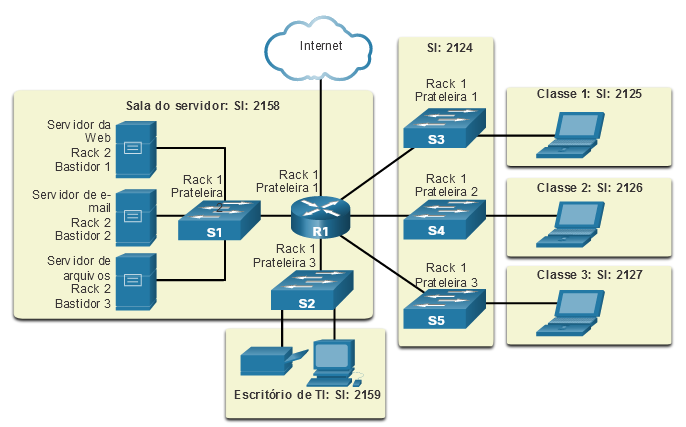
12.1.2

## Diagramas de Topologia

Os diagramas de topologia são documentação obrigatória para qualquer pessoa que trabalhe com uma rede. Eles fornecem um mapa visual de como a rede está conectada. Existem dois tipos de diagramas de topologia: físicos e lógicos.

**Diagramas de topologia física**

Os diagramas de topologia física ilustram a localização física dos dispositivos intermediários e a instalação dos cabos, conforme mostrado na figura. Você pode ver que as salas em que esses dispositivos estão localizados estão rotuladas nesta topologia física.



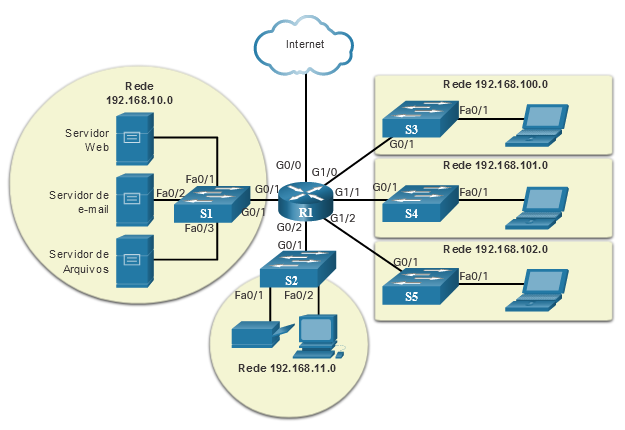
A topologia da rede física mostra seis salas, cada uma destacada em uma caixa amarela clara, com vários dispositivos de rede e cabeamento. No lado esquerdo está a sala do servidor rotulada sala 2158. Ele contém um roteador rotulado R1 montado no rack 1 prateleira com seis conexões de cabo. Um cabo na parte superior se conecta a uma nuvem rotulada como Internet. Um cabo à esquerda se conecta a um interruptor rotulado S1 montado no rack 1 prateleira 2. S1 está conectado a três servidores: um servidor web montado no rack 2 prateleira 1, um servidor de e-mail montado no rack 2 prateleira 2, e um servidor de arquivos montado no rack 2 prateleira 3. Um cabo conectado à parte inferior do R1 se conecta a um interruptor rotulado S2 montado no rack 1 prateleira 3. O S2 tem duas conexões que levam a uma impressora e um PC no escritório de TI rotulado sala 2159. R1 tem três cabos à direita conectados a três interruptores localizados na sala 2124. O interruptor superior é rotulado S3 e montado no rack 1 prateleira 1. O interruptor do meio é rotulado S4 e montado no rack 1 prateleira 2. O interruptor inferior é rotulado S5 e montado no rack 1 prateleira 3. S3 tem um cabo à esquerda conectado a um laptop em uma sala rotulada classe 1 quarto 2125. S4 tem um cabo à esquerda conectado a um laptop em uma sala rotulada classe 2 quarto 2126. S5 tem um cabo à esquerda conectado a um laptop em uma sala rotulada classe 3 quarto 2127.

R1 S1 S2 S3 S4

S5

InternetServidor de e-mail  
Rack 2  
Bastidor 2Servidor da Web  
Rack 2  
Bastidor 1Servidor de arquivos  
Rack 2  
Bastidor 3Rack 1  
Prateleira 2Rack 1  
Prateleira 1Rack 1  
Prateleira 2Rack 1  
Prateleira 1Rack 1  
Prateleira 3Rack 1  
Prateleira 3Sala do servidor: Sl: 2158Escritório de TI: Sl: 2159Classe 1: Sl: 2125Classe 2: Sl: 2126Classe 3: Sl: 2127Sl: 2124

**Diagramas de topologia lógica**



Diagramas de topologia lógica ilustram dispositivos, portas e o esquema de endereçamento da rede, conforme mostrado na figura. Você pode ver quais dispositivos finais estão conectados a quais dispositivos intermediários e que mídia está sendo usada.

A topologia de rede lógica mostra dispositivos, rótulos de porta e o esquema de endereçamento de rede. No meio da imagem é um roteador rotulado R1. Uma porta rotulada G0/0 se conecta a uma nuvem na Internet com o rótulo superior. Uma porta rotulada G0/1 conecta-se à esquerda a um switch rotulado S1 na porta G0/1. S1 está conectado a três servidores. S1 e os servidores são destacados em um círculo amarelo claro com a rede 192.168.10.0 escrita na parte superior. A porta F0/1 em S1 conecta a um servidor web. A porta F0/2 em S1 se conecta a um servidor de e-mail. A porta F0/3 em S1 se conecta a um servidor de arquivos. A porta F0/1 em R1 se conecta na parte inferior a um switch rotulado S2. S2 se conecta a uma impressora e um PC, todos os quais são destacados em um círculo amarelo claro com a rede 192.168.11.0 escrita na parte inferior. À esquerda de R1 há três conexões adicionais, cada uma conectando a um switch na porta G0/1 que é então conectado a um laptop na porta F0/1. Cada switch e laptop são destacados em amarelo e o endereço de rede mostrado. A porta G0/0 de R1 se conecta na parte superior a um switch chamado S3 na rede 192.168.100.0. A porta G1/1 de R1 se conecta no meio a um switch rotulado S4 na rede 192.169.101.0. A porta G1/2 em R1 se conecta na parte inferior a um switch rotulado S5 na rede 192.168.102.0.

R1 Fa0/1 Fa0/2 Fa0/3 G0/1 G0/1 G0/0 G1/0 G0/1 G0/1 G1/1 G0/1 Fa0/1 Fa0/1 Fa0/1 G1/2 G0/1 G0/2 S1 S2 S3 S4 S5 Fa0/2

Fa0/1

InternetServidor de e-mailServidor WebServidor de ArquivosRede  
192.168.10.0Rede 192.168.11.0Rede 192.168.100.0Rede 192.168.101.0Rede 192.168.102.0

As topologias mostradas nos diagramas físico e lógico são apropriadas para seu nível de entendimento nesse momento do curso. Pesquise na Internet “diagramas de topologia de rede” para ver alguns exemplos mais complexos. Se você adicionar a palavra "cisco" para sua frase de pesquisa, você encontrará muitas topologias usando ícones semelhantes ao que você viu nessas figuras.

12.1.3

## Redes de Vários Tamanhos

Agora que você está familiarizado com os componentes que compõem as redes e suas representações em topologias físicas e lógicas, você está pronto para aprender sobre os muitos tipos diferentes de redes.

Existem redes de vários tamanhos. Eles variam de redes simples compostas por dois computadores a redes que conectam milhões de dispositivos.

As redes domésticas simples permitem que você compartilhe recursos, como impressoras, documentos, imagens e música, entre alguns dispositivos finais locais.

As redes de pequeno escritório e escritório doméstico (SOHO) permitem que as pessoas trabalhem em casa ou em um escritório remoto. Muitos trabalhadores independentes usam esses tipos de redes para anunciar e vender produtos, pedir suprimentos e se comunicar com os clientes.

Empresas e grandes organizações usam redes para fornecer consolidação, armazenamento e acesso a informações em servidores de rede. As redes fornecem e-mail, mensagens instantâneas e colaboração entre funcionários. Muitas organizações usam a conexão de sua rede à Internet para fornecer produtos e serviços aos clientes.

A internet é a maior rede existente. Na verdade, o termo Internet significa uma “rede de redes”. É uma coleção de redes públicas e privadas interconectadas.

Em pequenas empresas e residências, muitos computadores funcionam como servidores e clientes na rede. Esse tipo de rede é chamado de rede ponto a ponto.

Clique em cada botão abaixo para obter mais informações.

**Redes domésticas pequenas**

As redes domésticas pequenas conectam alguns computadores entre si e com a Internet.



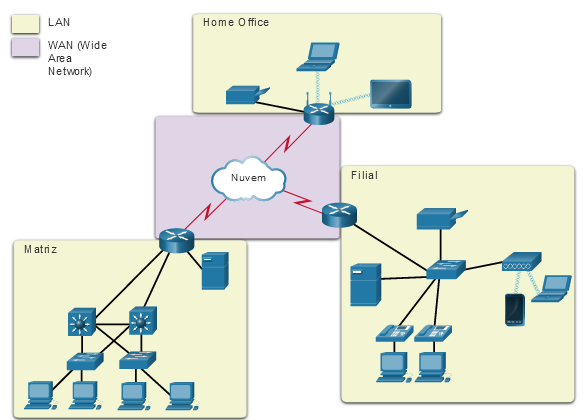
12.1.4

## LANs e WANs

As infra-estruturas de rede variam muito em termos de:

* Tamanho da área coberta;
* Número de usuários conectados;
* Número e tipos de serviços disponíveis;
* Área de responsabilidade.

Os dois tipos mais comuns de infraestruturas de rede são as redes locais (LANs) e as redes de longa distância (WANs). Uma LAN é uma infraestrutura de rede que fornece acesso a usuários e dispositivos finais em uma pequena área geográfica. Normalmente, uma LAN é usada em um departamento dentro de uma empresa, uma casa ou uma rede de pequenas empresas. Uma WAN é uma infraestrutura de rede que fornece acesso a outras redes em uma ampla área geográfica, que normalmente pertence e é gerenciada por uma corporação maior ou por um provedor de serviços de telecomunicações. A figura mostra LANs conectadas a uma WAN.



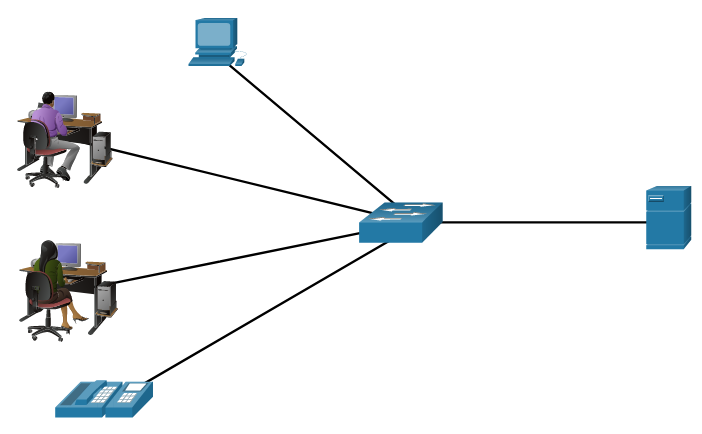
A topologia de rede mostra três LANs conectadas por meio de um link WAN no centro. Uma lenda mostra que as LANs são destacadas em amarelo e WANs em roxo claro. A WAN está localizada no centro do diagrama. Ele contém um símbolo de nuvem rotulado nuvem com conexões WAN vermelhas para três roteadores. Cada roteador está localizado em parte na WAN e em parte em uma LAN. No canto inferior esquerdo está a LAN central. Ele contém um servidor, dois switches multicamadas, dois switches LAN e quatro PCs. No canto inferior direito está a LAN da filial. Ele contém um switch, um servidor, uma impressora, dois telefones IP cada um conectado a um PC e um ponto de acesso sem fio com conexões sem fio a um laptop e um smartphone. No canto superior direito está a LAN do escritório doméstico. Ele contém um roteador sem fio com uma conexão com fio a uma impressora e conexões sem fio a um laptop e um monitor.

Home OfficeNuvemMatrizFilialLANWAN (Wide Area Network)

**LANs**

Uma LAN é uma infraestrutura de rede que abrange uma pequena área geográfica. As LANs têm características específicas:

* LANs interconectam dispositivos finais em uma área limitada, como uma casa, uma escola, um edifício de escritórios ou um campus.
* Uma LAN é geralmente administrada por uma única organização ou pessoa. O controle administrativo é imposto no nível da rede e governa as políticas de segurança e controle de acesso.
* As LANs fornecem largura de banda de alta velocidade para dispositivos finais internos e dispositivos intermediários, conforme mostrado na figura.



O diagrama é uma ilustração de uma LAN. No centro do diagrama é um switch. Há quatro conexões Ethernet no switch. No canto superior esquerdo há uma conexão com um PC. Abaixo disso está uma conexão com o computador na mesa de um trabalhador. Abaixo disso está outra conexão com o computador na mesa de um trabalhador. No canto inferior esquerdo há uma conexão com um telefone IP. À direita do switch há uma conexão com um servidor. O texto abaixo da figura diz: uma rede que atende uma casa, um prédio pequeno ou um campus pequeno é considerada uma LAN.

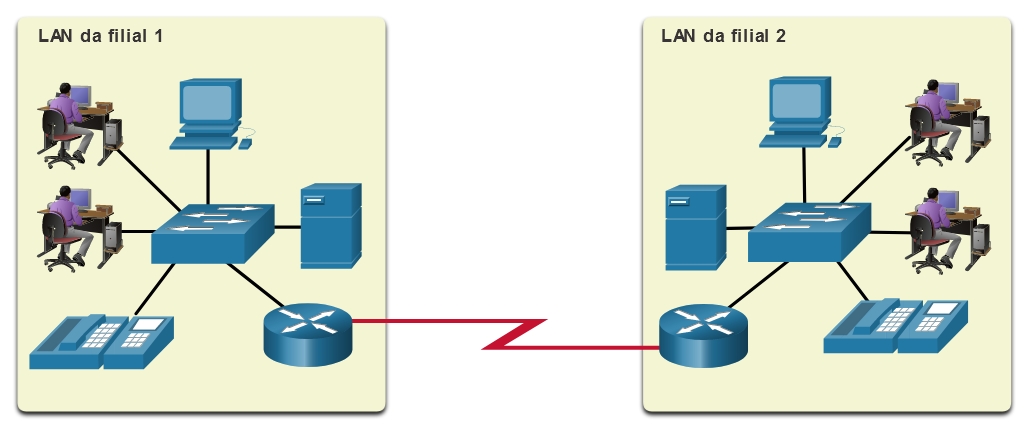
Uma rede que atende uma casa, prédio pequeno ou campus pequeno é considerada uma LAN.

**WANs**

A figura mostra uma WAN que interconecta duas LANs. Uma WAN é uma infraestrutura de rede que abrange uma ampla área geográfica. As WANs geralmente são gerenciadas por provedores de serviços (SPs) ou provedores de serviços de Internet (ISPs).

As WANs têm características específicas:

* As WANS interconectam as LANs em grandes áreas geográficas, como entre cidades, estados, províncias, países ou continentes.
* As WANs são geralmente administradas por vários prestadores de serviço.
* As WANs geralmente fornecem links de velocidade mais lenta entre as LANs.



A figura mostra duas LANs da filial conectadas através de um link WAN. Ambas as LANs são destacadas em uma caixa amarela clara e consistem em um switch central conectado a três PCs, um telefone IP, um servidor e um roteador. Os dois roteadores são conectados através de um link WAN vermelho. À esquerda está a ramificação 1 LAN e à direita está a ramificação 2 LAN.

**LAN da filial 1LAN da filial 2**

12.1.5

## O modelo de design de rede de três camadas

A LAN com fio do campus usa um modelo de design hierárquico para separar a topologia da rede em grupos ou camadas modulares. Separar o design em camadas permite que cada camada implemente funções específicas, o que simplifica o design da rede. Isso também simplifica a implantação e o gerenciamento da rede.

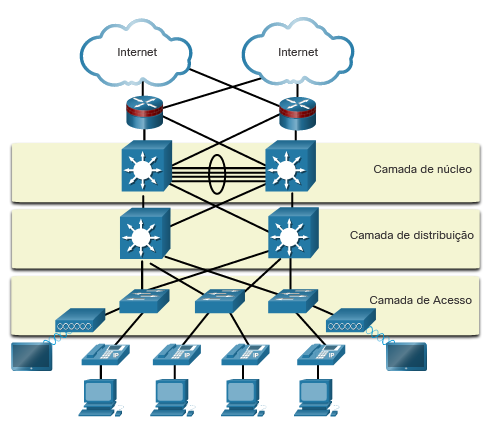
A LAN com fio do campus permite a comunicação entre dispositivos em um prédio ou grupo de prédios, bem como a interconexão com a WAN e a borda da Internet no núcleo da rede.

Um projeto de LAN hierárquico inclui as camadas de acesso, distribuição e núcleo, conforme mostrado na figura.

A figura mostra duas nuvens de internet na parte superior. Cada nuvem se conecta a dois roteadores, um à esquerda e outro à direita. Abaixo dos roteadores há dois switches de camada 3 dentro de uma caixa rotulada como camada de núcleo. Cada roteador se conecta a cada um dos switches. Os interruptores também têm várias linhas entre eles com um círculo em torno das linhas. Abaixo desses dois switches estão mais dois switches dentro de uma caixa rotulada camada de distribuição. Cada um dos interruptores superiores se conecta a cada um dos dois interruptores abaixo deles. Abaixo dos switches da camada de distribuição estão três switches de camada 2 e dois pontos de acesso dentro de uma caixa rotulada camada de acesso. Cada switch da camada de acesso tem uma conexão com cada um dos switches da camada de distribuição. Cada ponto de acesso se conecta a apenas um dos switches da camada de acesso. Abaixo da caixa da camada de acesso estão dois tablets sem fio. Cada tablet sem fio se conecta sem fio a um p sem fio. Também abaixo da caixa de camada de acesso são quatro telefones ip. Cada telefone tem um pc anexado. Um telefone se conecta ao switch da camada de acesso esquerdo, dois telefones se conectam ao switch da camada de acesso intermediário e o último telefone se conecta ao último switch da camada de acesso.

### Modelo do projeto hierárquico

InternetInternetCamada de núcleoCamada de distribuiçãoCamada de Acesso



Cada camada é projetada para atender a funções específicas.

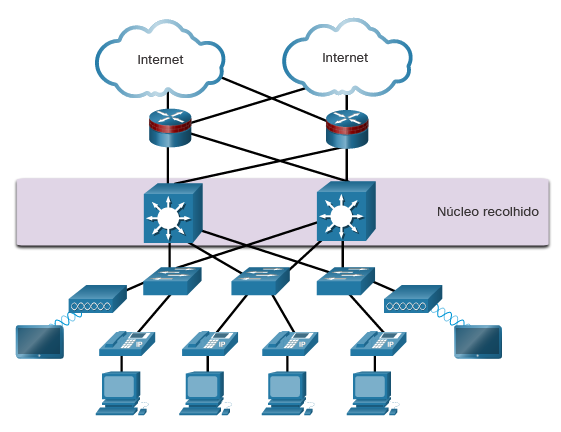
A camada de acesso oferece endpoints e acesso direto dos usuários à rede. A camada de distribuição agrega camadas de acesso e oferece ⁪conectividade aos serviços. Por fim, a camada de núcleo oferece conectividade entre as camadas de distribuição para os grandes ambientes de LAN. O tráfego do usuário é iniciado na camada de acesso e atravessa as demais camadas se a funcionalidade dessas camadas for necessária.

Embora o modelo hierárquico possua três camadas, algumas redes corporativas menores podem implementar um projeto hierárquico de duas camadas. Em um projeto hierárquico de duas camadas, as camadas de núcleo e distribuição são reduzidas em uma camada, reduzindo o custo e a complexidade, conforme mostrado na figura.

A figura mostra duas nuvens de internet na parte superior. Cada nuvem se conecta a dois roteadores, um à esquerda e outro à direita. Abaixo dos roteadores há dois switches de camada 3 dentro de uma caixa rotulada como núcleo recolhido. Cada roteador se conecta a cada um dos switches. Abaixo da caixa de núcleo recolhida estão três switches de camada 2 e dois pontos de acesso. Cada switch tem uma conexão com cada um dos switches dentro da caixa de núcleo recolhida. Cada ponto de acesso se conecta a apenas um dos switches da camada de acesso. Abaixo da caixa central recolhida estão dois tablets sem fios. Cada tablet sem fio se conecta sem fio a um p sem fio. Também abaixo da caixa do núcleo recolhido são quatro telefones i p. Cada telefone tem um pc anexado. Um telefone se conecta ao switch da camada de acesso esquerdo, dois telefones se conectam ao switch da camada de acesso intermediário e o último telefone se conecta ao último switch da camada de acesso.

### Switch de função dupla

Núcleo recolhidoInternetInternet



Em arquiteturas de rede simples ou em malha, as mudanças tendem a afetar um grande número de sistemas. O design hierárquico ajuda a restringir as alterações operacionais a um subconjunto da rede, o que facilita o gerenciamento e melhora a resiliência. A estruturação modular da rede em elementos pequenos e fáceis de entender também facilita a resiliência por meio de um melhor isolamento de falhas.

12.1.6

## Vídeo - Design de rede de três camadas

Assista a este vídeo para saber mais sobre o modelo de design de rede de três camadas.

12.1.7

## Arquiteturas de segurança comuns

O design do firewall é principalmente sobre interfaces de dispositivo que permitem ou negam tráfego com base na origem, no destino e no tipo de tráfego. Alguns designs são tão simples quanto designar uma rede externa e uma rede interna, que são determinados por duas interfaces em um firewall.

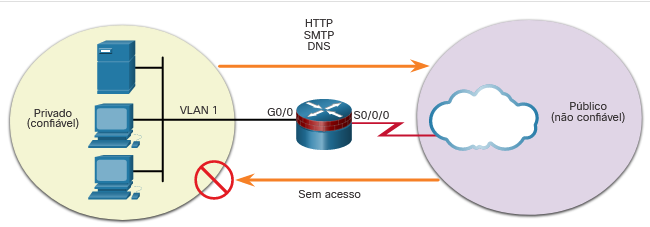
Aqui estão três designs comuns de firewall.

Privado e público

Como mostrado na figura, a rede pública (ou rede externa) não é confiável e a rede privada (ou rede interna) é confiável.

Normalmente, um firewall com duas interfaces é configurado da seguinte forma:

* O tráfego proveniente da rede privada é permitido e inspecionado à medida que viaja em direção à rede pública. É permitido o tráfego inspecionado que retorna da rede pública e associado ao tráfego originado da rede privada.
* O tráfego originado da rede pública e que viaja para a rede privada geralmente é bloqueado.

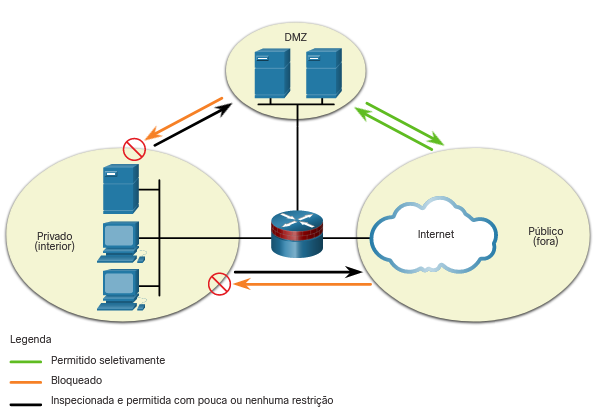


A figura privada e pública mostra uma nuvem dentro de um círculo rotulado como pública (não confiável). A nuvem se conecta a um firewall via s 0/0/0. A porta de firewall g 0/0 se conecta a um círculo rotulado v lan 1 privado (confiável) que tem um servidor e dois pc nele. Há uma seta indo do círculo privado para o círculo público com h t t p, s m t p, e d n s nele. Há outra seta indo do círculo público para o círculo privado com as palavras sem acesso.

Zona desmilitarizada

Uma zona desmilitarizada (DMZ) é um projeto de firewall onde normalmente há uma interface interna conectada à rede privada, uma interface externa conectada à rede pública e uma interface DMZ, conforme mostrado na figura.

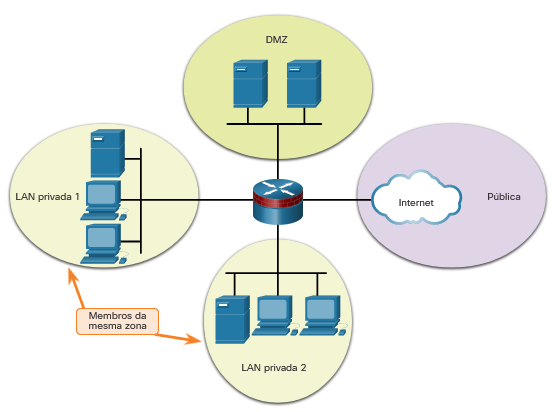
* O tráfego proveniente da rede privada é inspecionado à medida que ele viaja para a rede pública ou DMZ. Este tráfego é permitido com pouca ou nenhuma restrição. Tráfego inspecionado que retorna da DMZ ou da rede pública para a rede privada é permitido.
* O tráfego originado da rede DMZ e que viaja para a rede privada geralmente é bloqueado.
* O tráfego originado da rede DMZ e viajando para a rede pública é permitido seletivamente com base nos requisitos de serviço.
* O tráfego proveniente da rede pública e que viaja em direção à DMZ é seletivamente permitido e inspecionado. Esse tipo de tráfego normalmente é tráfego de email, DNS, HTTP ou HTTPS. O tráfego de retorno da DMZ para a rede pública é permitido dinamicamente.
* O tráfego originado da rede pública e que viaja para a rede privada está bloqueado.



Firewalls de política baseados em zona

Os firewalls de política baseados em zona (ZPFs) usam o conceito de zonas para fornecer flexibilidade adicional. Uma zona é um grupo de uma ou mais interfaces que têm funções ou recursos semelhantes. As zonas ajudam a especificar onde uma regra ou política de firewall do Cisco IOS deve ser aplicada. Na figura, as políticas de segurança para LAN 1 e LAN 2 são semelhantes e podem ser agrupadas em uma zona para configurações de firewall. Por padrão, o tráfego entre interfaces na mesma zona não está sujeito a nenhuma política e passa livremente. No entanto, todo o tráfego de zona para zona está bloqueado. Para permitir o tráfego entre as zonas, uma política que permite ou inspeciona o tráfego deve ser configurada.

A única exceção a esta política padrão **deny any** é a zona própria do roteador. A zona auto é o próprio roteador e inclui todos os endereços IP da interface do roteador. As configurações de política que incluem a zona automática aplicar-se-iam ao tráfego destinado e proveniente do roteador. Por padrão, não há nenhuma política para esse tipo de tráfego. O tráfego que deve ser considerado ao projetar uma política para a auto zona inclui o tráfego de plano de gerenciamento e plano de controle, como SSH, SNMP e protocolos de roteamento.



Qual camada de design de rede fornece terminais e usuários com uma conexão com a rede?

Acesso

Qual camada de design de rede fornece conectividade entre camadas de distribuição para grandes ambientes de LAN?

Núcleo

Quais grupos de design de rede interfaces em zonas com funções ou recursos semelhantes?

ZPF

Qual camada de design de rede agrega tráfego e fornece conectividade aos serviços?

Desmilitarizado

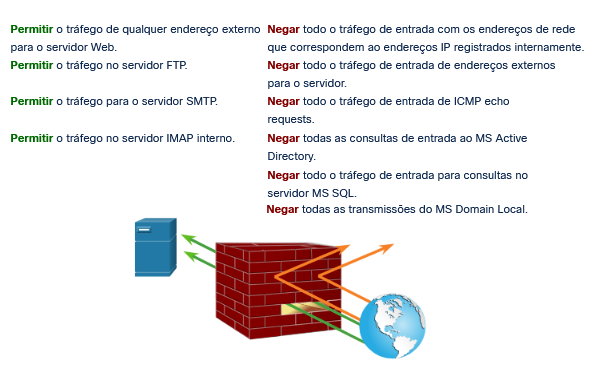
# Dispositivos de segurança

12.2.2

## Firewalls

Um firewall é um sistema ou grupo de sistemas que aplica uma política de controle de acesso entre redes.

Reproduza a animação na figura para visualizar um firewall em operação.



Propriedades comuns do firewall

Todos os firewalls compartilham algumas propriedades comuns:

* Os firewalls são resistentes a ataques de rede.
* Firewalls são o único ponto de trânsito entre redes corporativas internas e redes externas porque todo o tráfego flui através do firewall.
* Os firewalls aplicam a política de controle de acesso.

Benefícios do firewall

Existem vários benefícios do uso de um firewall em uma rede:

* Eles impedem a exposição de hosts, recursos e aplicações sensíveis a usuários não confiáveis.
* Eles sanitizam o fluxo do protocolo, o que impede a exploração de falhas no protocolo.
* Eles bloqueiam dados maliciosos de servidores e clientes.
* Eles reduzem a complexidade do gerenciamento de segurança descarregando a maior parte do controle de acesso à rede para alguns firewalls na rede.

Limitações do firewall

Os firewalls também têm algumas limitações:

* Um firewall mal configurado pode ter sérias conseqüências para a rede, como se tornar um único ponto de falha.
* Os dados de muitos aplicações não podem ser transmitidos por firewalls com segurança.
* Os usuários podem procurar proativamente maneiras de contornar o firewall para receber material bloqueado, o que expõe a rede a possíveis ataques.
* O desempenho da rede pode diminuir.
* O tráfego não autorizado pode ser encapsulado ou escondido como tráfego legítimo através do firewall.

12.2.3

## Descrições de tipo de firewall

É importante entender os diferentes tipos de firewalls e suas capacidades específicas para que o firewall correto seja usado para cada situação.

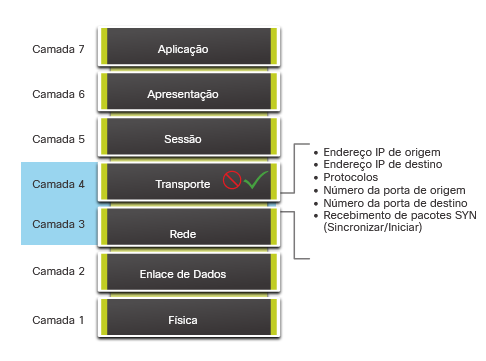
Os firewalls de filtragem de pacotes geralmente fazem parte de um firewall de roteador, que permite ou nega tráfego com base nas informações da Camada 3 e da Camada 4. Eles são firewalls sem estado que usam uma simples pesquisa de tabela de políticas que filtra o tráfego com base em critérios específicos.

Por exemplo, os servidores SMTP escutam a porta 25 por padrão. Um administrador pode configurar o firewall de filtragem de pacotes para bloquear a porta 25 de uma estação de trabalho específica para impedir que ele transmita um vírus de e-mail

Firewall de filtragem de pacotes (sem estado)

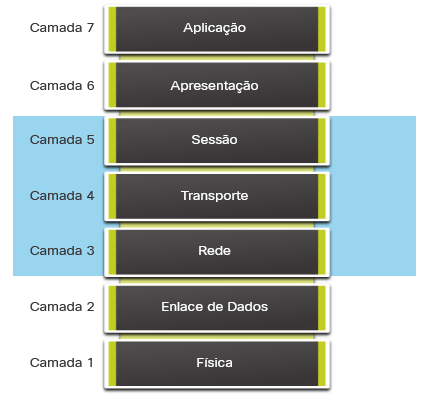
Os firewalls de filtragem de pacotes geralmente fazem parte de um firewall de roteador, que permite ou nega tráfego com base nas informações da Camada 3 e da Camada 4. Eles são firewalls sem estado que usam uma simples pesquisa de tabela de políticas que filtra o tráfego com base em critérios específicos.

Por exemplo, os servidores SMTP escutam a porta 25 por padrão. Um administrador pode configurar o firewall de filtragem de pacotes para bloquear a porta 25 de uma estação de trabalho específica para impedir que ele transmita um vírus de e-mail



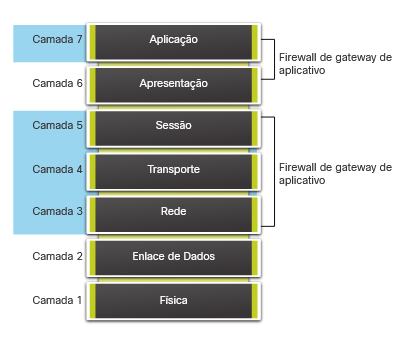
Firewall com monitoração de estado

Firewalls com estado são as tecnologias de firewall mais versáteis e mais comuns em uso. Os firewalls stateful fornecem filtragem de pacotes stateful usando informações de conexão mantidas em uma tabela de estado. Filtragem com estado é uma arquitetura de firewall classificada na camada de rede. Ele também analisa o tráfego na camada 4 da OSI e na camada 5.



Firewall de gateway de aplicativo

Um firewall de gateway de aplicação (firewall proxy), conforme mostrado na figura, filtra as informações nas camadas 3, 4, 5 e 7 do modelo de referência OSI. A maior parte do controle e filtragem do firewall é feita em software. Quando um cliente precisa acessar um servidor remoto, ele se conecta a um servidor proxy. O servidor proxy se conecta ao servidor remoto em nome do cliente. Portanto, o servidor só vê uma conexão do servidor proxy.



Firewall de última geração

Os firewalls de última geração (NGFW) vão além dos firewalls de estado, fornecendo:

* Prevenção de intrusão integrada
* Reconhecimento e controle de aplicações para ver e bloquear aplicativos arriscados
* Caminhos de atualização para incluir futuros feeds de informações
* Técnicas para lidar com ameaças de segurança em evolução

Outros métodos de implementação de firewalls incluem:

* **Firewall baseado em host (servidor e pessoal)** - Um PC ou servidor com software de firewall em execução nele.
* **Firewall transparente** - Filtra o tráfego IP entre um par de interfaces em ponte.
* **Firewall híbrido** - Uma combinação dos vários tipos de firewall. Por exemplo, um firewall de inspeção de aplicativos combina um firewall com estado com um firewall de gateway de aplicativo.

12.2.5

## Dispositivos de prevenção e detecção de intrusão

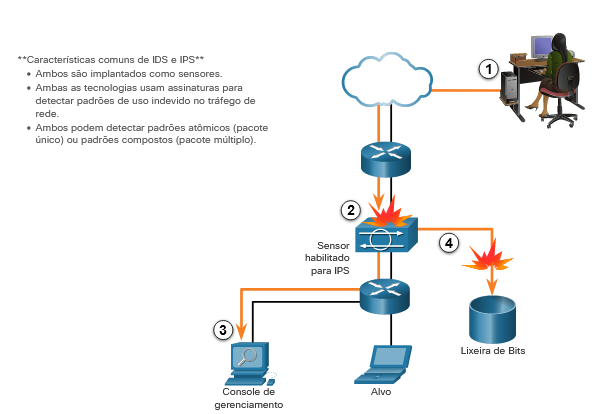
Uma mudança de paradigma de arquitetura de rede é necessária para se defender contra ataques rápidos e em evolução. Isso deve incluir sistemas de prevenção e detecção de baixo custo, como sistemas de detecção de intrusão (IDS) ou os sistemas de prevenção de intrusão mais escalonáveis (IPS). A arquitetura de rede integra essas soluções nos pontos de entrada e saída da rede.

Ao implementar IDS ou IPS, é importante estar familiarizado com os tipos de sistemas disponíveis, abordagens baseadas em host e em rede, o posicionamento desses sistemas, a função das categorias de assinatura e possíveis ações que um roteador Cisco IOS pode executar quando um ataque é detectado.

A figura mostra como um dispositivo IPS lida com tráfego malicioso.

A figura mostra um usuário no canto superior direito conectado e enviando tráfego para uma nuvem. A nuvem se conecta a um roteador e envia o tráfego através desse roteador. A nuvem se conecta a um sensor habilitado para i p s que se conecta a outro roteador que também tem conexões a um console de gerenciamento e a um laptop rotulado como destino. Há também um ícone para um bucket bit para o lado do sensor habilitado ips. As características de ids e ips incluem ambas as tecnologias são implantadas como sensores, ambas as tecnologias usam assinaturas para detectar padrões de uso indevido no tráfego de rede e ambas podem detectar padrões atômicos (pacote único) ou padrões compostos (multi-pacote).

### Características de IDS e IPS



Lixeira de Bits  
Sensor habilitado para IPSConsole de   
gerenciamentoAlvo\*\*Características comuns de IDS e IPS\*\*

* Ambos são implantados como sensores.
* Ambas as tecnologias usam assinaturas para detectar padrões de uso indevido no tráfego de rede.
* Ambos podem detectar padrões atômicos (pacote único) ou padrões compostos (pacote múltiplo).

1. O tráfego malicioso é enviado ao host de destino que está dentro da rede.
2. O tráfego é roteado para a rede e recebido por um sensor habilitado para IPS, onde é bloqueado.
3. O sensor habilitado para IPS envia informações de registro sobre o tráfego para o console de gerenciamento de segurança de rede.
4. O sensor habilitado para IPS elimina o tráfego. (Ele é enviado para o “Bit Bucket”.)

As tecnologias IDS e IPS são implantadas como sensores. Um sensor IDS ou IPS pode estar na forma de vários dispositivos diferentes:

* Um roteador configurado com o software Cisco IOS IPS
* Um dispositivo projetado especificamente para fornecer serviços IDS ou IPS dedicados
* Um módulo de rede instalado em um dispositivo de segurança adaptável (ASA), switch ou roteador

As tecnologias IDS e IPS usam assinaturas para detectar padrões no tráfego da rede. Uma assinatura é um conjunto de regras que um IDS ou IPS usa para detectar atividades maliciosas. As assinaturas podem ser usadas para detectar violações graves de segurança, para detectar ataques de rede comuns e para coletar informações. As tecnologias IDS e IPS podem detectar padrões de assinatura atômica (pacote único) ou padrões de assinatura composta (pacote múltiplo).

12.2.6

## Vantagens e desvantagens de IDS e IPS

**Vantagens e desvantagens do IDS**

The table lists the advantages and disadvantages of IDS and IPS.

| **Solução** | **Vantagens** | **Desvantagens** |
| --- | --- | --- |
| **IDS** | * Sem impacto na rede (latência, variação) * Sem impacto na rede se houver uma falha no sensor * Sem impacto na rede se houver sobrecarga do sensor | * Ação de resposta não pode parar pacotes de gatilho * Ajuste correto necessário para ações de resposta * Mais vulnerável a técnicas de evasão de segurança de rede |
| **IPS** | * Interrompe pacotes de gatilho * Pode usar técnicas de normalização de fluxo | * Problemas de sensor podem afetar o tráfego de rede * A sobrecarga do sensor afeta a rede * Algum impacto na rede (latência, jitter) |

Vantagens de desvantagens do IDS

**Vantagens IDS**

Um IDS é implantado no modo off-line e, portanto:

* Os IDs não afetam o desempenho da rede. Especificamente, ele não introduz latência, variação ou outros problemas de fluxo de tráfego.
* Os IDs não afetam a funcionalidade de rede se o sensor falhar. Isso afeta apenas a capacidade do IDS para analisar os dados.

**Desvantagens IDS**

As desvantagens de um IDS incluem:

* Um sensor IDS não pode parar o pacote de disparo e é menos útil na interrupção de vírus de e-mail e ataques automatizados, como worms.
* Ajustar os sensores IDS para atingir os níveis esperados de detecção de intrusão pode ser muito demorado. Os usuários que implantam ações de resposta do sensor IDS devem ter uma política de segurança bem projetada e uma boa compreensão operacional de suas implantações de IDS.
* Uma implementação de IDS é mais vulnerável a técnicas de evasão de segurança de rede porque não está em linha.

Vantagens de desvantagens do IPS

**Vantagens IPS**

As vantagens de um IPS incluem:

* Um sensor IPS pode ser configurado para executar uma perda de pacotes para interromper o pacote de gatilho, os pacotes associados a uma conexão ou os pacotes de um endereço IP de origem.
* Como os sensores IPS estão em linha, eles podem usar a normalização de fluxo. Normalização de fluxo é uma técnica usada para reconstruir o fluxo de dados quando o ataque ocorre em vários segmentos de dados.

**Desvantagens IPS**

As desvantagens de um IPS incluem:

* Como ele é implantado em linha, erros, falhas e sobrecarregar o sensor IPS com muito tráfego podem ter um efeito negativo no desempenho da rede.
* Um sensor IPS pode afetar o desempenho da rede introduzindo latência e jitter.
* Um sensor IPS deve ser dimensionado e implementado adequadamente para que aplicativos sensíveis ao tempo, como VoIP, não sejam afetados negativamente.

Considerações de implantação

Você pode implantar um IPS e um IDS. Usar uma dessas tecnologias não anula o uso da outra. Na verdade, as tecnologias IDS e IPS podem se complementar.

Por exemplo, um IDS pode ser implementado para validar a operação de IPS porque o IDS pode ser configurado para inspeção de pacotes mais profunda off-line. Isso permite que o IPS se concentre em menos, mas mais críticos padrões de tráfego em linha.

Decidir qual implementação usar se baseia nos objetivos de segurança da organização, conforme indicado em sua política de segurança de rede.

12.2.7

## Tipos de IPS

Existem dois tipos principais de IPS disponíveis: IPS baseado em host e IPS baseado em rede.

**IPS de host**

O IPS baseado em host (HIPS) é um software instalado em um host para monitorar e analisar atividades suspeitas. Uma vantagem significativa do HIPS é que ele pode monitorar e proteger o sistema operacional e os processos críticos do sistema que são específicos para esse host. Com conhecimento detalhado do sistema operacional, o HIPS pode monitorar atividades anormais e impedir que o host execute comandos que não correspondam ao comportamento típico. Esse comportamento suspeito ou mal-intencionado pode incluir atualizações de registro não autorizadas, alterações no diretório do sistema, execução de programas de instalação e atividades que causam estouros de buffer. O tráfego de rede também pode ser monitorado para impedir que o host participe de um ataque de negação de serviço (DoS) ou faça parte de uma sessão de FTP ilícita.

HIPS pode ser pensado como uma combinação de software antivírus, software antimalware e um firewall. Combinado com um IPS baseado em rede, o HIPS é uma ferramenta eficaz para fornecer proteção adicional para o host.

Uma desvantagem do HIPS é que ele opera apenas a nível local. Ele não tem uma visão completa da rede ou eventos coordenados que possam estar acontecendo em toda a rede. Para ser eficaz em uma rede, o HIPS deve ser instalado em cada host e ter suporte para cada sistema operacional. A tabela lista as vantagens e desvantagens do HIPS.

| **Vantagens** | **Desvantagens** |
| --- | --- |
| * Fornece proteção específica para um sistema operacional host * Fornece proteção em nível de aplicativo e sistema operacional * Protege o host depois que a mensagem é descriptografada | * Dependente do sistema operacional * Deve ser instalado em todos os hosts |

**IPS baseado em rede**

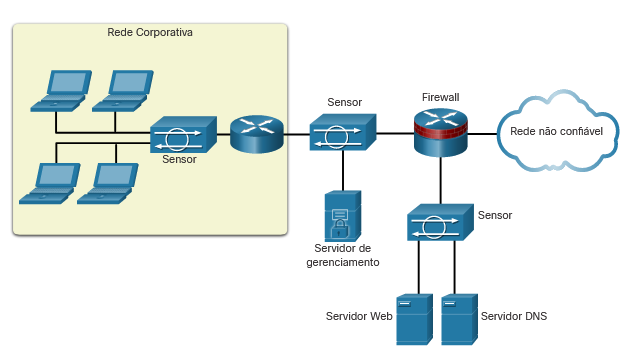
Um IPS baseado em rede pode ser implementado usando um dispositivo IPS dedicado ou não dedicado. As implementações de IPS baseadas em rede são um componente crítico da prevenção de intrusões. Existem soluções IDS/IPS baseadas em host, mas elas devem ser integradas a uma implementação IPS baseada em rede para garantir uma arquitetura de segurança robusta.

Os sensores detectam atividades maliciosas e não autorizadas em tempo real e podem agir quando necessário. Como mostrado na figura, os sensores são implantados em pontos de rede designados. Isso permite que os gerentes de segurança monitorem a atividade da rede enquanto ela estiver ocorrendo, independentemente do local do alvo de ataque.

A figura mostra uma nuvem rotulada como rede não confiável conectada a um firewall. O firewall tem uma conexão com um sensor que tem um servidor web e servidor d n s conectado a ele. O firewall também se conecta a outro sensor que tenha um servidor de gerenciamento e roteador conectados. O roteador tem outra conexão com outro sensor que se conecta a laptops. O roteador, sensor e laptops estão dentro de uma rede denominada rede corporativa.

### Exemplo de implantação do sensor IPS

Rede CorporativaSensorSensorSensorServidor de   
gerenciamentoServidor WebServidor DNSRede não confiávelFirewall



12.2.8

**Dispositivos de segurança especializados**

Há uma variedade de dispositivos de segurança especializados disponíveis. Aqui estão alguns exemplos.

AMP

Cisco Advanced Malware Protection (AMP) é uma solução de proteção e análise de malware avançada de classe empresarial. Ele fornece proteção abrangente contra malware para organizações antes, durante e depois de um ataque:

* Antes de um ataque, a AMP fortalece as defesas e protege contra ameaças conhecidas e emergentes.
* Durante um ataque, o AMP identifica e impede que tipos de arquivos violadores de políticas, tentativas de exploração e arquivos mal-intencionados se infiltrem na rede.
* Após um ataque ou após a inspeção inicial de um arquivo, o AMP vai além dos recursos de detecção pontual e monitora e analisa continuamente todas as atividades e tráfego de arquivos, independentemente da disposição, procurando por quaisquer indicações de comportamento malicioso. Se um arquivo com uma disposição desconhecida ou previamente considerada "boa" começar a se comportar mal, o AMP o detectará e alertará instantaneamente as equipes de segurança com uma indicação de comprometimento. Em seguida, ele proporciona visibilidade em relação à origem do malware, aos sistemas afetados e às ações dessa ameaça.

A AMP acessa a inteligência de segurança coletiva do Cisco Talos Security Intelligence and Research Group. O Talos detecta e correlaciona ameaças em tempo real usando a maior rede de detecção de ameaças do mundo.

WSA

Um Cisco Web Security Appliance (WSA) é um gateway da Web seguro que combina proteções líderes para ajudar as organizações a enfrentar os desafios crescentes de proteção e controle do tráfego da Web. O WSA protege a rede bloqueando automaticamente sites arriscados e testando sites desconhecidos antes de permitir que os usuários os acessem. O WSA fornece proteção contra malware, visibilidade e controle de aplicativos, controles de política de uso aceitável, relatórios criteriosos e mobilidade segura.

Embora o WSA proteja a rede contra intrusões de malware, ele não fornece proteção para usuários que desejam se conectar à Internet diretamente fora da rede protegida, como em um serviço Wi-Fi público. Neste caso, o PC do usuário pode ser infectado com malware que pode então se espalhar para outras redes e dispositivos. Para ajudar a proteger os PCs dos usuários contra esses tipos de infecções de malware, há o Cisco Cloud Web Security (CWS).

O CWS, juntamente com o WSA, fornece proteção abrangente contra malware e os impactos associados. A solução Cisco CWS impõe a comunicação segura de e para a Internet e fornece aos funcionários remotos o mesmo nível de segurança que os funcionários no local ao usar um laptop emitido pelo empregador. O Cisco CWS incorpora duas funções principais, filtragem da Web e segurança da Web, e ambas são acompanhadas por relatórios extensos e centralizados.

ESA

Um Cisco Email Security Appliance (ESA) /Cisco Cloud Email Security ajuda a mitigar ameaças baseadas em e-mail. O Cisco ESA defende sistemas de e-mail de missão crítica.

O Cisco ESA é constantemente atualizado por feeds em tempo real do Cisco Talos, que detecta e correlaciona ameaças usando um sistema mundial de monitoramento de banco de dados.

Estas são algumas das principais características da ESA:

* **Inteligência global contra ameaças** - O Cisco Talos oferece uma visão 24 horas da atividade de tráfego global. Ele analisa anomalias, descobre novas ameaças e monitora as tendências do tráfego.
* **Bloqueio de spam** - Uma defesa em várias camadas combina uma camada externa de filtragem com base na reputação do remetente e uma camada interna de filtragem que realiza uma análise profunda da mensagem.
* **Proteção avançada contra malware** — Inclui AMP que tira proveito da vasta rede de inteligência de segurança na nuvem do Sourcefire. Ele oferece proteção em todo o continuum do ataque antes, durante e depois de um ataque.
* **Controle de mensagens de saída** - Controla mensagens de saída para ajudar a garantir que mensagens importantes estejam em conformidade com os padrões do setor e estejam protegidas em trânsito.

# Serviços de segurança

12.3.1

## Vídeo - Serviços de Segurança

Assista ao vídeo para saber mais sobre serviços de segurança.

12.3.2

## Controle de tráfego com ACLs

Uma lista de controle de acesso (ACL) é uma série de comandos que controlam se um dispositivo encaminha ou descarta pacotes com base nas informações encontradas no cabeçalho do pacote. Quando configuradas, as ACLs executam as seguintes tarefas:

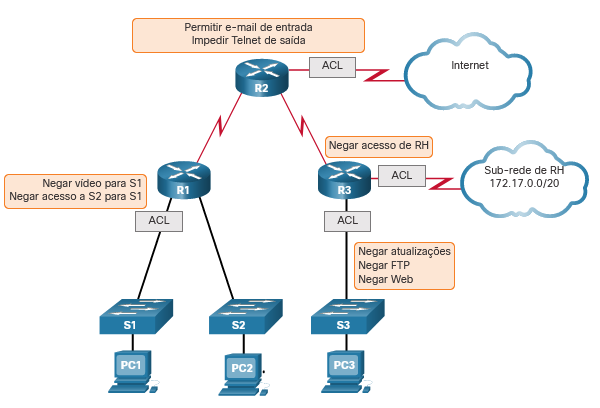
* Eles limitam o tráfego da rede para aumentar o desempenho da rede. Por exemplo, se a política corporativa não permite tráfego de vídeo na rede, as ACLs que bloqueiam tráfego de vídeo podem ser configuradas e aplicadas. Isso reduziria significativamente a carga da rede e aumentaria o desempenho da rede.
* Eles fornecem controle de fluxo de tráfego. As ACLs podem restringir o fornecimento de atualizações de roteamento para garantir que as atualizações sejam de uma fonte conhecida.
* Elas fornecem um nível básico de segurança para acesso à rede. As ACLs podem permitir que um host acesse uma parte da rede e impedir que outro host acesse a mesma área. Por exemplo, o acesso à rede de Recursos Humanos poderá ser restrito a usuários autorizados.
* Elas filtram o tráfego com base no tipo de tráfego. Por exemplo, uma ACL pode permitir tráfego de correio eletrônico, mas bloquear todo o tráfego de Telnet.
* Elas examinam hosts para permitir ou negar acesso aos serviços de rede. As ACLs podem permitir ou negar a um usuário o acesso a tipos de arquivo, como FTP ou HTTP.

Além da permissão ou negação de tráfego, as ACLs podem ser usadas selecionando tipos de tráfego que serão analisados, enviados ou processados de outras formas. Por exemplo, as ACLs podem ser usadas para classificar o tráfego para ativar o processamento de prioridade. Esse recurso é semelhante a ter um ingresso VIP em um show ou em evento esportivo. O ingresso VIP fornece aos convidados selecionados os privilégios não oferecidos aos portadores de bilhetes de admissão geral, como a entrada prioritária ou possibilidade de entrar em uma área restrita.

A figura mostra uma topologia de amostra com ACLs aplicadas aos roteadores R1, R2 e R3.

A figura mostra uma nuvem conectada a uma caixa chamada A C L. A caixa se conecta a um roteador rotulado R2 com as palavras permitir e-mail de entrada e negar telnet de entrada acima dele. R2 se conecta aos roteadores R1 e R3. O roteador R1 possui duas interfaces Ethernet. Cada interface se conecta a um switch (S1 e S2). P c 1 se conecta a S1 e p c 2 se conecta a s2. A interface R1 que se conecta a S1 tem uma caixa rotulada A C L e palavras ao lado do estado do roteador negam vídeo para S1 e negam acesso a S2 para S1. O roteador R3 tem uma conexão com uma nuvem rotulada H R sub-rede 172 ponto 17 ponto 0 ponto 0/20 e uma caixa na conexão rotulada A C L e as palavras negam acesso h r. R3 também tem uma conexão ethernet para S3. P c 3 também se conecta ao S3. A conexão Ethernet R3 tem uma caixa rotulada A C L nele com as palavras negar atualizações f t p e negar web.

### O que é uma ACL?



.3

## ACLs: recursos importantes

Dois tipos de ACLs Cisco IPv4 são padrão e estendidos. As ACLs padrão podem ser usadas para permitir ou negar tráfego somente dos endereços IPv4 origem. O destino do pacote e as portas envolvidas não são avaliados.

As ACLs estendidas filtram pacotes IPv4 com base em vários atributos que incluem:

* Tipo de protocolo
* Endereço IPv4 origem
* Endereço IPv4 destino
* Portas TCP ou UDP origem
* Portas TCP ou UDP destino
* Informações opcionais do tipo de protocolo para o melhor controle

As ACLs padrão e estendidas podem ser criadas usando-se um número ou um nome para identificar a ACL e sua lista de instruções.

Usar ACLs numeradas é um método eficaz para determinar o tipo de ACL em redes pequenas com tráfego definido de forma mais homogênea. No entanto, um número não fornece informações sobre o propósito da ACL. Portanto, um nome pode ser usado para identificar uma ACL da Cisco.

Ao configurar o registro de ACL, uma mensagem ACL pode ser gerada e registrada quando o tráfego atende aos critérios de permissão ou negação definidos na ACL.

As ACLs Cisco também podem ser configuradas para permitir apenas tráfego TCP que tenha um conjunto de bits ACK ou RST, de modo que apenas o tráfego de uma sessão TCP estabelecida seja permitido. Isso pode ser usado para negar qualquer tráfego TCP de fora da rede que está tentando estabelecer uma nova sessão TCP.

12.3.5

## SNMP

O protocolo SNMP (Simple Network Management Protocol) permite que os administradores gerenciem dispositivos finais como servidores, estações de trabalho, roteadores, switches e dispositivos de segurança em uma rede IP. Permite que os administradores de rede monitorem o desempenho da rede, encontrem e resolvam os problemas da rede e planejem o crescimento da rede.

O SNMP é um protocolo da camada de aplicação que fornece um formato de mensagem para a comunicação entre gerenciadores e agentes.

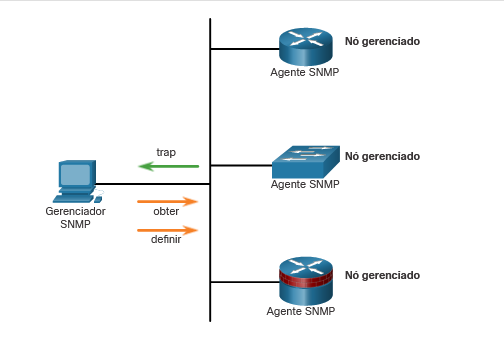
Como mostrado na figura, o sistema SNMP consiste em dois elementos.

* Gerenciador SNMP que executa o software de gerenciamento SNMP.
* Agentes SNMP que são os nós que estão sendo monitorados e gerenciados.

O Management Information Base (MIB) é um banco de dados dos agentes que armazena dados e estatísticas operacionais sobre o dispositivo.

Para configurar o SNMP em um dispositivo de rede, primeiramente é necessário definir a relação entre o gerenciador e o agente.

O gerenciador de SNMP faz parte de um sistema de gerenciamento de rede (NMS). O gerenciador de SNMP executa o software de gerenciamento de SNMP. Conforme mostrado na figura, o gerente SNMP pode coletar informações de um agente SNMP usando a ação "get" e pode alterar as configurações em um agente usando a ação "set". Além disso, os agentes SNMP podem encaminhar informações diretamente para um gerenciador de rede usando “traps”.



12.3.6

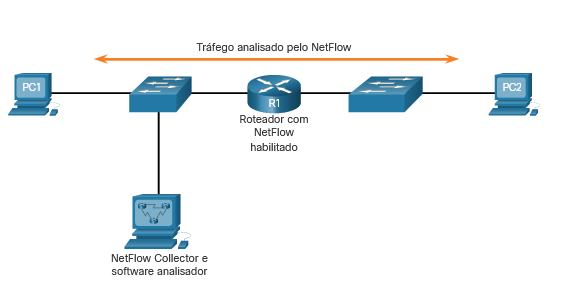
## NetFlow

NetFlow é uma tecnologia CISCO IOS que fornece estatísticas em pacotes que passam por meio de um switch multicamadas ou de um roteador da Cisco. Enquanto o SNMP tenta fornecer uma ampla gama de recursos e opções de gerenciamento de rede, o NetFlow está focado em fornecer estatísticas sobre pacotes IP que fluem através de dispositivos de rede.

O NetFlow fornece dados para permitir monitoramento de rede e segurança, planejamento de rede, análise de tráfego para incluir identificação de gargalos de rede e contabilidade IP para fins de faturamento. Por exemplo, na figura, o PC 1 se conecta ao PC 2 usando um aplicativo como HTTPS.

A figura mostra 3 dispositivos conectados a um switch, p c 1, um software de coletor e analisador de fluxo líquido de pc rotulado e roteador R1 rotulado roteador habilitado para fluxo líquido. R1 também se conecta a um interruptor que também tem p c 2 conectado. Na parte superior do diagrama há uma linha com setas em ambas as extremidades e as palavras fluxo líquido analisado fluxo de tráfego.

### NetFlow na rede



O NetFlow pode monitorar essa conexão de aplicativo, rastreando contagens de bytes e pacotes para esse fluxo de aplicativo individual. Em seguida, envia as estatísticas para um servidor externo chamado coletor NetFlow.

A tecnologia NetFlow tem visto várias gerações que oferecem mais sofisticação na definição de fluxos de tráfego, mas fluxos “NetFlow original” diferenciados usando uma combinação de sete campos. Caso um desses campos varie em valor de outro pacote, os pacotes podem ser determinados com segurança como sendo de fluxos diferentes:

* Endereço IP de origem
* Endereço IP de destino
* Número da porta de origem
* Número da porta de destino
* Tipo de protocolo da camada 3
* Marcação de tipo de serviço (ToS)
* Interface lógica de entrada

Os quatro primeiros campos que o NetFlow usa para identificar um fluxo devem ser familiares. Os endereços IP de origem e destino, além das portas de origem e destino, identificam a conexão entre o aplicativo de origem e de destino. O tipo de protocolo da Camada 3 identifica o tipo de cabeçalho que segue o cabeçalho IP (geralmente TCP ou UDP, mas outras opções incluem ICMP). O byte ToS no cabeçalho IPv4 contém informações sobre como os dispositivos devem aplicar regras de qualidade de serviço (QoS) aos pacotes nesse fluxo.

12.3.7

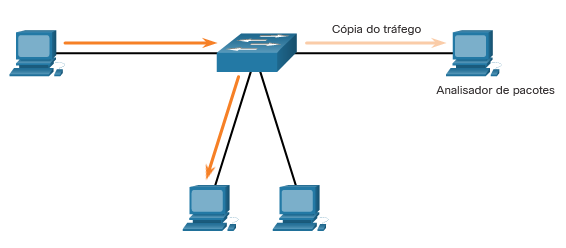
## Espelhamento de portas

Um analisador de pacotes (também conhecido como sniffer de pacotes ou sniffer de tráfego) é normalmente um software que captura pacotes que entram e saem da placa de interface de rede (NIC). Nem sempre é possível ou desejável ter o analisador de pacotes no dispositivo que está sendo monitorado. Às vezes, é melhor em uma estação separada designada para capturar os pacotes.

Como os switches de rede podem isolar o tráfego, os sniffers de tráfego ou outros monitores de rede, como IDS, não podem acessar todo o tráfego em um segmento de rede. O espelhamento de portas é um recurso que permite que um switch faça cópias duplicadas do tráfego que passa por um switch e, em seguida, enviá-lo para fora uma porta com um monitor de rede conectado. O tráfego original é encaminhado da maneira usual. Um exemplo de espelhamento de porta é ilustrado na figura.

A figura mostra um switch que tem 4 pcs conectados. O PC à esquerda tem uma seta indo para o switch. Outra seta vai do switch e aponta para o pc inferior esquerdo. Uma seta mais clara vai do switch o analisador de pacotes rotulado como pc mais à direita e as palavras cópia do tráfego estão acima da linha.

### Farejamento de tráfego usando um switch



12.3.8

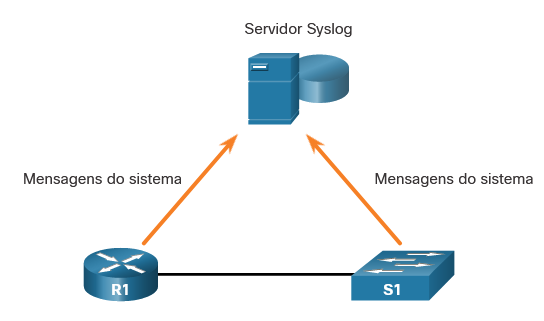
**Servidores Syslog**

Quando determinados eventos ocorrem em uma rede, os dispositivos de rede têm mecanismos confiáveis para notificar o administrador com mensagens de sistema detalhadas. Essas mensagens podem não ser críticas ou podem ser significativas. Os administradores de rede têm uma variedade de opções de armazenamento, interpretação, exibição dessas mensagens e para serem alertados sobre as mensagens que podem ter maior impacto na infraestrutura de rede.

O método mais comum de acessar mensagens do sistema é usar um protocolo chamado syslog.

Muitos dispositivos de rede são compatíveis com syslog, incluindo: roteadores, switches, servidores de aplicativos, firewalls e outros dispositivos de rede. O protocolo syslog permite que os dispositivos de rede enviem suas mensagens de sistema pela rede para os servidores syslog, conforme mostrado na figura.

### Syslog



O serviço de logging de syslog oferece três funções principais:

* A capacidade de coletar informações de registro para monitorar e solucionar problemas
* A capacidade de selecionar o tipo de informações de registro que são capturadas
* A capacidade de especificar o destino das mensagens syslog capturadas

12.3.9

## NTP

É importante sincronizar a hora em todos os dispositivos da rede porque todos os aspectos de gerenciamento, proteção, solução de problemas e planejamento de redes exigem um registro de data e hora preciso e consistente. Quando a hora não está sincronizada entre os dispositivos, será impossível determinar a ordem dos eventos que ocorreram em diferentes partes da rede.

Normalmente, as configurações de data e hora em um dispositivo de rede podem ser definidas usando um destes dois métodos:

* Configuração manual de data e hora
* Configurando o Network Time Protocol (NTP)

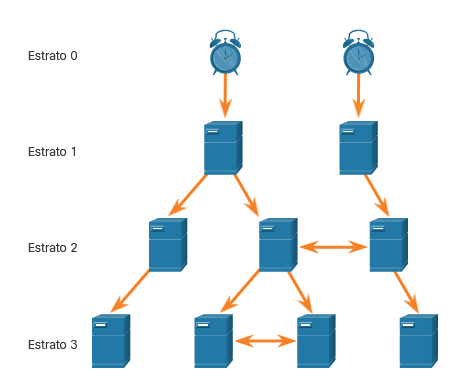
Conforme a rede cresce, torna-se cada vez mais difícil garantir que todos os dispositivos da infraestrutura operem com horário sincronizado. Mesmo em um ambiente de rede menor, o método manual não é o ideal. Se um dispositivo for reinicializado, como ele obterá uma data e um carimbo de hora precisos?

A melhor solução é configurar o NTP na rede. Esse protocolo permite que os roteadores na rede sincronizem as configurações de hora com um servidor NTP. Um grupo de clientes NTP que obtém informações de data e hora de uma única fonte tem configurações de hora mais consistentes. Quando o NTP é implementado na rede, ele pode ser configurado para sincronizar com um relógio mestre privado ou pode ser sincronizado com um servidor NTP disponível publicamente na Internet.

As redes NTP usam um sistema hierárquico de fontes de horário. Cada nível desse sistema hierárquico é denominado stratum. O nível do stratum é definido como o número de contagens de saltos da fonte oficial. O horário sincronizado é distribuído através da rede usando o NTP. A figura exibe uma amostra de uma rede NTP.

A figura mostra as palavras estrato 0 à esquerda e dois despertadores. Cada despertador tem uma seta que aponta para baixo para um servidor. À esquerda destes servidores estão as palavras estrato 1. Abaixo do servidor à esquerda no estrato 1 estão mais dois servidores e setas apontam do servidor no estrato 1 para cada um dos dois servidores no estrato 2. O servidor estrato 1 à direita tem um servidor estrato 2 abaixo dele e uma seta apontando para ele. Este servidor tem uma linha com setas em cada extremidade apontando para o servidor adjacente à esquerda. Há também uma seta apontando para um servidor estrato 3. O servidor estrato 2 mais à esquerda tem uma seta apontando para um servidor estrato 3. O servidor intermediário estrato 2 tem dois servidores estrato 3 abaixo dele e uma seta indo para cada um deles. Há também uma linha com seta em ambas as extremidades entre estes dois servidores estrato 3.

### Níveis de estrato NTP



Os servidores NTP são organizados em três níveis conhecidos como estratos:

* **Estrato 0** - uma rede NTP obtém a hora de fontes de hora oficiais. Essas fontes, também conhecidas como dispositivos de stratum 0, são dispositivos de pontualidade de alta precisão, com pouco ou nenhum atraso associado a eles.
* **Estrato 1** - Os dispositivos do estrato 1 estão diretamente conectados às fontes de tempo autorizadas. Eles atuam como o principal padrão de horário da rede.
* **Estrato 2** e estratos inferiores - Os servidores estrato 2 são conectados aos dispositivos estrato 1 por meio de conexões de rede. Os dispositivos do stratum 2, como os clientes NTP, sincronizam a hora usando os pacotes NTP dos servidores do stratum 1. Eles também podem atuar como servidores dos dispositivos do stratum 3.

Números menores de stratum indicam que o servidor está mais próximo da fonte de horário autorizada, se comparados aos números de strati maiores. Quanto maior o número do stratum, mais baixo seu nível. A valor máximo da contagem de saltos é 15. O Stratum 16, o nível mais baixo de stratum, indica que um dispositivo não está sincronizado. Servidores de horário no mesmo nível de stratum podem ser configurados para agir como pares com outros servidores de horário no mesmo nível de stratum, para finalidades de backup ou verificação da hora.

12.3.10

## Servidores AAA

A tabela lista as três funções de segurança independentes fornecidas pela estrutura arquitetônica AAA.

| **AAA Fornece** | **Descrição** |
| --- | --- |
| **Autenticação** | * Os usuários e administradores devem provar quem são. * A autenticação pode ser estabelecida usando combinações de nome de usuário e senha, perguntas e respostas de desafio, tokens e outros métodos. * A autenticação AAA fornece uma maneira centralizada de controlar o acesso à rede. |
| **Autorização** | * Após a autenticação do usuário, os serviços de autorização determinam quais recursos o usuário pode acessar e quais operações ele tem permissão para executar. * Um exemplo é “O usuário 'estudante' pode acessar o host ServerXYZ usando apenas SSH.” |
| **Accounting** | * O accounting registra o que o usuário faz, incluindo o que é acessado, a quantidade de tempo em que o recurso é acessado e todas as alterações efetuadas. * O accounting rastreia como os recursos de rede são usados. * Um exemplo é “Usuário 'aluno' acessado host ServerXYZ usando SSH por 15 minutos.“ |

Terminal Access Controller Access-Control System Plus (TACACS) e Remote Authentication Dial-In User Service (RADIUS) são protocolos de autenticação usados para se comunicar com servidores AAA. A seleção do TACACS+ ou RADIUS depende das necessidades da empresa.

Embora ambos os protocolos possam ser usados para comunicação entre um roteador e os servidores de AAA, o TACACS+ é considerado o protocolo mais seguro. Isto é porque todas as trocas de protocolo TACACS+ são criptografadas, enquanto o RADIUS criptografa apenas a senha do usuário. O RADIUS não criptografa nomes de usuário, informações de contabilidade ou qualquer outra informação transportada na mensagem RADIUS.

A tabela lista as diferenças entre os dois protocolos.

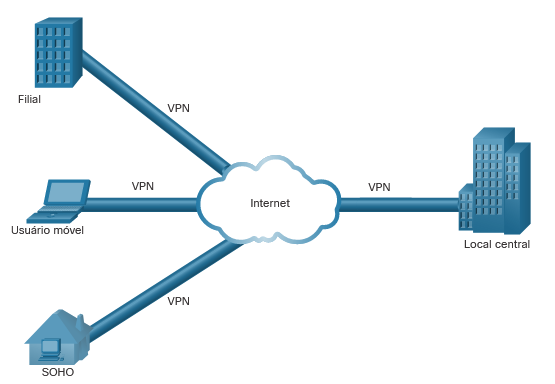
|  | **TACACS+** | **RADIUS** |
| --- | --- | --- |
| **Funcionalidade** | Separa o AAA de acordo com a arquitetura AAA, permitindo a modularidade da implementação do servidor de segurança | Combina autenticação e autorização, mas separa a contabilidade, permitindo menos flexibilidade na implementação do que o TACACS+ |
| **Padrão** | Principalmente com suporte Cisco | Padrão aberto / RFC |
| **Transporte** | TCP | UDP |
| **Protocolo CHAP** | Desafio bidirecional e resposta conforme usado no protocolo de autenticação de handshake de desafio (CHAP) | Desafio unidirecional e resposta do servidor de segurança RADIUS para o cliente RADIUS |
| **Confidencialidade** | Pacote inteiro criptografado | Senha criptografada |
| **Personalização** | Fornece autorização de comandos do roteador por usuário ou por grupo | Não tem opção de autorizar comandos de roteador por usuário ou por grupo |
| **Contabilidade** | Limitado | Abrangente |

12.3.11

**VPN**

Uma VPN é uma rede privada criada em uma rede pública, geralmente a Internet, conforme mostrado na figura.

### Rede Virtual Privada



Em vez de usar uma conexão física dedicada, uma VPN usa conexões virtuais que são roteadas pela Internet da organização para o site remoto. As primeiras VPNs eram túneis IP restritos que não incluíam autenticação ou criptografia dos dados. Por exemplo, Generic Routing Encapsulation (GRE) é um protocolo de encapsulamento desenvolvido pela Cisco que pode encapsular uma ampla variedade de tipos de pacote de protocolo de camada de rede dentro de túneis IP. Isso cria um link ponto-a-ponto virtual com roteadores Cisco em pontos remotos sobre uma rede interconectada IP.

Uma VPN é virtual, pois carrega informações dentro de uma rede privada, mas essas informações são realmente transportadas por uma rede pública. Uma VPN é privada, pois o tráfego é criptografado para manter os dados confidenciais enquanto são transportados pela rede pública.

A VPN é um ambiente de comunicações no qual o acesso é controlado rigorosamente para permitir conexões de mesmo nível em uma comunidade com interesses definidos. A confidencialidade é alcançada criptografando o tráfego dentro da VPN. Hoje, uma implementação segura de VPN com criptografia é o que geralmente é equiparado ao conceito de rede virtual privada.

No sentido mais simples, uma VPN conecta dois endpoints, como um escritório remoto a um escritório central, através de uma rede pública, para formar uma conexão lógica. As conexões lógicas podem ser feitas na Camada 2 ou na Camada 3. Exemplos comuns de VPNs de Camada 3 são GRE, MPLS (Multiprotocol Label Switching) e IPsec. As VPNs de camada 3 podem ser conexões de site ponto a ponto, como GRE e IPsec, ou podem estabelecer qualquer conectividade para muitos sites usando MPLS.

O IPsec é um conjunto de protocolos desenvolvido com o apoio do IETF para obter serviços seguros em redes IP comutadas por pacotes.

Os serviços de IPsec permitem a autenticação, integridade, controle de acesso e confidencialidade. Com o IPsec, as informações trocadas entre sites remotos podem ser criptografadas e verificadas. As VPNs são normalmente implantadas em uma topologia site a site para conectar sites centrais com locais remotos com segurança. Eles também são implantados em uma topologia de acesso remoto para fornecer acesso remoto seguro a usuários externos que viajam ou trabalham de casa. As VPNs de acesso remoto e site-to-site podem ser implantadas usando IPsec.

# Resumo da infraestrutura de segurança de rede

12.4.1

## O que aprendi neste módulo?

**Topologias de rede**

Neste capítulo, você aprendeu a operação básica da infra-estrutura de rede. As infra-estruturas de rede variam muito em função da dimensão da área de cobertura, do número de utilizadores ligados, do número e dos tipos de serviços disponíveis e da área de responsabilidade. As redes são normalmente representadas como topologias físicas e lógicas. Uma topologia física representa as conexões físicas e como os dispositivos finais são conectados. Uma topologia lógica refere-se aos padrões e protocolos que os dispositivos usam para se comunicar. A maioria dos diagramas de topologias são uma combinação de ambos, mostrando como os dispositivos estão fisicamente e logicamente conectados. Os dois tipos mais comuns de infraestruturas de rede são LANs e WANs. O design de LAN com fio do campus consiste em camadas hierárquicas com funções específicas atribuídas a cada camada. A camada de acesso fornece acesso direto à rede para terminais. A camada de distribuição agrega camadas de acesso e oferece ⁪conectividade aos serviços. Por último, a camada central fornece conectividade entre camadas de distribuição em grandes ambientes. Em alguns casos, a distribuição e as camadas principais podem ser combinadas para reduzir o custo e a complexidade.

Arquiteturas de segurança comuns definem os limites do tráfego de entrada e saída da rede. Ao examinar uma topologia que tem acesso a redes externas ou públicas, você deve ser capaz de determinar a arquitetura de segurança. Alguns projetos são tão simples como designar uma rede externa e uma rede interna que são determinados por duas interfaces em um firewall. As redes que exigem acesso público aos serviços geralmente incluem uma DMZ que o público pode acessar, enquanto bloqueia estritamente o acesso à rede interna. ZPFs usam o conceito de zonas para fornecer flexibilidade adicional. Uma zona é um grupo de uma ou mais interfaces que têm funções, recursos e requisitos de segurança semelhantes.

**Dispositivos de segurança**

Existem vários tipos diferentes de firewalls. Os firewalls de filtragem de pacotes (sem estado) fornecem filtragem de Camada 3 e, por vezes, Camada 4. Um firewall de inspeção com estado permite ou bloqueia o tráfego com base no estado, na porta e no protocolo. Firewalls de gateway de aplicativo (firewall proxy) filtram informações nas Camadas 3, 4, 5 e 7. Os firewalls de próxima geração fornecem serviços adicionais além dos gateways de aplicativos, como prevenção integrada de intrusões, reconhecimento e controle de aplicativos para ver e bloquear aplicativos arriscados, acesso a futuros feeds de informações e técnicas para lidar com ameaças de segurança em evolução. Os sistemas de prevenção de intrusões (IPS) e os sistemas de detecção de intrusões (IDS) são usados para detectar potenciais riscos de segurança e alertar/parar tráfego inseguro. IDS/IPS pode ser implementado como baseado em host ou em rede, com vantagens e desvantagens específicas para cada implementação. Dispositivos de segurança especializados estão disponíveis, incluindo o Cisco Advanced Malware Protection (AMP), Cisco Web Security Appliance (WSA) e Cisco Email Security Appliance (WSA). Esses appliances de segurança utilizam os serviços do Cisco Talos Security Intelligence and Research Group. O Talos detecta e correlaciona ameaças em tempo real usando a maior rede de detecção de ameaças do mundo.

**Serviços de segurança**

Os serviços de segurança de rede incluem as seguintes tecnologias. ACLs são uma série de instruções que controlam se um dispositivo encaminha ou descarta pacotes com base nas informações encontradas no cabeçalho do pacote. O SNMP permite que os administradores de rede monitorem e gerenciem o desempenho da rede, localizem e resolvam problemas de rede e planejem o crescimento da rede. O NetFlow fornece estatísticas sobre os pacotes que estão fluindo através de um roteador Cisco ou switch multicamadas. O espelhamento de porta é um recurso que permite que um switch faça cópias duplicadas do tráfego que está passando pelo switch e, em seguida, enviá-lo por uma porta que tenha um monitor de rede conectado. Os servidores Syslog compilam e fornecem acesso às mensagens do sistema geradas pelos dispositivos de rede. O NTP sincroniza a hora do sistema em todos os dispositivos na rede para garantir um carimbo de data/hora preciso e consistente das mensagens do sistema. O AAA é uma estrutura para configurar serviços de autenticação, autorização e contabilidade do usuário. O AAA normalmente usa um servidor TACACS+ ou RADIUS para esse fim. VPNs são redes privadas criadas entre dois pontos de extremidade em uma rede pública.