

Tópicos da Rede Corporativa

**Segurança em Redes de Comunicações
Mestrado em Cibersegurança**

**Mestrado em Engenharia de Computadores e
telemática**

DETI-UA



Objetivos do projeto de rede

- A rede deve ser **modular**

- A rede deve ser **modular**
 - ◆ Apoiar o crescimento e a mudança.
 - ◆ O dimensionamento da rede é facilitado pela adição de novos módulos em vez de redesenhos completos.

- A rede deve ser **resiliente**

- A rede deve ser **resiliente**
 - ◆ Tempo de atividade próximo a 100 por cento.
 - ➡ Se a rede falhar em algumas empresas (por exemplo, financeira), mesmo que por um segundo, pode representar milhões de receita perdida.
 - ➡ Se a rede falhar em um hospital moderno, isso pode representar a perda de vidas.
 - ◆ A resiliência tem custos.
 - ➡ O nível de resiliência deve ser uma compensação entre o orçamento disponível e o risco aceitável.

- Rede deve ter **Flexibilidade** Os

- Rede deve ter **Flexibilidade** Os
 - ◆ negócios mudam e evoluem.
 - ◆ A rede deve se adaptar rapidamente.



Equipamentos

● Trocar

- ◆ Interconexão de Camada 2 OSI
- ◆ Implementa VLAN
- ◆ Roteamento baseado em Spanning Tree
 - ◆ STP, RSTP, MSTP
- ◆ Pontos de acesso sem fio

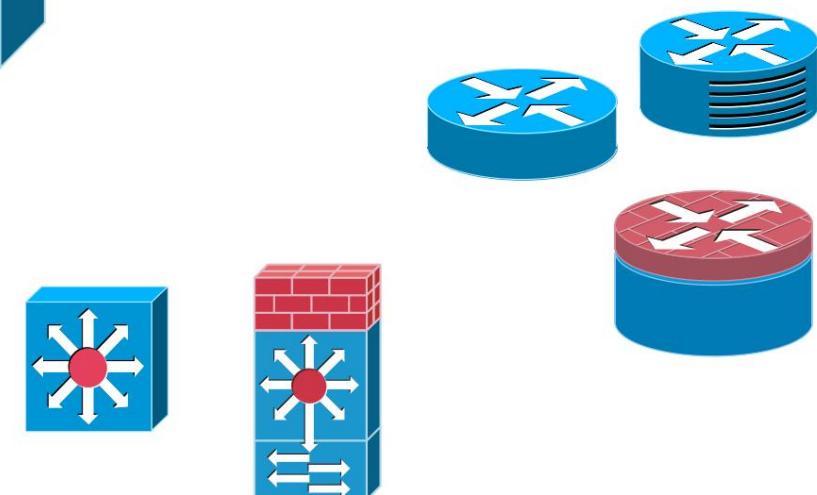


● Roteador

- ◆ Interconexão OSI Layer 3 Possui
- ◆ funcionalidades extras como QoS, Segurança, gateway VPN, monitoramento de rede, etc...

● Interruptor L3

- ◆ Switch+Roteador
- ◆ As funcionalidades de roteamento de gama baixa e média são limitadas
- ◆ High-end tem funcionalidades de roteamento completas
- ◆ Muitos possuem hardware de roteamento L2 dedicado

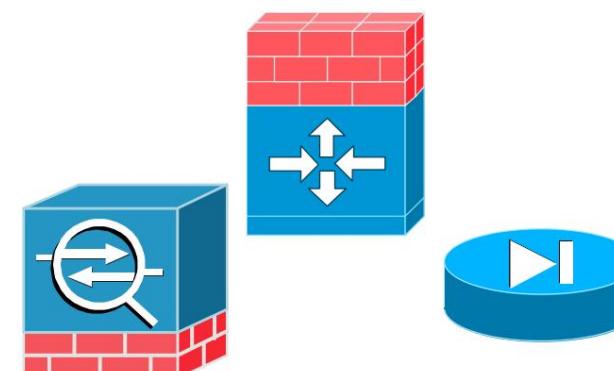


● Roteador com módulos de comutação

- ◆ Switch L3 com recursos completos de roteamento

● Dispositivo de segurança

- ◆ Firewall
- ◆ IDS/IPS (Sistema de Detecção/Prevenção de Intrusão)
- ◆ NAT/PAT
- ◆ Gateway de VPN
- ◆ Proxy de serviços



Como Escolher os Equipamentos

• Tipo

- ◆ L2 Switch, L3 Switch, Roteador + Módulo de comutação, Roteador, ...

• Fabricante

◆ Confiabilidade

◆(esperada) Máximo MTBF (tempo médio entre falhas) possível.

◆Depende de vários fatores:

– Arquiteturas redundantes de Hardware/Eletrônicos, qualidade inerente, restrições ambientais, etc...

◆ Preço

◆Normalmente (nem sempre), um preço mais baixo significa menor confiabilidade.

◆ Assistência

• Faixa/Modelo

◆ Velocidade de processamento/

◆comutação Número de bytes/pacotes processados/comutados por segundo.

– Menor que a soma da velocidade de todas as portas.

◆ Versão do software

◆Protocolos e funcionalidades suportados.

◆Determina também os requisitos de memória.

◆ Número de portas (e velocidade das portas)

◆Ethernet (10 Mbps, 100 Mbps, 1 Gbps, 10 Gbps, ...)

◆Conectores

– Ao cobre ou à fibra.

– RJ-45, conectável de fator de forma pequeno (SFP), conectável de fator de forma pequeno aprimorado (SFP+) ...

◆Com ou sem PoE (Power over Ethernet)

– Para telefones VoIP, Access Points, etc...

◆ Número de vagas

◆Para módulos adicionais de porta/processamento.

NETGEAR®



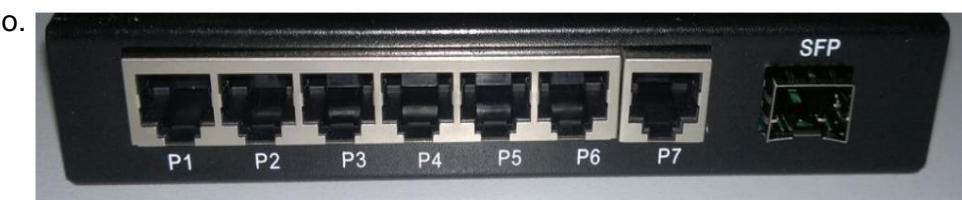
D-Link®
Building Networks for People

JUNIPER
NETWORKS

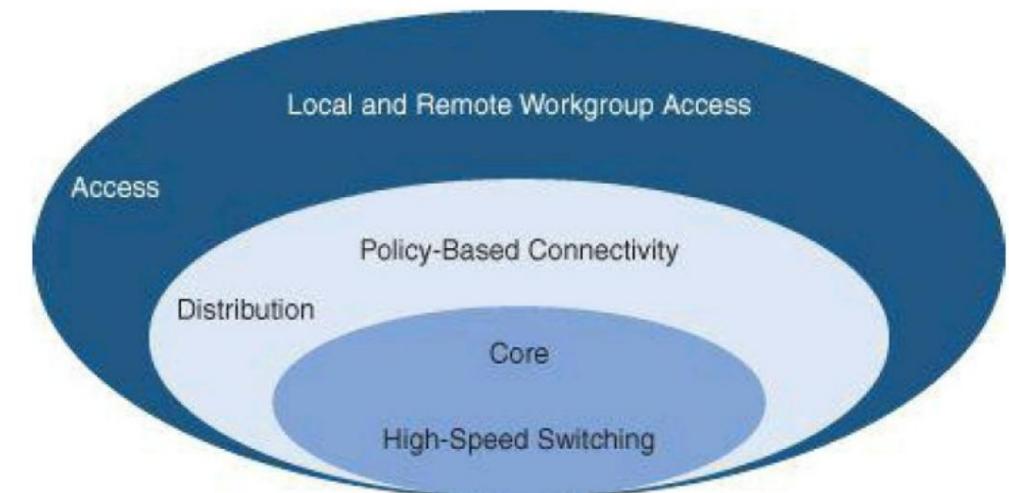


HUAWEI

Alcatel-Lucent



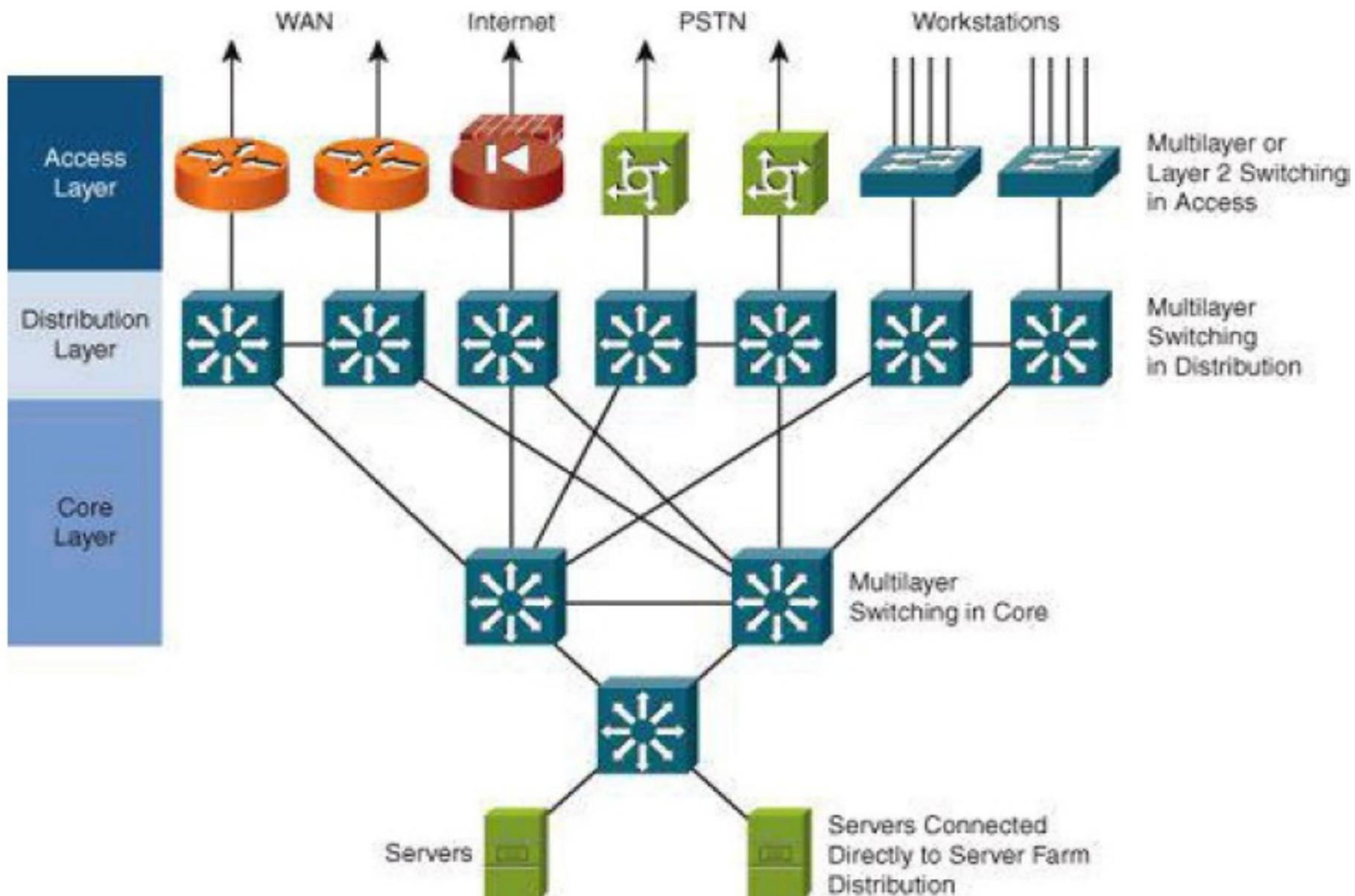
Modelo de rede hierárquica



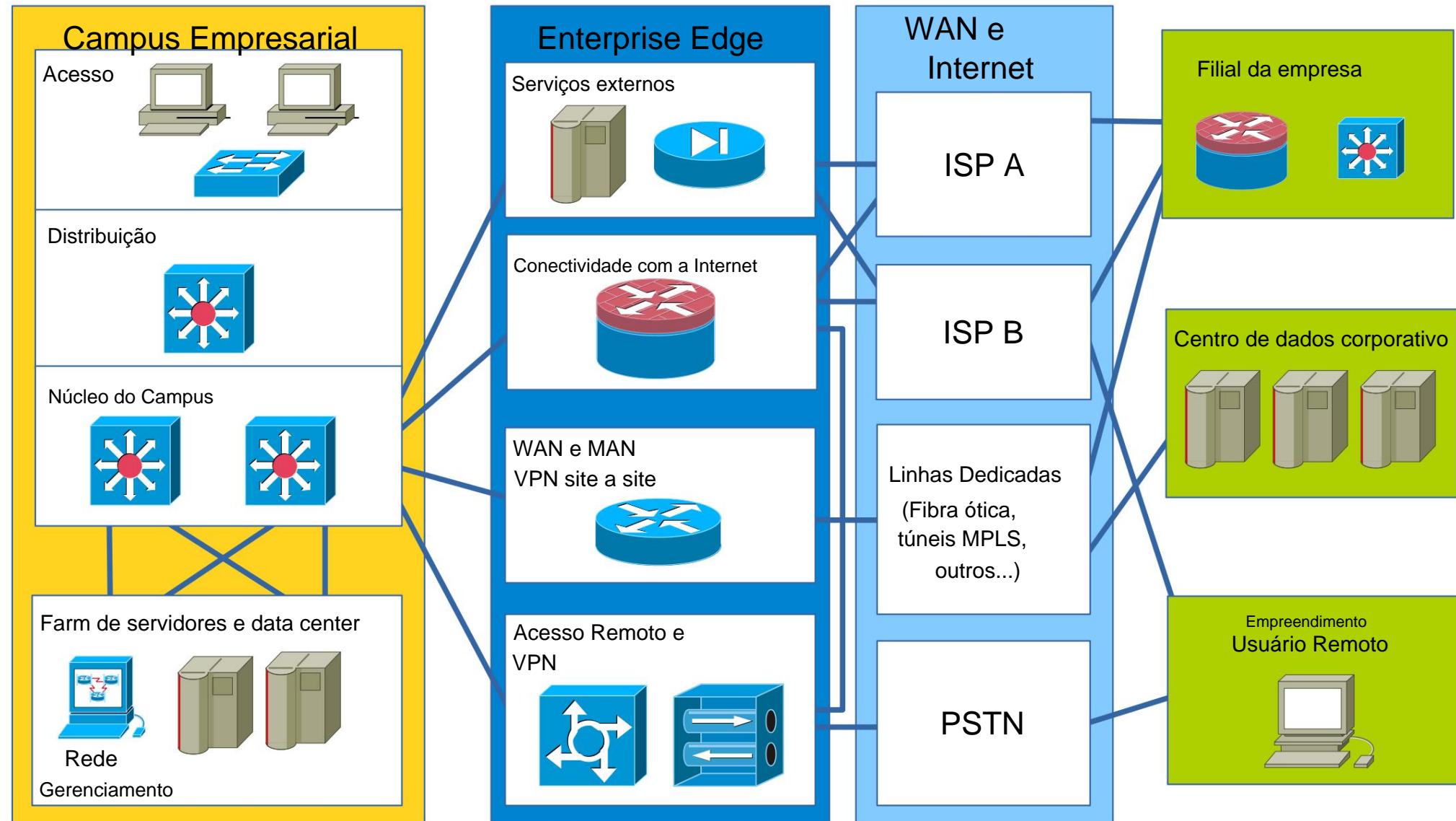
- Camada de acesso
 - ◆ Fornece acesso do usuário à rede.
 - ◆ Geralmente incorpora dispositivos LAN comutados que fornecem conectividade a estações de trabalho, telefones IP, servidores e pontos de acesso sem fio.
 - ◆ Para usuários remotos ou sites remotos, forneça uma entrada para a rede através da tecnologia WAN.
- Camada de distribuição
 - ◆ Agrega dispositivos LAN.
 - ◆ Segmenta grupos de trabalho e isola problemas de rede.
 - ◆ Agrega conexões WAN na borda do campus e fornece conectividade baseada em políticas.
 - ◆ Implementa políticas de QoS.
- Camada central
 - ◆ Um backbone de alta velocidade.
 - ◆ Core é crítico para a conectividade, deve fornecer um alto nível de disponibilidade e se adaptar rapidamente às mudanças.
 - ◆ Deve fornecer escalabilidade e convergência rápida.
 - ◆ Deve fornecer um ponto de integração para o data center.



Uma Rede Hierárquica



Projeto de Rede Modular



Módulos de rede (1)

- Campus

- Campus
 - ◆ Centro operacional de uma empresa.
 - ◆ Este módulo é onde a maioria dos usuários acessa a rede.
 - ◆ Combina uma infraestrutura básica de comutação e roteamento inteligentes com mobilidade e segurança avançada.

- Centro de dados

- Centro de dados
 - ◆ Datacenters redundantes fornecem backup e replicação de aplicativos.
 - ◆ A rede e os dispositivos oferecem balanceamento de carga de servidor e aplicativo para maximizar o desempenho.
 - ◆ Permite que a empresa escala sem grandes mudanças na infraestrutura.
 - ◆ Pode ser localizado no campus como um farm de servidores e/ou em uma instalação remota.

- Filial

- Filial
 - ◆ Permite que as empresas estendam aplicativos e serviços da matriz para locais e usuários remotos ou para um pequeno grupo de filiais.
 - ◆ Fornece acesso seguro a aplicativos de vídeo, dados de missão crítica e voz.
 - ◆ Deve fornecer uma arquitetura robusta com altos níveis de resiliência para todas as filiais.



Módulos de rede (2)

- **WAN e MAN**

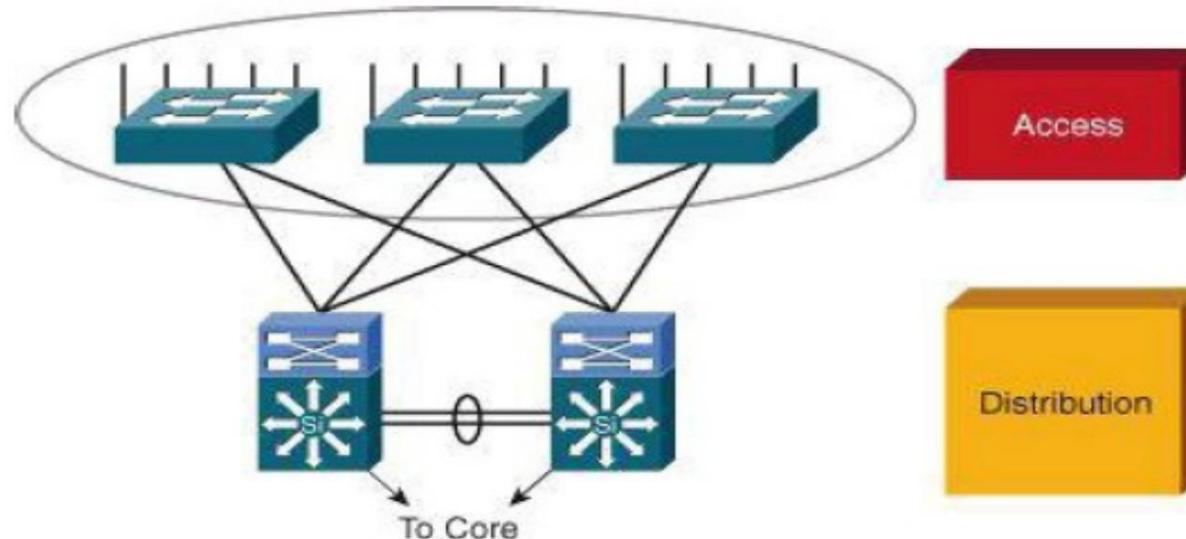
- ◆ Oferece a convergência de serviços de voz, vídeo e dados.
- ◆ Permite à empresa uma presença econômica em grandes áreas geográficas.
- ◆ QoS, níveis de serviço granulares e opções abrangentes de criptografia ajudam a garantir a entrega segura para todos os sites.
- ◆ A segurança é fornecida com VPNs multiserviço (IPsec e MPLS) sobre comunicações de Camada 2 ou Camada 3.

- **Usuário Remoto**

- ◆ Permite que as empresas forneçam serviços de voz e dados com segurança para um pequeno escritório remoto/escritório doméstico (SOHO) por meio de um serviço de acesso de banda larga padrão.
- ◆ Permite um login seguro na rede por meio de uma VPN e acesso a aplicativos e serviços autorizados.



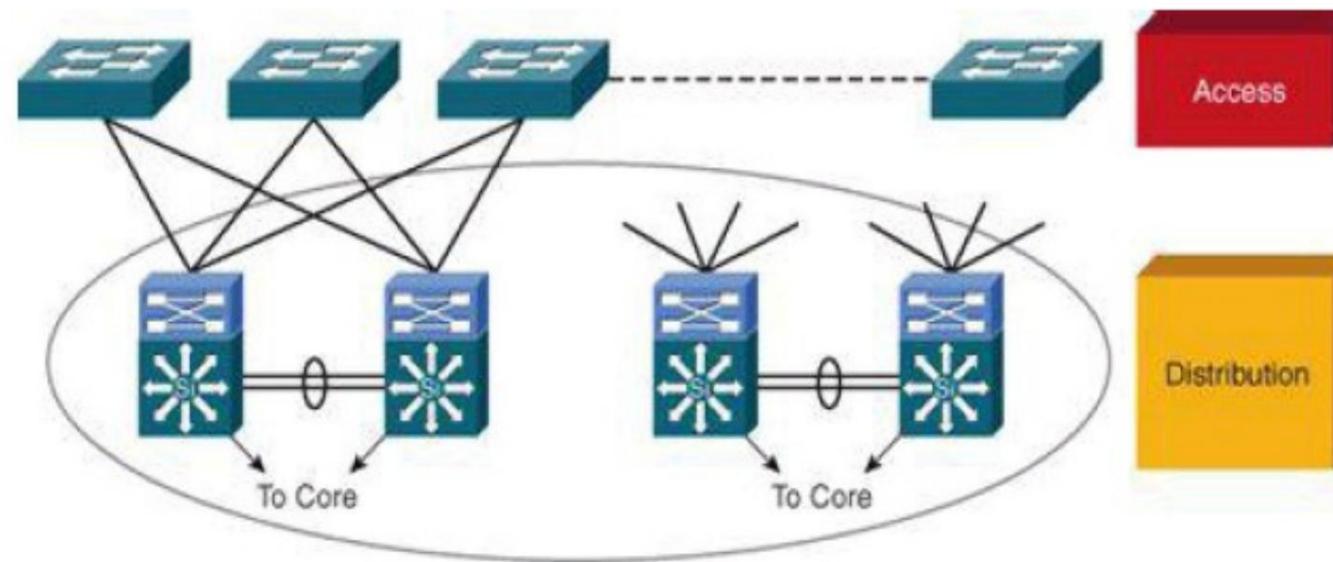
Projetando a Camada de Acesso



- Alta disponibilidade
 - ◆ Redundância de gateway padrão usando várias conexões de switches de acesso a switches redundantes da camada de distribuição.
 - ◆ Fontes de alimentação redundantes.
- Outras considerações
 - ◆ Convergência: a camada de acesso deve fornecer convergência perfeita de voz para rede de dados e fornecer roaming LAN sem fio (WLAN).
 - ◆ Segurança: para segurança adicional contra acesso não autorizado à rede, a camada de acesso deve fornecer ferramentas como IEEE 802.1X, segurança de porta, snooping DHCP e inspeção ARP dinâmica (DAI).
 - ◆ Qualidade de serviço (QoS): A camada de acesso deve permitir a priorização do tráfego de rede crítico usando classificação de tráfego e enfileiramento o mais próximo possível da entrada da rede.
 - ◆ IP multicast: a camada de acesso deve suportar rede eficiente e gerenciamento de largura de banda usando recursos como snooping do Internet Group Management Protocol (IGMP).



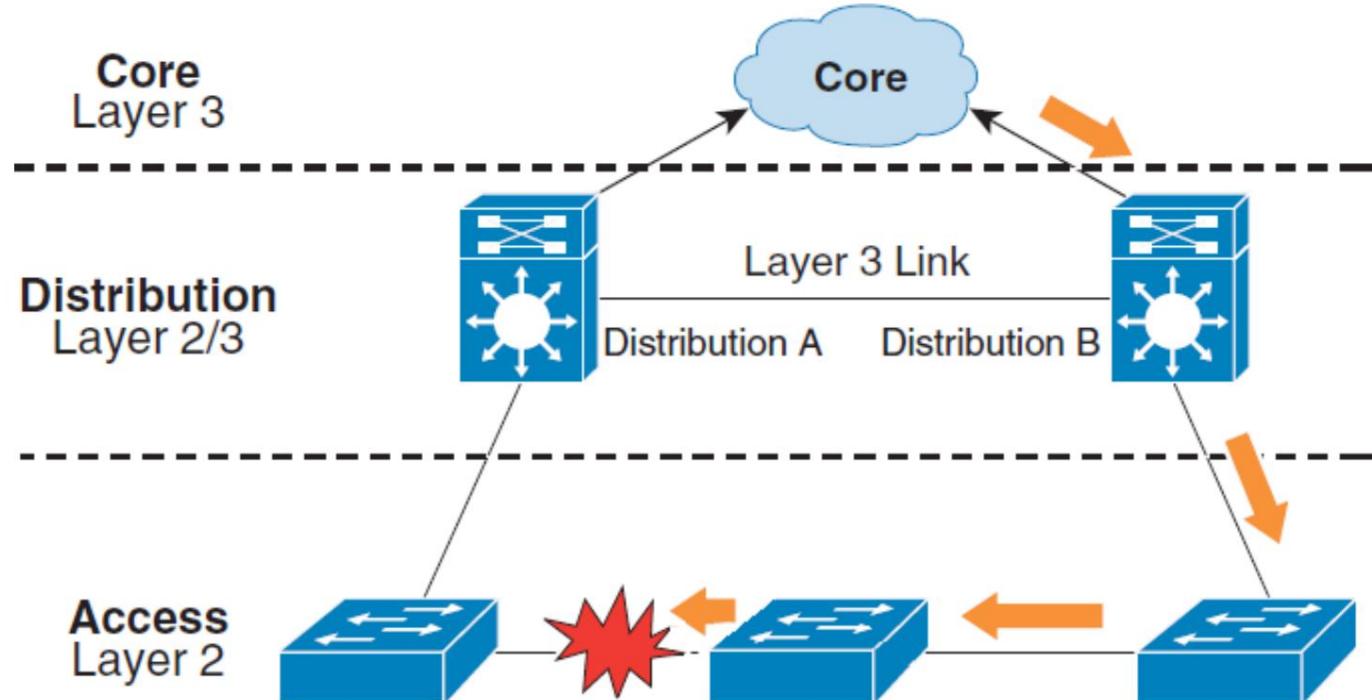
Projetando a camada de distribuição



- Usa uma combinação de Camada 2 e comutação multicamada para segmentar grupos de trabalho e isolar problemas de rede, evitando que afetem a camada central.
- Conecta serviços de rede à camada de acesso e implementa QoS, segurança, balanceamento de carga de tráfego e implementa políticas de roteamento.
- Principais preocupações de design: alta disponibilidade, balanceamento de carga, QoS e provisionamento.
- Em algumas redes, oferece uma rota padrão para acessar roteadores de camada e executa protocolos de roteamento dinâmico ao se comunicar com roteadores principais.
- A camada de distribuição geralmente é usada para encerrar VLANs dos switches da camada de acesso.
- Para melhorar ainda mais o desempenho do protocolo de roteamento, resume as rotas da camada de acesso.
- Para implementar a conectividade baseada em políticas, executa tarefas como roteamento e filtragem controlados e QoS.

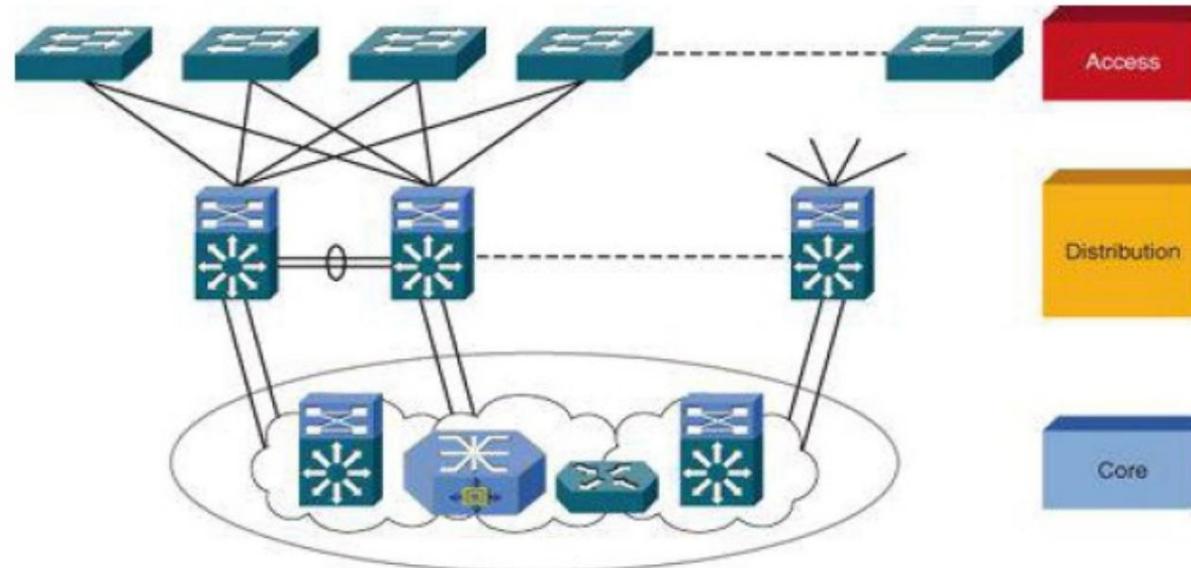


Evite o encadeamento



- Ao usar um link L3 entre switches da camada de distribuição
 - ◆ Na camada de acesso, qualquer caminho de um switch não deve exigir outro switch da camada de acesso.
 - ◆ Na camada de distribuição, qualquer caminho entre os switches da camada de distribuição não deve exigir um switch da camada de acesso.
- Ao usar um link L2 entre switches da camada de distribuição
 - ◆ A cadeia em série é aceitável, no entanto, pode
 - ➡ sobrecarregar alguns switches da camada de acesso.
 - ➡ Poderia aumentar a convergência STP em caso de falha.

Projetando a camada principal

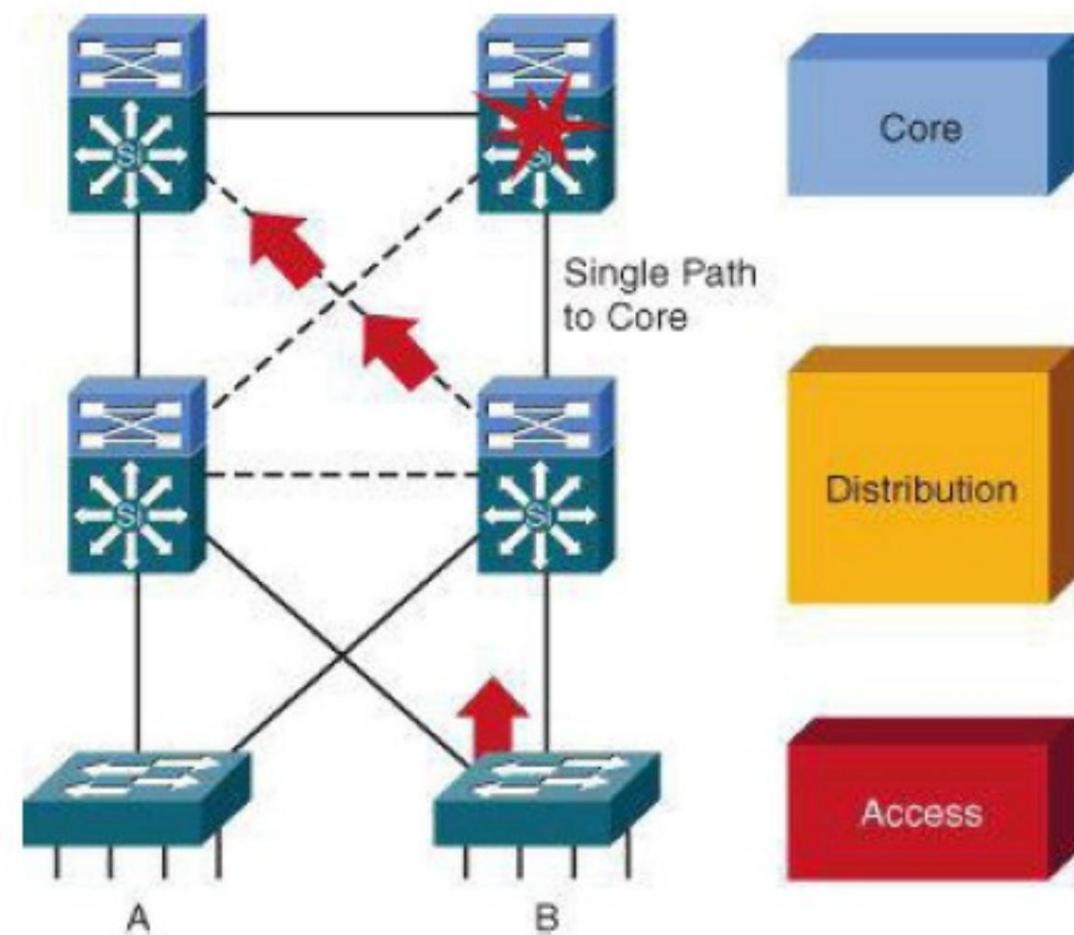


- Backbone para conectividade do campus e é o ponto de agregação para as outras camadas.
- Deve fornecer escalabilidade, alta disponibilidade e convergência rápida para a rede.
 - ◆ A camada principal deve ser dimensionada facilmente.
 - ◆ Ambiente de alta velocidade que deve usar aceleração de hardware, se possível.
 - ◆ O núcleo deve fornecer um alto nível de redundância e se adaptar às mudanças rapidamente.
 - ◆ Dispositivos principais devem ser mais confiáveis
 - ◆ Acomode falhas redirecionando o tráfego e respondendo rapidamente às mudanças na topologia da rede.
 - ◆ Implementa protocolos e tecnologias escaláveis.
 - ◆ Fornece caminhos alternativos e balanceamento de carga.
 - ◆ A manipulação de pacotes deve ser evitada, como verificação de listas de acesso e filtragem, o que pode retardar a comutação de pacotes.
- Nem todas as implementações de campus exigem um núcleo de campus.
- As funções do núcleo e da camada de distribuição podem ser combinadas na camada de distribuição para um campus menor.



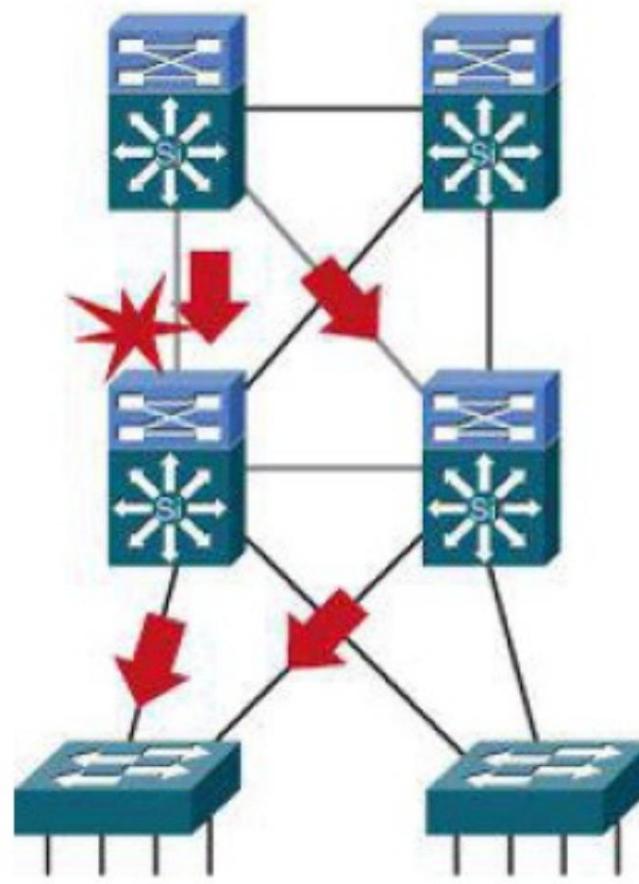
Forneça caminhos alternativos

- Um link adicional que fornece um caminho alternativo para um segundo switch principal de cada switch de distribuição oferece redundância para suportar uma única falha de link ou nó.



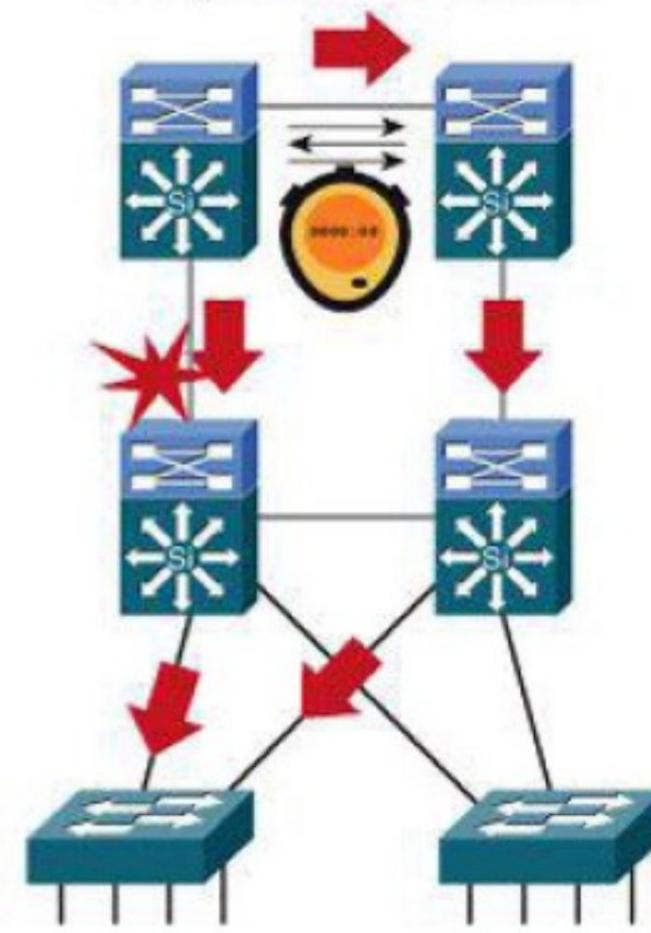
Núcleo Triângulos Redundantes

Triangles: Link or box failure does *not* require routing protocol convergence.



Model A

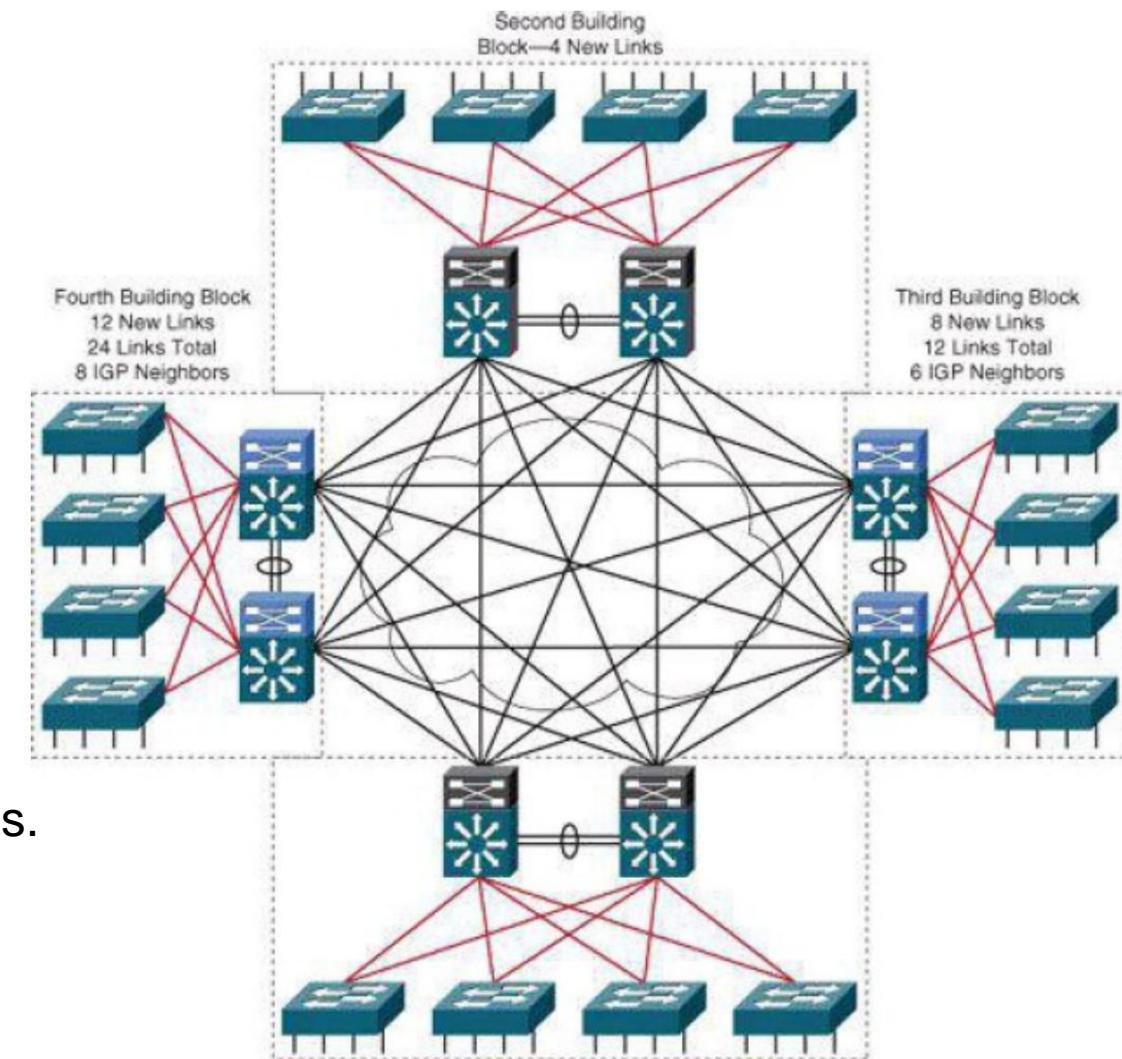
Squares: Link or box failure requires routing protocol convergence.



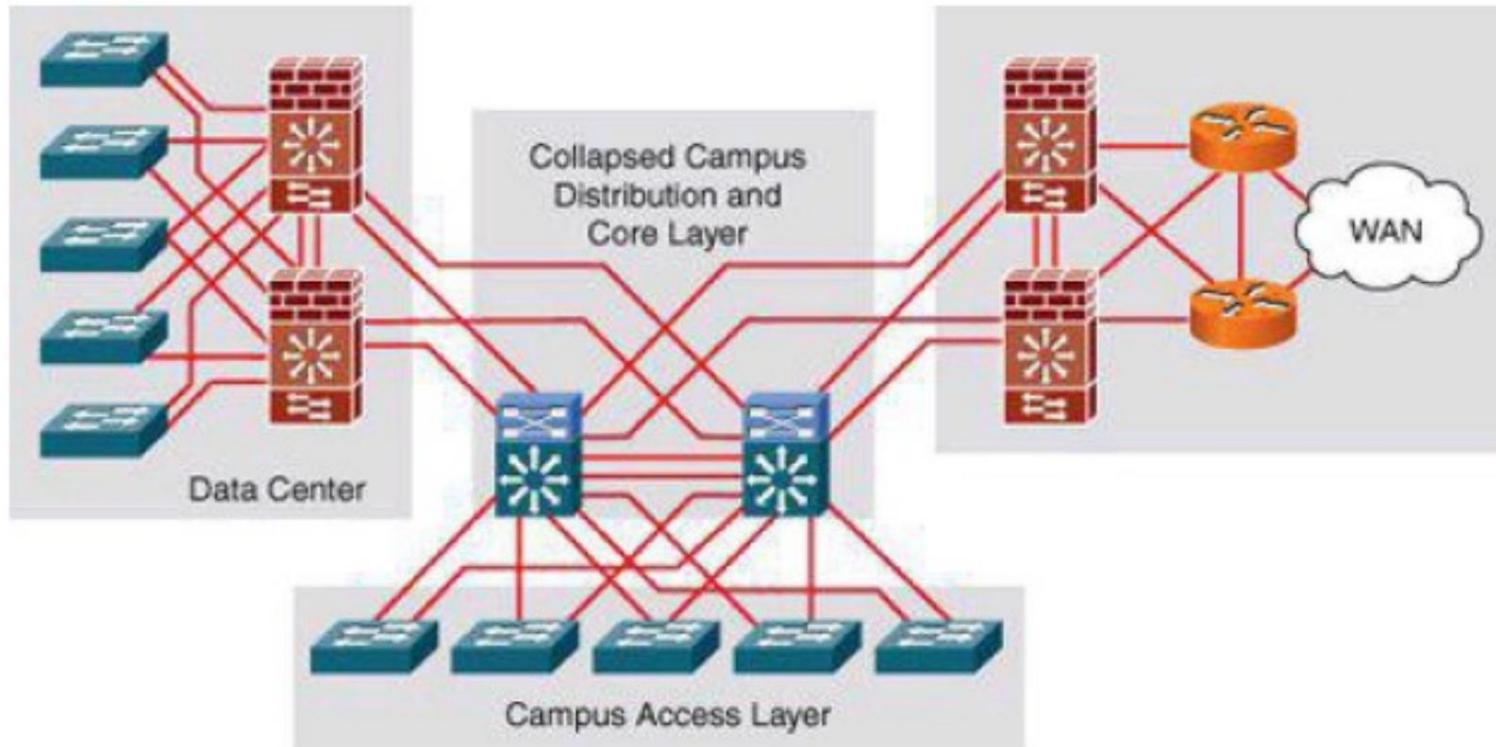
Model B

Sem uma camada central

- Os switches da camada de distribuição precisam estar totalmente em malha.
- Pode ser difícil de dimensionar.
- Aumenta os requisitos de cabeamento.
- A complexidade de roteamento de um projeto de malha completa aumenta à medida que novos vizinhos são adicionados.
- Pode ser usado em campus pequeno sem perspectiva de crescimento.



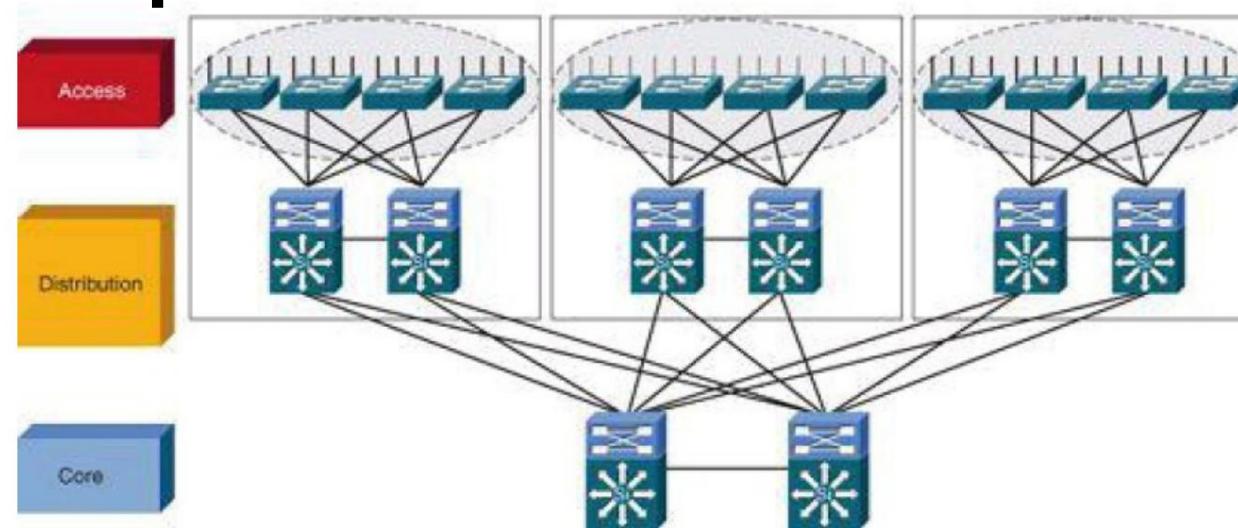
Arquitetura da Camada Principal Recolhida



- Em redes menores, o núcleo e a camada de distribuição podem ser apenas um,
 - ◆ Elimina a necessidade de hardware de comutação extra e simplifica a implementação da rede.
- No entanto, elimina as vantagens da arquitetura multicamada, especificamente o isolamento de falhas.



Evite pontos únicos de falha



- Com um design hierárquico,
 - ◆ Nas camadas de distribuição e núcleo, os pontos únicos de falha são fáceis de evitar com links redundantes.
 - ✚ Não se esqueça de energia e refrigeração redundantes!
 - ◆ Na Camada de Acesso, todos os switches L2 são pontos únicos de falha (somente) para o usuário conectado a eles,
 - ✚ Solução 1, hardware de backup redundante ativado por um mecanismo de supervisão (proprietário) para “substituir” o equipamento defeituoso.
 - Copia a configuração e o estado completos para o hardware de backup.
 - ✚ Solução 2, ter múltiplas conexões entre cada terminal de usuário e diferentes chaves de acesso
 - Requer várias placas de rede nos terminais do usuário e mais plugues/fiação.
 - Mais barato?

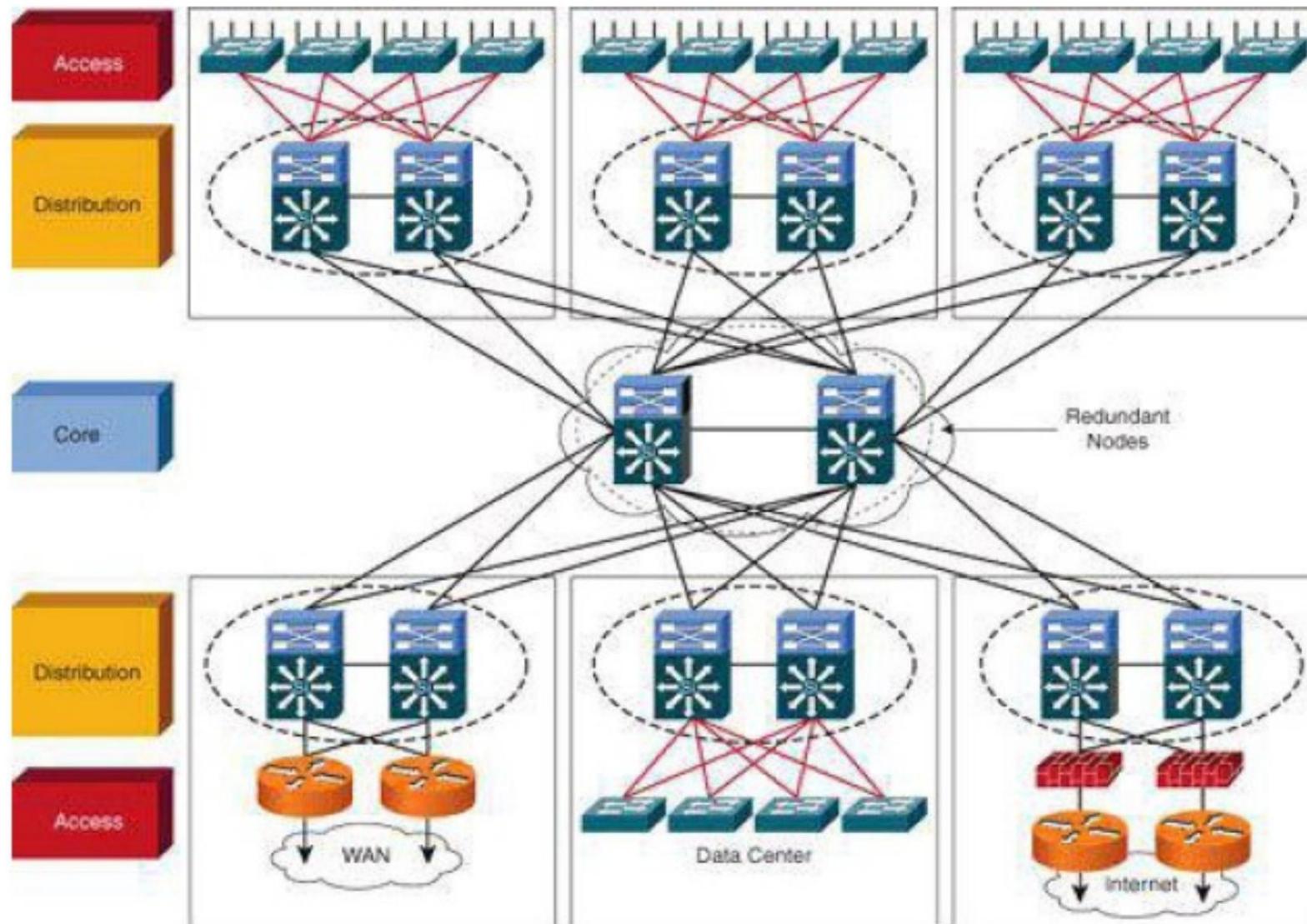


Evite muita redundância



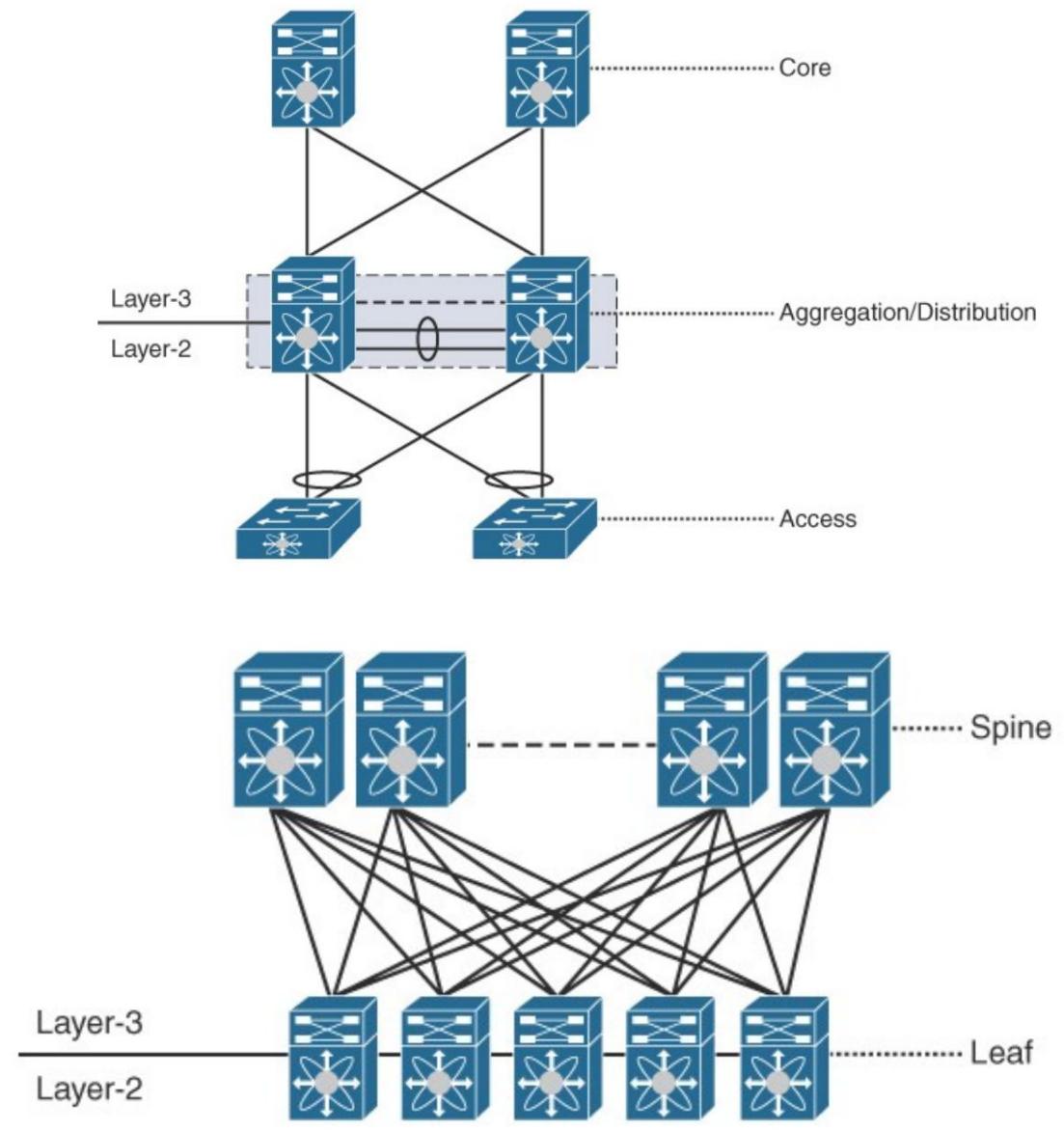
- aumenta,
 - ◆ Complexidade de roteamento
 - ◆ Número de portas usadas
 - ◆ Fiação

Redundância ideal



Topologia CLOS do Datacenter

- Com implantações de data center em larga escala, as topologias de três camadas se tornaram gargalos de escala.
- A topologia clássica de três camadas evoluiu para uma topologia CLOS.
 - Original projetado por Charles Clos em 1950 para encontrar uma maneira mais eficiente de lidar com transferências de chamadas telefônicas.
- Eliminando a necessidade de STP a rede evoluiu para maior estabilidade e escalabilidade.
- A Camada 3 se move para a Camada de Acesso.
- Geralmente chamada de arquitetura Spine-and-Leaf.



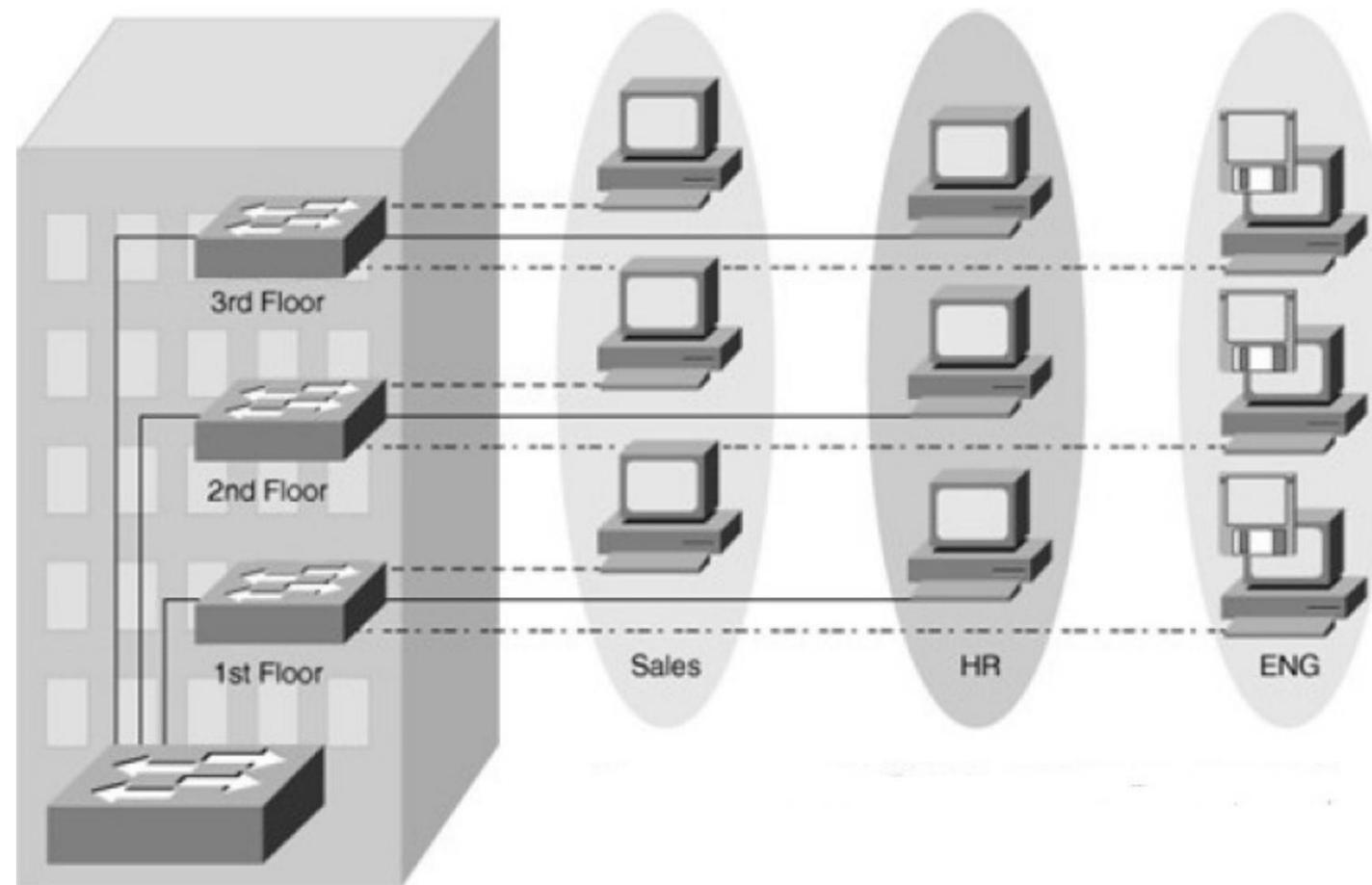
LANs virtuais

- Grupo de portas de switch individuais em *grupo de trabalho lógico* comutado
 - ◆ Restringir o domínio de transmissão a portas de membro de VLAN
 - ◆ designadas A comunicação entre VLANs requer um roteador.
- Resolve os problemas de escalabilidade de grandes redes planas ,
 - ◆ dividindo um único domínio de broadcast em vários domínios de broadcast menores.

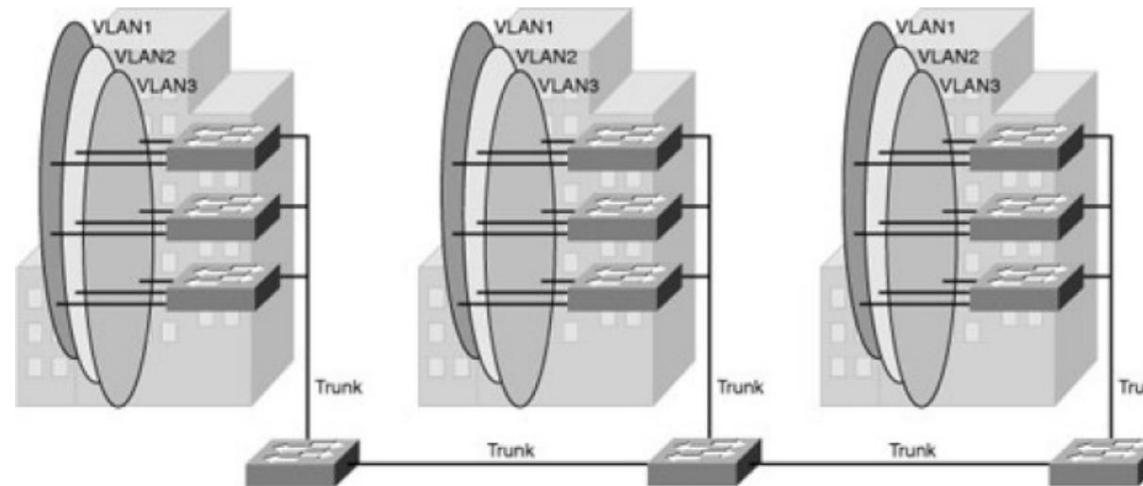


Implementando VLANs

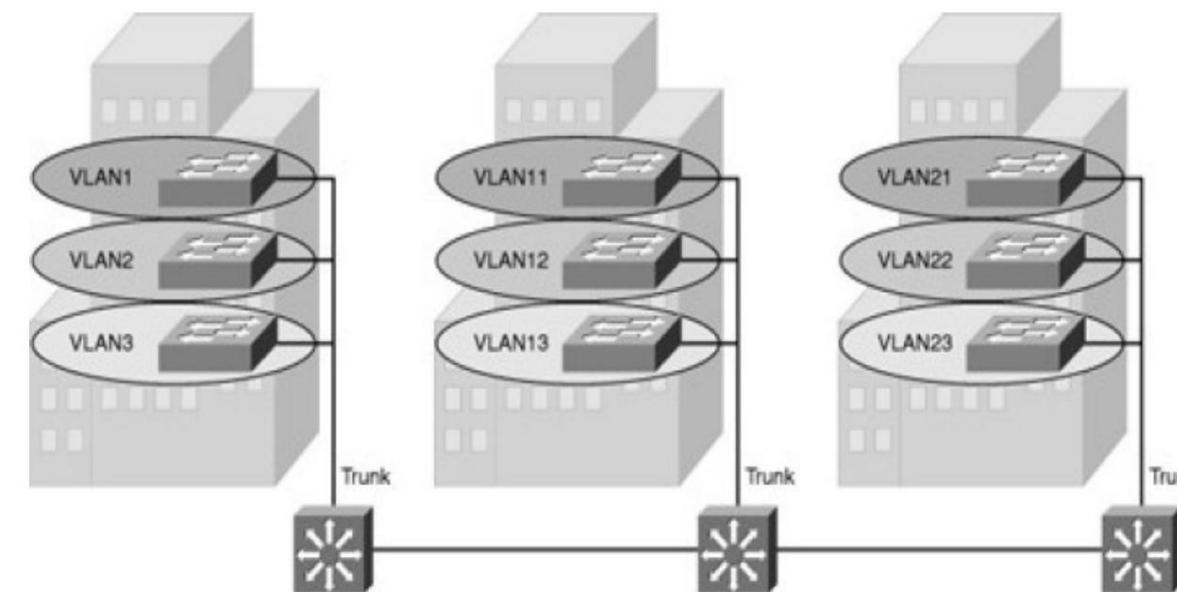
- VLAN é um grupo lógico de dispositivos finais com um conjunto comum de requisitos independente de sua localização física.



Modelos de segmentação de VLAN



- VLAN de ponta a ponta
 - ◆ As VLANs estão associadas a portas de switch amplamente分散 pelas redes



- VLAN Local
 - ◆ As VLANs locais são geralmente confinadas a um armário de fiação.

Segmentação de VLAN (exemplos)

• VLANs locais

- ◆ Por serviço/função
 - Telefones VoIP, Videoconferência, impressoras, câmeras, PCs, servidores, ...
- ◆ Por função de usuário
 - Engenheiros I, engenheiros II, técnicos, administradores, ...
- ◆ Por local
 - Edifício I, piso 4, ala direita, etc...
- ◆ Mistura de serviço/função, função, localização,
 - por exemplo: VLAN de telefones VoIP, dos Engenheiros no Prédio I.

• VLANs de ponta a ponta

- ◆ Serviços/funções que têm um escopo global dentro da rede.
- ◆ rede sem fio
 - Mesma rede IP (mesmo endereço IP) independentemente da localização.
 - Para evitar alterações de IP ao se deslocar de um local para outro.
- ◆ VLAN de administração (opcional)
 - VLAN utilizada pelo administrador da rede para acessar remotamente os equipamentos da rede.
 - Mesmo administrador de (todos) os equipamentos independente da localização.



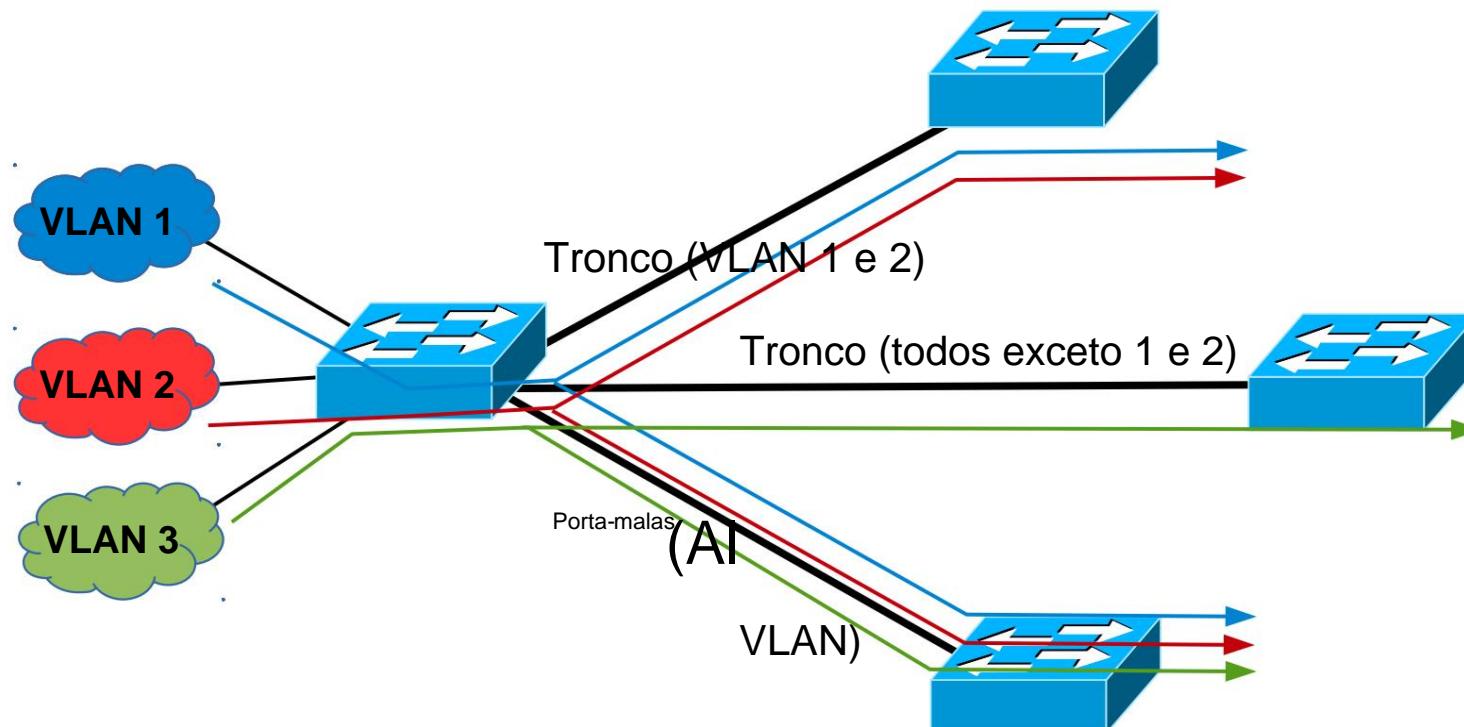
Finalidade da segmentação de VLAN

- Juntar na mesma rede lógica serviços/terminais/usuários com as mesmas políticas de tráfego/segurança/QoS.
 - ◆ Cada VLAN deve ter uma (sub-)rede IP exclusiva.
 - ◆ Pode ter mais de uma (sub-)rede IP.
 - Incluindo redes IPv4 públicas e IPv4 privadas.
 - E redes IPv6.
- VLANs vizinhas (locais) com políticas de tráfego/segurança/QoS semelhantes devem ter (sub-)redes IP que possam ser resumidas/agregadas.
 - ◆ Ex: VLAN de telefones VoIP no Prédio 1 (VLAN 21: 200.0.0.0/24)
 - ◆ VLAN de telefones VoIP no Edifício 2 (VLAN 22: 200.0.1.0/24)
 - ◆ Endereço resumido/agregado de VLAN21+VLAN22: 200.0.0.0/23.

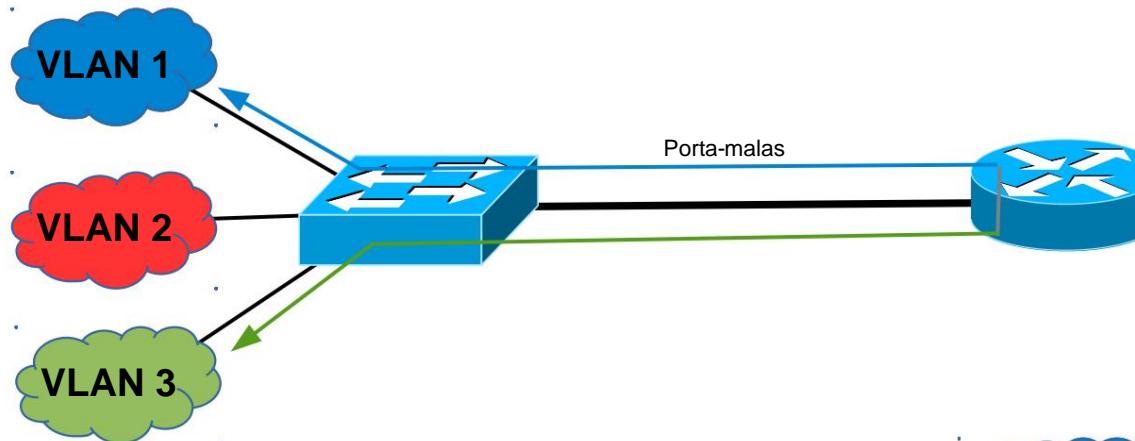


Links Troncos

- Um tronco VLAN transporta tráfego para várias VLANs usando IEEE 802.1Q.
 - O encapsulamento Inter-Switch Link (ISL) é uma alternativa, mas está ficando obsoleto.
- Trunks podem transportar todas as VLANs ou apenas algumas!

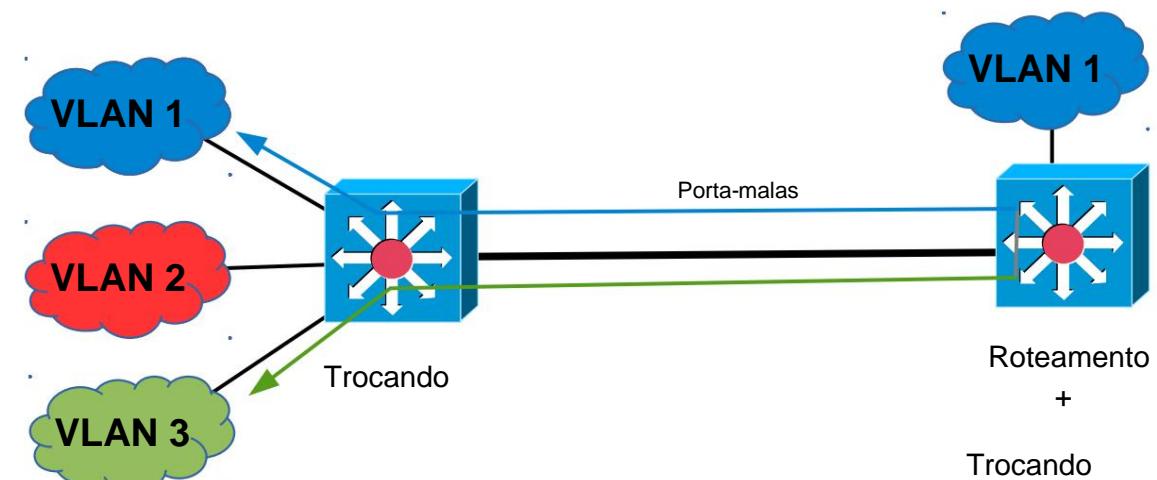
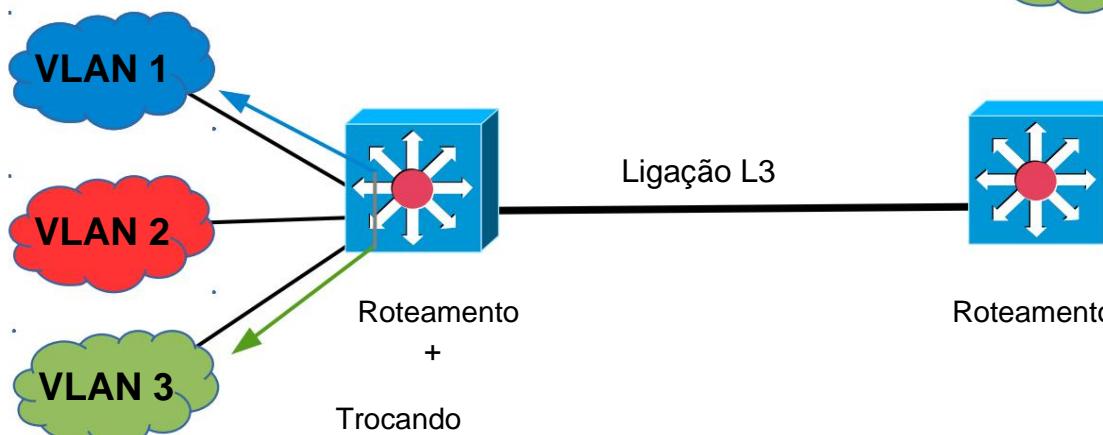


Roteamento Inter-(V)LAN



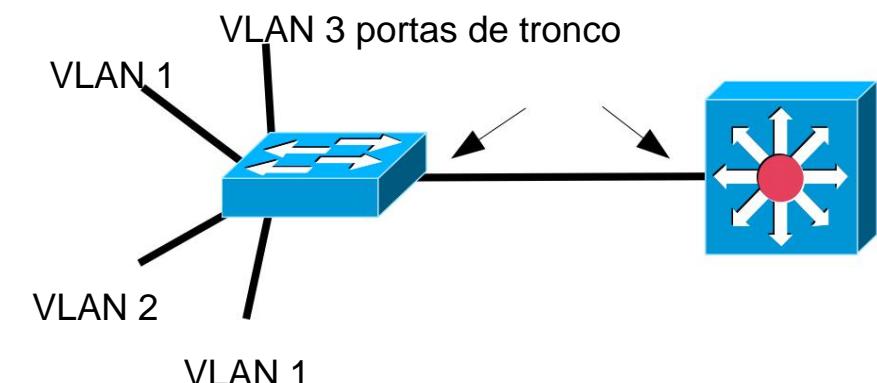
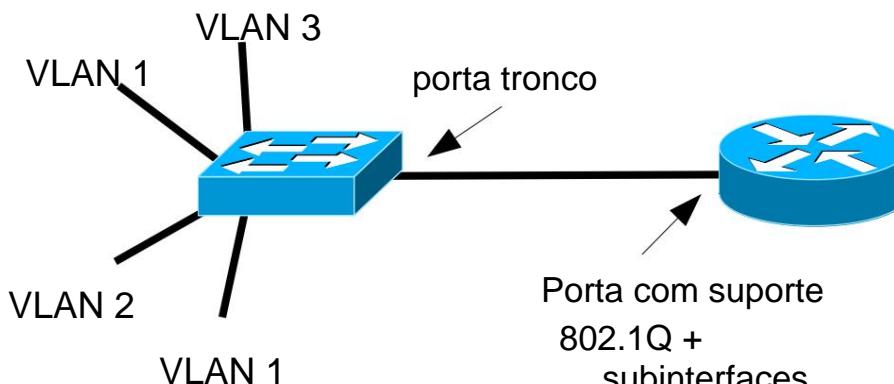
- Chave L2 + Roteador
 - ◆ Não permite VLANs de ponta a ponta.

- Interruptor L3 + Interruptor L3
 - ◆ O tráfego entre VLANs deve “viajar” até o primeiro Switch L3 realizando o Roteamento.

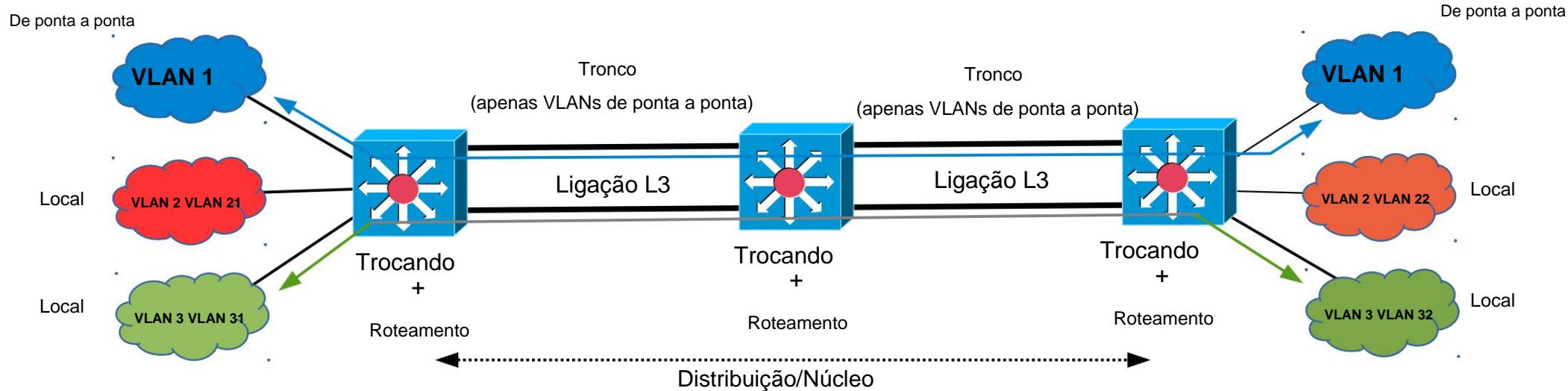


Conexão IP entre VLANs

- Para se comunicar entre diferentes VLANs é necessário usar a Camada 3 (Roteamento IP).
- Soluções comuns:
 - Um roteador com suporte para 802.1Q,
 - conectando a interface do roteador físico a uma porta de tronco.
 - A interface física do roteador é subdividida em subinterfaces (uma para cada VLAN).
 - O gateway IP para um host VLAN é o endereço IP da respectiva subinterface no Roteador.
 - Um switch de camada
 - 3, conectando ambos os switches (L3 e L2) usando portas de tronco.
 - Cada VLAN é mapeada para uma interface virtual da Camada 3.
 - O gateway IP para um host VLAN é o endereço IP da respectiva interface virtual no switch L3.



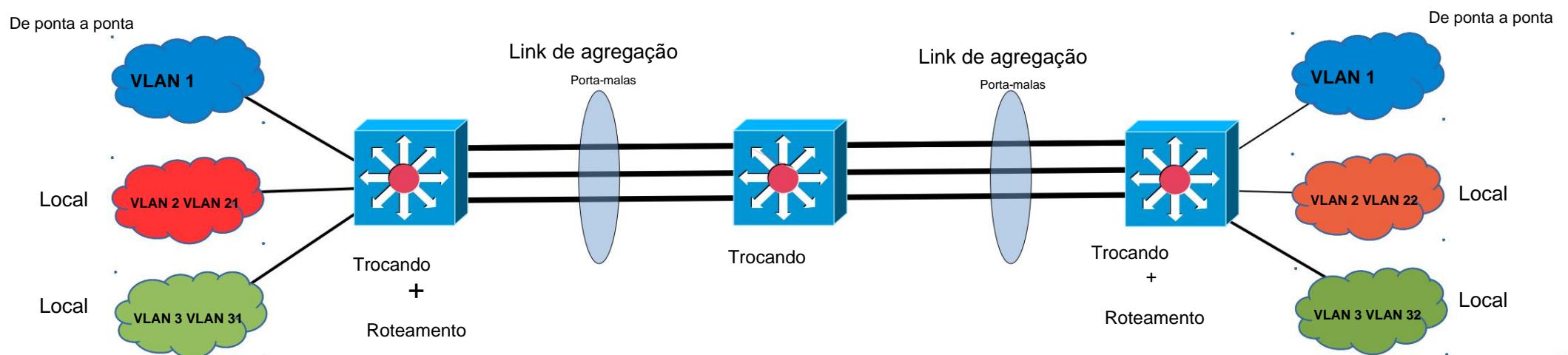
Tráfego Inter-(V)LAN (1)



- O tráfego de VLANs de ponta a ponta **deve ser alternado** nas camadas de distribuição/núcleo usando
 - ◆ um tronco (somente para VLANs de ponta a ponta).
- O tráfego de VLANs locais **deve ser roteado** pelas camadas de distribuição/núcleo
 - ◆ Usando links padrão da camada 3.
 - ◆ Usando roteamento estático (não é a melhor solução!).
 - ◆ Troque as informações de roteamento apenas por meio dos links L3
 - ◆ As VLANs de ponta a ponta devem ser interfaces passivas para os processos de roteamento.
 - As rotas não são trocadas → O tráfego não é roteado!

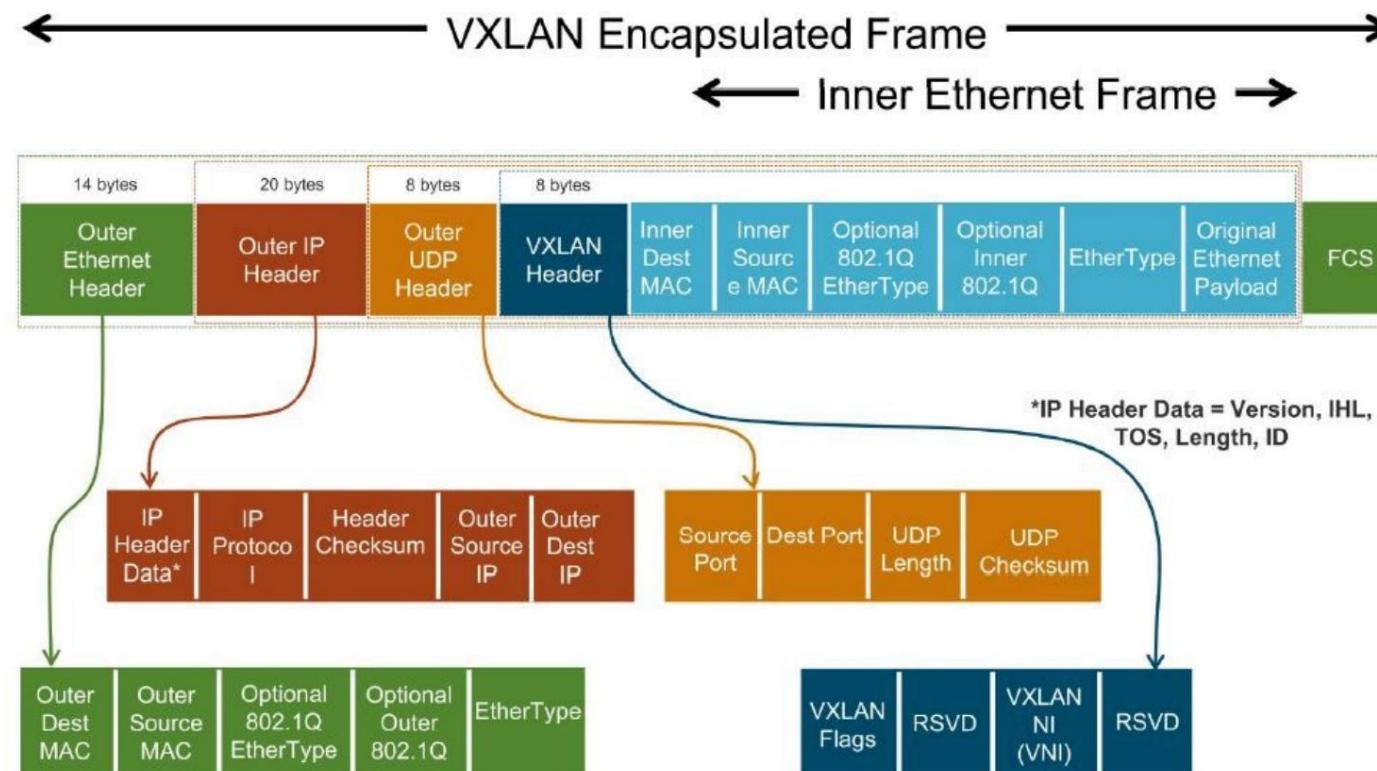
Agregação de Link Ethernet

- A taxa de transferência/velocidade de um link de conexão pode não ser suficiente para atender aos requisitos.
- Múltiplos links Ethernet podem ser agregados, fornecendo uma conexão de tronco contínua com N vezes a taxa de transferência/velocidade única de um link.
- Os quadros Ethernet são “balanceados por carga” entre todos os links físicos disponíveis.



LAN virtual extensível (VXLAN)

- Encapsula quadros Ethernet de Camada 2 OSI em datagramas UDP de Camada 4.
 - ◆ Porta padrão 4789.
- Alternativa para 802.1Q.

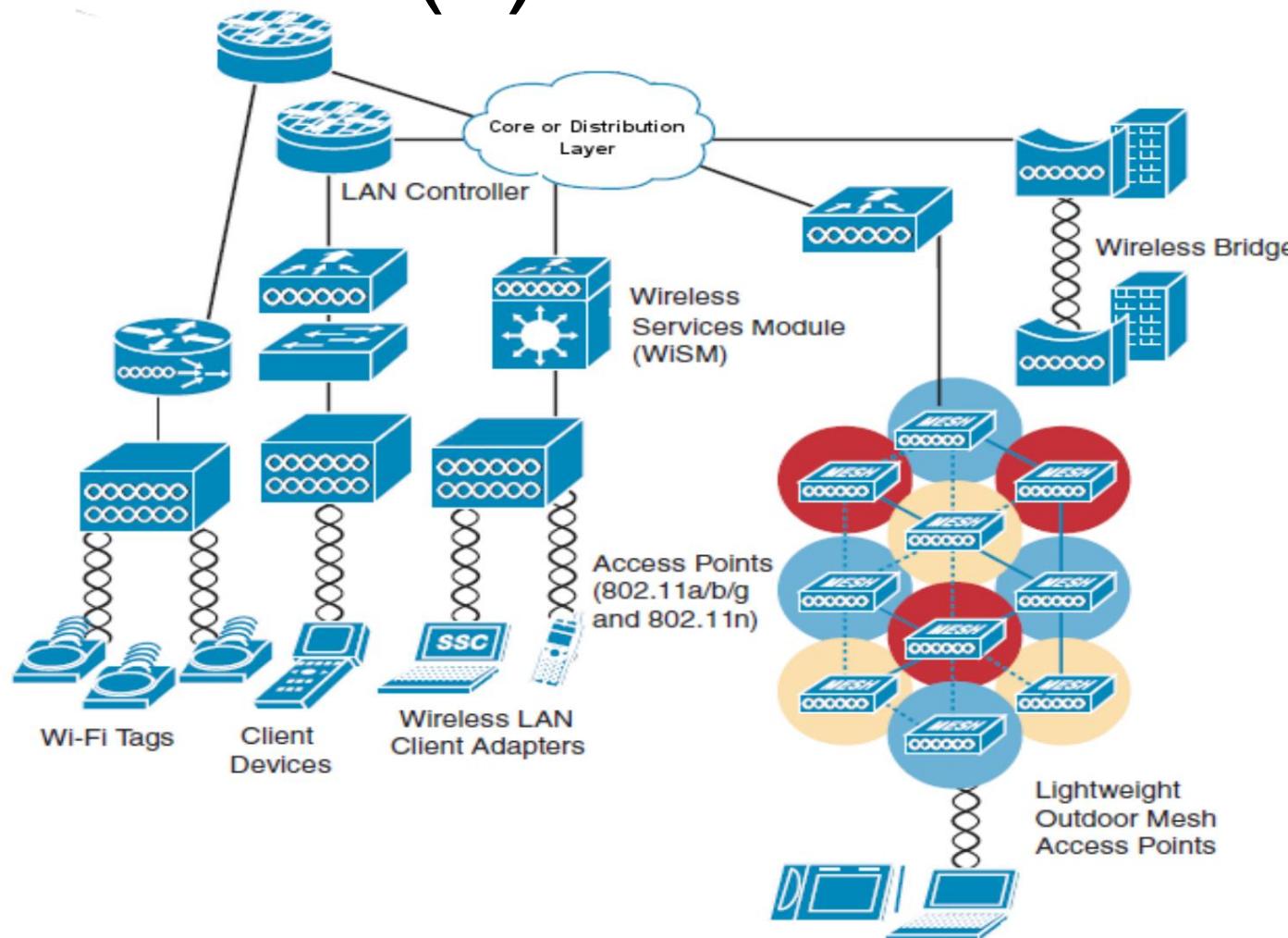


Protocolo Spanning Tree

- O STP permite que a rede bloquee interfaces de forma determinística e forneça uma topologia sem loop em uma rede com links redundantes.
- Existem vários padrões e recursos do STP:
 - ◆ STP é a versão IEEE 802.1D original (802.1D-1998) que fornece uma topologia sem loop em uma rede com links redundantes.
 - ◆ RSTP, ou IEEE 802.1W, é uma evolução do STP que fornece convergência mais rápida do STP.
 - ◆ Multiple Spanning Tree (MST) é um padrão IEEE. O MST mapeia várias VLANs na mesma instância de spanning tree.
 - ◆ Per VLAN Spanning Tree Plus (PVST+) é um aprimoramento Cisco do STP que fornece uma instância de spanning-tree 802.1D separada para cada VLAN configurada na rede.
 - ◆ RPVST+ é um aprimoramento Cisco do RSTP que usa PVST+. Ele fornece uma instância separada de 802.1W por VLAN.
- Práticas Recomendadas para STP
 - ◆ Defina pela configuração (usando a prioridade STP) o root bridge/switch.
 - ◆ Use o mesmo custo em todas as interfaces (se possível).



Rede(s) sem fio



- As tecnologias de rede sem fio devem ter um ponto de integração no núcleo ou nas camadas de distribuição.
- Em termos de arquitetura de rede, uma WLAN pode ser vista como qualquer LAN.
 - Exceto que temos mobilidade e devemos ter roaming contínuo enquanto nos movemos.
- Um grande número de AP pode ser gerenciado por um controlador LAN (sem fio).

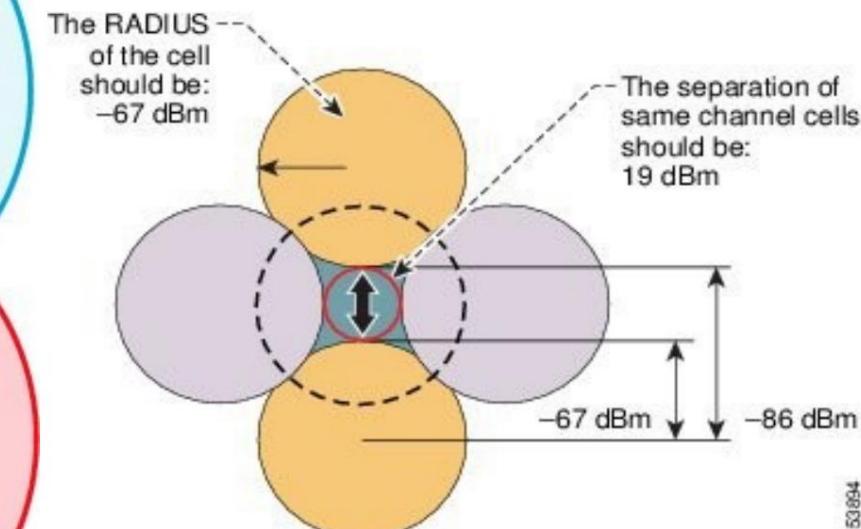
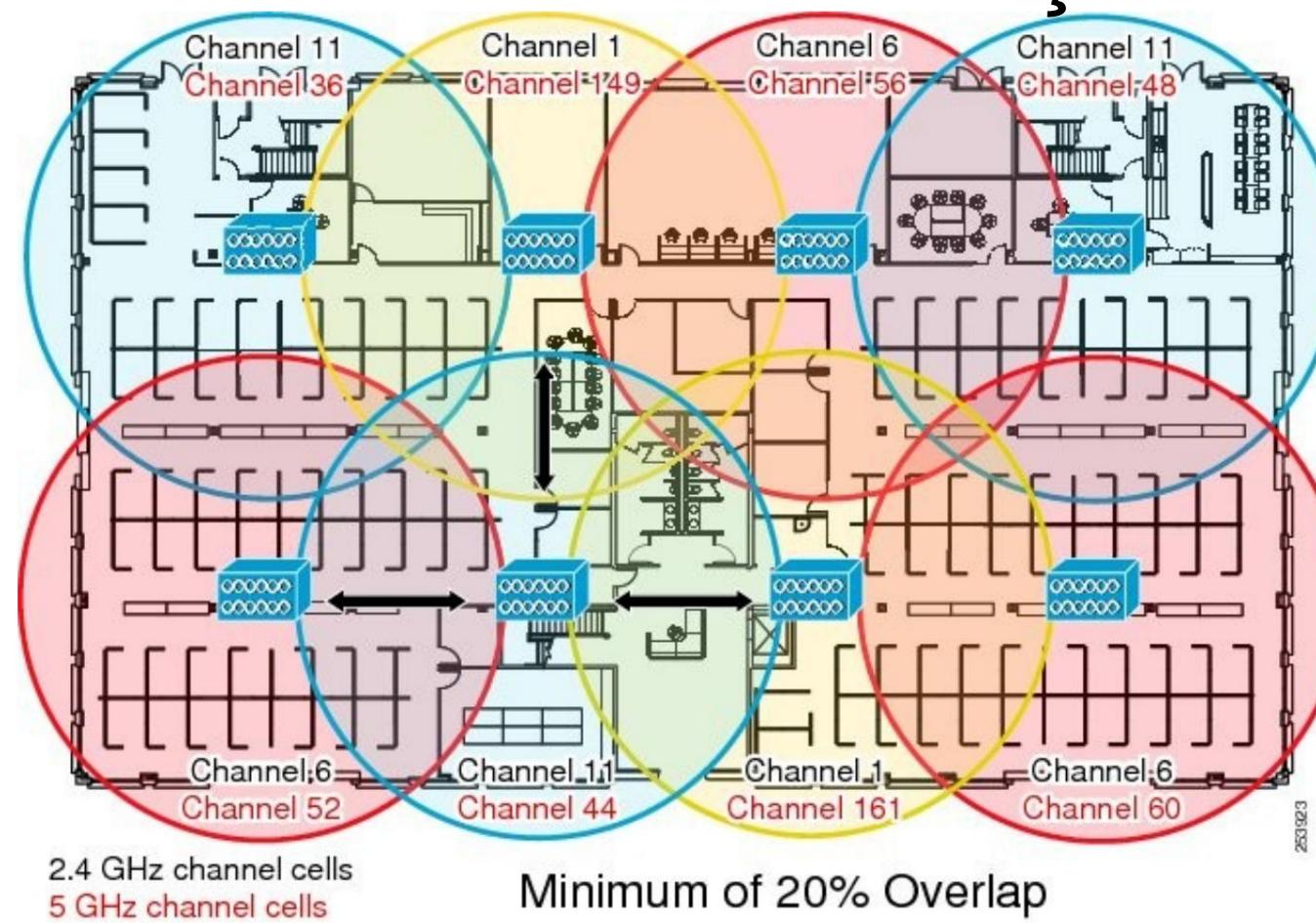
VLANs em pontos de acesso

- O AP tem portas de tronco para switches de distribuição/núcleo.
- As VLANs “com fio” devem/podem ser estendidas para o domínio sem fio.
 - ◆ por exemplo, VLAN 30 “Verde” e VLAN 10 “Vermelho”.
- Cada SSID pode ser mapeado para uma VLAN.
 - ◆ SSID/VLAN diferentes podem ter políticas de segurança diferentes.
- As VLANs sem fio devem ser configuradas de ponta a ponta.
 - ◆ Mobilidade e roaming de AP não devem interromper a conectividade da Camada 3.
 - ◆ O endereço IP deve ser o mesmo à mesma VLAN do campus.
- Uma VLAN nativa é necessária para fornecer capacidade de gerenciamento e autenticações de cliente.
 - ◆ Nunca estendido para o domínio wireless!!
 - ◆ por exemplo, VLAN 1.



Posicionamento AP e Canal

Alocação



- A implantação de 802.11n ou 802.11ac de 5 GHz não apresenta os problemas de domínio de sobreposição ou colisão de 2,4 GHz.



Visão geral do roteamento IP

- Os roteadores encaminham pacotes para as redes de destino.
 - Os roteadores devem estar cientes das redes de destino para poder encaminhar pacotes para elas.
 - Um roteador conhece as redes conectadas diretamente às suas interfaces
 - No entanto, para redes não conectadas diretamente a uma de suas interfaces, o roteador deve contar com informações externas.
 - Um roteador pode ser informado sobre redes remotas por:
 - ◆ **Roteamento estático:** um administrador configura manualmente as informações.
 - ◆ **Roteamento dinâmico:** aprende com outros roteadores.
- Roteamento baseado em política:** regras de roteamento manual que superam o roteamento estático/dinâmico e podem depender de outros parâmetros além do endereço de destino.



Rotas Padrão

- Em algumas circunstâncias, um roteador não precisa reconhecer os detalhes das redes remotas.
- O roteador pode ser configurado para enviar todo o tráfego (ou todo o tráfego para o qual não há uma entrada mais específica na tabela de roteamento) para um roteador vizinho específico.
- Isso é conhecido como uma rota padrão.
- As rotas padrão são anunciadas dinamicamente usando protocolos de roteamento ou configuradas estaticamente.
- Rota padrão IPv4 - 0.0.0.0/0
- Rota padrão IPv6 - ::/0

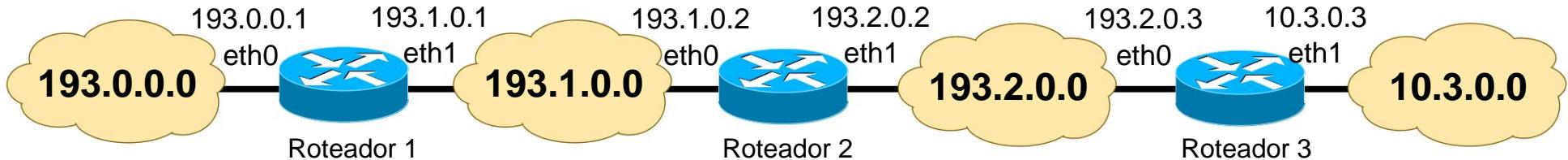


Roteamento Estático

- O roteamento de declaração não reage às mudanças na topologia da rede.
 - ◆ Se um link falhar, a rota estática não será mais válida se estiver configurada para usar esse link com falha, portanto, uma nova rota estática deve ser configurada.
 - ◆ A conectividade pode ser perdida até a intervenção de um administrador.
- O roteamento estático não escala bem quando a rede cresce.
 - ◆ A carga administrativa para manter as rotas pode se tornar excessiva.
- As rotas estáticas podem ser usadas nas seguintes circunstâncias:
 - ◆ Quando o administrador precisa de controle total sobre as rotas utilizadas pelo roteador.
 - ◆ Quando é necessário um backup para uma rota reconhecida dinamicamente.
 - ◆ Quando é usado para alcançar uma rede acessível por apenas um caminho (uma rede stub).
 - ◆ Não há link de backup, portanto, o roteamento dinâmico não tem vantagem.
 - ◆ Quando um roteador se conecta ao seu ISP e precisa ter apenas uma rota padrão apontando para o roteador do ISP, em vez de aprender muitas rotas do ISP.
 - ◆ Novamente, um único caminho de acesso sem backup.
 - ◆ Quando um roteador está com pouca energia e não possui os recursos de CPU ou memória necessários para lidar com um protocolo de roteamento dinâmico.
 - ◆ Quando é indesejável ter atualizações de roteamento dinâmicas encaminhadas em links de baixa largura de banda.



Exemplos de roteamento estático



- **Exemplo 1**

- Router2 não conhece as redes 193.0.0.0/24 e 10.3.0.0/24
- Rotas estáticas necessárias:
 - 193.0.0.0/24 acessível através de 193.1.0.1 (eth1, Router1)
 - 10.3.0.0/24 acessível através de 193.2.0.3 (eth0, Router3)

- **Exemplo 2**

- Router1 não conhece as redes 193.2.0.0/24 e 10.3.0.0/24
- Rotas estáticas necessárias:
 - 193.2.0.0/24 acessível através de 193.1.0.2 (eth0, Router2)
 - 10.3.0.0/24 acessível através de 193.1.0.2 (eth0, Router2)
OU
 - Usando rota padrão: 0.0.0.0/0 acessível através de 193.1.0.2 (eth0, Router2)



Roteamento Dinâmico

- O roteamento dinâmico permite que a rede se ajuste às mudanças na topologia automaticamente, sem envolvimento do administrador.
- Os roteadores trocam informações sobre as redes alcançáveis e o estado de cada rede/link.
 - ◆ Os roteadores trocam informações apenas com outros roteadores executando o mesmo protocolo de roteamento.
 - ◆ Quando a topologia da rede muda, as novas informações são propagadas dinamicamente por toda a rede e cada roteador atualiza sua tabela de roteamento para refletir as mudanças.



Tabelas de roteamento (complexas)

- Um endereço IP pode ter várias correspondências em uma tabela de roteamento: Exemplo: 192.168.1.12
 - ◆ Irá corresponder:
 - 192.168.1.0/25 via ...
 - 192.168.1.0/24 via ...
 - 192.168.0.0/23 via ...
 - 192.168.0.0/16 via ...
 - ...
 - ◆ O roteador escolherá a entrada com o maior prefixo de rede (rede mais específica).
 - ou seja, 192.168.1.0/25 via ...
- Balanceamento de carga
 - ◆ As tabelas de roteamento podem ter mais de um caminho para cada rede
 - ◆ O tráfego será dividido por todas as entradas.
 - ◆ Por pacote, fluxo (sessão TCP, IPs/porta UDP), etc...
 - Por exemplo, pacote 1 caminho 1, pacote 2 caminho 2, pacote 3 caminho 1, ...
 - Fluxo 1 caminho 1, fluxo 2 caminho 2, fluxo 3 caminho 3, fluxo 4 caminho 1, fluxo 5 caminho 2, ...



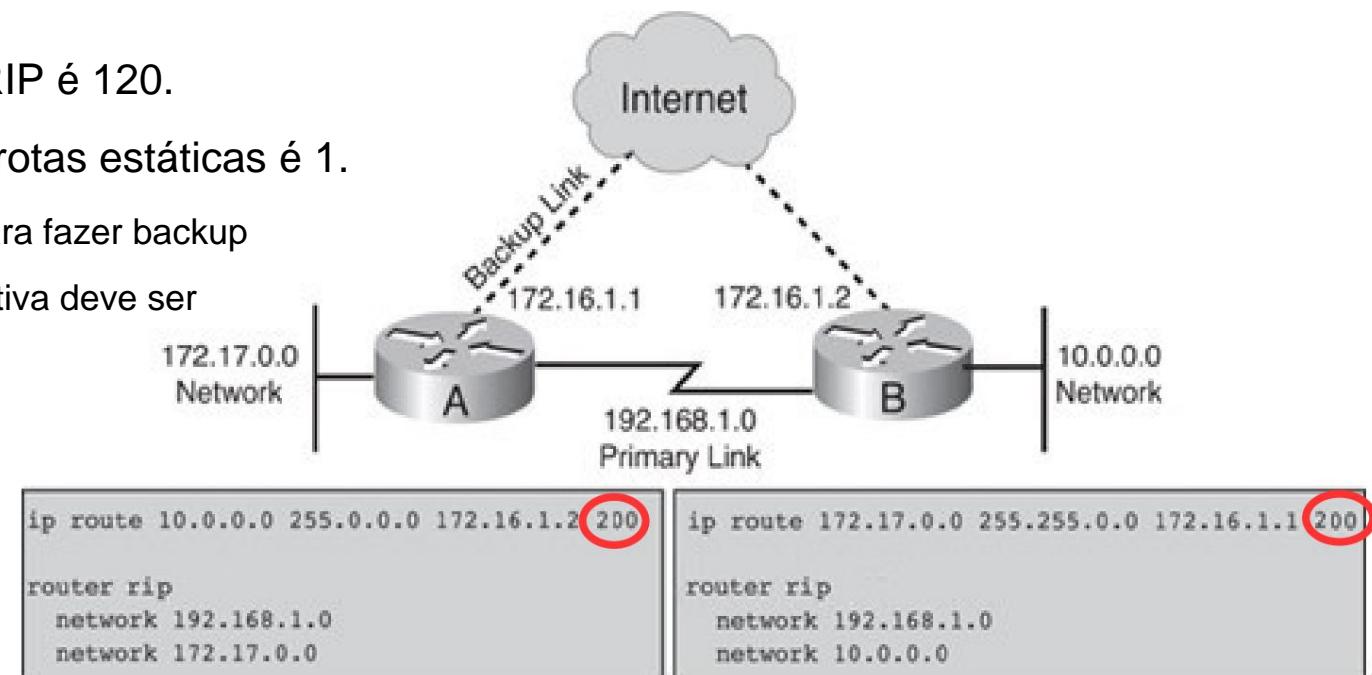
Distância Administrativa

- A maioria dos protocolos de roteamento possui estruturas métricas e algoritmos incompatíveis com outros protocolos.
- É fundamental que uma rede que usa vários protocolos de roteamento seja capaz de trocar informações de rota sem interrupções e selecionar o melhor caminho entre vários protocolos.
- Os roteadores usam um valor chamado distância administrativa para selecionar o melhor caminho quando aprendem com diferentes protocolos de roteamento o mesmo destino (mesmo prefixo de rede e comprimento de máscara).
- O Protocolo/Método com a menor Distância Administrativa é o preferido
 - ◆ O valor da Distância Administrativa é configurável.
- Exemplo:
 - ◆ Estático [1/1] 192.168.1.0/24 via ... é Escolhido!
 - ◆ RIP [120/1] 192.168.1.0/24 via ...
 - ◆ OSPF [110/1] 192.168.1.0/24 via...



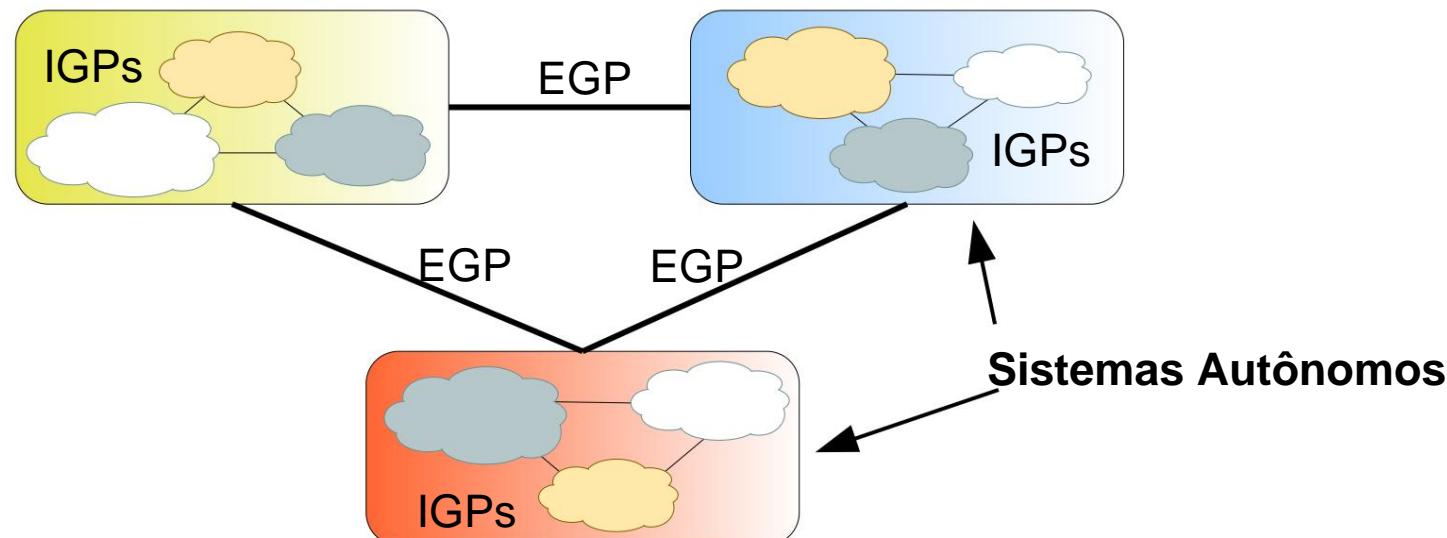
Rotas Estáticas Flutuantes

- Com base nas distâncias administrativas padrão, os roteadores usam rotas estáticas em qualquer rota aprendida dinamicamente.
 - No entanto, esse comportamento padrão pode não ser o comportamento desejado.
 - Por exemplo, quando você configura uma rota estática como um backup para uma rota aprendida dinamicamente, você não deseja que a rota estática seja usada enquanto a rota dinâmica estiver disponível.
- Uma rota estática que aparece na tabela de roteamento somente quando a rota principal desaparece é chamada de rota estática flutuante.
 - A distância administrativa da rota estática é configurada para ser maior que a distância administrativa da rota primária e ela “flutua” acima da rota primária, até que a rota primária não esteja mais disponível.
- A distância administrativa padrão do RIP é 120.
- A distância administrativa padrão das rotas estáticas é 1.
 - Para criar uma rota estática flutuante (para fazer backup de uma rota RIP), a distância administrativa deve ser maior que 120.
 - Exemplo: 200.



Sistemas Autônomos

- AS (Sistema Autônomo) – conjunto de roteadores/redes com uma política de roteamento comum e sob a mesma administração.
- O roteamento dentro de um AS é realizado por IGPs (Interior Gateway Protocols) como RIPv1, RIPv2, OSPF, IS-IS e EIGRP.
 - ◆ Roteamento Interno Chamado
- O roteamento entre AS é realizado por EGPs (Exterior Gateway Protocols), como o BGP.
- IGPs e EGPs têm objetivos diferentes: IGPs: otimizam
 - ◆ o desempenho do roteamento EGPs:
 - ◆ otimizam o desempenho do roteamento obedecendo a políticas políticas, econômicas e de segurança.



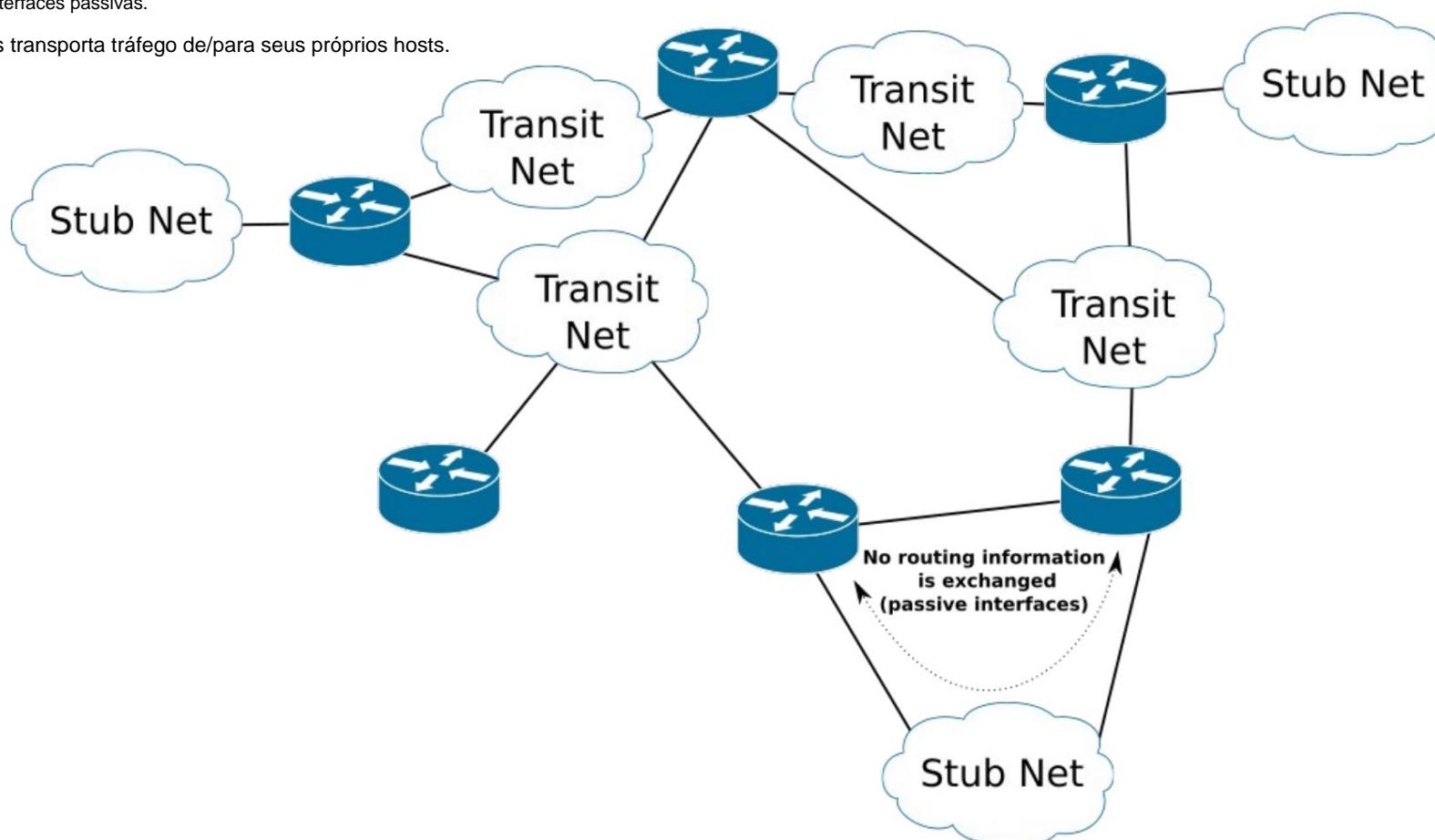
Tipo de redes

Trânsito/Transporte

- Usado para interligar redes.
- Os roteadores trocam informações de roteamento usando-o.
- Transporta tráfego de/para outros hosts de rede e de/para seus próprios hosts.

Stub

- Rede de roteador único.
- ou rede de vários roteadores, se os roteadores não trocarem informações de roteamento.
 - Interfaces passivas.
- Apenas transporta tráfego de/para seus próprios hosts.



Vector de distância versus estado do link

Protocolos

- Vetor de distância
 - ◆ Cada roteador aprende as redes e o melhor caminho com base nas informações enviadas periodicamente por seus vizinhos.
 - ◆ Rede e custo (distância) para essa rede.
 - ◆ Cada roteador determina os caminhos mais curtos para todas as redes conhecidas com base em uma versão distribuída e assíncrona do algoritmo de Bellman-Ford.
 - ◆ Exemplos: RIPv1, RIPv2, IGRP, EIGRP.
- Estado do link
 - ◆ Os roteadores aprendem a topologia de rede completa e usam um algoritmo centralizado para determinar os caminhos mais curtos para todas as redes conhecidas.
 - ◆ As informações necessárias para construir e manter em cada roteador um banco de dados com a topologia da rede são obtidas por um processo de flooding.
 - ◆ As informações de rede são trocadas apenas no bootstrap e após qualquer mudança de topologia.
 - ◆ Exemplos: OSPF, IS-IS.



Abra o caminho mais curto primeiro (OSPF)

O protocolo

- OSPF é um protocolo de padrão aberto baseado principalmente no RFC 2328.
- OSPF é um protocolo de roteamento de estado de link
 - ◆ Responda rapidamente a alterações de rede,
 - ◆ envie atualizações acionadas quando ocorrer uma alteração de rede,
 - ◆ envie atualizações periódicas, conhecidas como atualização de estado de link, em intervalos de tempo longos, como a cada 30 minutos.
- Roteadores executando OSPF coletam informações de roteamento de todos os outros roteadores da rede (ou de uma área definida da rede)
- E então cada roteador calcula independentemente seus melhores caminhos para todos os destinos na rede, usando o algoritmo de Dijkstra (SPF).



Roteamento Necessário OSPF

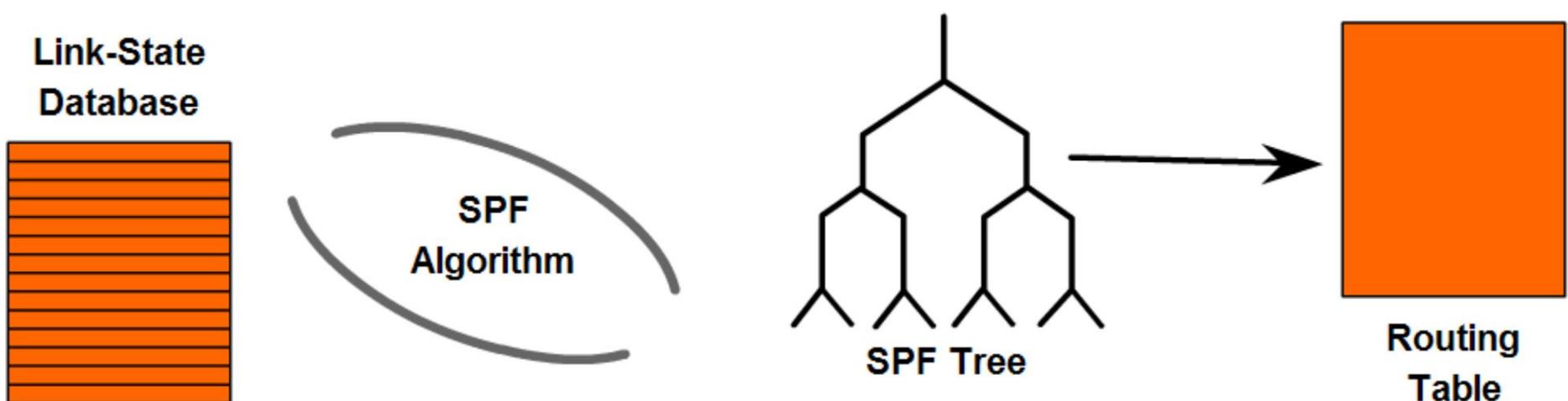
Informação

- Para que todos os roteadores na rede tomem decisões de roteamento consistentes, cada roteador link-state deve manter um registro das seguintes informações:
 - ◆ vizinhos imediatos Se o roteador
 - perder o contato com um roteador vizinho, dentro de alguns segundos ele invalidará todos os caminhos através dele. esse roteador e recalcula seus caminhos pela rede.
 - Para OSPF, as informações de adjacência sobre vizinhos são armazenadas na tabela de vizinhos OSPF, também conhecida como banco de dados de adjacência.
 - ◆ Todos os outros roteadores da rede, ou em sua área de rede, e suas redes anexadas
 - O roteador reconhece outros roteadores e redes por meio de LSAs, que são inundados pela rede.
 - Os LSAs são armazenados em uma tabela de topologia ou banco de dados (que também é chamado de LSDB).
 - ◆ Os melhores caminhos para cada destino
 - Cada roteador calcula independentemente os melhores caminhos para cada destino na rede usando o algoritmo de Dijkstra (SPF).
 - Todos os caminhos são mantidos no LSDB.
 - Os melhores caminhos são então oferecidos à tabela de roteamento (também chamada de banco de dados de encaminhamento).
 - Os pacotes que chegam ao roteador são encaminhados com base nas informações contidas na tabela de roteamento.



Operação do Protocolo Link-State

- Os protocolos de roteamento link-state geram atualizações de roteamento somente quando ocorre uma alteração na topologia da rede.
- Quando um link muda de estado, o dispositivo que detectou a alteração cria um Link State Advertisement (LSA) referente a esse link.
 - ◆ O LSA se propaga para os dispositivos vizinhos usando um endereço multicast especial.
- Cada roteador armazena o LSA, encaminha o LSA para dispositivos vizinhos e atualiza seu Link-State DataBase (LSDB).
- Os roteadores link-state encontram os melhores caminhos para um destino aplicando o algoritmo de Dijkstra, também conhecido como SPF, contra o LSDB para construir a árvore SPF.
- Cada roteador seleciona os melhores caminhos de sua árvore SPF e os coloca em sua tabela de roteamento.



Anúncio de estado de link (LSA)

- Os LSAs relatam o estado dos roteadores e os links entre os roteadores.
- As informações de estado do link devem ser sincronizadas entre os roteadores.
- Os LSAs têm as seguintes características:
 - ◆ LSAs são confiáveis. Existe um método para confirmar a entrega.
 - ◆ Os LSAs são inundados em toda a área (ou em todo o domínio, se houver apenas uma área).
 - ◆ Os LSAs têm um número de sequência e um tempo de vida definido, de modo que cada roteador reconhece que possui a versão mais atual do LSA.
 - ◆ Os LSAs são atualizados periodicamente para confirmar as informações de topologia antes que desapareçam do LSDB.



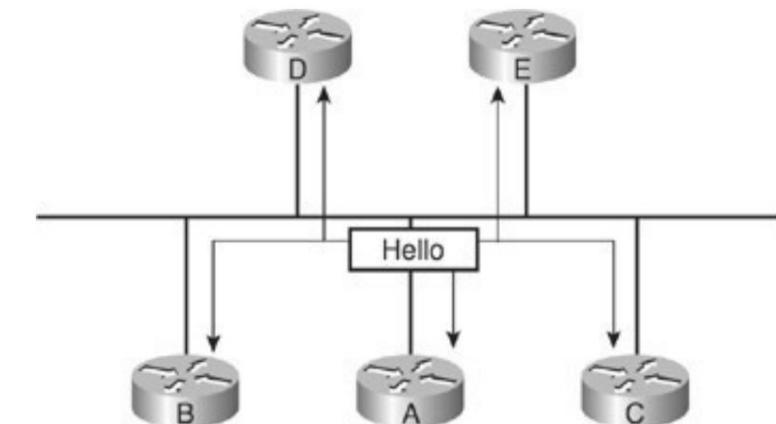
Identificação do roteador OSPF (RID)

- O ID do roteador identifica o roteador e é:
 - ◆ O endereço IPv4 mais alto de todas as interfaces do roteador no momento da ativação do processo OSPF.
 - ◆ Um valor definido administrativamente.
- Se um endereço de interface física estiver sendo usado como o ID do roteador e essa interface física falhar e o roteador (ou processo OSPF) for reiniciado, o ID do roteador será alterado.
 - ◆ Essa alteração na ID do roteador torna mais difícil para os administradores de rede solucionar problemas e gerenciar o OSPF.
- Definir administrativamente o RID ou usar interfaces de loopback para o ID do roteador força o ID do roteador a permanecer o mesmo, independentemente do estado das interfaces físicas



Adjacências OSPF

- Um roteador executando um protocolo de roteamento link-state deve primeiro estabelecer adjacências vizinhas, trocando pacotes hello com os roteadores vizinhos. O roteador envia e recebe pacotes Hello de e para seus roteadores vizinhos.
 - O endereço de destino é normalmente um endereço multicast.
 - É possível definir relações OSPF unicast.
- Os roteadores trocam pacotes hello sujeitos a parâmetros específicos do protocolo, como verificar se o vizinho está na mesma área, usando o mesmo intervalo hello e assim por diante.
 - Os roteadores declaram o vizinho ativo quando a troca é concluída.
- Dois roteadores OSPF em um link serial ponto a ponto, geralmente encapsulados em High Level Data Link Control (HDLC) ou Point-to-Point Protocol (PPP), formam uma adjacência completa entre si.
- No entanto, os roteadores OSPF em redes de transmissão, como links de LAN, elegem um roteador como o roteador designado (DR) e outro como o roteador designado de backup (BDR).
 - Todos os outros roteadores na LAN formam adjacências completas com esses dois roteadores e passam LSAs somente para eles.



Eleição de DR e BDR

- O primeiro roteador OSPF a inicializar se torna o Designated Router (DR).
- O segundo roteador a inicializar se torna o Backup Designated Router (BDR).
- Se vários roteadores inicializarem
 - ◆ simultaneamente, o DR será o roteador com maior prioridade. O BDR o segundo.
 - ◆ A prioridade OSPF é um parâmetro definido administrativamente.
 - ◆ Em caso de empate, será escolhido o roteador com maior Router ID (RID).
- Quando o DR falha, o BDR assume o papel de DR.
 - ◆ O BDR não executa nenhuma função DR quando o DR está operando.
 - ◆ A escolha do novo BDR é feita de acordo com alguns critérios da eleição inicial.
- Após a eleição, o DR e o BDR mantêm esse papel, independentemente de quais roteadores ingressam no processo OSPF.
- O ID de uma rede OSPF é o endereço IP da interface do roteador designado (DR) da rede.



Banco de dados OSPF LS

- O banco de dados OSPF (LSDB) é organizado em duas tabelas.
 - Router Link States – Tabela de informações relacionadas aos roteadores.
 - Os roteadores são identificados por seus RID.
 - Net Link States – Tabela de informações relacionadas a redes/links.
 - As redes são identificadas por seu ID.

Roteador OSPF com ID (20.20.20.1) (ID do processo 1)				
Estados de link do roteador (área 0)				
ID do link	roteador ADV	Idade	Seq#	Contagem de link de soma de verificação
20.20.20.1	20.20.20.1	40	0x8000000A	0x00E7FB 2
30.30.30.2	30.30.30.2	69	0x80000006	0x002906 2
30.30.30.3	30.30.30.3	41	0x80000007	0x00283D 2

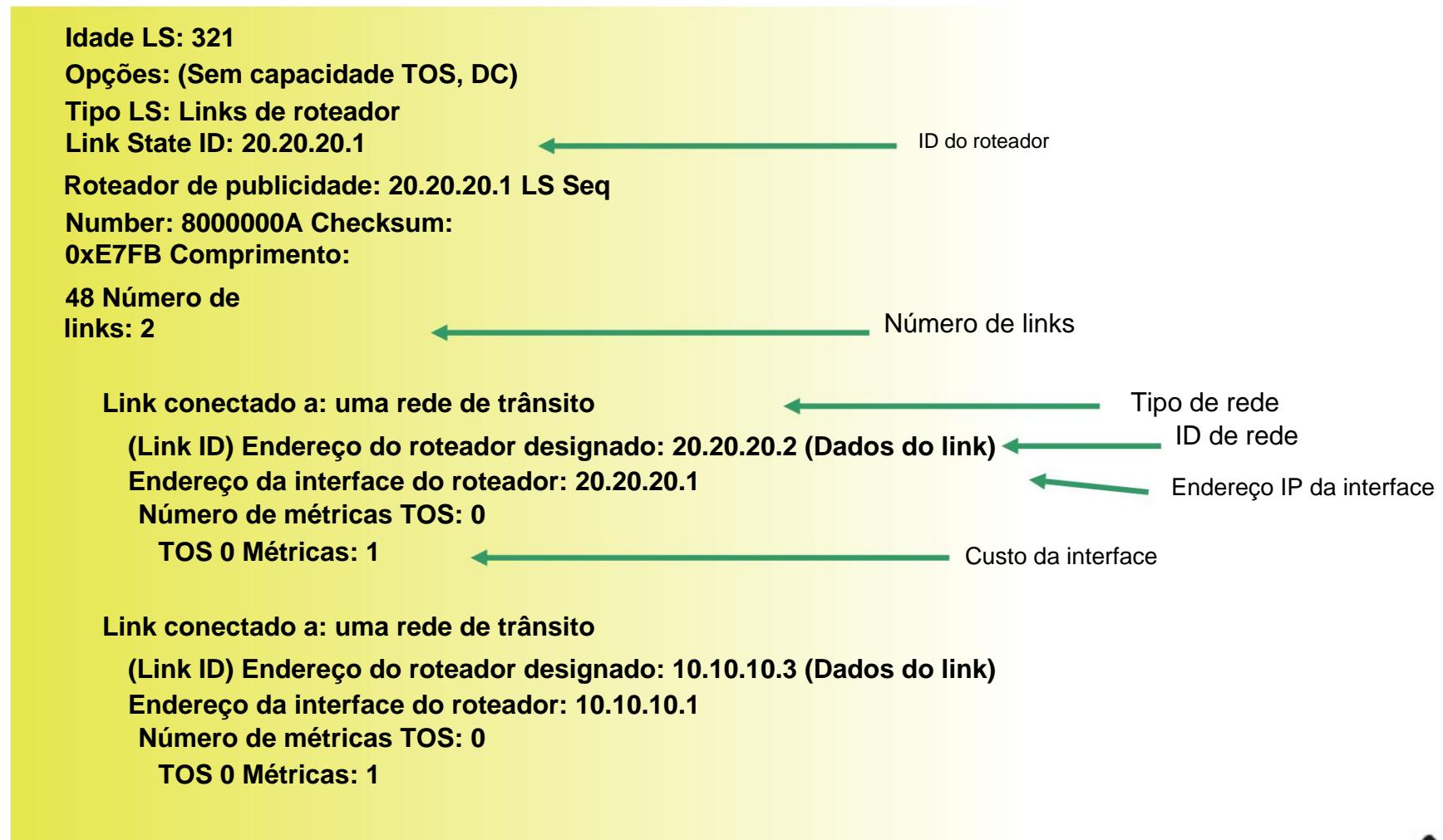
Estados de link de rede (área 0)				
ID do link	Roteador ADV	41	Seq#	Soma de
10.10.10.3	30.30.30.3	anos	verificação	0x80000001 0x00051C
20.20.20.2	30.30.30.2	70	0x80000001	0x00A164
30.30.30.3	30.30.30.3	154	0x80000001	0x00A91C



Tabelas de banco de dados OSPF LS (1)

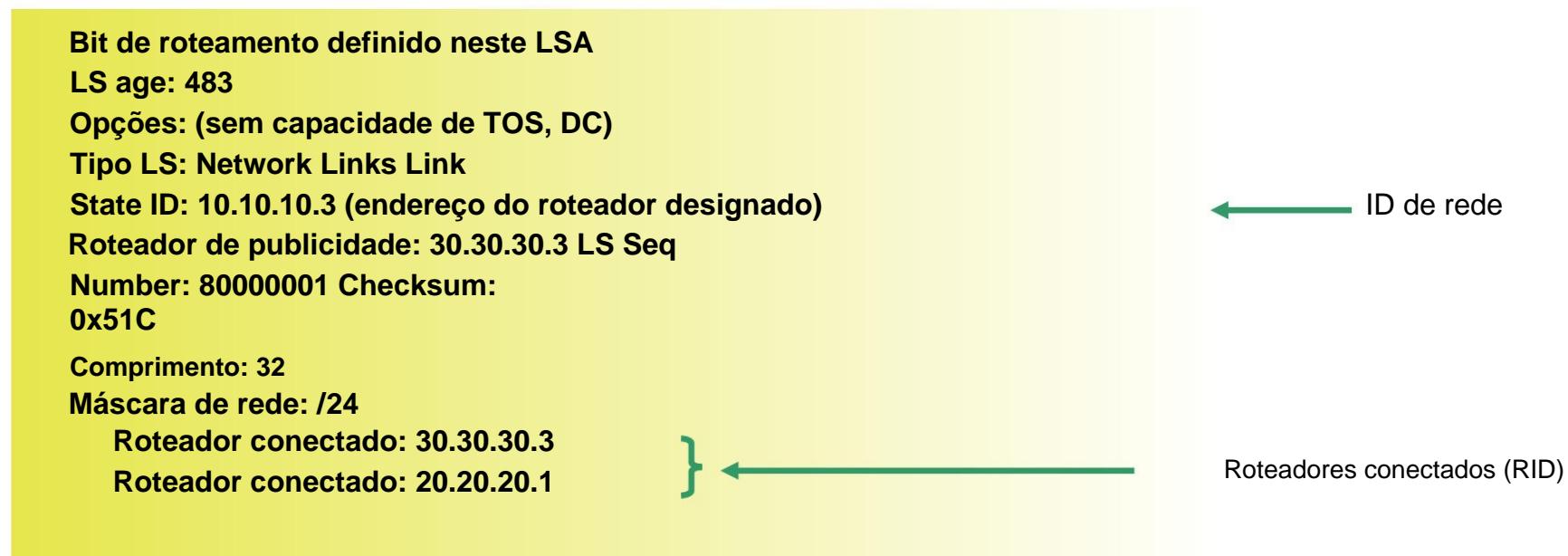
- Estados de link do roteador

- Para cada roteador, contém as informações sobre as redes conectadas diretamente a esse roteador.



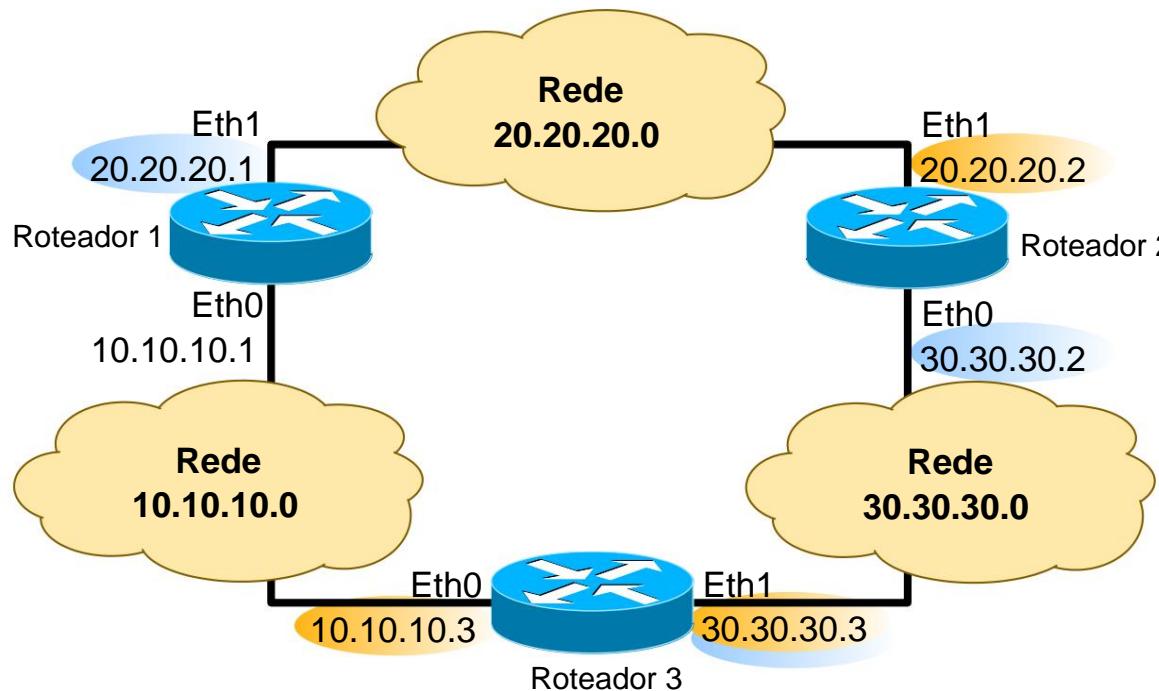
Tabelas de banco de dados OSPF LS (2)

- Estados de link de rede
 - ◆ Para cada rede, contém as informações sobre os roteadores diretamente conectados a essa rede.



OSPF LSDatabase

Exemplo



Bit de roteamento definido neste LSA

LS age: 208

Opções: (sem capacidade de TOS, DC)

Tipo LS: Network Links Link

State ID: 20.20.20.2 (endereço do roteador designado)

Roteador de publicidade: 30.30.30.2 LS Seq

Number: 80000001 Checksum:

0xA164

Comprimento: 32

Máscara de rede: /24

Roteador conectado: 30.30.30.2

Roteador conectado: 20.20.20.1

Estado do link de rede da rede 20.20.20.0

LS idade: 321

Opções: (sem capacidade de TOS, DC)

Tipo LS: Links de roteador

ID do estado do link: 20.20.20.1

Roteador de publicidade: 20.20.20.1 LS Seq

Number: 8000000A

Soma de verificação: 0xE7FB

Comprimento: 48

Número de links: 2

Link conectado a: uma rede de trânsito

(Link ID) Endereço do roteador designado: 20.20.20.2

(Dados do link) Endereço da interface do roteador: 20.20.20.1

Número de métricas TOS: 0

TOS 0 Métricas: 1

Link conectado a: uma rede de trânsito

(Link ID) Endereço do roteador designado: 10.10.10.3

(Dados do link) Endereço da interface do roteador: 10.10.10.1

Número de métricas TOS: 0

TOS 0 Métricas: 1

Estado do link do roteador do roteador 1



Pacotes OSPF

- Hello - Descobre vizinhos e constrói adjacências entre eles.
- Descrição do banco de dados (DBD) - Verifica a sincronização do banco de dados entre os roteadores.
- Solicitação de estado de link (LSR) - Sólicita registros de estado de link específicos de outro roteador.
- Atualização de estado de link (LSU) - Envia registros de estado de link solicitados especificamente.
- LSAck - reconhece os outros tipos de pacotes.



Formato do pacote OSPF

- Número da versão
 - ◆ Defina como 2 para OSPF Versão 2, a versão IPv4 do OSPF.
 - ◆ Defina como 3 para OSPF Versão 3, a versão IPv6 do OSPF.

- Tipo
 - ◆ Diferencia os cinco tipos de pacotes OSPF.

- Comprimento do
 - ◆ pacote O comprimento do pacote OSPF em bytes.

- ID do roteador
 - ◆ Define qual roteador é a origem do pacote.

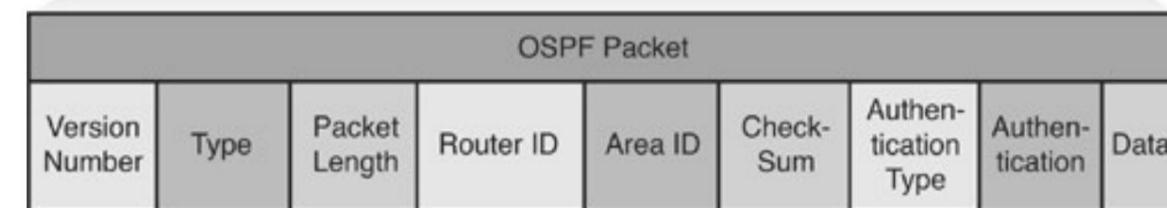
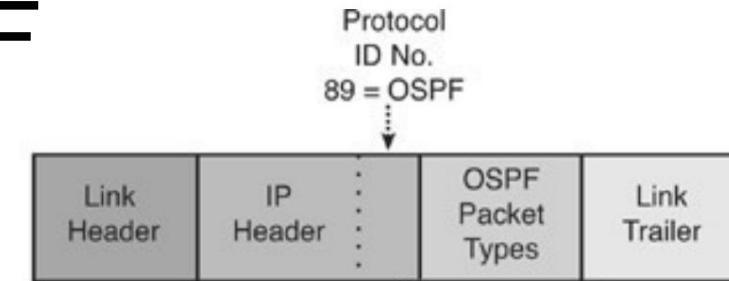
- ID da área
 - ◆ Define a área de origem do pacote.

- soma de verificação
 - ◆ Usado para detecção de erro de cabeçalho de pacote para garantir que o pacote OSPF não foi corrompido durante a transmissão.

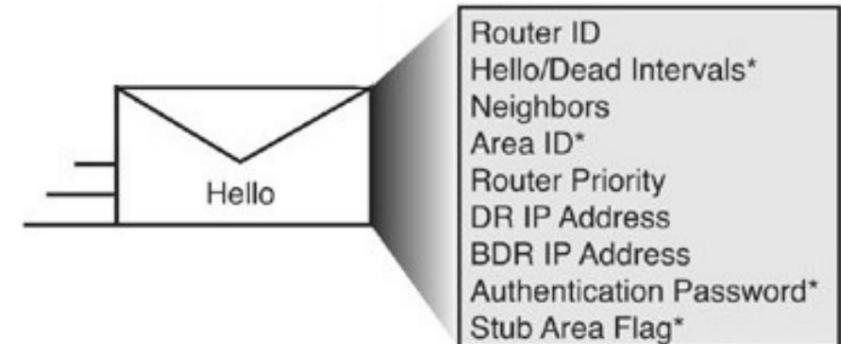
- Tipo de Autenticação
 - ◆ Uma opção no OSPF que descreve nenhuma autenticação, senhas de texto não criptografado ou resumo de mensagem criptografada 5 (MD5) para autenticação de roteador.

- Autenticação
 - ◆ Usado com o tipo de autenticação.

- Dados, contém informações diferentes, dependendo do tipo de pacote OSPF:
 - ◆ Para o pacote Hello - Contém uma lista de vizinhos conhecidos.
 - ◆ Para o pacote DBD - Contém um resumo do LSDB, que inclui todos os Ids de roteador conhecidos e seu último número de sequência, entre vários outros campos.
 - ◆ Para o pacote LSR - Contém o tipo de LSU necessário e o ID do roteador que possui o LSU necessário.
 - ◆ Para o pacote LSU - Contém as entradas LSA completas. Várias entradas LSA podem caber em um pacote de atualização OSPF.
 - ◆ Para o pacote LSAck - Este campo de dados está vazio.



Pacotes Olá OSPF



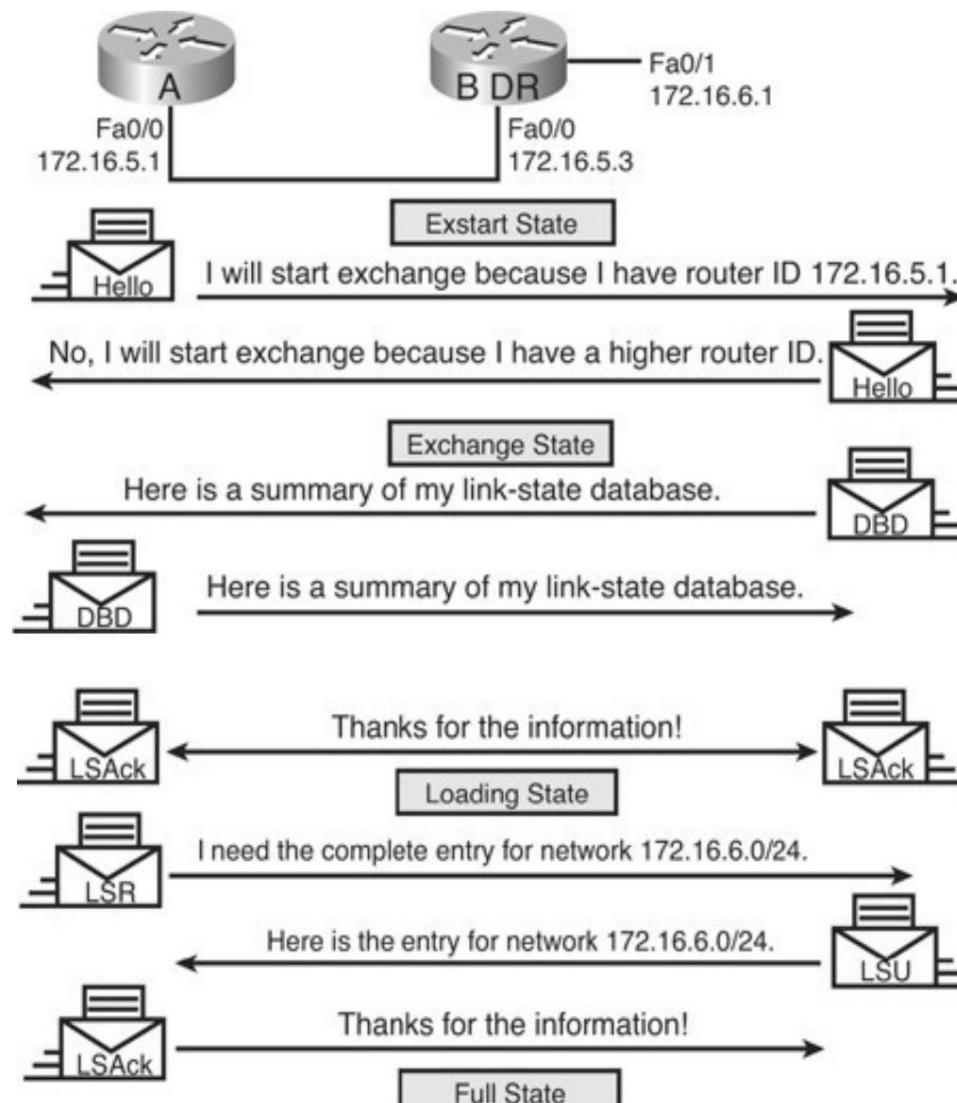
- Um pacote hello contém as seguintes informações:

- ◆ ID do roteador
 - ◆ Um número de 32 bits que identifica exclusivamente o roteador.
- ◆ Olá e intervalos mortos
 - ◆ O intervalo hello especifica com que frequência, em segundos, um roteador envia pacotes hello (10 segundos é o padrão em redes multiacesso).
 - ◆ O intervalo morto é a quantidade de tempo em segundos que um roteador espera para ouvir de um vizinho antes de declarar o roteador vizinho fora de serviço (o intervalo morto é quatro vezes o intervalo de saudação por padrão).
 - ◆ Esses temporizadores devem ser os mesmos nos roteadores vizinhos; caso contrário, uma adjacência não será estabelecida.
- ◆ Vizinhos O
 - ◆ campo Vizinhos lista os roteadores adjacentes com os quais este roteador estabeleceu comunicação bidirecional.
 - ◆ A comunicação bidirecional é indicada quando o roteador se vê listado no campo Vizinhos do pacote de saudação do vizinho.
- ◆ ID da área
 - ◆ Para se comunicar, dois roteadores devem compartilhar um segmento comum e suas interfaces devem pertencer à mesma área OSPF nesse segmento.
 - ◆ Todos esses roteadores terão as mesmas informações de estado de link para essa área.
- ◆ Prioridade do
 - ◆ roteador Um número de 8 bits que indica a prioridade de um roteador. A prioridade é usada ao escolher um DR e BDR.
- ◆ Endereços IP DR e BDR
 - ◆ Se conhecido, os endereços IP do DR e BDR para a rede multiacesso específica.
- ◆ senha de autenticação
 - ◆ Se a autenticação do roteador estiver habilitada, dois roteadores devem trocar a mesma senha.
 - ◆ A autenticação não é necessária, mas se estiver habilitada, todos os roteadores pares devem ter a mesma senha.
- ◆ Sinalizador de área de
 - ◆ stub Uma área de stub é uma área especial.
 - ◆ A técnica de área de stub reduz as atualizações de roteamento, substituindo-as por uma rota padrão.
 - ◆ Dois roteadores vizinhos devem concordar com o sinalizador de área de stub nos pacotes de saudação.

- Os campos Hello Interval, Dead Interval, Area ID, Authentication Password e Stub Area Flag devem corresponder aos roteadores vizinhos para que eles estabeleçam uma adjacência.



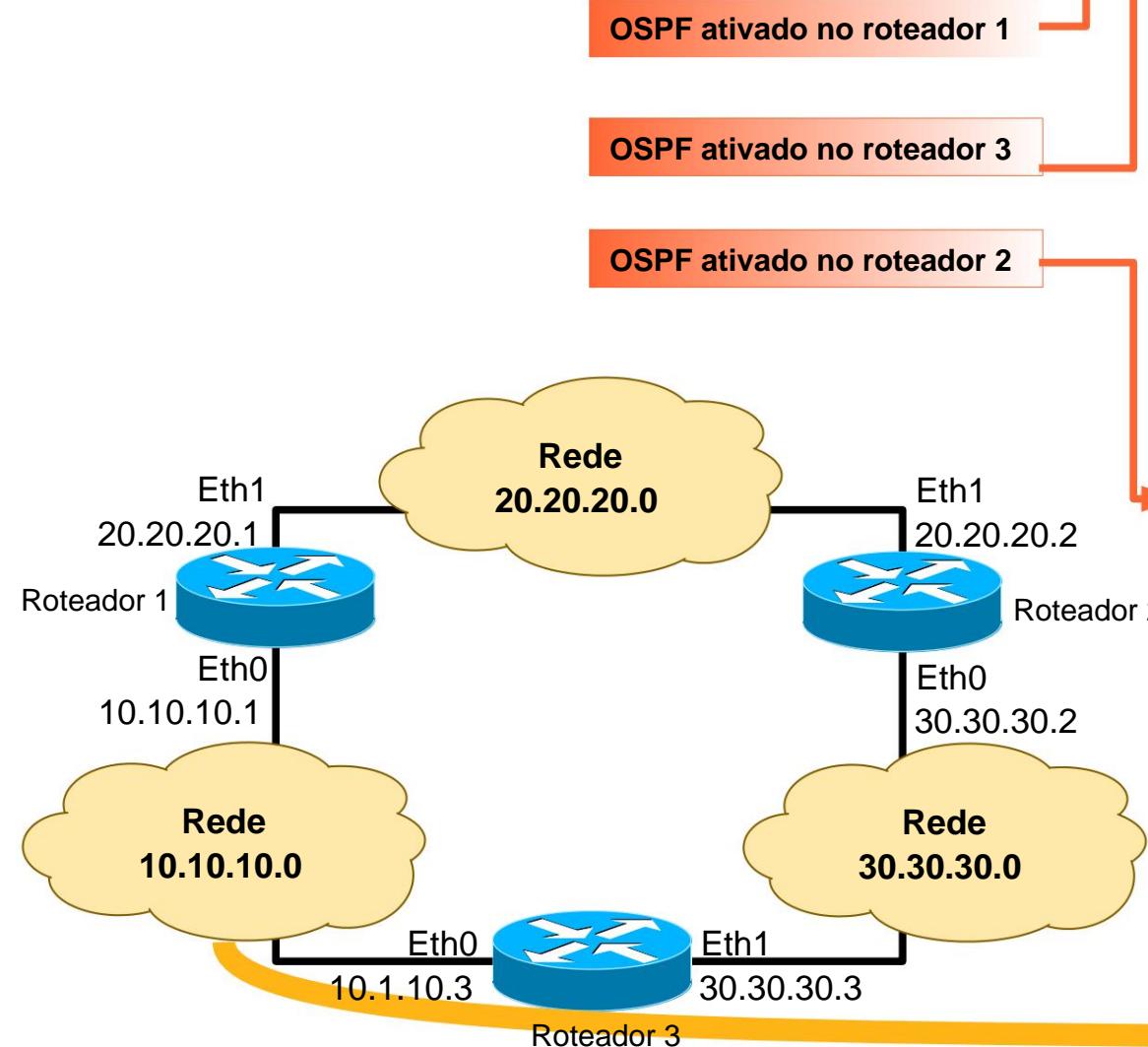
Descobrindo as rotas de rede



- Um relacionamento mestre e escravo é criado entre cada roteador e seus DR e BDR adjacentes.
 - Somente o DR troca e sincroniza informações de estado de link com os roteadores aos quais estabeleceu adjacências.
- Os roteadores mestre e escravo trocam um ou mais pacotes DBD.
 - Um DBD inclui informações sobre o cabeçalho de entrada LSA que aparece no LSDB do roteador.
 - As entradas podem ser sobre um link ou sobre uma rede.
 - Cada cabeçalho de entrada LSA inclui informações sobre o tipo de estado do link, o endereço do roteador de publicidade, o custo do link e o número de sequência.
 - O roteador usa o número de sequência para determinar a “novidade” das informações de estado do link recebidas.
- Ele confirma o recebimento do DBD usando o pacote LSack.
 - Ele compara as informações que recebeu com as informações que possui em seu próprio LSDB.
- Se o DBD tiver uma entrada de estado de link mais atual, o roteador enviará um LSR para o outro roteador.
- O outro roteador responde com as informações completas sobre a entrada solicitada em um pacote LSU.
- Novamente, quando o roteador recebe um LSU, ele envia um LSack.
- O roteador adiciona as novas entradas de estado de link ao seu LSDB.



Exemplo de OSPF



OSPF ativado no roteador 1

OSPF ativado no roteador 3

OSPF ativado no roteador 2

fonte de tempo	Informações do protocolo de destino
0,000000 10.10.10.1	224.0.0.5 OSPF Hello Packet
10.002318 10.10.10.1	224.0.0.5 OSPF Hello Packet
20.003116 10.10.10.1	224.0.0.5 OSPF Hello Packet

80.000000 10.10.10.3	224.0.0.5 OSPF Hello Packet
83.683033 10.10.10.3	224.0.0.5 OSPF LS Update 224.0.0.5 OSPF Hello Packet
83.715683 10.10.10.3	10.10.10.3 Pacote Hello OSPF
83.717864 10.10.10.1	10.10.10.1 OSPF DB Descr.
83.726166 10.10.10.3	10.10.10.1 Pacote Hello OSPF
83.726258 10.10.10.3	10.10.10.3 OSPF DB Descr.
83.728433 10.10.10.1	10.10.10.1 OSPF DB Descr.
83.732590 10.10.10.3	10.10.10.3 OSPF DB Descr.
83.734733 10.10.10.1	10.10.10.1 OSPF LS Request 10.10.10.3
83.738942 10.10.10.3	OSPF LS Update 224.0.0.5 OSPF LS
83.741083 10.10.10.1	Update 224.0.0.5 OSPF LS Acknowledge
84.240362 10.10.10.3	224.0.0.5 OSPF Hello Packet
86.245792 10.10.10.3	224.0.0.5 OSPF LS Acknowledge 224.0.0.5 OSPF Hello Packet
86.380876 10.10.10.1	224.0.0.5 OSPF Hello Packet
86.741036 10.10.10.1	224.0.0.5 OSPF Hello Packet
93.721376 10.10.10.3	224.0.0.5 OSPF LS Acknowledge 224.0.0.5 OSPF Hello Packet
96.380005 10.10.10.1	224.0.0.5 OSPF Hello Packet

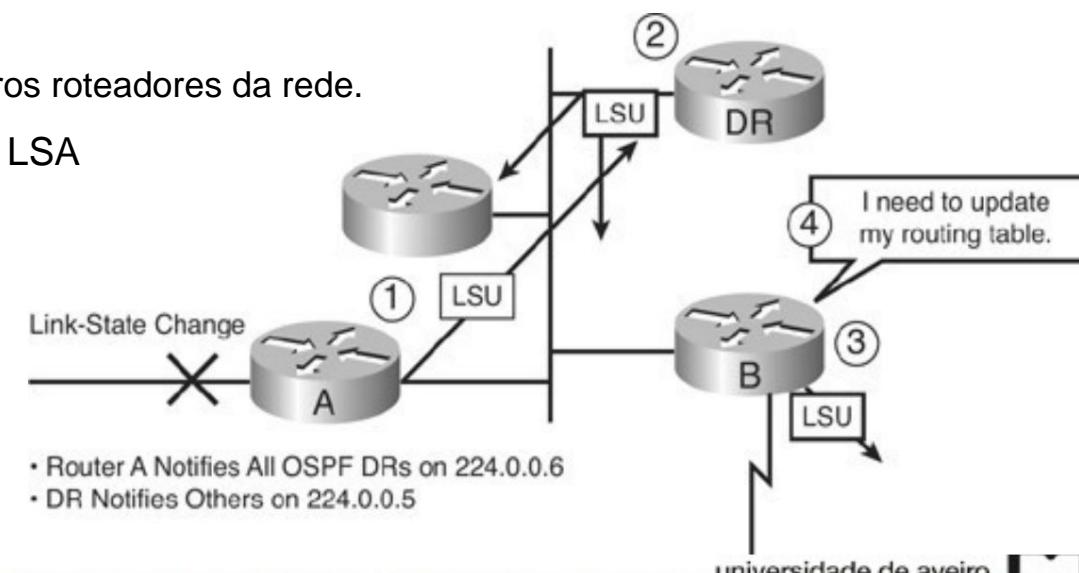
213.780338 10.10.10.3	224.0.0.5 OSPF Hello Packet
216.542473 10.10.10.1	224.0.0.5 OSPF Hello Packet
216.568852 10.10.10.1	224.0.0.5 OSPF LS Update 224.0.0.5 OSPF LS
217.048427 10.10.10.1	Update 224.0.0.5 OSPF LS Acknowledge
217.084909 10.10.10.1	224.0.0.5 OSPF LS Update 224.0.0.5 OSPF LS
219.067748 10.10.10.3	Acknowledge 224.0.0.5 OSPF Hello
219.650308 10.10.10.1	Packet 224.0.0.5 OSPF LS Update 224.0.0.5 OSPF LS
222.150349 10.10.10.3	Update 224.0.0.5 OSPF LS Update 224.0.0.5 OSPF LS
223.779492 10.10.10.3	OSPF Hello Packet
224.284149 10.10.10.3	224.0.0.5 OSPF LS Reconhecimento 224.0.0.5 OSPF LS
224.789598 10.10.10.1	Reconhecimento 224.0.0.5 OSPF Hello Packet
224.789775 10.10.10.3	224.0.0.5 OSPF LS Reconhecimento 224.0.0.5 OSPF Hello Packet
226.545718 10.10.10.1	
226.785254 10.10.10.1	
227.294756 10.10.10.3	
233.779863 10.10.10.3	
236.544658 10.10.10.1	224.0.0.5 OSPF Hello Packet



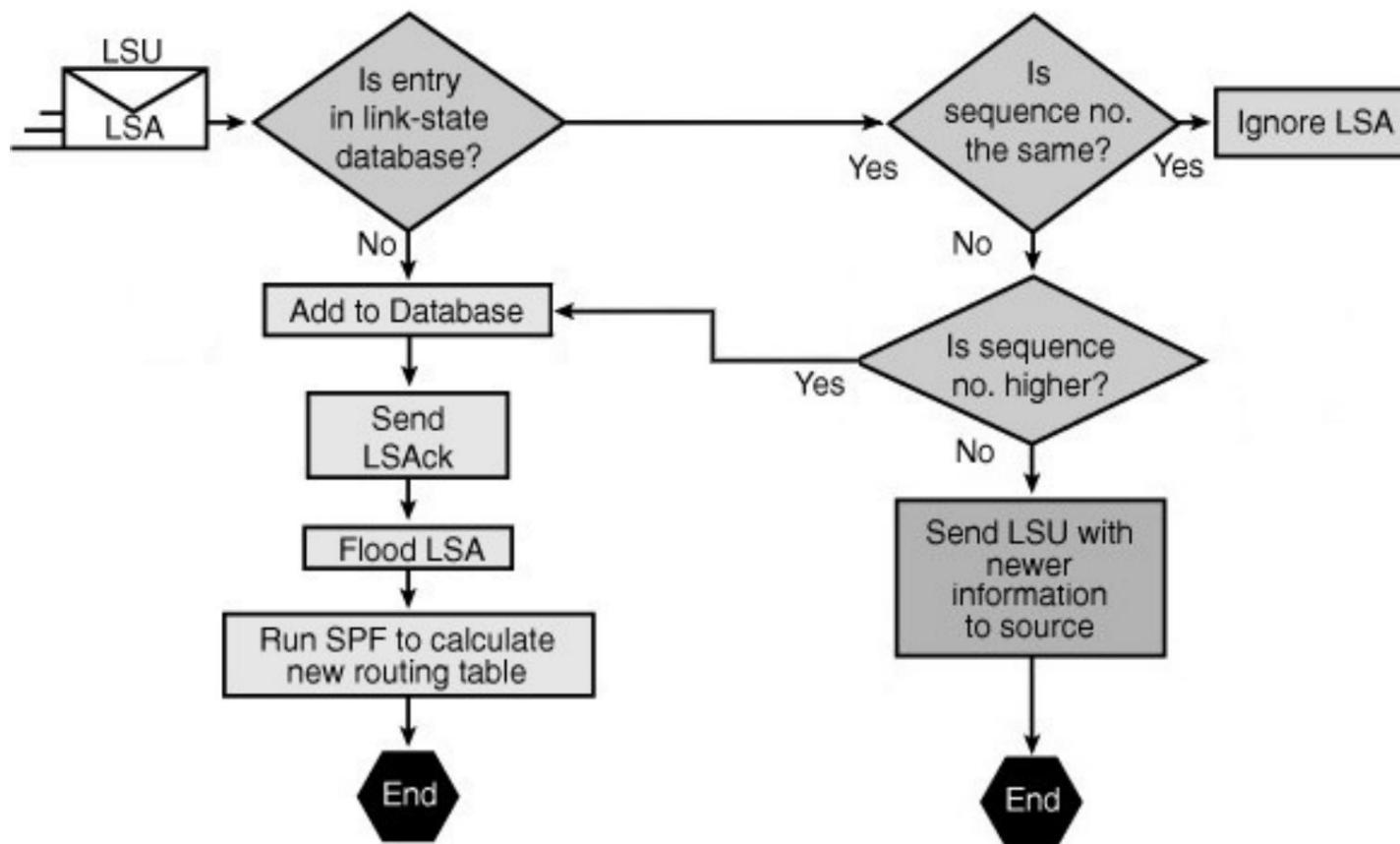
Manutenção de informações de roteamento

- Processo de inundação:

- Um roteador percebe uma mudança no estado de um link e faz multicast de um pacote LSU, que inclui a entrada LSA atualizada com o número de sequência incrementado, para 224.0.0.6.
 - Este endereço vai para todos os DRs e BDRs OSPF.
 - Em links ponto a ponto, o LSU é multicast para 224.0.0.5.)
 - Um pacote LSU pode conter vários LSAs distintos.
- O DR recebe o LSU, processa-o, confirma o recebimento da alteração e inunda o LSU para outros roteadores na rede usando o endereço OSPF multicast 224.0.0.5.
 - Depois de receber o LSU, cada roteador responde ao DR com um LSAck.
 - Para tornar o procedimento de inundação confiável, cada LSA deve ser reconhecido separadamente.
- Se um roteador estiver conectado a outras redes, ele inunda o LSU para essas outras redes encaminhando o LSU para o DR da outra rede (ou para o roteador adjacente se estiver em uma rede ponto a ponto).
 - Esse DR, por sua vez, faz multicast do LSU para os outros roteadores da rede.
- O roteador atualiza seu LSDB usando o LSU que inclui o LSA alterado.
- Em seguida, ele recalcula o algoritmo SPF no banco de dados atualizado após um pequeno atraso e atualiza a tabela de roteamento conforme necessário.



Operação LSA



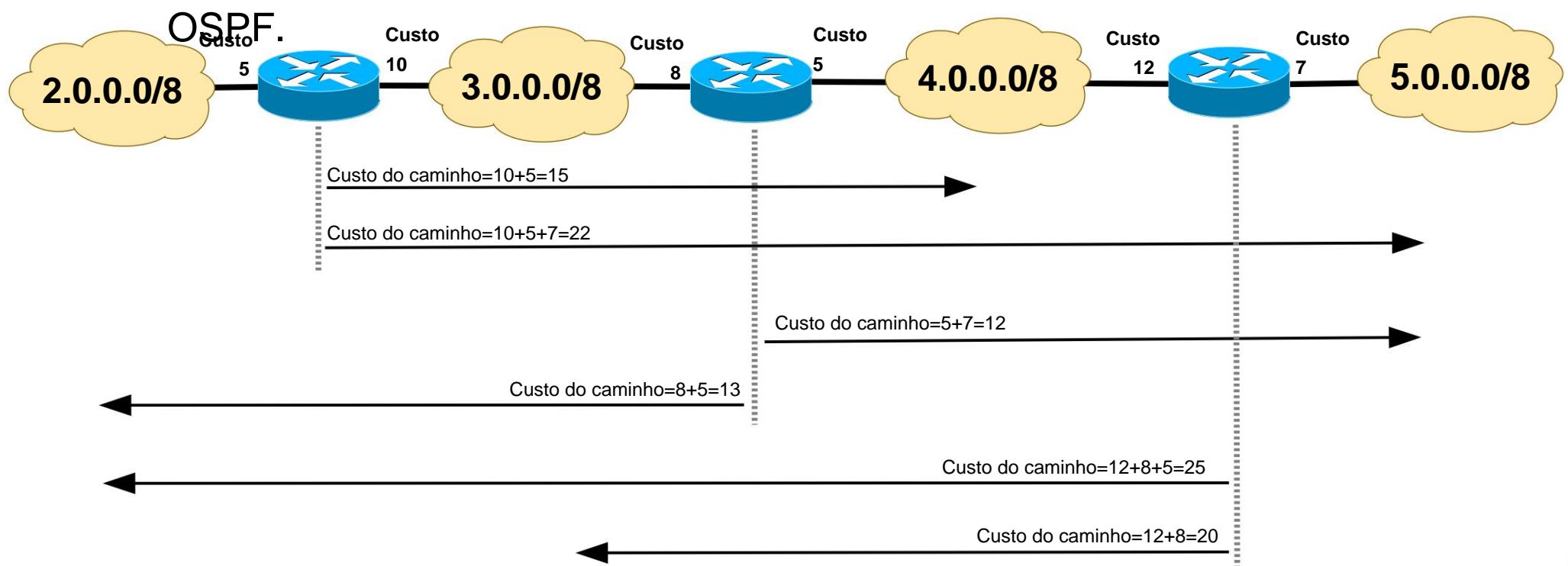
- Quando cada roteador recebe o LSU:

- Se a entrada LSA ainda não existir, o roteador adiciona a entrada ao seu LSDB, envia de volta um reconhecimento de estado de link (LSAck), inunda as informações para outros roteadores, executa o SPF e atualiza sua tabela de roteamento.
- Se a entrada já existir e o LSA recebido tiver o mesmo número de sequência, o roteador ignorará a entrada do LSA.
- Se a entrada já existe, mas o LSA inclui informações mais recentes (tem um número de sequência maior), o roteador adiciona a entrada ao seu LSDB, envia de volta um LSAck, inunda as informações para outros roteadores, executa o SPF e atualiza sua tabela de roteamento.
- Se a entrada já existir, mas o LSA incluir informações mais antigas, ele enviará um LSU ao remetente com suas informações mais recentes.

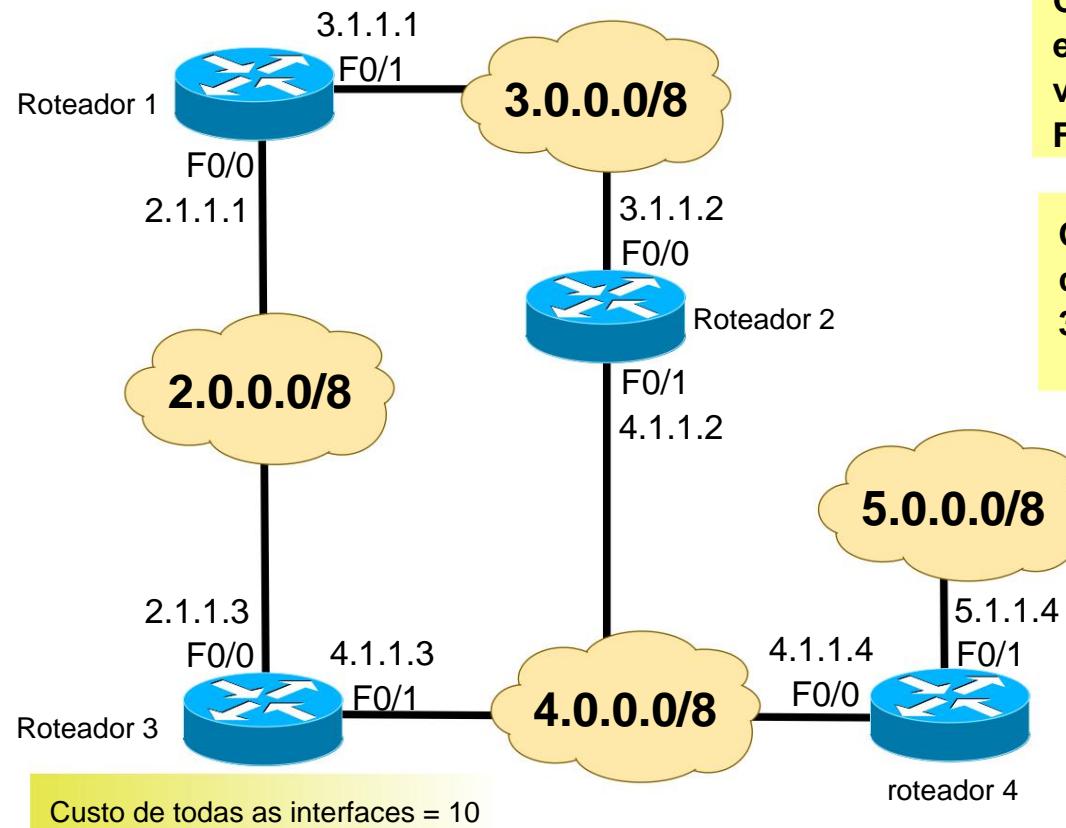


Custos de Caminho OSPF

- Cada link/interface do roteador tem um custo OSPF associado.
- O custo total entre um roteador e uma rede é dado pela soma de todos os custos OSPF das interfaces de saída (roteadores) ao longo do caminho.
 - Os roteadores para acessar redes de conexão direta nunca usam caminhos OSPF.



Exemplo de OSPF



C 2.0.0.0/8 está conectado diretamente, F0/0 C 3.0.0.0/8
está conectado diretamente, F0/1 O 4.0.0.0/8 [110/20]
via 2.1.1.3, 00:01:18, F0/0 O 5.0.0.0/8 [110/30] via 2.1.1.3, 00:01:00,
F0/0

O 2.0.0.0/8 [110/20] via 3.1.1.1, 00:01:13, F0/0 C 3.0.0.0/8 está
conectado diretamente, F0/0 O 4.0.0.0/8 [110/30] via
3.1.1.1, 00:01:13, F0/0 O 5.0.0.0/8 [110/40] via 3.1.1.1, 00:01:10, F0/0

Roteador 1 e Roteador 2 após desconectar o F0/1 no Roteador2

C 2.0.0.0/8 está conectado diretamente, F0/0 C 3.0.0.0/8
está conectado diretamente, F0/1 O 4.0.0.0/8 [110/15]
via 3.1.1.2, 00:01:13, F0/1 O 5.0.0.0/8 [110/25] via 3.1.1.2, 00:01:10,
F0/1

Router1, agora com o custo da interface Router2 F0/1 igual a 5

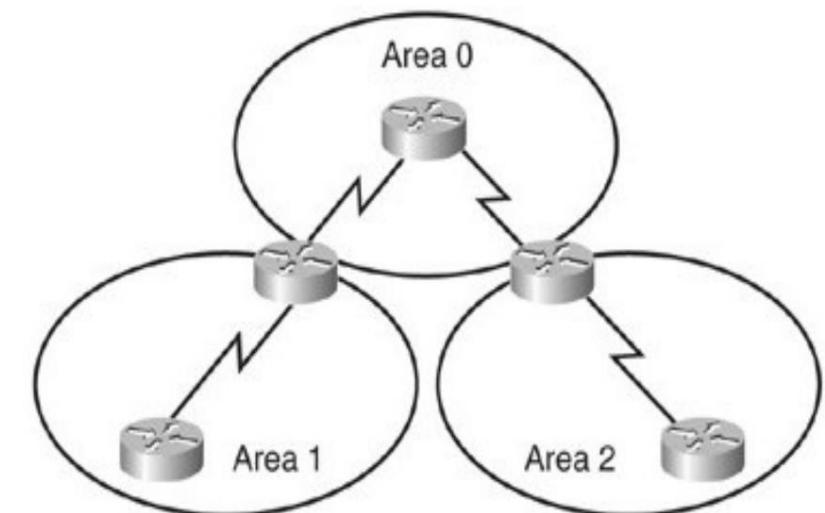
C 2.0.0.0/8 está conectado diretamente, F0/0 C 3.0.0.0/8
está conectado diretamente, F0/1 O 4.0.0.0/8 [110/20]
via 3.1.1.2, 00:01:13, F0/1 [110/20] via 2.1.1.3, 00:01:31, F0/0 O
5.0.0.0/8 [110/30] via 3.1.1.2, 00:01:10, F0/1
[110/30] via 2.1.1.3, 00:01:10, F0/0

Tabela inicial do roteador 1



Roteamento Hierárquico OSPF (1)

- Em redes pequenas, a teia de links do roteador não é complexa e os caminhos para destinos individuais são facilmente deduzidos.
- Em grandes redes, a teia resultante é altamente complexa e o número de caminhos potenciais para cada destino é grande.
 - ◆ Os cálculos de Dijkstra comparando todas essas rotas possíveis podem ser muito complexos e podem levar um tempo significativo.
 - Grande LSDB. Como o LSDB abrange a topologia de toda a rede, cada roteador deve manter uma entrada para cada rede na área, mesmo que nem todas as rotas sejam selecionadas para a tabela de roteamento.
 - Cálculos frequentes do algoritmo SPF. Em uma grande rede, as mudanças são inevitáveis, então os roteadores gastam muitos ciclos de CPU recalculando o algoritmo SPF e atualizando a tabela de roteamento.
 - Grande tabela de roteamento. O OSPF não executa o resumo de rota por padrão. Se as rotas não forem resumidas, as tabelas de roteamento podem ficar muito grandes, dependendo do tamanho da rede.
- Os protocolos de roteamento link-state geralmente reduzem o tamanho dos cálculos de Dijkstra particionando a rede em áreas.



Roteamento Hierárquico OSPF (2)

- O uso de várias áreas OSPF tem várias vantagens importantes:
 - ◆ Frequência reduzida de cálculos de SPF.
 - ◆ Informações de rota detalhadas existem apenas dentro de cada área.
 - ◆ Não é necessário inundar todas as alterações de estado de link para todas as outras áreas.
 - ◆ Somente os roteadores afetados pela alteração precisam recalcular o algoritmo SPF e o impacto da alteração é localizado dentro da área.
 - ◆ Sobrecarga de atualizações reduzida.
 - ◆ Em vez de enviar uma atualização sobre cada rede dentro de uma área, um roteador pode anunciar uma única rota resumida ou um pequeno número de rotas entre as áreas, reduzindo assim a sobrecarga associada às atualizações quando elas se cruzam. áreas.
 - ◆ Tabelas de roteamento menores.
 - ◆ Entradas de rota detalhadas para redes específicas dentro de uma área podem permanecer no área.
 - ◆ Os roteadores podem ser configurados para resumir as rotas em um ou mais endereços de resumo.
 - ◆ A divulgação desses resumos reduz o número de mensagens propagadas entre as áreas, mas mantém todas as redes acessíveis.



Sistema Integrado-Integrado Protocolo do Sistema (IS-IS)

- O IS-IS foi definido em 1992 na recomendação ISO/IEC 10589.
- IS-IS é um protocolo de roteamento de estado de link.
 - ◆ Fornece convergência rápida e excelente escalabilidade.
 - ◆ Muito eficiente no uso da largura de banda da rede.
- Usa o algoritmo Shortest Path First (SPF) de Dijkstra.
- Tipos de pacotes IS-IS
 - ◆ Hello packet (IIH), Link State Packet (LSP), Partial Sequence Number Packet (PSNP) e Complete Sequence Number Packet (CSNP).
- Estados de link são chamados de LSPs
 - ◆ Contêm todas as informações sobre adjacências de um roteador, prefixos IP conectados, sistemas finais OSI, endereços de área, etc.
 - ◆ Um LSP por roteador (mais fragmentos).
 - ◆ Um LSP por rede LAN.
- IS-IS tem 2 camadas de hierarquia O
 - ◆ backbone é chamado de nível 2.
 - ◆ As áreas são chamadas de nível 1.
 - ◆ Um roteador pode participar do roteamento entre áreas L1 e L2 (ou roteamento entre níveis).



Roteamento aprimorado de gateway interno

Protocolo (EIGRP) Protocolo

- O EIGRP é um protocolo proprietário da Cisco que combina as vantagens dos protocolos de roteamento link-state e distance vector.
- O EIGRP tem suas raízes como um protocolo de roteamento de vetor de distância e é previsível em seu comportamento.
- O que torna o EIGRP um protocolo de vetor de distância avançado é a adição de vários recursos de estado de link, como a descoberta dinâmica de vizinhos.
 - ◆ O EIGRP mantém uma tabela de vizinhos, uma tabela de topologia e uma tabela de roteamento.
- O EIGRP tem suporte para máscara de sub-rede de comprimento variável (VLSM).
- Possui uma métrica sofisticada que considera cinco critérios: Dois por
 - ◆ padrão: Largura
 - ◆ de banda - A menor (mais lenta) largura de banda entre a origem e o destino.
 - ◆ Atraso - O atraso cumulativo da interface ao longo do caminho.
 - ◆ Disponível, não são comumente usados porque normalmente resultam em recálculo frequente da tabela de topologia:
Confiabilidade - A
 - ◆ pior confiabilidade entre a origem e o destino, com base em keepalives.
 - ◆ Carregamento - A pior carga em um link entre a origem e o destino com base na taxa de pacotes e na largura de banda configurada da interface.
 - ◆ Unidade máxima de transmissão (MTU) - A menor MTU no caminho.
- Uma vantagem significativa do EIGRP (e IGRP) em relação a outros protocolos é seu suporte para balanceamento de carga métrico desigual que permite aos administradores distribuir melhor o fluxo de tráfego em suas redes.



RIPng para roteamento IPv6

- Semelhante ao IPv4 RIPv2:

- ◆ Conceito de vetor de distância, raio de 15 saltos, métrica infinita é 16, horizonte dividido, atualização acionada.

- Diferenças entre RIPv2 e RIPng

- ◆ Usa IPv6 para transporte.
 - ◆ Usa endereços locais de link (não os globais).
 - ◆ Prefixo IPv6, endereço local de link IPv6 do próximo salto.
 - ◆ Usa o endereço de grupo multicast FF02::9 (todos os roteadores RIP) como endereço de destino para atualizações RIP.
 - ◆ Os roteadores sempre adicionam o custo da interface à métrica recebida.
 - ◆ A métrica é a soma dos custos das “interfaces de saída” até o destino e não o número de saltos.
 - ◆ Se todos os custos forem 1, a métrica é o número de “interfaces de saída” para o destino.
 - ◆ Permite custos de nó/interface diferentes de 1.
 - ◆ A Cisco chama isso de “compensação de custo” por interface (fora ou na direção).
 - ◆ O custo para a rede é dado pela soma de todos os custos das interfaces de saída ao longo do caminho.
 - ◆ Com o valor da métrica infinita em 16, isso requer configurações cuidadosas.
 - ◆ Os roteadores sempre anunciam redes conectadas direcionadas. em
 - ◆ IOS Cisco
 - ◆ Ativação por interface, processo nomeado, mais de um processo ativo.

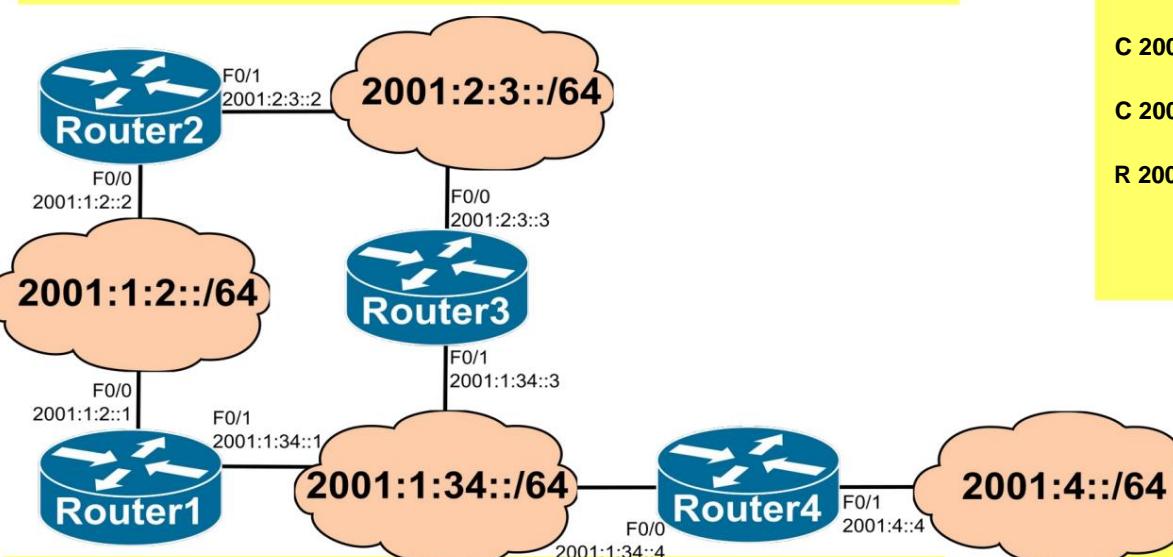


Tabelas de roteamento IPv6 com RIPng

Roteador2

```
C 2001:1:2::/64 [0/0] via
    FastEthernet0/0, conectado diretamente
R 2001:1:34::/64 [120/2]
    via FE80::C801:54FF:FE41:8, FastEthernet0/0 via
    FE80::C803:56FF:FE0A:8, FastEthernet0/1
C 2001:2:3::/64 [0/0] via
    FastEthernet0/1, conectado diretamente
R 2001:4::/64 [120/3] via
    FE80::C801:54FF:FE41:8, FastEthernet0/0 via
    FE80::C803:56FF:FE0A:8, FastEthernet0/1
```

Assumindo todas as interfaces com custo 1.



Roteador1

```
C 2001:1:2::/64 [0/0] via
    FastEthernet0/0, conectado diretamente
C 2001:1:34::/64 [0/0] via
    FastEthernet0/1, conectado diretamente
R 2001:2:3::/64 [120/2]
    via FE80::C802:54FF:FEF5:8, FastEthernet0/0 via
    FE80::C803:56FF:FE0A:6, FastEthernet0/1
R 2001:4::/64 [120/2] via
    FE80::C804:56FF:FEAD:8, FastEthernet0/1
```

Roteador3

```
R 2001:1:2::/64 [120/2]
    via FE80::C802:54FF:FEF5:6, FastEthernet0/0 via
    FE80::C801:54FF:FE41:6, FastEthernet0/1
C 2001:1:34::/64 [0/0]
    via FastEthernet0/1, conectado diretamente
C 2001:2:3::/64 [0/0] via
    FastEthernet0/0, conectado diretamente
R 2001:4::/64 [120/2] via
    FE80::C804:56FF:FEAD:8, FastEthernet0/1
```

Roteador4

```
R 2001:1:2::/64 [120/2]
    via FE80::C801:54FF:FE41:6, FastEthernet0/0
C 2001:1:34::/64 [0/0]
    via FastEthernet0/0, conectado diretamente
R 2001:2:3::/64 [120/2]
    via FE80::C803:56FF:FE0A:6, FastEthernet0/0
C 2001:4::/64 [0/0] via
    FastEthernet0/1, conectado diretamente
```



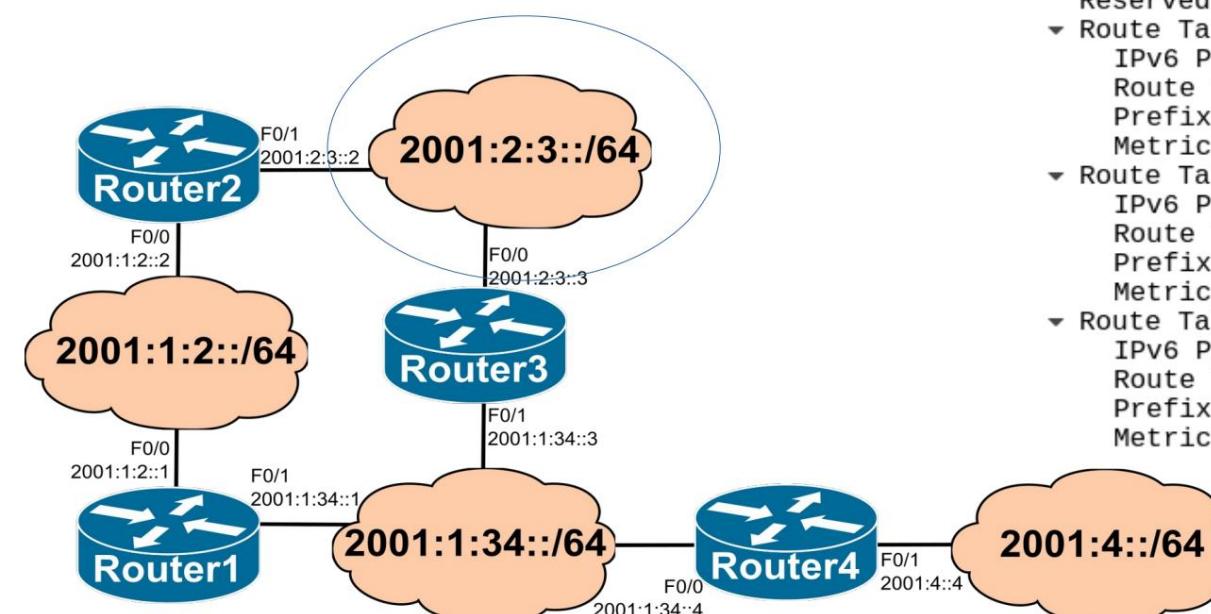
Mensagens RIPng (Exemplo)

Enviado por Router2 com Split-Horizon

```

▶ Internet Protocol Version 6, Src: fe80::c802:54ff:fef5:6, Dst: ff02::9
▶ User Datagram Protocol, Src Port: 521, Dst Port: 521
▼ RIPng
  Command: Response (2)
  Version: 1
  Reserved: 0000
▼ Route Table Entry: IPv6 Prefix: 2001:1:2::/64 Metric: 1
  IPv6 Prefix: 2001:1:2::
  Route Tag: 0x0000
  Prefix Length: 64
  Metric: 1
▼ Route Table Entry: IPv6 Prefix: 2001:2:3::/64 Metric: 1
  IPv6 Prefix: 2001:2:3::
  Route Tag: 0x0000
  Prefix Length: 64
  Metric: 1

```



Enviado por Router3 com Split-Horizon

```

▶ Internet Protocol Version 6, Src: fe80::c803:56ff:fe0a:8, Dst: ff02::9
▶ User Datagram Protocol, Src Port: 521, Dst Port: 521
▼ RIPng
  Command: Response (2)
  Version: 1
  Reserved: 0000
▼ Route Table Entry: IPv6 Prefix: 2001:2:3::/64 Metric: 1
  IPv6 Prefix: 2001:2:3::
  Route Tag: 0x0000
  Prefix Length: 64
  Metric: 1
▼ Route Table Entry: IPv6 Prefix: 2001:1:34::/64 Metric: 1
  IPv6 Prefix: 2001:1:34::
  Route Tag: 0x0000
  Prefix Length: 64
  Metric: 1
▼ Route Table Entry: IPv6 Prefix: 2001:4::/64 Metric: 2
  IPv6 Prefix: 2001:4::
  Route Tag: 0x0000
  Prefix Length: 64
  Metric: 2

```



Roteamento - OSPFv3

- Baseado em OSPFv2, com melhorias:
 - ◆ Usa IPv6 para transporte
 - ◆ Distribui prefixos IPv6
 - ◆ Usa endereços de grupo multicast FF02::5 (OSPF IGP) e FF02::6 (Roteadores designados IGP OSPF)
 - ◆ Executa sobre um link em vez de uma sub-rede
 - ◆ Múltiplas instâncias por link
 - ◆ Topologia não específica do IPv6
 - ➡ ID do roteador, ID da área, ID do link permanecem um número de 4 bytes
 - ➡ Os vizinhos são sempre identificados pelo ID do roteador (4 bytes)
 - ➡ Com uma tabela adicional com mapeamento entre prefixos IPv6 e Link IDs
 - ◆ Usa endereços locais de link como endereços de origem IPv6

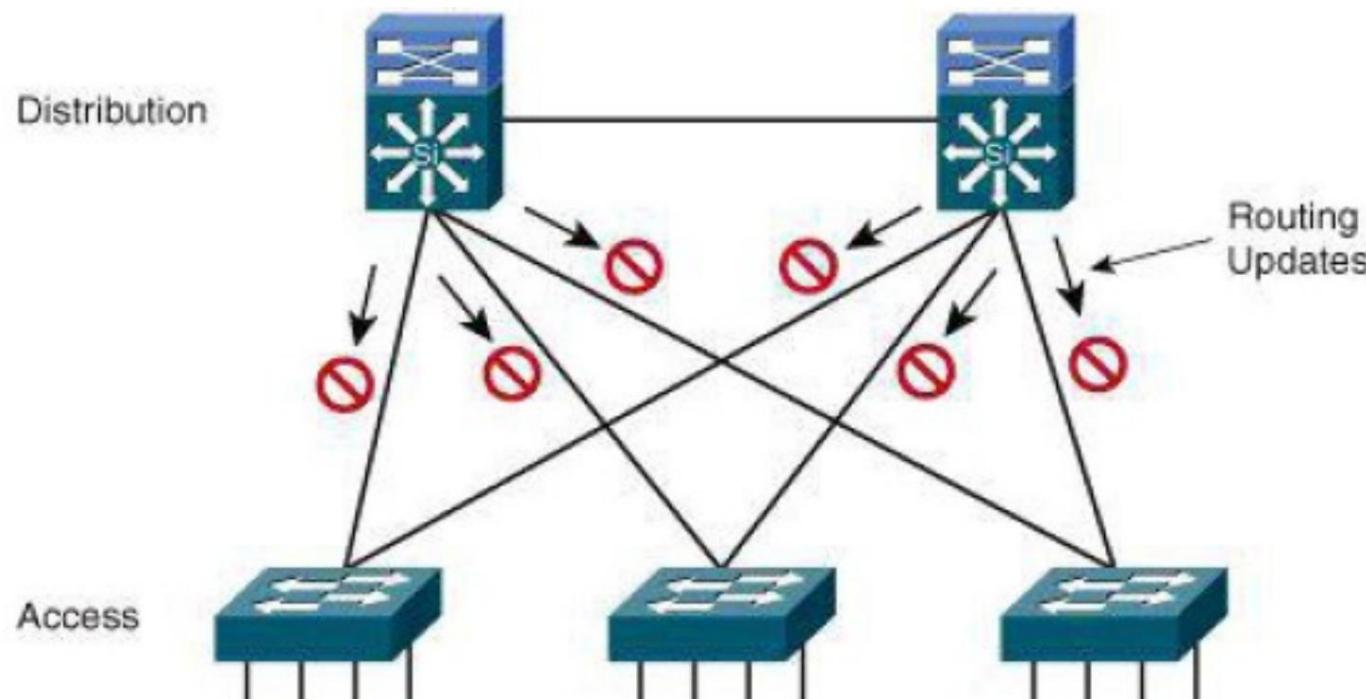


OSPFv3 - Tipos de LSA

- Link LSA (Tipo 8)
 - ◆ Informa os vizinhos sobre o endereço local do link
 - ◆ Informa os vizinhos sobre os prefixos IPv6 no link
- Prefixo intra-área LSA (Tipo 9)
 - ◆ Associa prefixos IPv6 a uma rede ou roteador
- O escopo de inundação para LSAs foi generalizado
 - ◆ Três escopos de inundação para LSAs
 - ✚ Link-local
 - ✚ Área
 - ✚ COMO
- Codificação de tipo LSA expandida para 16 bits
 - ◆ Inclui escopo de inundação



Interfaces Passivas na Camada de Acesso

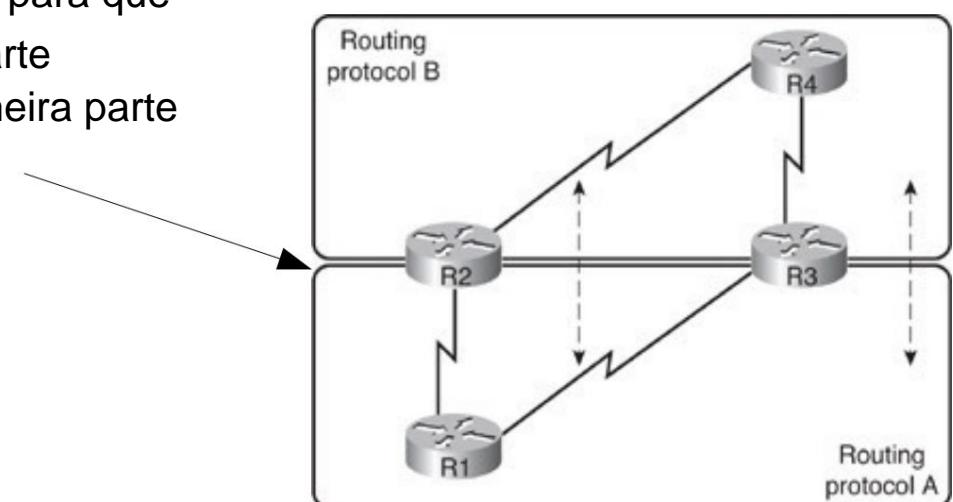
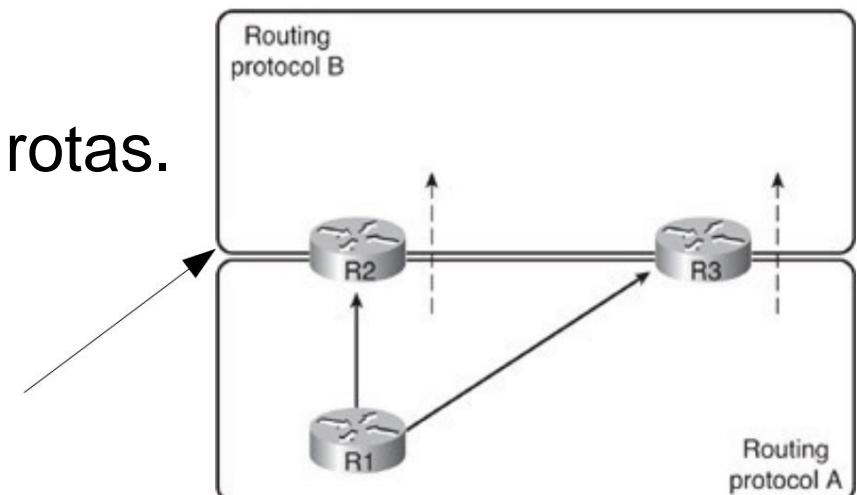


- Como prática recomendada, limite as adjacências de peer de roteamento L3 desnecessárias configurando as portas para os switches de acesso da Camada 2 como passivas.
 - ◆ Suprimir a publicidade de atualizações de roteamento.
 - ◆ Se um switch de distribuição não receber atualizações de roteamento L3 de um par em potencial em uma interface específica, ele não formará uma adjacência de vizinho com o par em potencial nessa interface.



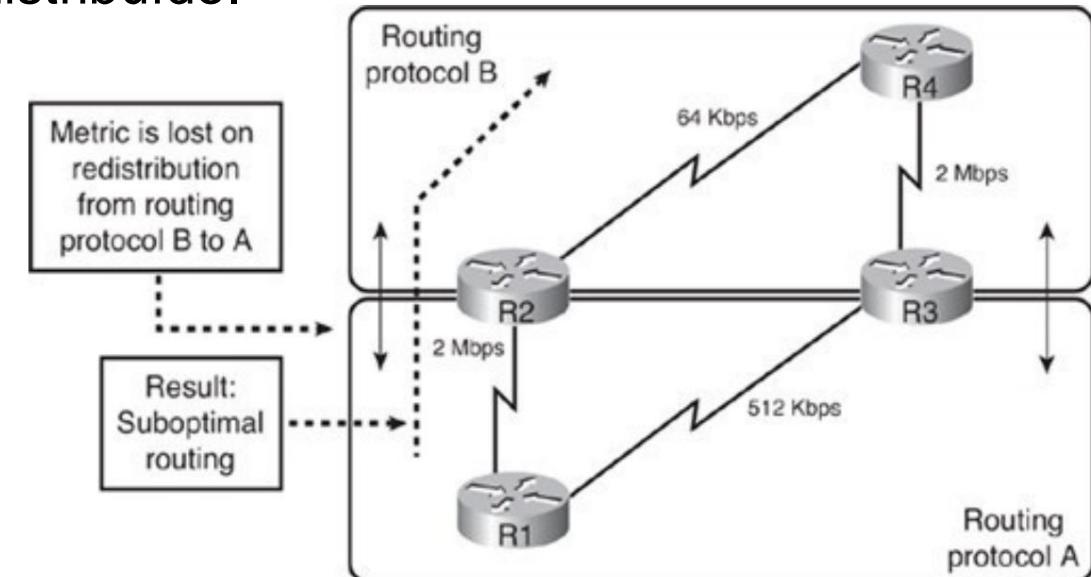
Redistribuição de rota

- Domínios com protocolos de roteamento diferentes podem trocar rotas.
 - ◆ Isso é chamado de redistribuição de rota.
 - ✚ Redistribuição unidirecional
 - Redistributioni apenas as redes aprendidas de um protocolo de roteamento para o outro protocolo de roteamento.
 - Usa uma rota padrão ou estática para que os dispositivos naquela outra parte da rede possam alcançar a primeira parte da rede
 - ✚ Redistribuição bidirecional - Redistribui as rotas entre os dois processos de roteamento em ambas as direções
 - ◆ As rotas estáticas também podem ser redistribuídas.



Problemas de redistribuição

- Métrica perdida do protocolo redistribuído.
 - ◆ Não é possível obter um roteamento geral ideal.

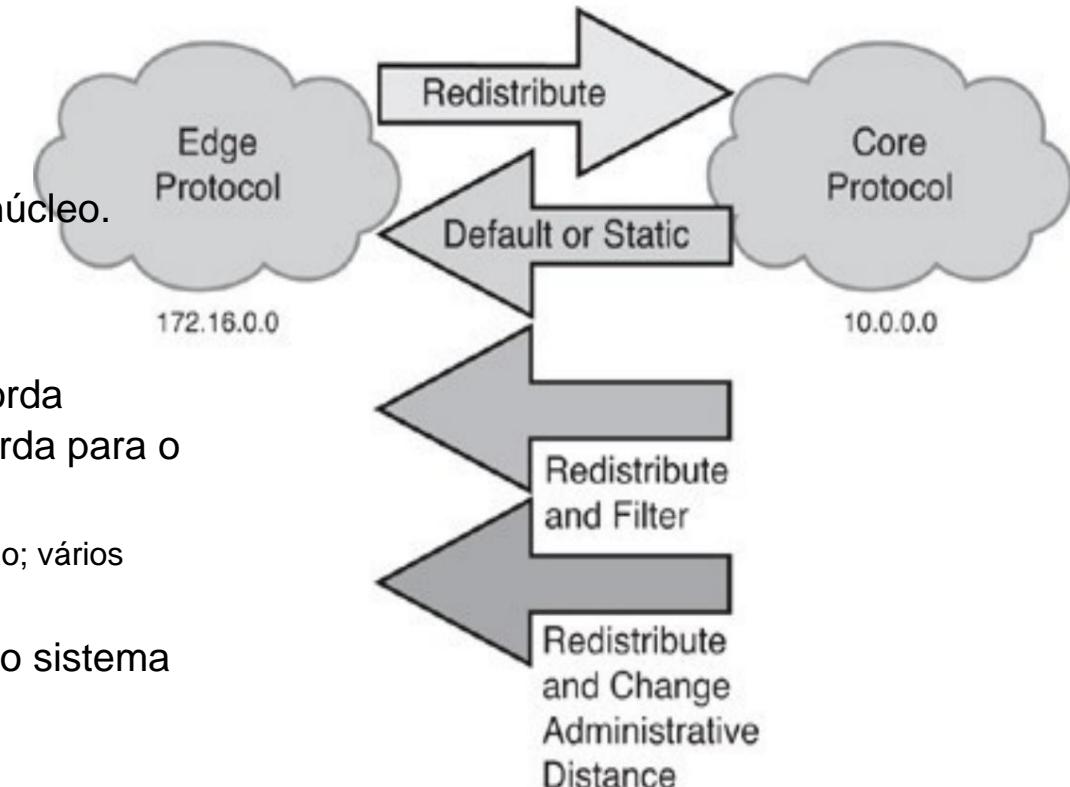


- Prevenção de loops de roteamento em um ambiente de redistribuição.
 - ◆ A maneira mais segura de executar a redistribuição é redistribuir as rotas em apenas uma direção, em apenas um roteador de limite dentro da rede.
 - ➡ No entanto, isso resulta em um único ponto de falha na rede.
 - ◆ Se a redistribuição deve ser feita em ambas as direções ou em vários roteadores de limite, a redistribuição deve ser ajustada para evitar problemas como roteamento abaixo do ideal e loops de roteamento.



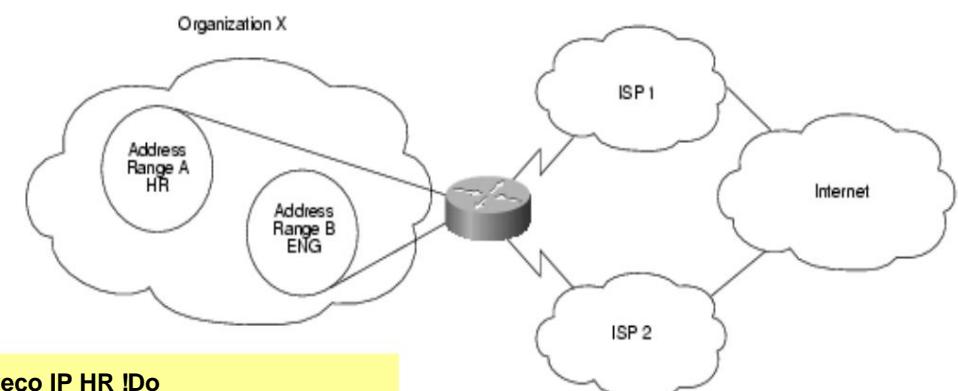
Técnicas de Redistribuição

- Redistribua uma rota padrão do sistema autônomo de núcleo para o sistema autônomo de borda e redistribua as rotas dos protocolos de roteamento de borda para o protocolo de roteamento de núcleo.
 - Essa técnica ajuda a evitar feedback de rota, roteamento abaixo do ideal e loops de roteamento.
- Redistribua várias rotas estáticas sobre as redes do sistema autônomo central para o sistema autônomo de borda e redistribua as rotas dos protocolos de roteamento de borda para o protocolo de roteamento central.
 - Esse método funciona se houver apenas um ponto de redistribuição; vários pontos de redistribuição podem causar feedback de rota.
- Redistribua as rotas do sistema autônomo principal para o sistema autônomo de borda com filtragem para bloquear rotas inapropriadas.
 - Por exemplo, quando há vários roteadores de limite, as rotas redistribuídas do sistema autônomo de borda em um roteador de limite não devem ser redistribuídas de volta para o sistema autônomo de borda do núcleo em outro ponto de redistribuição.
- Redistribuir todas as rotas do sistema autônomo central para o sistema autônomo de borda e do sistema autônomo de borda para o sistema autônomo central e, em seguida, modificar a distância administrativa associada às rotas redistribuídas para que não sejam as rotas selecionadas quando existirem várias rotas para o mesmo destino.



Roteamento baseado em políticas (PBR)

- O PBR permite que o operador defina uma política de roteamento diferente do roteamento baseado em destino básico usando a tabela de roteamento.
- As regras PBR podem ser usadas para corresponder endereços de origem e destino, tipos de protocolo e aplicativos de usuário final.
- Quando ocorre uma correspondência, um comando set pode ser usado para definir a interface ou o endereço do próximo salto para o qual o pacote deve ser enviado.



```
lista de acesso 1 permissão 209.165.200.225 lista de acesso
2 permissão 209.165.200.226 ! interface ethernet 1 ip policy
```

```
!Do endereço IP HR !Do
endereço IP ENG
```

```
route-map ChooseISP ! mapa de
rota Escolha ISP permit 10 match ip address 1
```

Define a ordem das regras

```
set ip next-hop 209.165.200.227 ! mapa de rota
Escolher ISP permitir 20
corresponder ao endereço IP 2 configurar ip
```

!Para o próximo salto do ISP2

```
próximo salto 209.165.200.228
```

!Para o próximo salto do ISP1



Introdução a Segurança de rede

Segurança em Redes de Comunicações

Mestrado em Cibersegurança

**Mestrado em Engenharia de Computadores e
telemática**

DETI-UA



Tipo de Ataques (1)

- Objetivos:
 - ◆ Diversão e/ou reputação
 - ◆ hacker Fins
 - ◆ políticos Fins
 - ◆ militares Fins
 - ◆ econômicos Outros?
- Objetivos técnicos:
 - ◆ interrupção da operação
 - ◆ Para interceptação de dados
 - ◆ Ambos
 - ◆ Perturbação para interceptar!
 - ◆ Interceptar para atrapalhar!



Tipo de Ataques (2)

- Objetivos técnicos:

- ◆ Interrupção da operação.

- ✚ (Negação de serviço distribuída.

- ◆ Sequestro de recursos.

- ✚ Spam,

- ✚ mineração/masternodes de criptomoedas,

- ✚ plataforma para outros ataques!

- ◆ Interceptação/roubo de dados.

- ✚ Dados pessoais

- Como objetivo

- final, – Ou como ferramenta para obter mais informações de valor!

- ✚ Dados técnicos, –

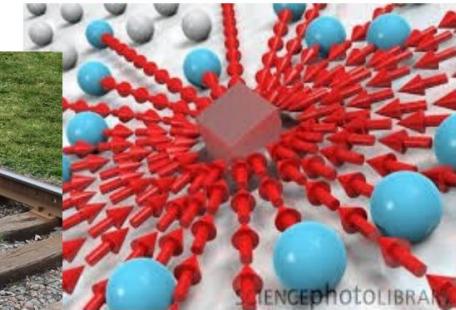
- Geralmente usados para obter mais informações de valor!

- ✚ Dados comerciais

- Objetos digitais, planos financeiros e/ou de engenharia, ...

- A interrupção pode ser usada para conseguir a interceptação!

- A interceptação pode ser usada para obter disruptão (operacional ou comercial)!



Ataques de interrupção

DoS distribuído

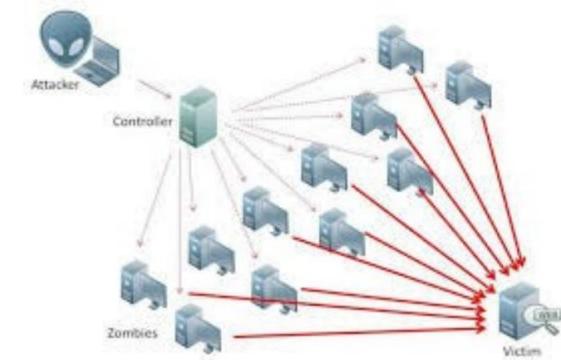
- ◆ Vários dispositivos lentos/pequenos gerando tráfego para um destino
 - ➡ TCP x UDP
- ◆ Finalidade da interrupção
 - ➡ Por político/econômico/"reputação"
 - ➡ Redirecionamento para outro serviço/local?
- ◆ Solução no alvo
 - ➡ balanceadores de carga
 - ➡ Para TCP, talvez seja possível sobreviver fazendo redefinições de sessão ativas (com validação de cliente lícita) (servidor/firewalls)
 - Solução de lista branca, para negociação de sessão concluída
 - ➡ Para UDP/DNS, bloqueia solicitações para servidores DNS de retransmissão/redirecionamento externos conhecidos (bloqueia amplificação de ataque, falsificação de destino de IP)
 - Não funciona com botnets grandes e solicitações diretas ao alvo

Solução na fonte

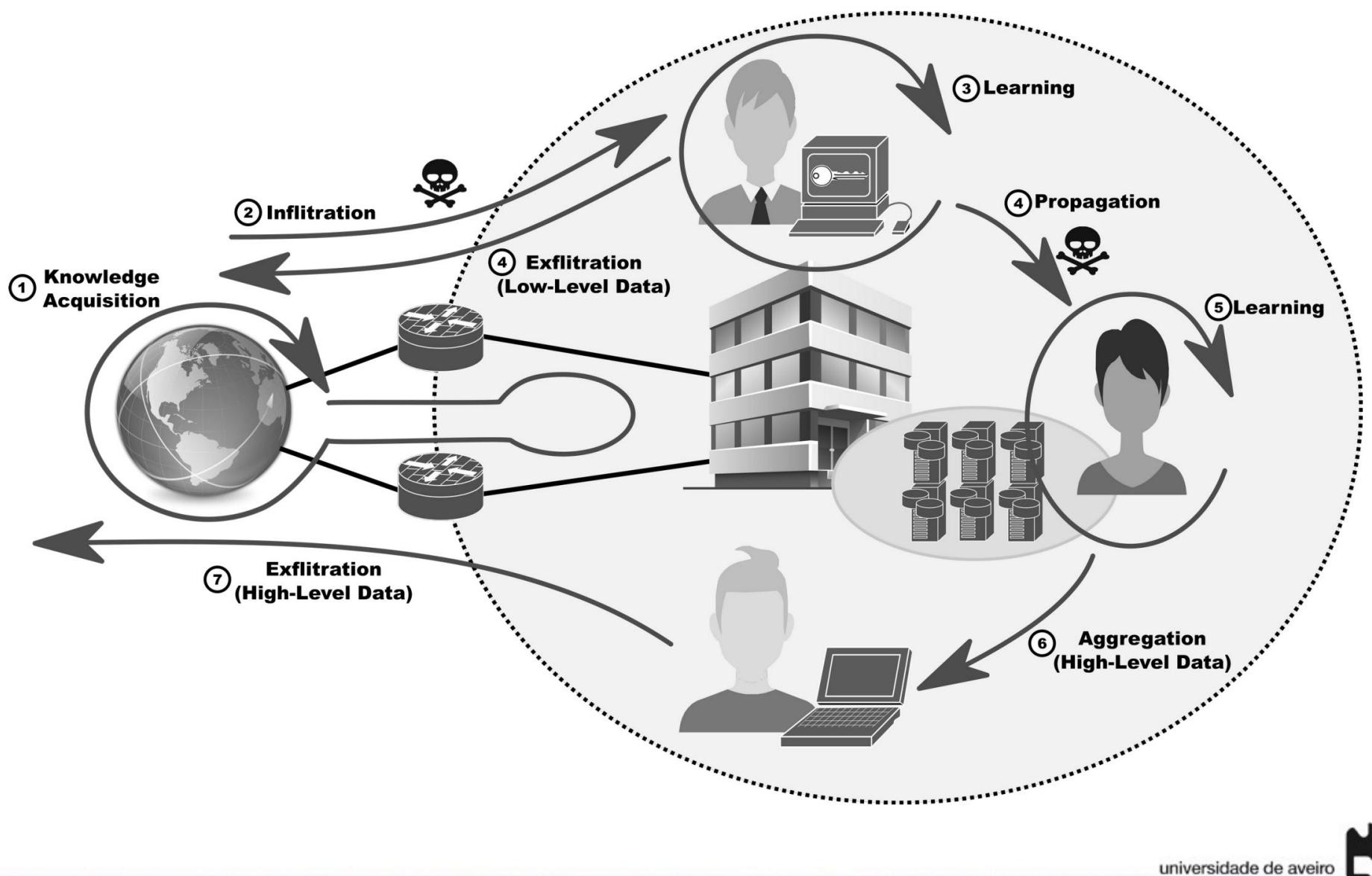
- ➡ Detecção de comportamentos anômalos
 - Baixas variações de tráfego difíceis de detectar
 - Mudanças de tempo e periodicidade são mais fáceis de detectar
 - Destinos de mudanças de tráfego
 - Com taxas de dados "realmente baixas" é impossível detectar

Negação de serviço por bloqueio de sinal físico

- ◆ Disrupção pura,
- ◆ ou Disrupção para ativar canais secundários (mais facilmente comprometidos).
- ◆ Solução
 - ➡ Detecte, localize a fonte e neutralize fisicamente.



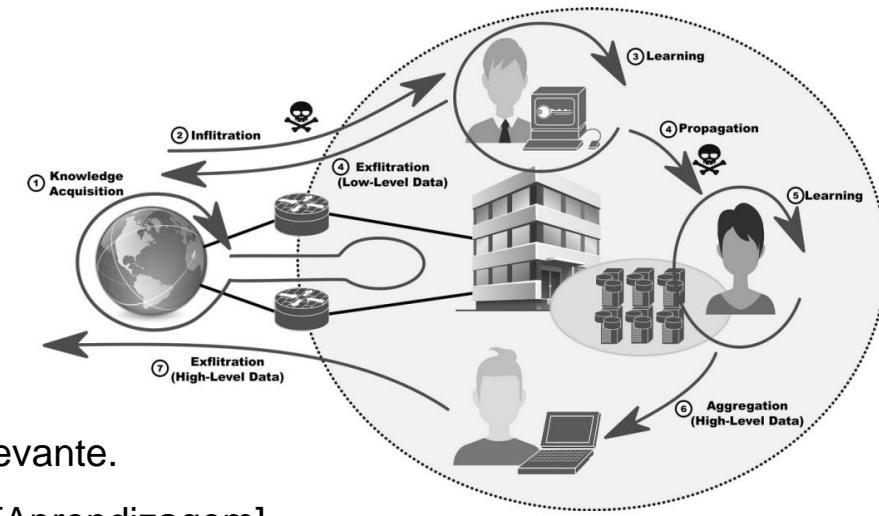
Fases dos Ataques



Os ataques são feitos de forma incremental

- Escalação de metas e privilégios.

- Escalação de metas e privilégios.
 - ◆ O conhecimento público abre portas para informações privadas e acesso a domínios protegidos [Infiltração].
 - ◆ O primeiro acesso ilícito a um domínio protegido pode não fornecer um resultado relevante.
 - ◆ O atacante deve adquirir mais conhecimento [Aprendizagem].
 - ◆ O conhecimento adicional permite acessar outras zonas/dispositivos/dados de domínio seguro com relevância crescente [Propagação].
 - ➡ Em qualquer fase, o invasor pode exigir conhecimento adicional [Aprendizagem].
 - ◆ Quando um resultado relevante é adquirido, ele deve ser transferido para fora do domínio protegido [Exfiltration].
 - ◆ A exfiltração direta pode denunciar os pontos relevantes dentro do domínio seguro.
 - ➡ O resultado relevante deve ser primeiro transferido dentro do domínio protegido para um ponto menos importante [Agregação].
 - ➡ O atacante escolhe um ponto que pode ser detectado e perdido sem danos.



Vulnerabilidades de rede técnica

• Programas

- ◆ Formulários
- ◆ Estruturas/API
- ◆ Protocolos
- ◆ Sistemas operacionais
 - ➡ Kernel, módulos do kernel, drivers e aplicativos básicos.
 - ➡ Configurações!
- ◆ Código de baixo nível
 - ➡ Microcódigo da CPU, firmware e BIOS/UEFI.



• hardware

- ◆ Têmpera física
- ◆ Emissões físicas
 - ➡ Emissões eletromagnéticas, sonoras, ...
- ◆ Instabilidade de energia, Pulso Eletromagnético (EMP), etc...



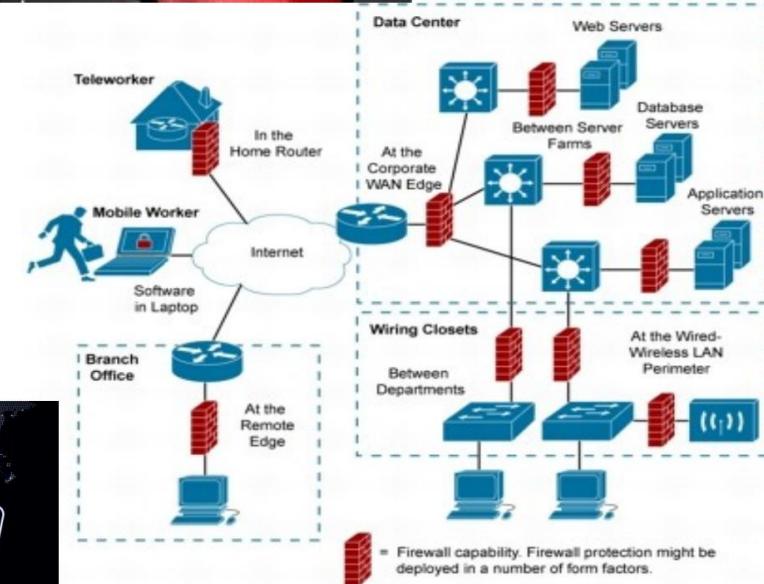
• Conhecido vs. desconhecido

- ◆ CVE
- ◆ Bancos de dados IDS/IPS e antivírus



Defesas Tradicionais

- Correção de vulnerabilidades.
- firewalls
 - ◆ Centralizado.
 - ◆ Distribuído.
- Sistemas de Prevenção e Detecção de Intrusão (IDS/IPS)
- Antivírus.



- **Todos dependem do conhecimento prévio da ameaça e/ou problema!**



Defesas “inteligentes”

- Detecção de ameaças e/ou problemas desconhecidos.
 - ◆ A tempo de implantar contra-medidas.
- Aplicação de técnicas de Big Data e Data Science a dados de monitoramento de redes e sistemas.
- Algumas soluções tradicionais começam a incorporar IA em seus equipamentos
 - ◆ Por exemplo, Palo Alto Network Firewalls, Cisco Appliances, ...
- Ainda limitado a soluções baseadas no fabricante e dados localizados.
- Ainda limitado em escopo.
 - ◆ Ameaças óbvias vs. Ameaças furtivas.
- A implantação ideal requer um conhecimento geral de rede e sistemas.
 - ◆ Rede e Sistemas (Cyber) Consciência Situacional.



Fase de Infiltração

- As máquinas lícitas devem ser comprometidas para implementar as diferentes fases dos ataques.
 - ◆ Idealmente numa “zona” privilegiada da rede, e/ou Com credenciais de acesso, e/ou
 - ◆ Credenciais de Utilizador, morada(s), chave de hardware, etc...
 - ◆ Com software “especial” e/ou dados
 - ◆ de alvo.
- Pode incluir a instalação de software ou uso de software vulnerável lícito.
- Pode ser controlado remotamente (constantemente ou não).
 - ◆ Comando e controle (C&C).
- Pode ter bots autônomos (AI) instalados para realizar ações ilícitas.
 - ◆ Quando o C&C remoto não é possível ou está sujeito a detecção fácil.



Fase de Propagação

- Feito usando uma mistura de metodologias:
 - ◆ Exploração de credenciais.
 - Uso direto ou usando aplicativos permitidos.
 - ◆ Representando usuários e sistemas.
 - Semelhante à exploração de credenciais, mas mais avançado com base no conhecimento adquirido (comportamento lícito).
 - Requer tempo para aprender e imitar o comportamento lícito.
 - Padrões de tempo, padrões de tráfego, padrões de aplicação, etc...
 - ◆ Exploração de vulnerabilidade.
 - Dentro de um domínio protegido, os sistemas são muitas vezes considerados em uma zona segura.
 - Sistemas operacionais/aplicativos menos mantidos e legados podem ser necessários para execução (sem aplicação de patches).
 - Gama mais ampla de vulnerabilidades



Fase de Agregação e Exfiltração

- Dados transferidos de máquina para máquina.
- Internamente [Agregação] pode ser feito usando canais existentes.
- Externamente [Exfiltração]
 - ◆ Isso pode ser feito diretamente usando os canais existentes.
 - ✚ Cópia de arquivo, e-mail, compartilhamento de arquivo, etc...
 - ✚ Pode ser detectado.
 - ◆ Pode ser feito ocultando informações dentro de canais existentes/permitidos e comunicações lícitas.
 - ✚ Transferência de dados mais lenta, mais difícil (impossível?) de detectar.
 - ✚ Exemplos: –
 - Uso de esteganografia em fotos (via redes sociais).
 - Uso de dados incorporados em mensagens de texto e voz.
 - ...



Métricas de segurança/KPI

- gerenciamento de acesso
 - ◆ Quantos usuários têm acesso administrativo e com que frequência é usado.
 - ◆ Senhas compartilhadas entre funcionários.
- Preparação
 - ◆ Porcentagem de dispositivos totalmente corrigidos e atualizados.
- Dias para corrigir o
 - ◆ tempo médio entre a disponibilidade e a implantação do patch.
- Dispositivos não identificados
 - ◆ Dispositivos implantados ilicitamente.
 - ◆ Política BYoD, dispositivos legados, dispositivos não listados, dispositivos IoT, etc...
- Carga média/máxima dos dispositivos de segurança por período de tempo.
- Tentativas de invasão
 - ◆ Quantidade de tentativas detectadas e não detectadas (em tempo real ou após auditoria off-line).
- Custo por incidente Inclui
 - ◆ horas extras da equipe, suporte externo, custos de investigação, perda de produtividade do funcionário, perda de comunicação, falha de serviço, etc.
- Tempo médio entre falhas (MTBF)
 - ◆ Tempo médio entre falhas (hardware e/ou software).
 - ◆ Geral ou por dispositivo/serviço.
- Tempo médio de recuperação (MTTR)
 - ◆ Tempo médio entre falha e recuperação (hardware e/ou software).
- Tempo médio de detecção (MTTD)
 - ◆ Tempo médio entre a invasão e a detecção.
- Tempo médio para reconhecimento (MTTA)
 - ◆ Tempo médio entre a detecção e o início da implantação das contramedidas.
- Tempo médio de contenção (MTTC)
 - ◆ Tempo médio entre o início da implantação das contramedidas e a mitigação completa.
- Tempo médio para resolver (MTTR)
 - ◆ MTTA+MTTR



Controle de acesso à rede

**Segurança em Redes de Comunicações
Mestrado em Cibersegurança**

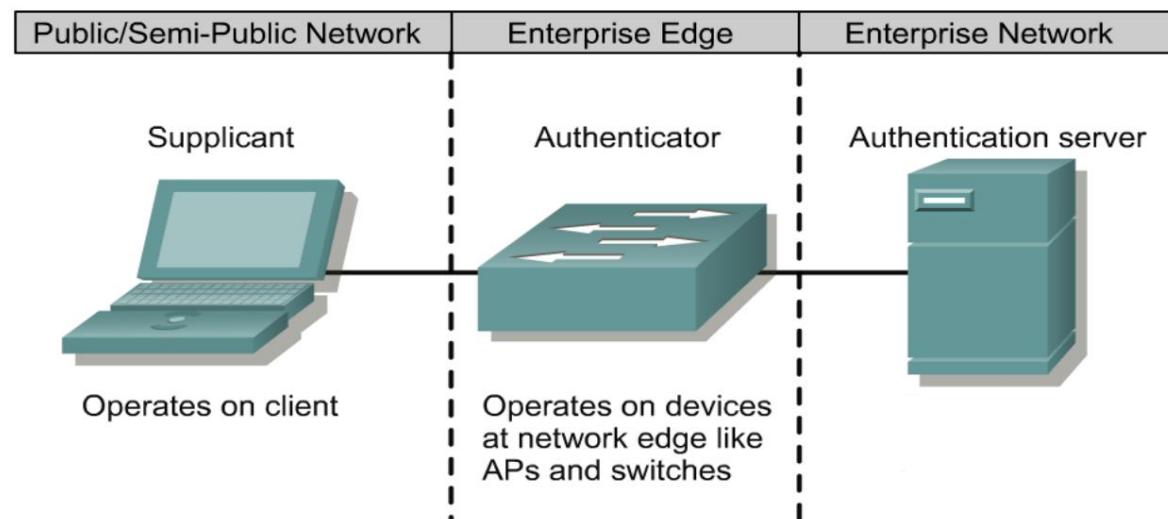
**Mestrado em Engenharia de Computadores e
telemática**

DETI-UA



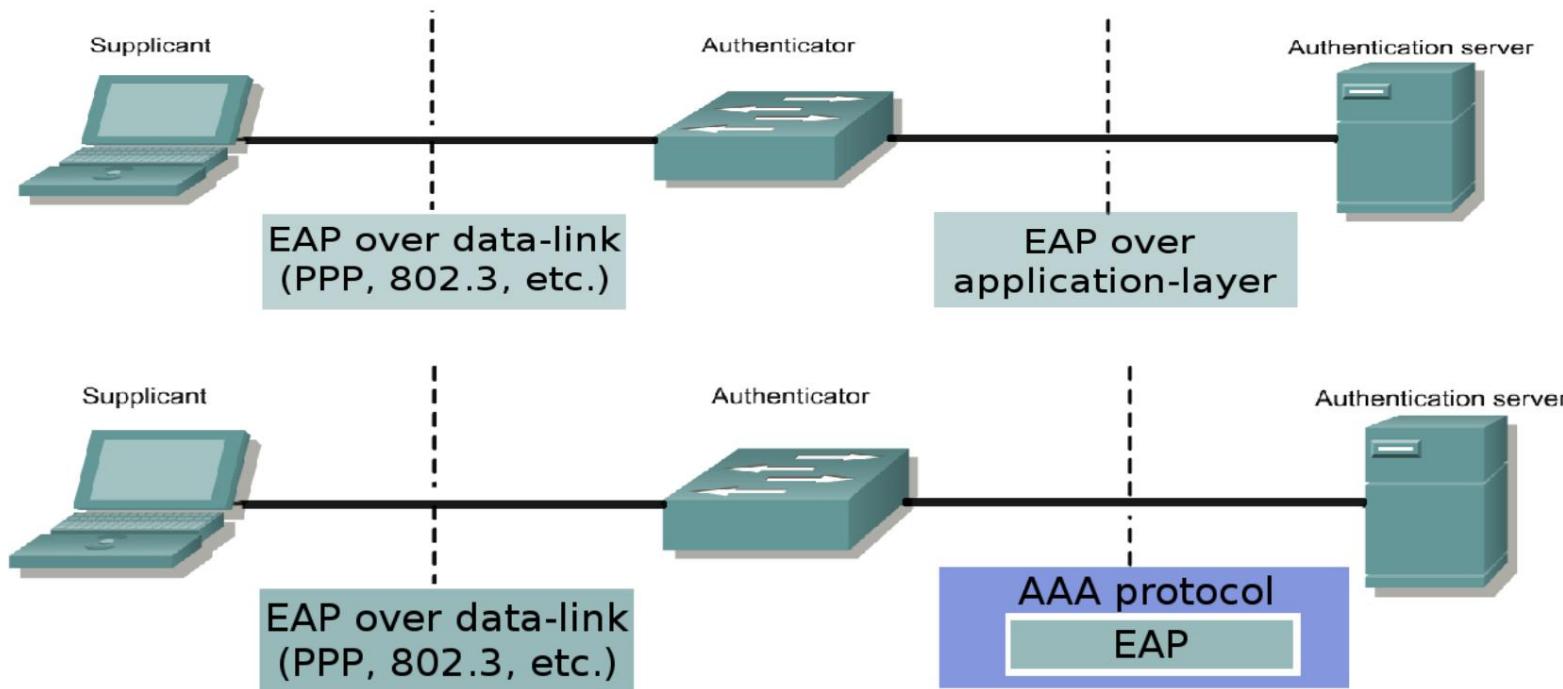
Arquitetura AAA

- Permite segurança de acesso sistemático
 - ◆ Autenticação identifica um usuário
 - ◆ A autorização determina o que esse usuário pode fazer
 - ◆ A contabilidade monitora o tempo de uso da rede para fins de cobrança
- As informações AAA são normalmente armazenadas em um banco de dados externo ou servidor de autenticação remota
- Implementação AAA Tradicional



802.1X

- IEEE 802.1X é um padrão IEEE para controle de acesso à rede (NAC)
 - 802.1X-2001 e 802.1X-2004 fornecem apenas autenticação.
 - 802.1X-2010 adiciona criptografia opcional no segmento LAN.
- Ele fornece um mecanismo de autenticação para dispositivos que desejam se conectar a uma LAN.
- Baseado no Extensible Authentication Protocol (EAP).
- Protocolos/serviços AAA: TACACS+, RADIUS e DIAMETER.



Protocolo de Autenticação Extensível (EAP)

- O EAP definido em [RFC3748] foi projetado para permitir autenticação extensível para acesso à rede em situações nas quais o protocolo IP (Internet Protocol) não está disponível.
 - ◆ Originalmente desenvolvido para uso com protocolo ponto a ponto (PPP) [RFC1661]
 - ◆ Posteriormente, também foi aplicado a redes com fio IEEE 802 [IEEE 802.1X], Internet Key Exchange Protocol versão 2 (IKEv2) [RFC4306] e redes sem fio como [IEEE-802.11] e [IEEE-802.16e].
- EAP é um protocolo de duas partes falado entre o par EAP e servidor.
 - ◆ O material de chaveamento é gerado por algoritmos de autenticação EAP, conhecidos como "métodos".
 - ◆ Parte desse material de codificação pode ser usado pelos próprios métodos EAP e parte desse material pode ser exportado.



Visão geral do EAP (1)

- Onde a derivação de chave EAP é suportada, a conversa normalmente ocorre em três fases:
 - Fase 0: Descoberta
 - Fase 1: Autenticação
 - ◆ 1a: Autenticação EAP
 - ◆ 1b: Transporte de chave AAA (opcional)
 - Fase 2: protocolo de associação segura
 - ◆ 2a: Associação Segura Unicast
 - ◆ 2b: Associação Segura Multicast (opcional)



Visão geral do EAP (2)

- As camadas inferiores do EAP implementam as fases 0, 2a e 2b de diferentes maneiras:
 - ◆ IEEE 802.1X
 - IEEE 802.1X-2004 não suporta descoberta (fase 0), nem fornece derivação de associações seguras unicast ou multicast (fase 2).
 - ◆ IEEE 802.11
 - Lida com a descoberta por meio dos mecanismos Beacon e Probe Request/Response.
 - Pontos de acesso (APs) anunciam periodicamente seus Identificadores de conjunto de serviços (SSIDs), bem como recursos usando quadros Beacon.
 - As estações podem consultar APs enviando uma solicitação de sondagem.
 - Nem os quadros Beacon nem Probe Request/Response estão protegidos.
 - Um handshake de 4 vias permite a derivação de associações seguras unicast (fase 2a) e multicast/broadcast (fase 2b).



TACACS+

- Controlador de Acesso Terminal Sistema de Controle de Acesso Plus
- Encaminha informações de nome de usuário e senha para um servidor de segurança centralizado
- O servidor centralizado pode ser um banco de dados TACACS ou um banco de dados como o arquivo de senha UNIX com suporte a TACACS
- Características
 - ◆ Separa todas as funcionalidades AAA
 - ◆ Usa TCP
 - ◆ autenticação bidirecional
 - ◆ Todos os pacotes são criptografados
 - ◆ Customização contábil limitada

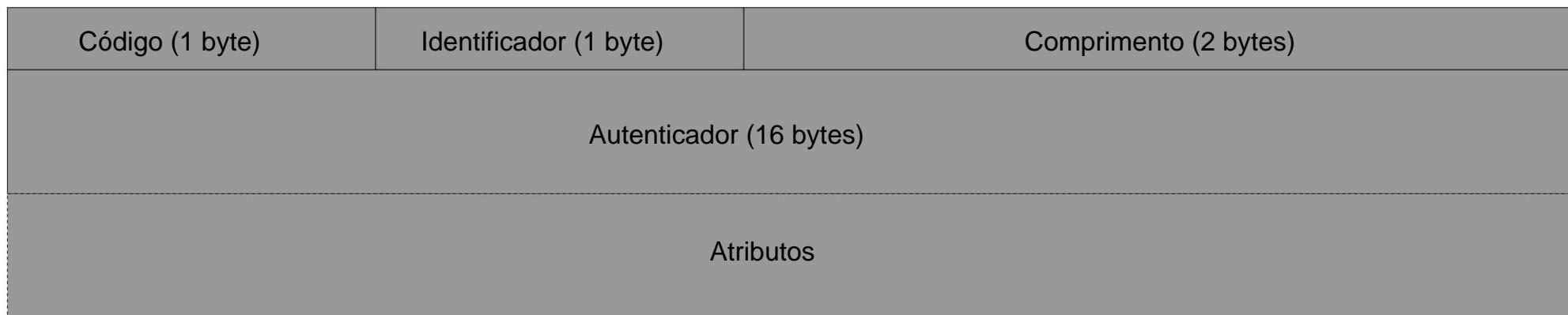


RAIO

- Serviço de usuário de discagem de autenticação remota
- O dispositivo de acesso à rede funciona como um cliente RADIUS
- Os servidores RADIUS são responsáveis por
 - ◆ Recebendo solicitações de conexão do usuário
 - ◆ Autenticando o usuário
 - ◆ Retorne todas as informações de configuração necessárias para que o cliente entregue o serviço ao usuário
- As transações entre o cliente e o servidor RADIUS são autenticadas usando um segredo compartilhado
- Suporta uma variedade de métodos para autenticar um usuário
 - ◆ PAP, CHAP ou MS-CHAP, login UNIX e outros mecanismos de autenticação
- Combina autenticação e autorização. Separa a Contabilidade (menos flexível que o TACACS+)
- Usa UDP (menos robusto)
- autenticação unidirecional
- Criptografa apenas a senha (menos seguro)
- A contabilidade RADIUS pode conter mais informações



Pacote RADIUS

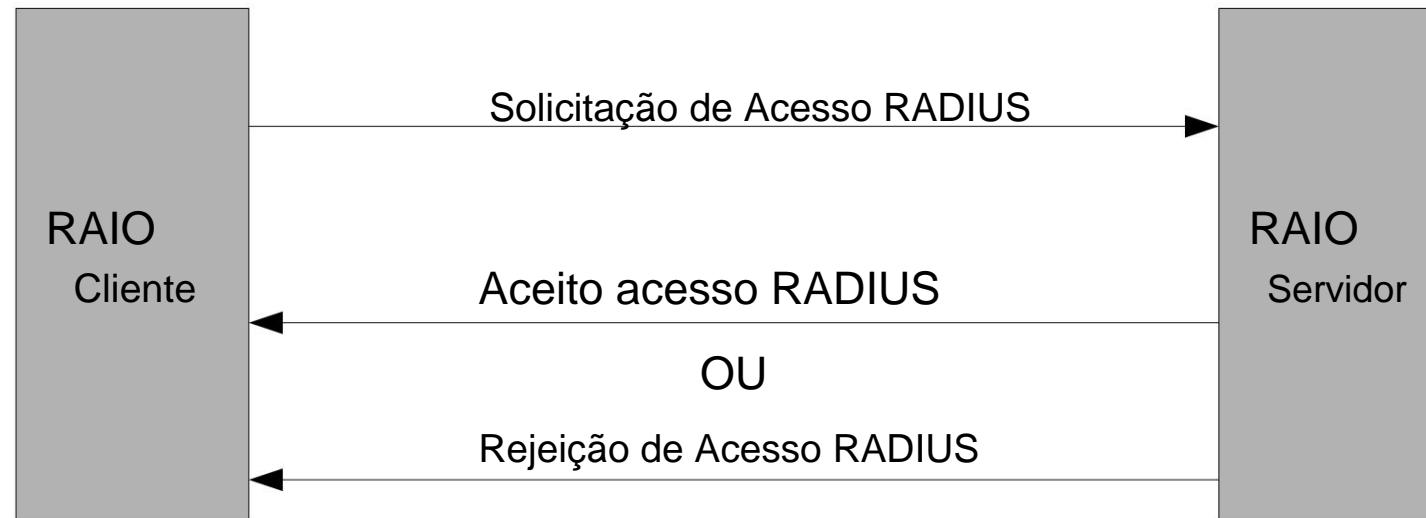


- Código - Identifica o tipo de pacote RADIUS
 - ◆ (1) Solicitação de acesso, (2) Aceitação de acesso, (3) Rejeição de acesso, (4) Solicitação de contabilidade, (5) Contabilidade-Resposta e (11) Acesso-Desafio
- Identificador - permite que o cliente RADIUS corresponda a uma resposta RADIUS com a solicitação pendente correta (geralmente é implementado como um contador)
- Autenticador
 - ◆ Nas solicitações do cliente - valor aleatório
 - ◆ Nas respostas do servidor - função Hash MD5 de (código, ID, comprimento, solicitação Autenticação, Atributos, Segredo Compartilhado)
- Atributos - Seção onde um número arbitrário de campos de atributos pode ser enviado (por exemplo, atributos de nome de usuário e senha de usuário)



Protocolo RADIUS (1)

Exemplo - troca de RADIUS envolvendo apenas um nome de usuário e senha de usuário:



- Apenas a senha é criptografada
 - O segredo compartilhado seguido pelo Request Authenticator é colocado em um hash MD5 para criar um valor de 16 octetos que é XORed com a senha digitada pelo usuário
 - Se a senha do usuário for maior que 16 octetos, a senha será dividida em blocos de 16 octetos e cálculos MD5 adicionais serão executados

Protocolo RADIUS (2)

- O protocolo RADIUS tem um conjunto de vulnerabilidades
 - ◆ O pacote Access-Request não é autenticado.
 - ◆ Muitas implementações de cliente não criam autenticadores de solicitação suficientemente aleatórios.
 - ◆ Muitos administradores escolhem segredos compartilhados RADIUS com entropia de informações insuficiente e muitas implementações limitam o espaço de chaves secretas compartilhadas.

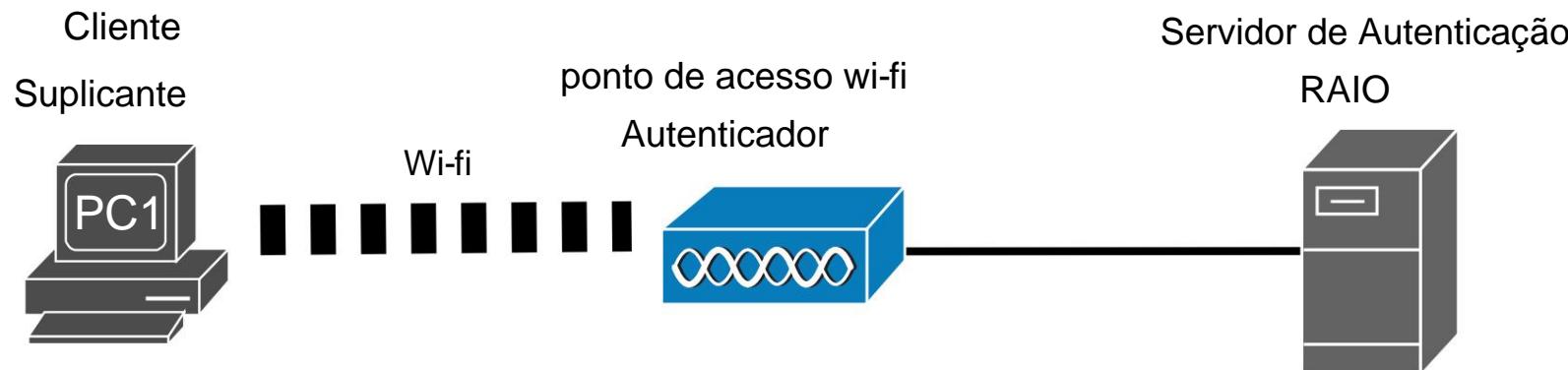
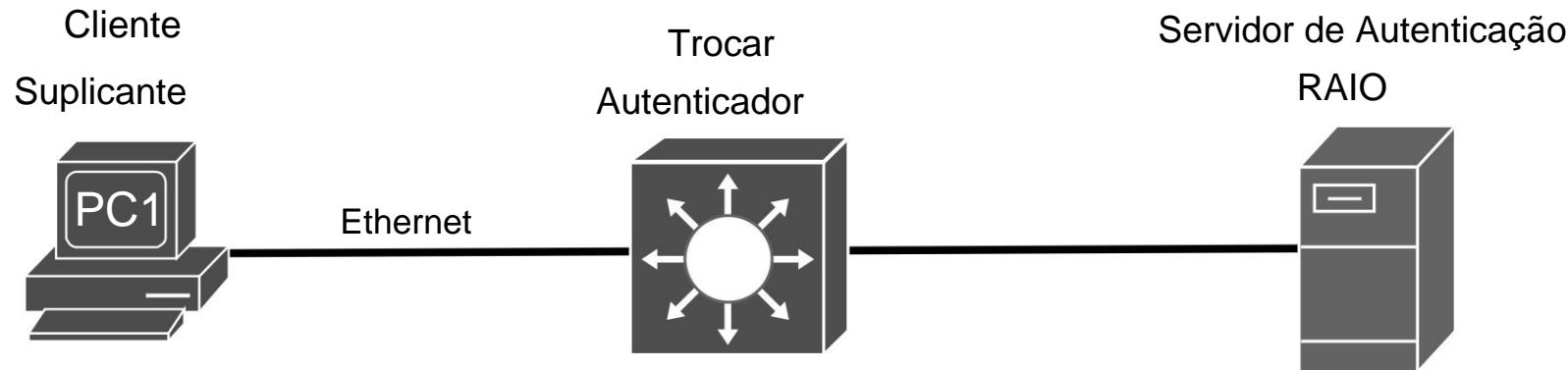


DIÂMETRO

- DIAMETER é uma estrutura mais recente no IETF para o servidor AAA de próxima geração
- Fornece uma estrutura AAA para Mobile-IP
- Não usa a mesma unidade de dados do protocolo RADIUS, mas é compatível com versões anteriores do RADIUS para facilitar a migração
- autenticação bidirecional
- Ele usa UDP mas tem um esquema que regula o fluxo de pacotes
- Os atributos de desafio/resposta podem ser protegidos usando criptografia e autenticação de ponta a ponta
- Suporta segurança de ponta a ponta



802.1X - Ethernet x WiFi



Ethernet - EAP e RADIUS

11.564981	c2:01:d1:5d:f1:00	PcsCompu_64:26:6d	EAP	60 Request, Identity
11.565227	PcsCompu_64:26:6d	Nearest-non-TPMR-bridge	EAP	60 Response, Identity
11.585255	c2:01:d1:5d:f1:00	PcsCompu_64:26:6d	EAP	60 Request, MD5-Challenge EAP (EAP-MD5-CHALLENGE)
11.585554	PcsCompu_64:26:6d	Nearest-non-TPMR-bridge	EAP	60 Response, Legacy Nak (Response Only)
11.605541	c2:01:d1:5d:f1:00	PcsCompu_64:26:6d	EAP	60 Request, Protected EAP (EAP-PEAP)
11.606107	PcsCompu_64:26:6d	Nearest-non-TPMR-bridge	TLSv1	221 Client Hello
11.625805	c2:01:d1:5d:f1:00	PcsCompu_64:26:6d	EAP	1022 Request, Protected EAP (EAP-PEAP)
11.626628	PcsCompu_64:26:6d	Nearest-non-TPMR-bridge	EAP	60 Response, Protected EAP (EAP-PEAP)
11.646176	c2:01:d1:5d:f1:00	PcsCompu_64:26:6d	TLSv1	212 Server Hello, Certificate, Server Key Exchange, Server Hello Done
11.649978	PcsCompu_64:26:6d	Nearest-non-TPMR-bridge	TLSv1	162 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
11.666300	c2:01:d1:5d:f1:00	PcsCompu_64:26:6d	TLSv1	83 Change Cipher Spec, Encrypted Handshake Message
11.666636	PcsCompu_64:26:6d	Nearest-non-TPMR-bridge	EAP	60 Response, Protected EAP (EAP-PEAP)
11.686625	c2:01:d1:5d:f1:00	PcsCompu_64:26:6d	TLSv1	61 Application Data
11.686915	PcsCompu_64:26:6d	Nearest-non-TPMR-bridge	TLSv1	98 Application Data, Application Data
11.706925	c2:01:d1:5d:f1:00	PcsCompu_64:26:6d	TLSv1	93 Application Data
11.708108	PcsCompu_64:26:6d	Nearest-non-TPMR-bridge	TLSv1	162 Application Data, Application Data
11.727323	c2:01:d1:5d:f1:00	PcsCompu_64:26:6d	TLSv1	109 Application Data
11.728248	PcsCompu_64:26:6d	Nearest-non-TPMR-bridge	TLSv1	98 Application Data, Application Data
11.747691	c2:01:d1:5d:f1:00	PcsCompu_64:26:6d	TLSv1	61 Application Data
11.748540	PcsCompu_64:26:6d	Nearest-non-TPMR-bridge	TLSv1	98 Application Data, Application Data
11.768072	c2:01:d1:5d:f1:00	PcsCompu_64:26:6d	EAP	60 Success

0.000000	10.0.0.1	10.0.0.100	RADIUS	154 Access-Request id=1
0.000594	10.0.0.100	10.0.0.1	RADIUS	122 Access-Challenge id=1
0.020271	10.0.0.1	10.0.0.100	RADIUS	165 Access-Request id=2
0.020944	10.0.0.100	10.0.0.1	RADIUS	106 Access-Challenge id=2
0.040451	10.0.0.1	10.0.0.100	RADIUS	362 Access-Request id=3
0.049097	10.0.0.100	10.0.0.1	RADIUS	1110 Access-Challenge id=3
0.060742	10.0.0.1	10.0.0.100	RADIUS	165 Access-Request id=4
0.062137	10.0.0.100	10.0.0.1	RADIUS	294 Access-Challenge id=4
0.081103	10.0.0.1	10.0.0.100	RADIUS	303 Access-Request id=5
0.081845	10.0.0.100	10.0.0.1	RADIUS	165 Access-Challenge id=5
0.101366	10.0.0.1	10.0.0.100	RADIUS	165 Access-Request id=6
0.101883	10.0.0.100	10.0.0.1	RADIUS	143 Access-Challenge id=6
0.121651	10.0.0.1	10.0.0.100	RADIUS	239 Access-Request id=7
0.122255	10.0.0.100	10.0.0.1	RADIUS	175 Access-Challenge id=7
0.141930	10.0.0.1	10.0.0.100	RADIUS	303 Access-Request id=8
0.143019	10.0.0.100	10.0.0.1	RADIUS	191 Access-Challenge id=8
0.162277	10.0.0.1	10.0.0.100	RADIUS	239 Access-Request id=9
0.163695	10.0.0.100	10.0.0.1	RADIUS	143 Access-Challenge id=9
0.182642	10.0.0.1	10.0.0.100	RADIUS	239 Access-Request id=10
0.184255	10.0.0.100	10.0.0.1	RADIUS	212 Access-Accept id=10



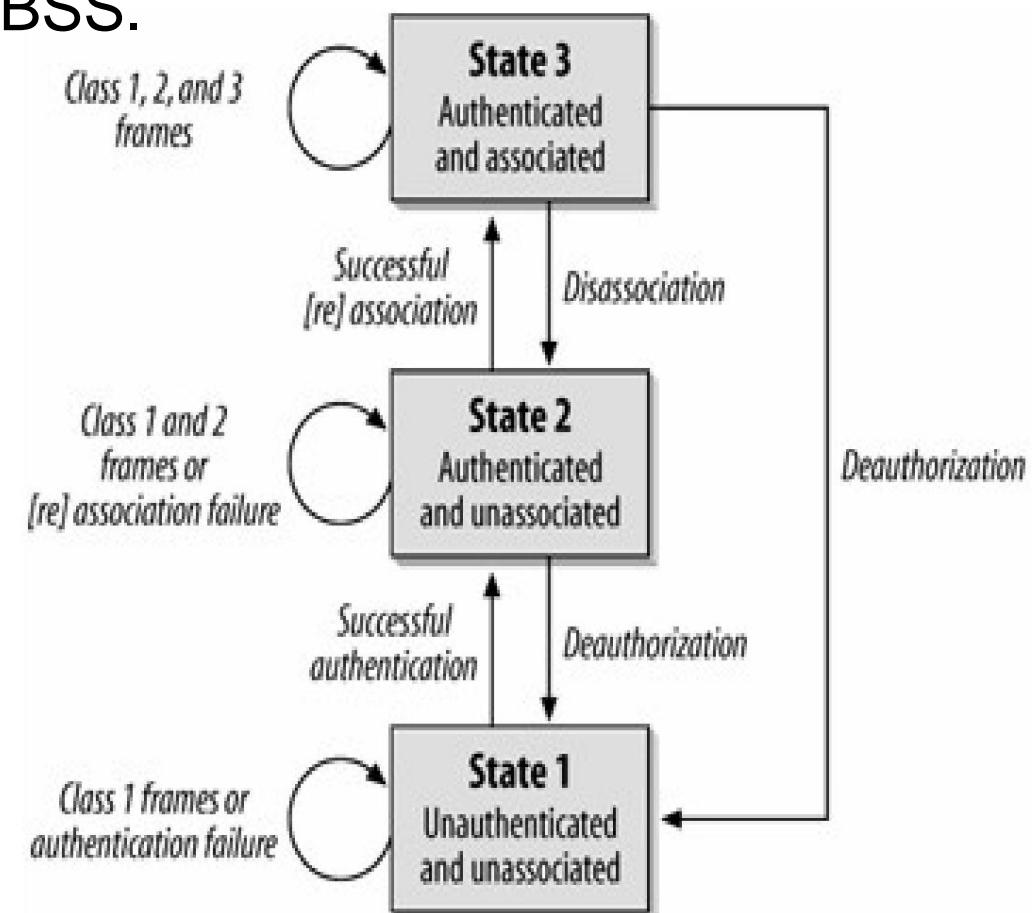
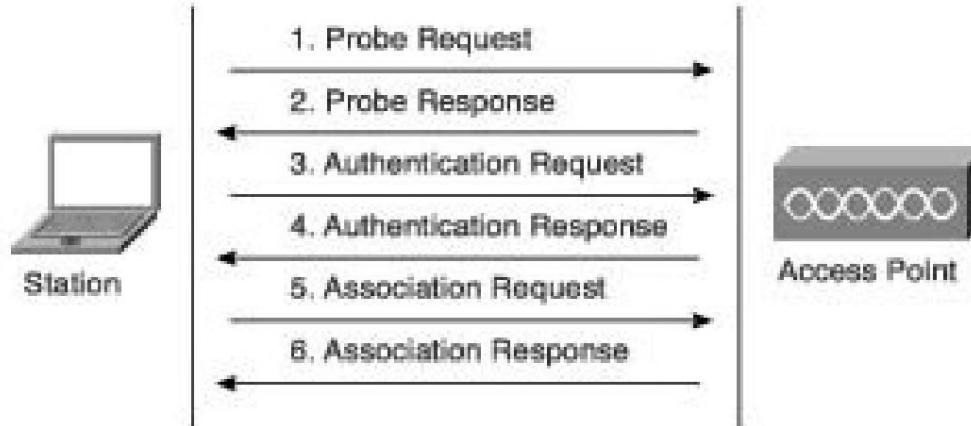
serviços IEEE 802.11

- Serviços de estação (semelhante à rede com fio)
 - ◆ Autenticação (login)
 - ◆ Desautenticação (logout)
 - ◆ Privacidade
 - ◆ entrega de dados
- serviços de distribuição
 - ◆ Associação
 - Faça conexão lógica entre o AP e a estação – o AP não receberá nenhum dado de uma estação antes da associação Reassociação
 - ◆ (semelhante à associação)
 - Envie repetidamente para o AP.
 - Ajude o AP a saber se a estação mudou de/para outro BSS.
 - Após economia de energia
 - ◆ dissociação
 - Desconecte manualmente (o PC é desligado ou o adaptador é ejetado)



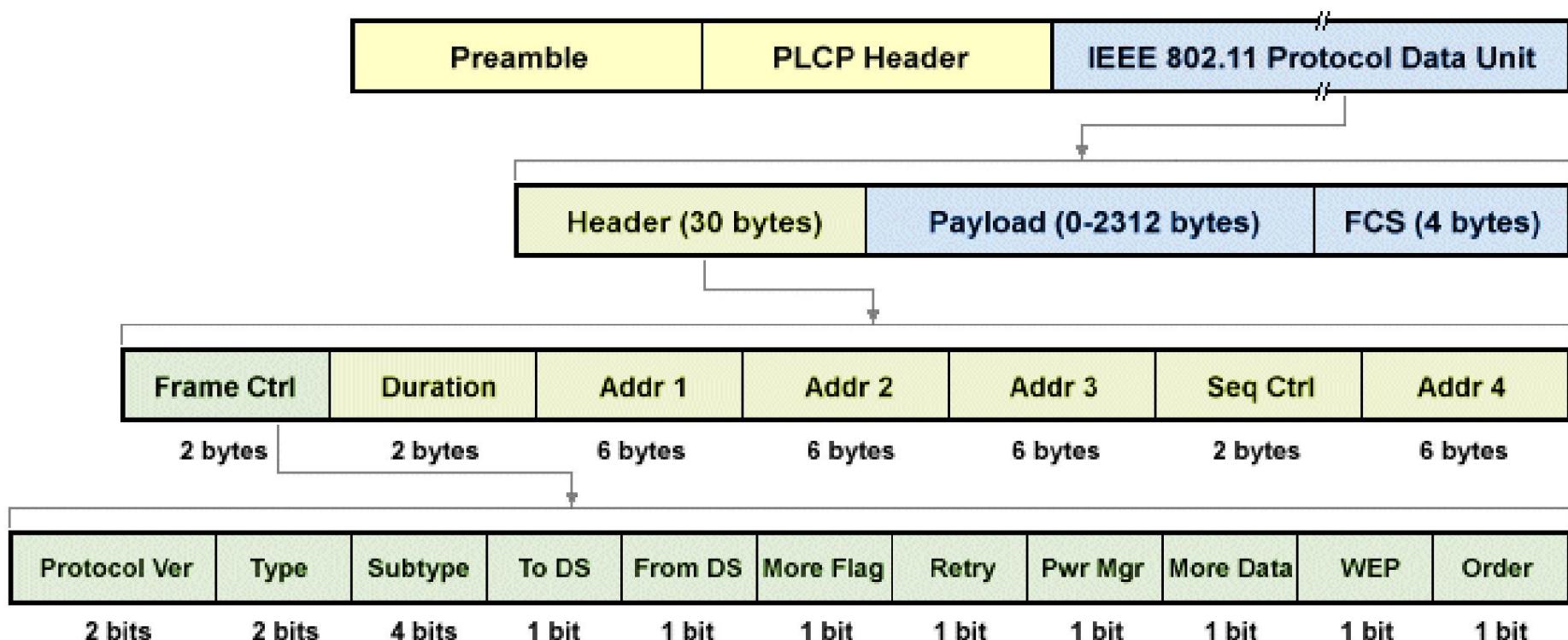
Juntando-se a um BSS

- A estação encontra BSS/AP por **varredura/sondagem**.
- BSS com AP: tanto a **Autenticação** quanto a **Associação** são necessárias para ingressar em um BSS.



Quadros WLAN

- Três tipos de molduras
 - ◆ Controle: RTS, CTS, ACK
 - ◆ Gerenciamento
 - ◆ Dados
 - O cabeçalho é diferente para os diferentes tipos de quadros.



Unindo BSS com AP: Scanning

- Uma estação que deseja ingressar em um BSS deve entrar em contato com o AP. Isso pode acontecer por
 - meio de: 1. Varredura passiva
 - ◆ A estação varre os canais em busca de um quadro Beacon que é enviado periodicamente de um AP para anunciar sua presença e fornecer o SSID e outros parâmetros para WNICs dentro
 - do intervalo 2. Varredura ativa (a estação tenta encontrar um AP)
 - ◆ A estação envia um quadro de solicitação de sondagem - Enviado de uma estação quando requer informações de outra estação Todos
 - ◆ os APs dentro do alcance respondem com um quadro de resposta de sondagem - Enviado de um AP contendo informações de capacidade, taxas de dados suportadas, etc., após receber uma solicitação de sondagem quadro



quadro de farol

- IEEE 802.11 Beacon frame, Flags:c
 - Type/Subtype: Beacon frame (0x0008)
 - › Frame Control Field: 0x8000
 - .000 0000 0000 0000 = Duration: 0 microseconds
 - Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
 - Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
 - Transmitter address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
 - Source address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
 - BSS Id: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
 - 0000 = Fragment number: 0
 - 1001 1000 1010 = Sequence number: 2442
 - Frame check sequence: 0x6f0b825c [unverified]
 - [FCS Status: Unverified]
 - IEEE 802.11 wireless LAN
 - Fixed parameters (12 bytes)
 - Timestamp: 660070796
 - Beacon Interval: 0.102400 [Seconds]
 - › Capabilities Information: 0x0421
 - Tagged parameters (123 bytes)
 - › Tag: SSID parameter set: LABCOM
 - › Tag: Supported Rates 1(B), 2(B), 5.5(B), 6, 9, 11(B), 12, 18, [Mbit/sec]
 - › Tag: DS Parameter set: Current Channel: 13
 - › Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
 - › Tag: ERP Information
 - › Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
 - › Tag: Cisco CCX1 CKIP + Device Name
 - › Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
 - › Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Unknown (1) (1)
 - › Tag: Vendor Specific: Cisco Systems, Inc.: Aironet CCX version = 5
 - › Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Unknown (11) (11)
 - › Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Client MFP Disabled



Quadros de solicitação/resposta de sondagem

- IEEE 802.11 Probe Request, Flags:

Type/Subtype: Probe Request (0x0004)
 Frame Control Field: 0x4000
 .000 0000 0000 = Duration: 0 microseconds
 Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
 Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
 Transmitter address: Microsoft_0a:43:e3 (c0:33:5e:0a:43:e3)
 Source address: Microsoft_0a:43:e3 (c0:33:5e:0a:43:e3)
 BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
 0000 = Fragment number: 0
 1100 1011 0001 = Sequence number: 3249
 Frame check sequence: 0xc7056d0a [unverified]
 [FCS Status: Unverified]

- IEEE 802.11 wireless LAN

- Tagged parameters (62 bytes)
 - › Tag: SSID parameter set: TD_WIFI_GUEST
 - › Tag: Supported Rates 1, 2, 5.5, 6, 9, 11, 12, 18, [Mbit/sec]
 - › Tag: DS Parameter set: Current Channel: 13
 - › Tag: HT Capabilities (802.11n D1.10)
 - › Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]

- IEEE 802.11 Probe Response, Flags:

Type/Subtype: Probe Response (0x0005)
 Frame Control Field: 0x5000
 .000 0001 0011 1010 = Duration: 314 microseconds
 Receiver address: IntelCor_d2:98:58 (28:b2:bd:d2:98:58)
 Destination address: IntelCor_d2:98:58 (28:b2:bd:d2:98:58)
 Transmitter address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
 Source address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
 BSS Id: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
 0000 = Fragment number: 0
 1010 0010 1001 = Sequence number: 2601
 Frame check sequence: 0x80831320 [unverified]
 [FCS Status: Unverified]

- IEEE 802.11 wireless LAN

- Fixed parameters (12 bytes)
 - › Timestamp: 664064263
 - › Beacon Interval: 0.102400 [Seconds]
 - › Capabilities Information: 0x0421
- Tagged parameters (117 bytes)
 - › Tag: SSID parameter set: LABCOM
 - › Tag: Supported Rates 1(B), 2(B), 5.5(B), 6, 9, 11(B), 12, 18, [Mbit/sec]
 - › Tag: DS Parameter set: Current Channel: 13
 - › Tag: ERP Information
 - › Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
 - › Tag: Cisco CCX1 CKIP + Device Name
 - › Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
 - › Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Unknown (1) (1)
 - › Tag: Vendor Specific: Cisco Systems, Inc.: Aironet CCX version = 5
 - › Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Unknown (11) (11)
 - › Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Client MFP Disabled



Unindo BSS com AP: Autenticação

- Uma vez que um AP é encontrado/selecionado, uma estação passa por autenticação
- Autenticação de sistema aberto (padrão, processo de 2 etapas)
 - ◆ Estação envia quadro de autenticação com sua identidade
 - ◆ AP envia quadro como um Ack/NAck
- Autenticação de chave compartilhada
 - ◆ Estações recebem chave secreta compartilhada através de canal seguro independente de 802.11
 - ◆ Após o WNIC enviar sua solicitação de autenticação inicial, ele receberá um quadro de autenticação do AP contendo um texto de desafio. O WNIC envia um quadro de autenticação contendo a versão criptografada do texto de desafio para o AP.
 - ◆ O AP garante que o texto foi criptografado com a chave correta, descriptografando-o com sua própria chave.
 - ◆ O resultado desse processo determina o status de autenticação do WNIC.



Quadros de Autenticação

- Atualmente, as redes de segurança WPA* usam "Sistema Aberto".
- A autenticação não "Sistema Aberto" foi usada para redes protegidas por WEP (não seguras e funcionalmente obsoletas).

- IEEE 802.11 Authentication, Flags:

Type/Subtype: Authentication (0x000b)

ÿ Da estação

› Frame Control Field: 0xb000

.000 0001 0011 1010 = Duration: 314 microseconds

Receiver address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)

Destination address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)

Transmitter address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)

Source address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)

BSS Id: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)

....0000 = Fragment number: 0

0001 0100 1011 = Sequence number: 331

- IEEE 802.11 Authentication, Flags:c

Type/Subtype: Authentication (0x000b)

› Frame Control Field: 0xb000

.000 0001 0011 1010 = Duration: 314 microseconds

Receiver address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)

Destination address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)

Transmitter address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)

Source address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)

BSS Id: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)

....0000 = Fragment number: 0

1010 1001 0000 = Sequence number: 2704

Frame check sequence: 0x9f8350e1 [unverified]

[FCS Status: Unverified]

- IEEE 802.11 wireless LAN

› Fixed parameters (6 bytes)

Authentication Algorithm: Open System (0)

Authentication SEQ: 0x0002

Status code: Successful (0x0000)

De AP ÿ

Juntando BSS com AP: Associação

- Depois que uma estação é autenticada, ela inicia o processo de associação, ou seja, troca de informações sobre as capacidades do AP/estação e roaming STA →
 - AP: Associate Request frame Permite
 - que o AP aloque recursos e sincronize. O quadro carrega informações sobre o WNIC, incluindo taxas de dados suportadas e o SSID da rede com a qual a estação deseja se associar.
 - AP → STA: quadro de resposta de associação
 - Aceitação ou rejeição de um pedido de associação. Se for uma aceitação, o quadro conterá informações como ID de associação e taxas de dados suportadas.
 - Novo AP informa AP antigo (se for um handover).
- Somente após a conclusão da associação, uma estação pode transmitir e receber quadros de dados.



Solicitação/Resposta da Associação

Molduras

- IEEE 802.11 Association Request, Flags:
 - Type/Subtype: Association Request (0x0000)
 - Frame Control Field: 0x0000
 - .000 0001 0011 1010 = Duration: 314 microseconds
 - Receiver address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
 - Destination address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
 - Transmitter address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)
 - Source address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)
 - BSS Id: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
 - 0000 = Fragment number: 0
 - 0001 0100 1100 = Sequence number: 332

De estação

- IEEE 802.11 wireless LAN
 - Fixed parameters (4 bytes)
 - Capabilities Information: 0x0421
 - Listen Interval: 0x000a
 - Tagged parameters (43 bytes)
 - Tag: SSID parameter set: LABCOM
 - Tag: Supported Rates 1, 2, 5.5, 11, 6, 9, 12, 18, [Mbit/sec]
 - Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
 - Tag: Extended Capabilities (8 octets)
 - Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Information E

De AP

- IEEE 802.11 Association Response, Flags:
 - Type/Subtype: Association Response (0x0001)
 - Frame Control Field: 0x1000
 - .000 0001 0011 1010 = Duration: 314 microseconds
 - Receiver address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)
 - Destination address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)
 - Transmitter address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
 - Source address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
 - BSS Id: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
 - 0000 = Fragment number: 0
 - 1010 1001 0001 = Sequence number: 2705
 - Frame check sequence: 0xe7103b15 [unverified]
 - [FCS Status: Unverified]
- IEEE 802.11 wireless LAN
 - Fixed parameters (6 bytes)
 - Capabilities Information: 0x0421
 - Status code: Successful (0x0000)
 - ..00 0000 0000 0001 = Association ID: 0x0001
 - Tagged parameters (42 bytes)
 - Tag: Supported Rates 1(B), 2(B), 5.5(B), 6, 9, 11(B), 12, 18, [Mbit/sec]
 - Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
 - Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element

Quadro de dados

- IEEE 802.11 QoS Data, Flags: .p.....TC

Type/Subtype: QoS Data (0x0028)

› Frame Control Field: 0x8841

.000 0001 0011 1010 = Duration: 314 microseconds

Receiver address: Cisco_61:ee:d1 (00:1c:f6:61:ee:d1)

ÿ Nó que receberá o quadro (AP) ÿ

Transmitter address: IntelCor_e8:14:53 (b8:8a:60:e8:14:53)

Nó que envia o quadro ÿ

Destination address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)

Estação que receberá os

Source address: IntelCor_e8:14:53 (b8:8a:60:e8:14:53)

dados ÿ Estação que enviou os dados

BSS Id: Cisco_61:ee:d1 (00:1c:f6:61:ee:d1)

STA address: IntelCor_e8:14:53 (b8:8a:60:e8:14:53)

.... 0000 = Fragment number: 0

0000 0000 0011 = Sequence number: 3

Frame check sequence: 0xc72771e8 [unverified]

[FCS Status: Unverified]

› Qos Control: 0x0000

› CCMP parameters

- Data (1244 bytes)

Data: f8002648417037bc923106ead1717d4821fde0989beb08b1...

[Length: 1244]

- Estação “IntelCor*” enviando dados para estação “D-LinkIn*” (via AP).
- Quadro capturado entre a estação “IntelCor*” e o AP (“Cisco*”).



WPA e 802.11i (WPA2)

- IEEE 802.11i - Grupo de tarefas IEEE 802.11 “Aprimoramento MAC para segurança sem fio”.
- Wi-Fi Protected Access (WiFi Alliance), WPA, é um subconjunto interno em 802.11i.
 - ◆ Compatível com trabalhos desenvolvidos em 802.11i.
 - ◆ Suporta apenas BSS.
 - ◆ Definido para trabalhar em equipamentos reais.
 - ➡ Apenas atualização de firmware.
 - ◆ Frase secreta constante e compartilhada, mas as chaves são geradas por sessão.
 - ◆ Usado no AP e na estação.
- WPA tem dois componentes distintos.
 - ◆ Autenticação, baseada em 802.1X.
 - ◆ Cifragem baseada em TKIP (Temporal Key Integrity Protocol).



WPA

- Autenticação

- ◆ 802.1X (às 802.11x) – definido para sessões com e sem fio, como um protocolo de transporte EAP (Extensible
 - ➡ Authentication Protocol) – como um wrapper para o tráfego de autenticação específico

- ➡ Impacto do EAP

- A autenticação não atravessa o AP (STA - servidor)
 - É possível usar diferentes métodos de autenticação sem alterar os APs

- ◆ Define também uma chave pré-compartilhada (PSK)
 - ➡ Para redes locais

- Temporal Key Integrity Protocol (TKIP) – solução interna com melhor proteção, para equipamentos reais

- ◆ Maior privacidade
 - ➡ Usa a mesma cifra, mas agora associada ao MAC e um IV maior
 - ➡ “Key rollover” com validade temporal
- ◆ Maior integridade
 - ➡ Chave separada por integridade



802.11i (WPA2)

- Melhor que WPA
 - ◆ Também inclui TKIP
 - ◆ Autenticação IBSS (modo ad-hoc)?
 - ◆ Protocolo RSN (Robust Security Network)
 - Autenticação e cifragem entre APs e estações Suporta
 - novos protocolos de cifragem, recorrendo a 802.1x e EAP
 - Suporta problemas de cifragem AES (Advanced
- Encryption Standard)
 - ◆ Não cifra quadros de controle e gerenciamento
 - (desassociar, potência de saída, etc).
 - ◆ Requer novo hardware



Troca de chaves WPA* (EAP fase 2)

- Feito durante o processo de Associação.
 - ◆ Depois de quadros de solicitação/resposta de associação.
 - ◆ Usa quadros de dados (QoS)

```

205 595.669409767 IntelCor_e8:14:53 Cisco_61:ee:d1 802.11 110 Association Request, SN=38, FN=0, Flags=....., SSID=LABCOM_SEC
206 595.671214291 Cisco_61:ee:d1 IntelCor_e8:14:53 802.11 128 Association Response, SN=14, FN=0, Flags=.....
207 595.673042781 Cisco_61:ee:d1 IntelCor_e8:14:53 EAPOL 211 Key (Message 1 of 4)
208 595.678333124 IntelCor_e8:14:53 Cisco_61:ee:d1 EAPOL 168 Key (Message 2 of 4)
209 595.681795313 Cisco_61:ee:d1 IntelCor_e8:14:53 EAPOL 269 Key (Message 3 of 4)
210 595.683690439 IntelCor_e8:14:53 Cisco_61:ee:d1 EAPOL 146 Key (Message 4 of 4)

```

Frame 207: 211 bytes on wire (1688 bits), 211 bytes captured (1688 bits) on interface 0

Radiotap Header v0, Length 56

802.11 radio information

IEEE 802.11 QoS Data, Flags:F.

Type/Subtype: QoS Data (0x0028)

Frame Control Field: 0x8802

.000 0001 0011 1010 = Duration: 314 microseconds

Receiver address: IntelCor_e8:14:53 (b8:8a:60:e8:14:53)

Transmitter address: Cisco_61:ee:d1 (00:1c:f6:61:ee:d1)

Destination address: IntelCor_e8:14:53 (b8:8a:60:e8:14:53)

Source address: Cisco_61:ee:d1 (00:1c:f6:61:ee:d1)

BSS Id: Cisco_61:ee:d1 (00:1c:f6:61:ee:d1)

STA address: IntelCor_e8:14:53 (b8:8a:60:e8:14:53)

.... 0000 = Fragment number: 0

0000 0001 1100 = Sequence number: 28

Qos Control: 0x0007

Logical-Link Control

802.1X Authentication

Version: 802.1X-2004 (2)

Type: Key (3)

Length: 117

Key Descriptor Type: EAPOL RSN Key (2)

[Message number: 1]

Key Information: 0x008a

Key Length: 16

Replay Counter: 1

WPA Key Nonce: 4f65d0b4e9e77b88f2cbb135749eefb105a3aa1ef65de66a8...

Key IV: 00000000000000000000000000000000

WPA Key RSC: 0000000000000000

WPA Key ID: 0000000000000000

WPA Key MIC: 00000000000000000000000000000000

WPA Key Data Length: 22

WPA Key Data: dd14000fac046616ebb59b83e8cc1816ced0e542a935



Controle de Fluxo de Rede

**Segurança em Redes de Comunicações
Mestrado em Cibersegurança**

**Mestrado em Engenharia de Computadores e
telemática**

DETI-UA



Sistemas de segurança de rede

- Firewall
- Sistema de Prevenção de Intrusão (IPS)
 - ◆ Executa inspeção profunda de pacotes
- Sistemas de Detecção de Intrusão (IDS)
 - ◆ Executa inspeção de pacotes profundos (DPI) e de pacotes rasos (SPI)
- Dispositivo de segurança
 - ◆ Segurança de comunicações unificadas
 - ◆ serviços de firewall
 - ◆ Defesa contra ameaças em tempo real
 - ◆ Acesso remoto seguro
 - ◆ Serviços de comunicações seguras
 - ◆ segurança de conteúdo



firewalls

- Um firewall fornece um único ponto de defesa entre as redes e protege uma rede das outras É um sistema ou grupo de sistemas que impõe uma política de controle entre duas ou mais redes (controle de acesso, controle de fluxo e controle de conteúdo).
- É um gateway de rede que impõe as regras de segurança de rede.
- Minimiza vulnerabilidades locais.
- Avalia cada pacote de rede em relação às políticas de segurança de rede.
- Pode monitorar todo o tráfego de rede e alertar para qualquer tentativa de burlar a segurança ou para quaisquer padrões de uso inapropriado.
- Pode ser baseado em hardware ou software.



Firewalls Segurança/Serviços de rede

- NAT (tradução de endereço de rede).
- Autorização
 - ◆ Fluxos (filtragem de pacotes).
 - ◆ Usuários (nível de aplicação e circuito).
- Redirecionando.
 - ◆ Para máquinas específicas.
 - ◆ Proxy.
- Análise de conteúdo.
- Comunicação segura.
 - ◆ VPN site a site.
 - ◆ IPsec.
 - ◆ VPN de acesso remoto.
- Detecção e defesa de DoS e DDoS.



Tipos de Firewall

Firewalls em nível de rede (L2/L3)

- ◆ Filtragem de pacotes
- ◆ Inspeção de cabeçalhos de pacotes e filtragem de tráfego com base em
 - o endereço IP da origem e do destino, a porta e o serviço (L3) origem e os
 - endereços MAC de destino (L2)

Firewalls em nível de circuito (L4)

- ◆ Monitore o handshake TCP entre pacotes para garantir que uma sessão seja legítima
- ◆ O tráfego é filtrado com base nas regras de sessão especificadas

Firewalls em nível de aplicativo (L4+)

- ◆ Os firewalls em nível de aplicativo às vezes são chamados de proxies
- ◆ Olhando mais profundamente os dados do aplicativo
- ◆ Considere o contexto das solicitações do cliente e das respostas do aplicativo
- ◆ Tentar impor o comportamento correto do aplicativo e bloquear atividades maliciosas
- ◆ A filtragem no nível do aplicativo também pode incluir proteção contra spam e vírus e bloquear sites indesejados com base no conteúdo, e não apenas em seu endereço IP
- ◆ Tarefas lentas e que consomem recursos

Firewalls de vários níveis com estado (L*)

- ◆ Filtre pacotes no nível da rede e eles reconhecem e processam dados no nível do aplicativo
- ◆ Como eles não empregam proxies, eles têm um desempenho razoavelmente bom, mesmo realizando análises profundas de pacotes

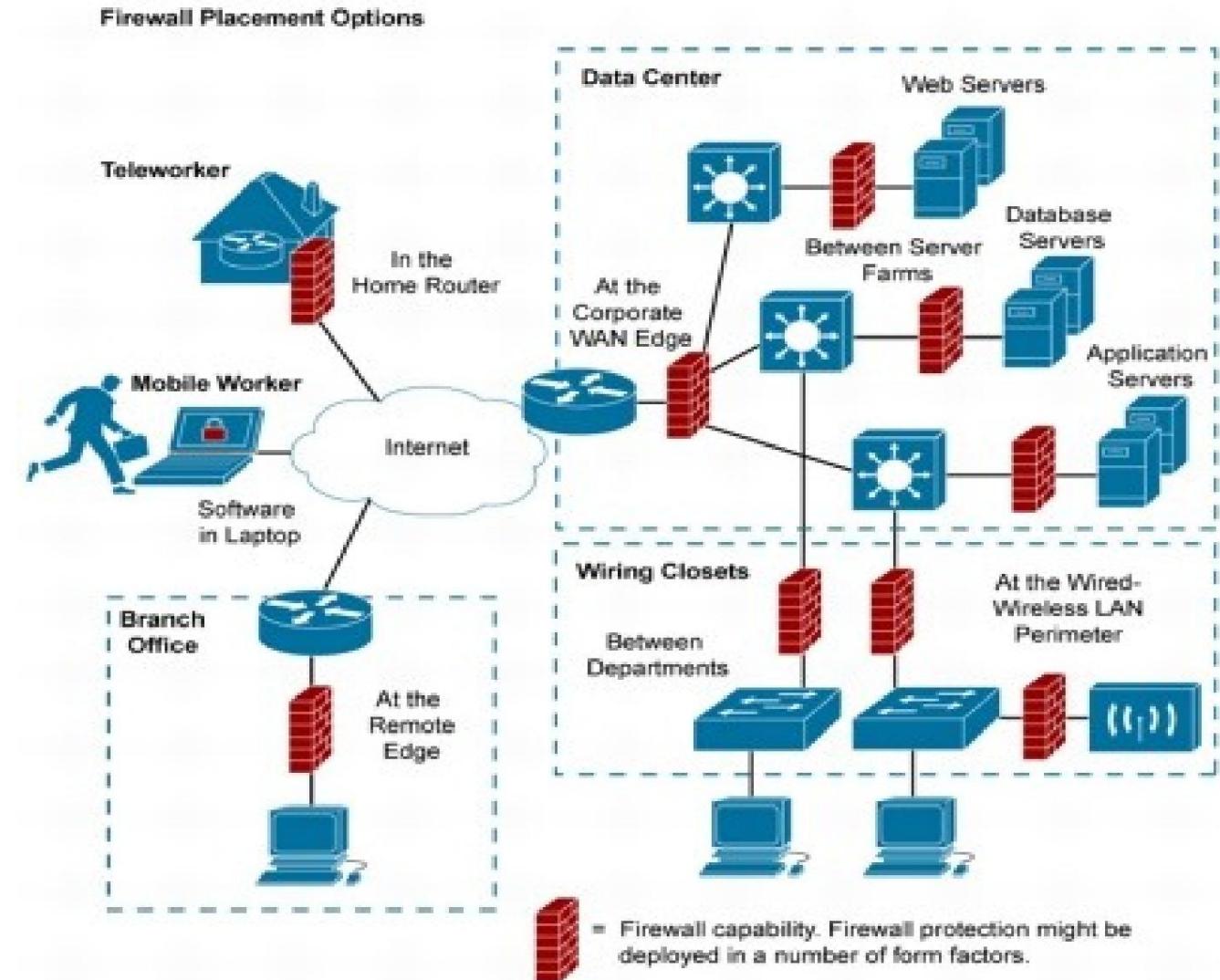
Nível de host / Firewalls pessoais

- ◆ Agir apenas dentro de um host específico
- ◆ Filtre todas as camadas de comunicação
- ◆ Controlar processos/aplicativos do sistema operacional



Implantando Firewalls

- A rede deve ser protegida em vários níveis e locais



Firewalls com estado x sem estado

• Firewalls sem estado

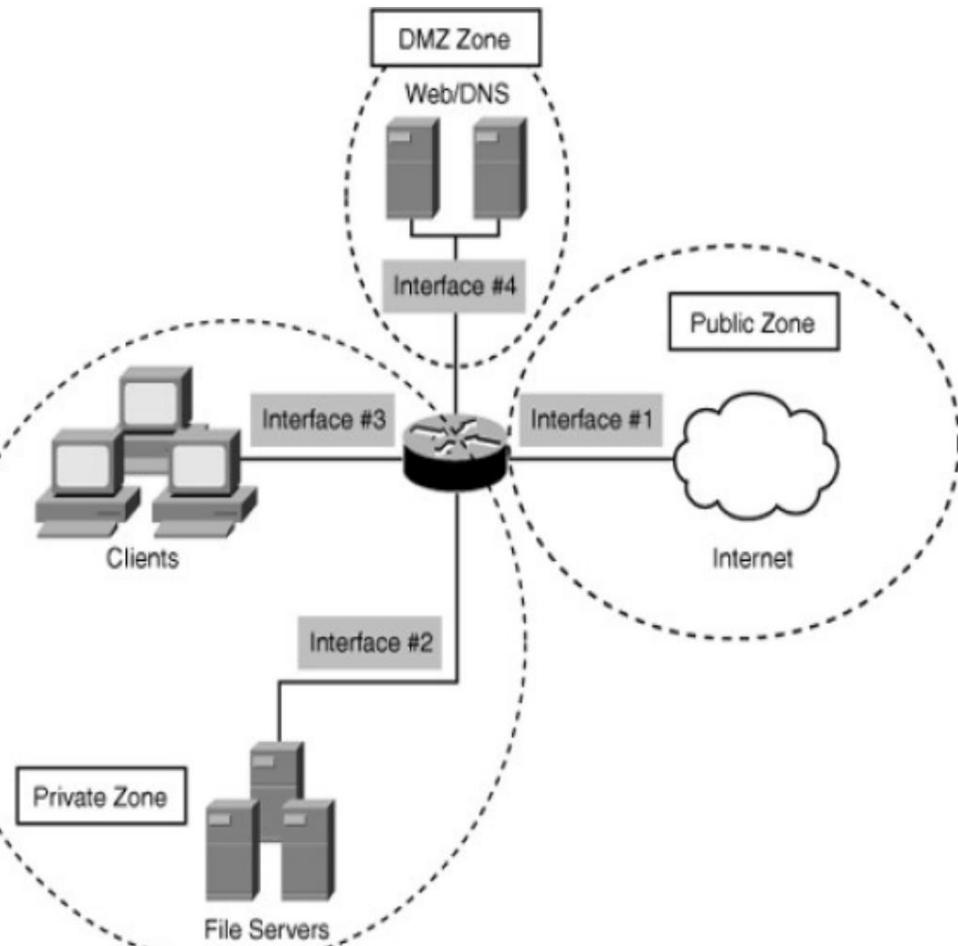
- ◆ Controla o tráfego aplicando regras a quadros/pacotes únicos Não precisa
 - ➡ rastrear fluxos/sessões de tráfego.
- ◆ Regras baseadas em valores específicos em cabeçalhos disponíveis de quadros/pacotes.
 - ➡ Conjunto de ações básicas de permissão/negação para entrada e saída com base em endereços IP, portas UDP/TCP etc.
 - ➡ Geralmente chamado de ACL (lista de acesso).
- ◆ Eles são rápidos e consomem muito poucos recursos de computação.
 - ➡ Tenha um bom desempenho sob carga de tráfego pesado.
 - ➡ Ideal para defesa contra ataques DDoS na primeira linha de defesa da rede.
 - ➡ Custo-benefício em comparação com os tipos de firewall com monitoramento de estado.

• Firewalls com estado

- ◆ Monitore todos os fluxos/sessões de tráfego.
- ◆ Controla o tráfego com base no estado da conexão de um fluxo/sessão.
 - ➡ Regras bidirecionais automáticas (regras reflexivas).
- ◆ O estado da conexão é mantido em uma tabela de estado.
 - ➡ As tabelas de estado devem ser sincronizadas com outros firewalls quando em um cenário redundante (balanceamento de carga) ou cenário de alta disponibilidade (backup em caso de falha).



Zonas/Grupo de Firewall

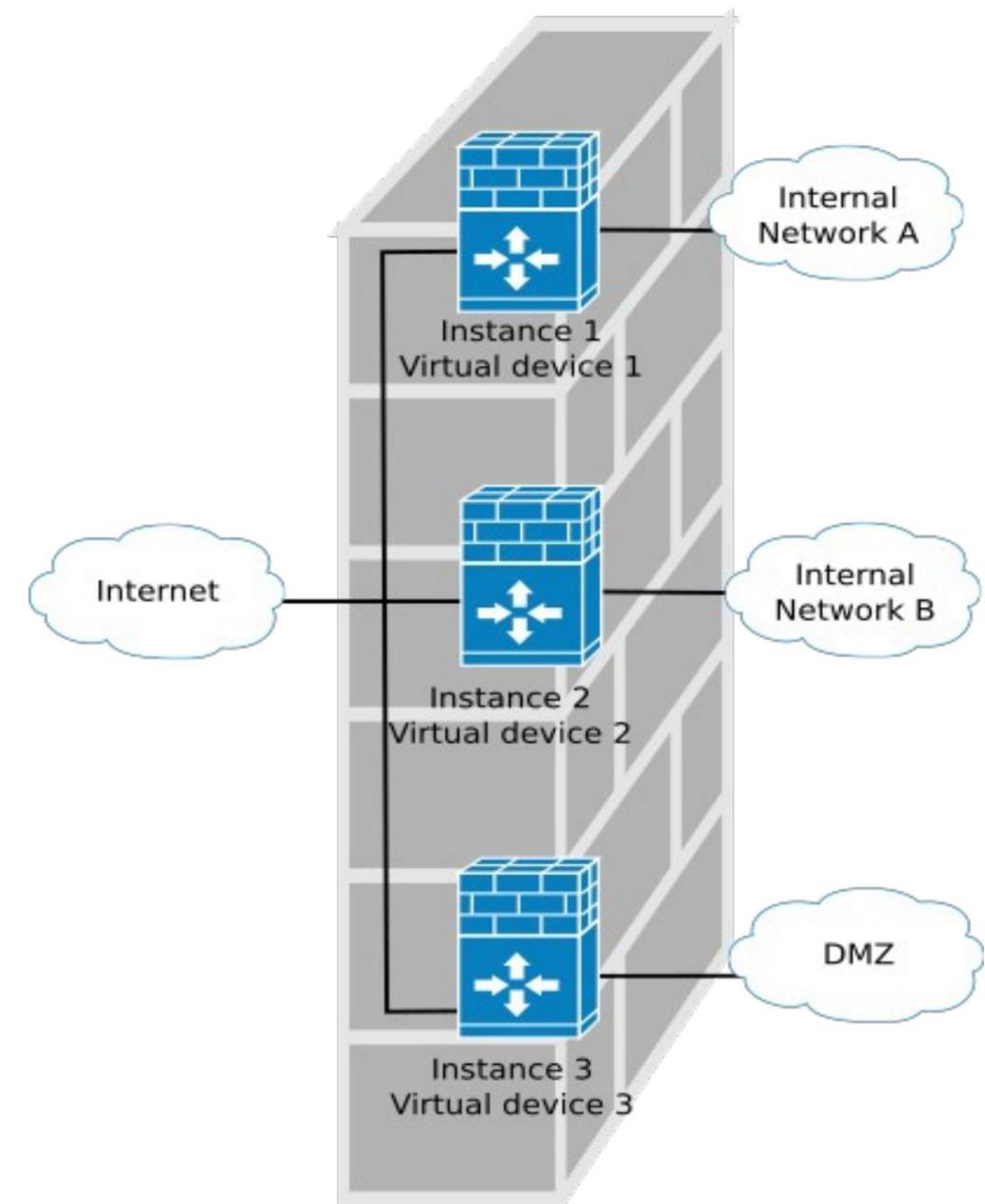


- Uma rede pode ser dividida em várias zonas/grupos com diferentes níveis de segurança.
 - ◆ Conjuntos de endereços IP, redes ou portas.
- Depois de criado, um grupo pode ser referenciado por regras de firewall como origem ou destino.
- Exemplo: uma Zona Desmilitarizada (DMZ) é uma rede perimetral fora da rede interna/privada protegida Utilizada para
 - ◆ colocar servidores/serviços públicos.
 - ◆ A DMZ é uma zona "semi-protegida".
 - ◆ Deve-se presumir que qualquer máquina colocada na DMZ está em risco.

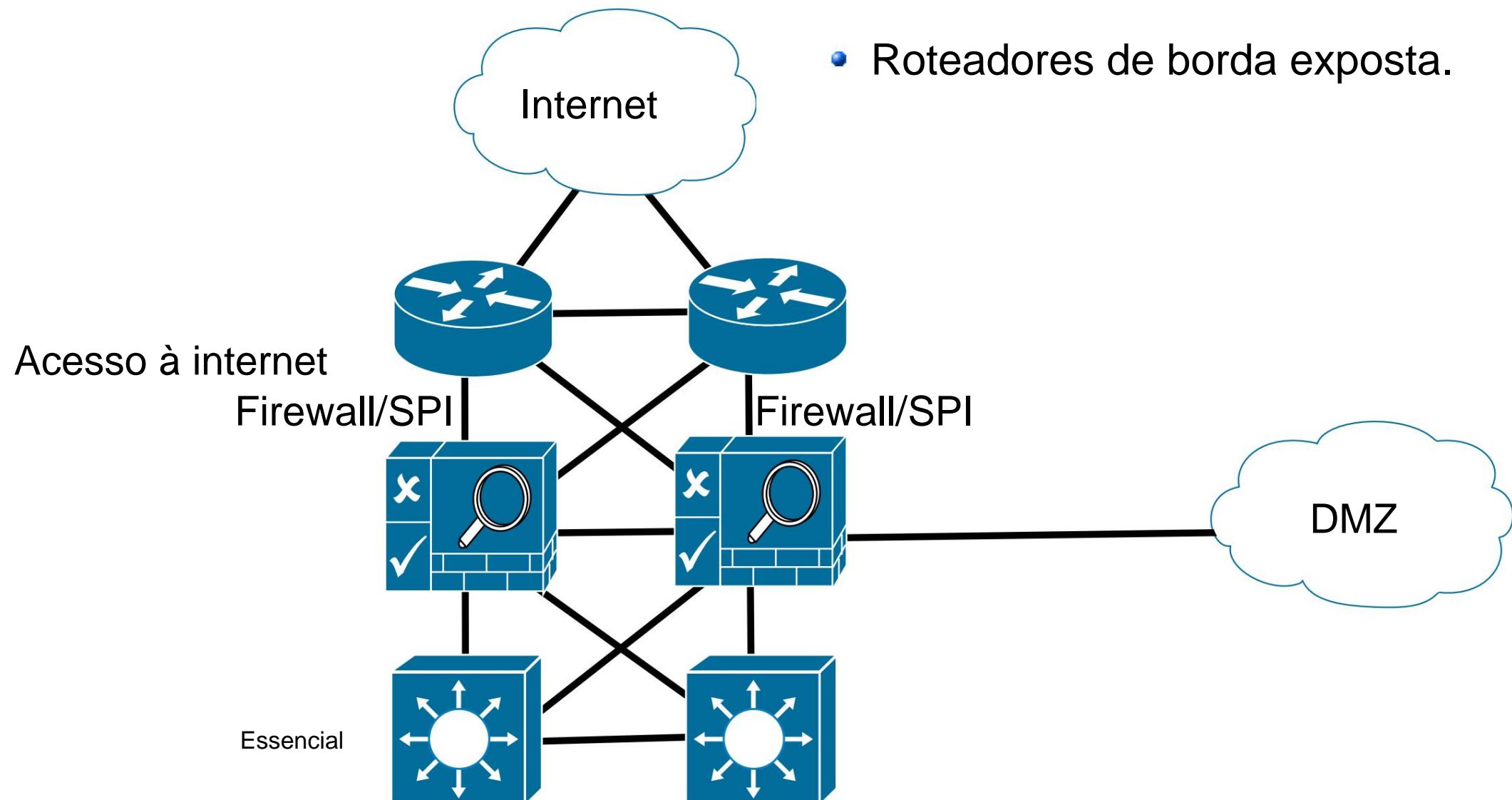


Instâncias Virtuais de Firewall

- Os firewalls podem ter instâncias isoladas (teóricas) para lidar com diferentes zonas/grupos.
- Cada instância é um dispositivo virtual que pode realizar controle de fluxo, switch e/ou roteamento.

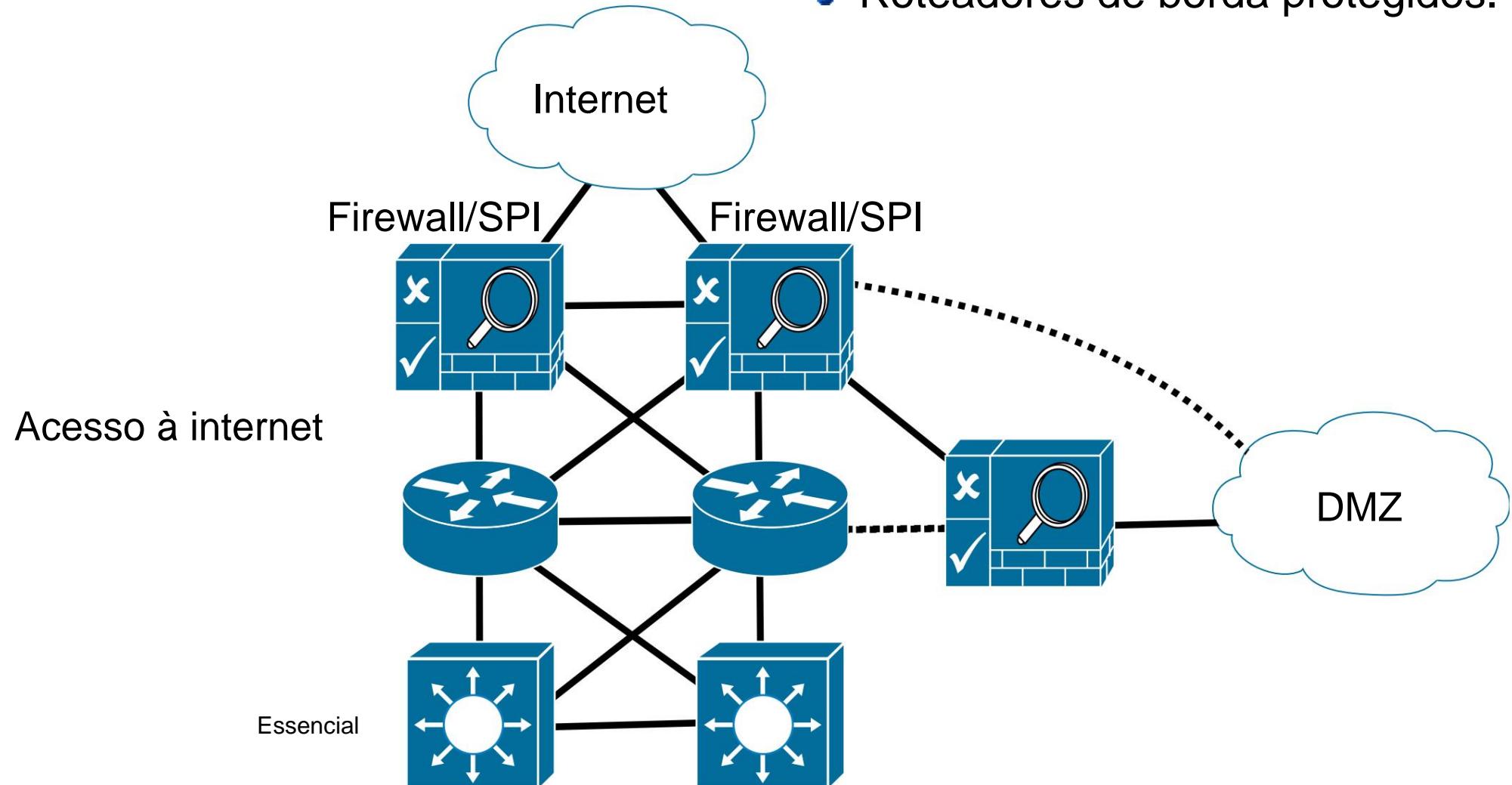


Colocação de firewall (com redundância)



Colocação de firewall (com redundância)

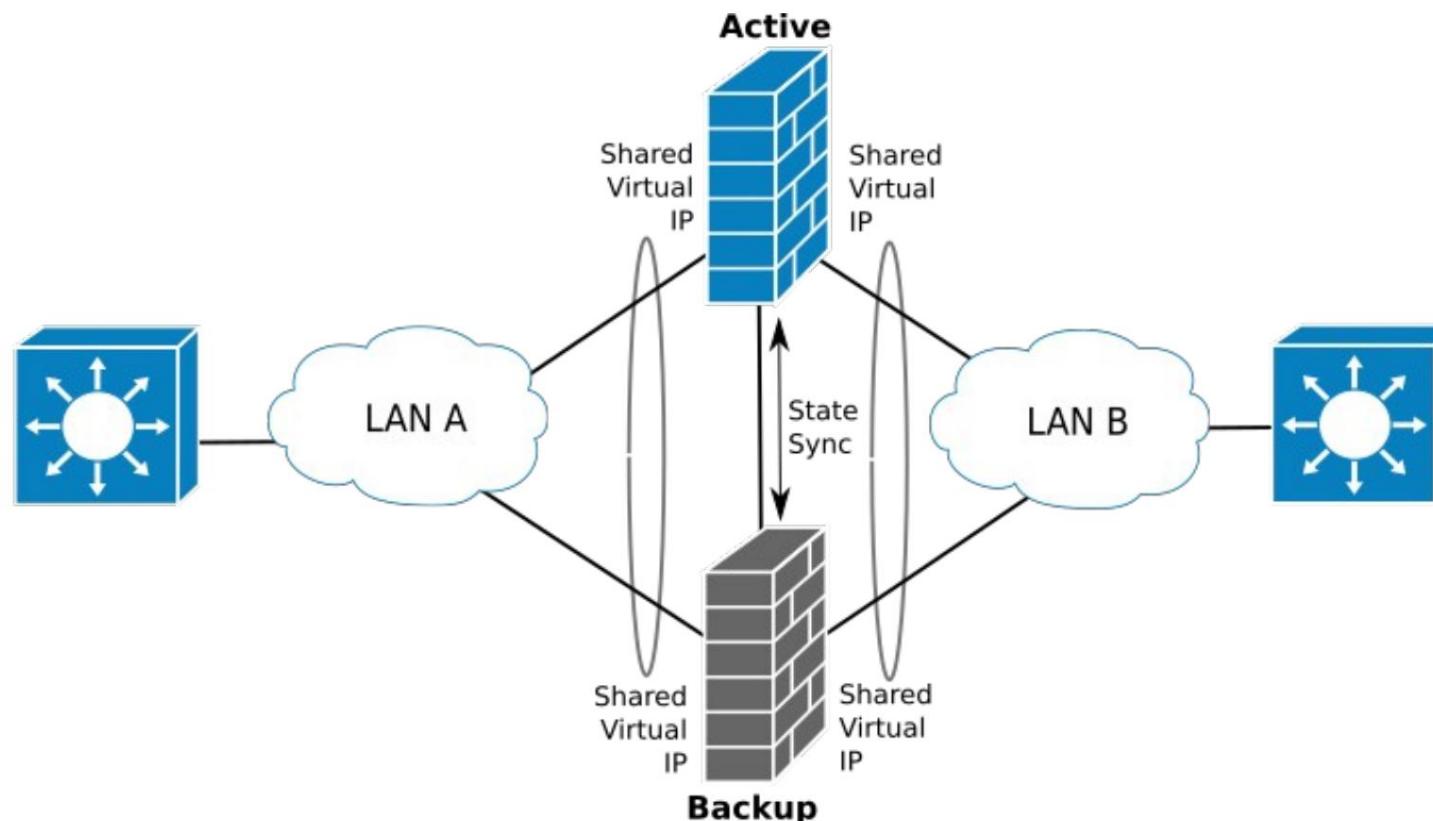
- Roteadores de borda protegidos.



Alta disponibilidade (1)

- Cenário de backup ativo

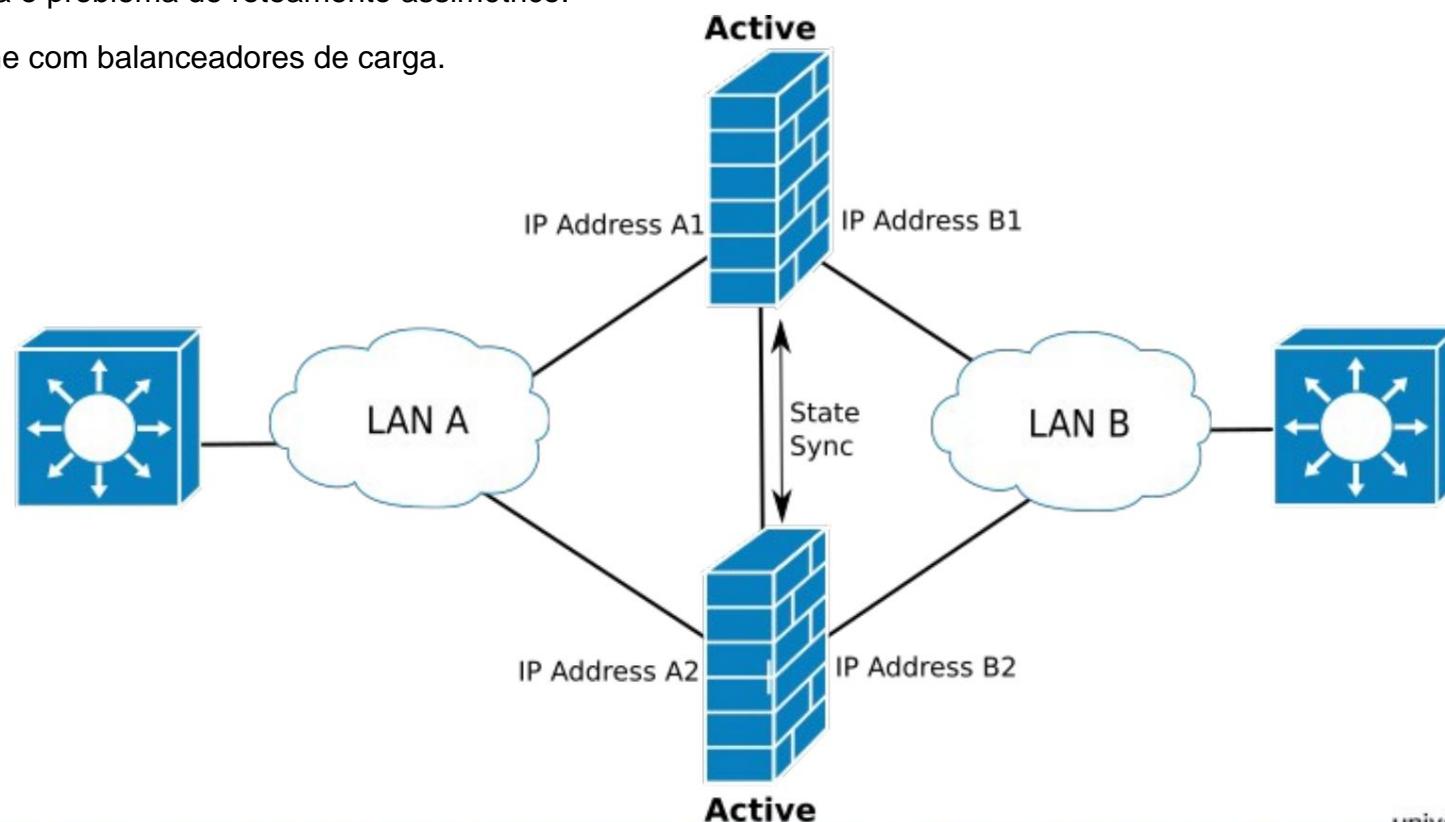
- Os firewalls compartilham o estado por meio de uma conexão dedicada
- Os firewalls compartilham endereços IP da LAN (Virtual).
- O firewall de backup assume IP e serviços em caso de falha do firewall ativo.



Alta disponibilidade (2)

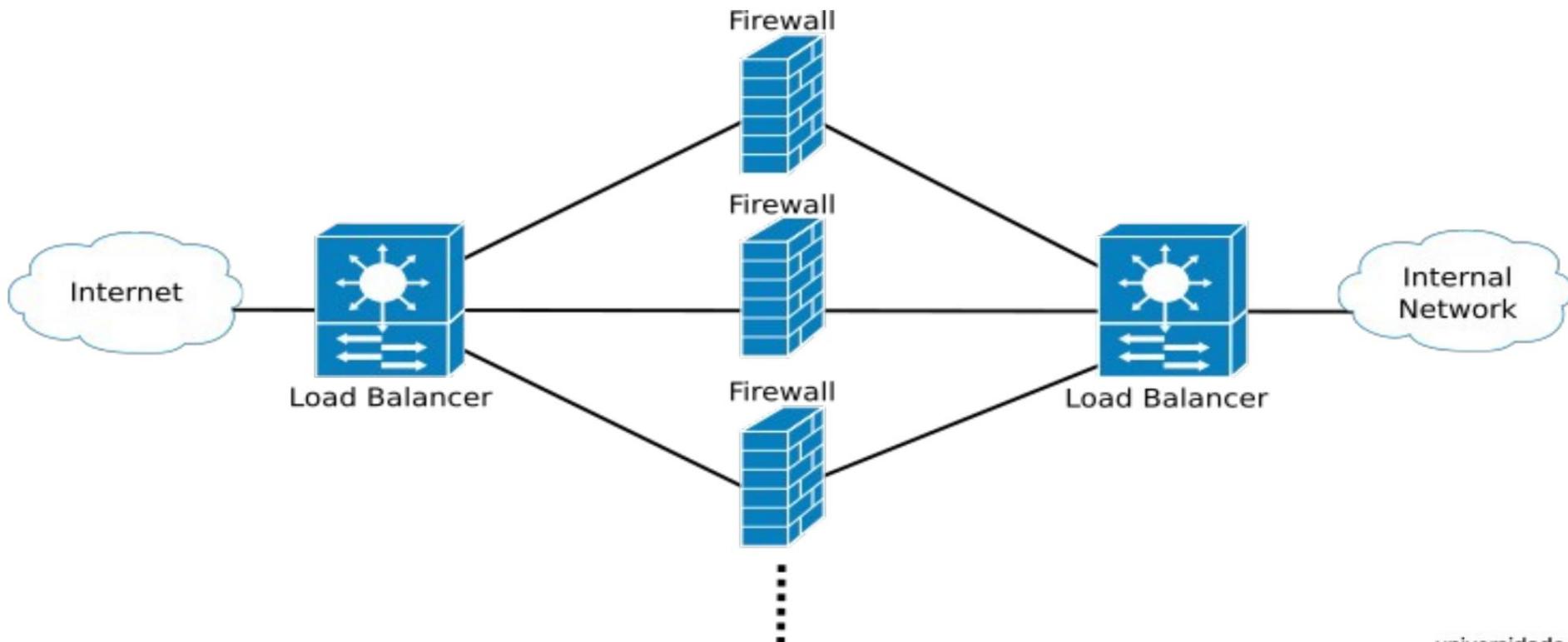
- Cenário Ativo-Ativo

- Os firewalls compartilham o estado por meio de uma conexão dedicada
- Os firewalls têm seus endereços IP.
- Ambos funcionam simultaneamente.
 - Compartilhar carga.
 - Resolva o problema de roteamento assimétrico.
 - Trabalhe com平衡adores de carga.



Carga de firewall de balanceamento de carga

- O equipamento de平衡amento de carga pode distribuir o tráfego por vários firewalls.
- Quando o balanceador de carga roteia o tráfego do mesmo fluxo SEMPRE para o mesmo firewall (depende do algoritmo LB):
 - ◆ Os firewalls não precisam compartilhar os estados das conexões!
 - ◆ Diminua os requisitos de processamento e memória de cada firewall.
 - ◆ Permite um crescimento escalável do tráfego.
 - ◆ Torna a rede menos vulnerável a ataques DoS.
 - ◆ Quando também é responsável por distribuir políticas/regras é chamado de Orquestrador.



Algoritmos de balanceamento de carga

• Hash IP

- ◆ O endereço IP (ou um conjunto de identificadores de fluxo) do cliente é usado para determinar qual servidor/firewall recebe o fluxo ou solicitação.
- ◆ Não requer sincronização de estado (FW ou LB). A saída da função hash determina o destino.

• Round Robin

- ◆ As solicitações são distribuídas sequencialmente pelo grupo de dispositivos.
- ◆ Se os firewalls não compartilharem o estado, os平衡adores de carga devem “memorizar” a interface pela qual receberam o tráfego dos firewalls e usar a mesma interface para rotear o tráfego de resposta.

• Menos Conexões

- ◆ Uma nova solicitação é enviada ao servidor/firewall com o menor número de conexões atuais.
- ◆ A capacidade de computação relativa de cada servidor/firewall é considerada para determinar qual deles tem menos conexões.

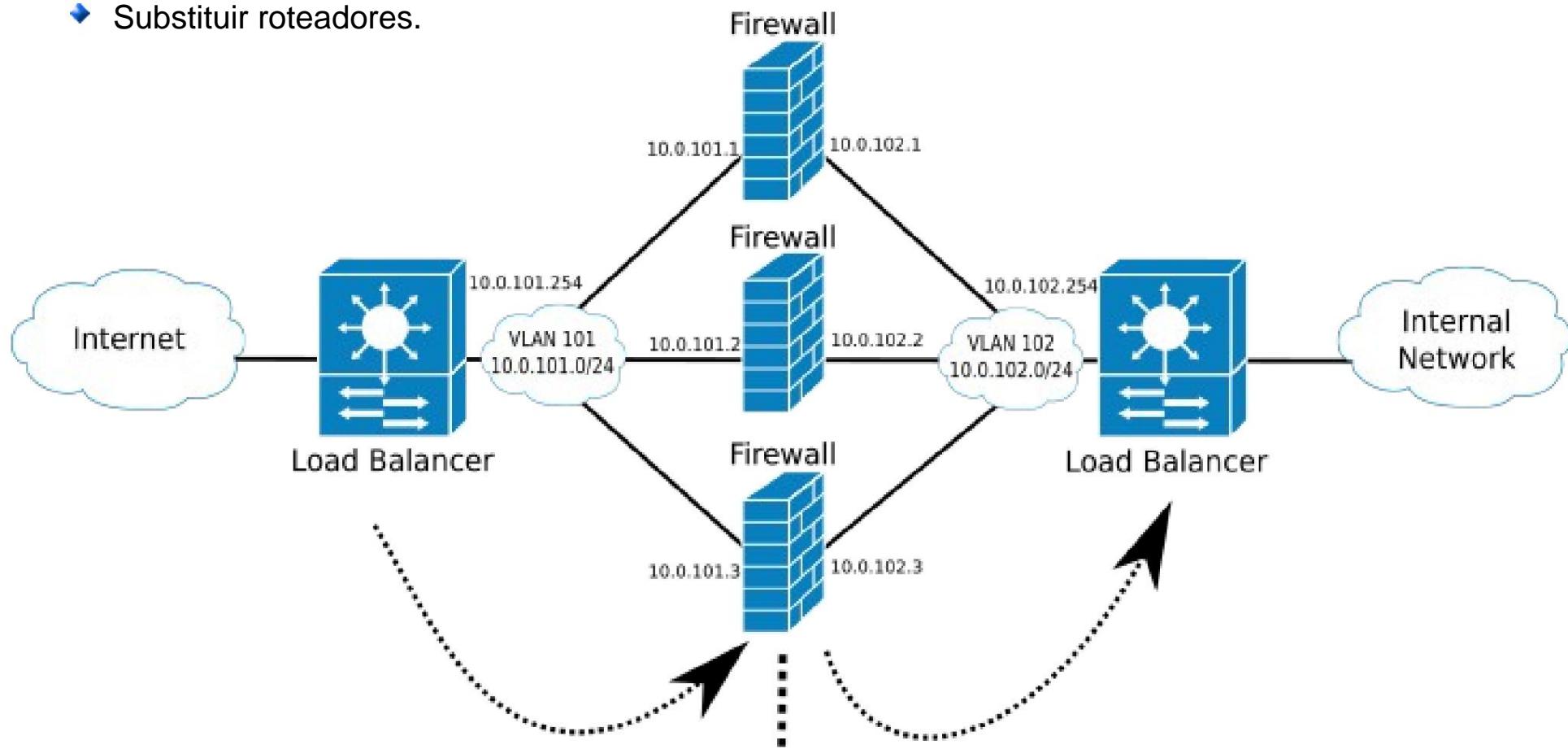
• "Inteligente"

- ◆ Com base em uma fonte externa de informações.



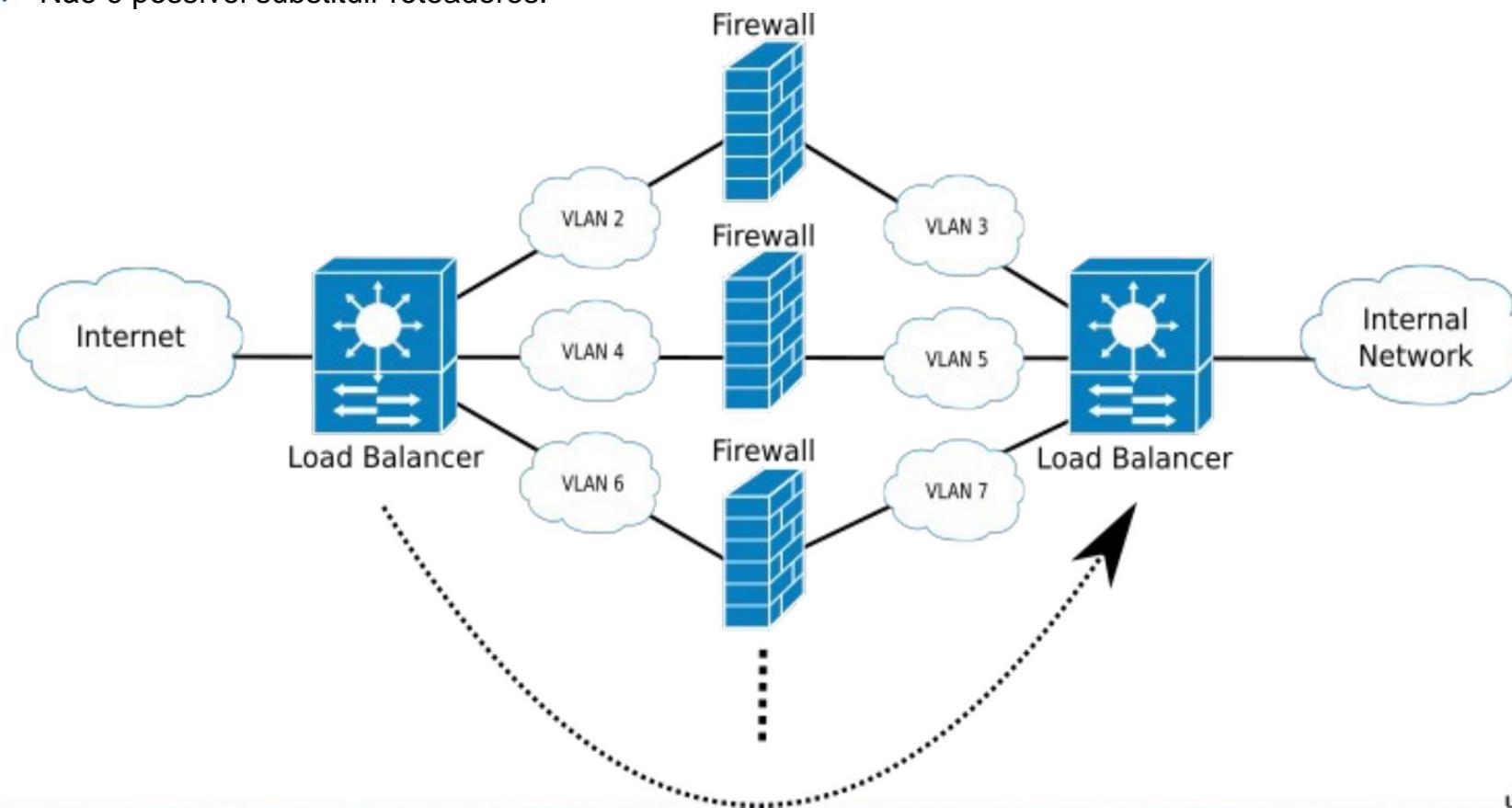
Firewalls Endereçados

- As interfaces têm endereços IP.
- Os平衡adores de carga (ou roteadores) roteiam o tráfego como um próximo salto de IP.
- Pode fornecer serviços de roteamento.
 - Substituir roteadores.



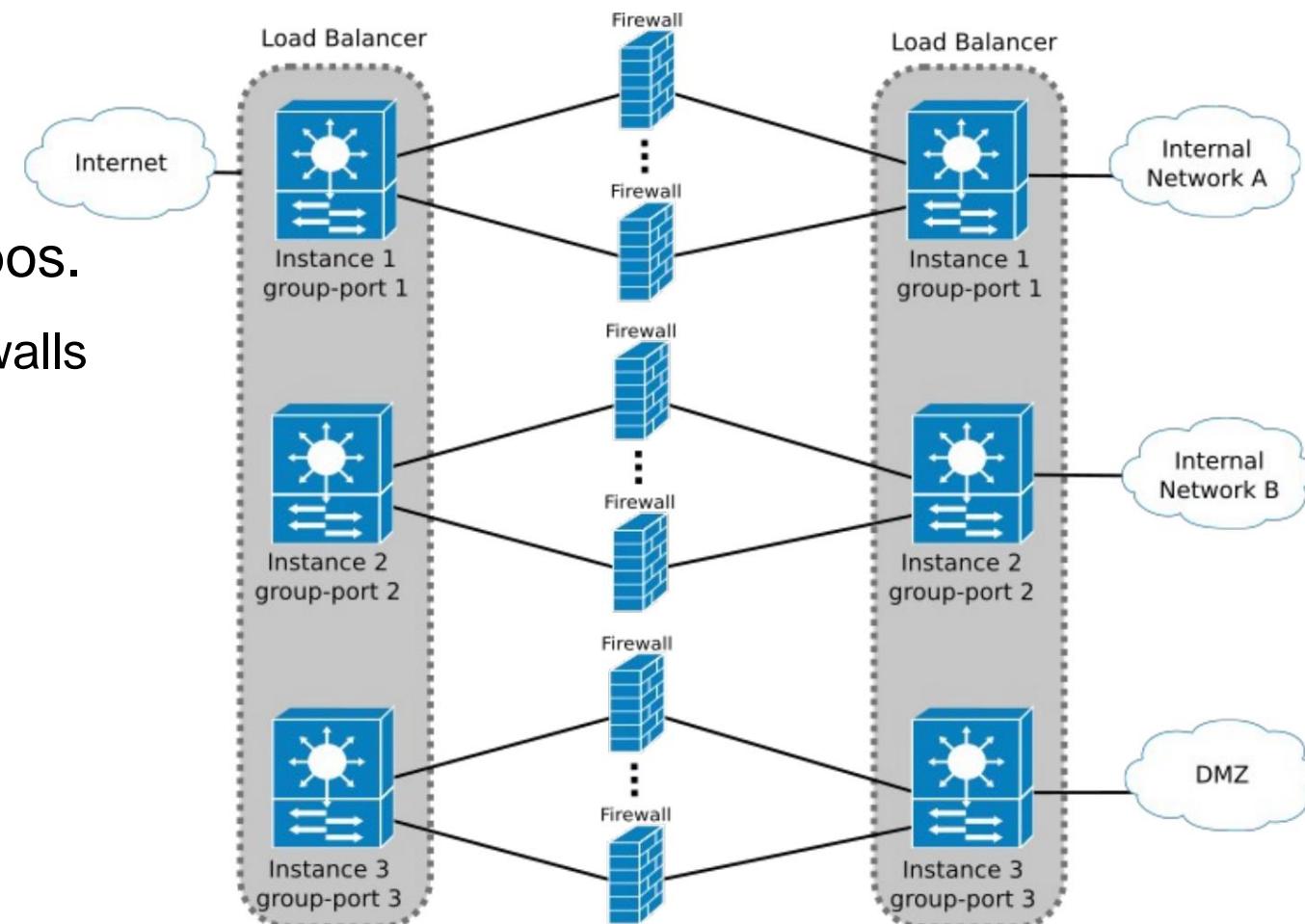
Firewalls furtivos

- As interfaces não têm endereços IP.
 - Pode ter várias regras de camada.
- Os平衡adores de carga (ou comutadores) roteiam o tráfego por interface/VLAN.
- Não pode fornecer serviços de roteamento ou NAT/PAT.
 - Não é possível substituir roteadores.



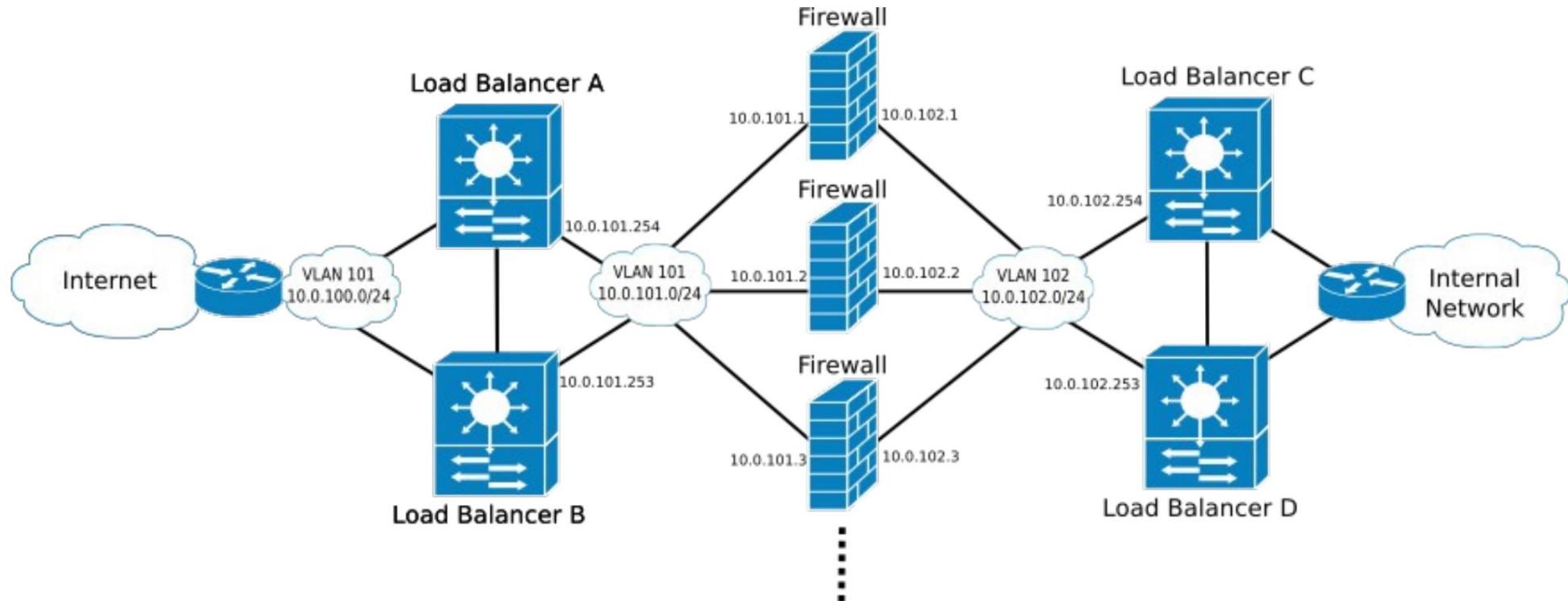
Instâncias de平衡adores de carga

- Os平衡adores de carga podem ter instâncias isoladas (teóricas) para lidar com diferentes zonas/grupos.
 - ◆ Com um conjunto de firewalls por zona/grupo.
- Partições físicas ou virtuais.
- Alguns fornecedores chamam isso de portas de grupo.



Balanceadores de carga redundantes

Firewalls Endereçados

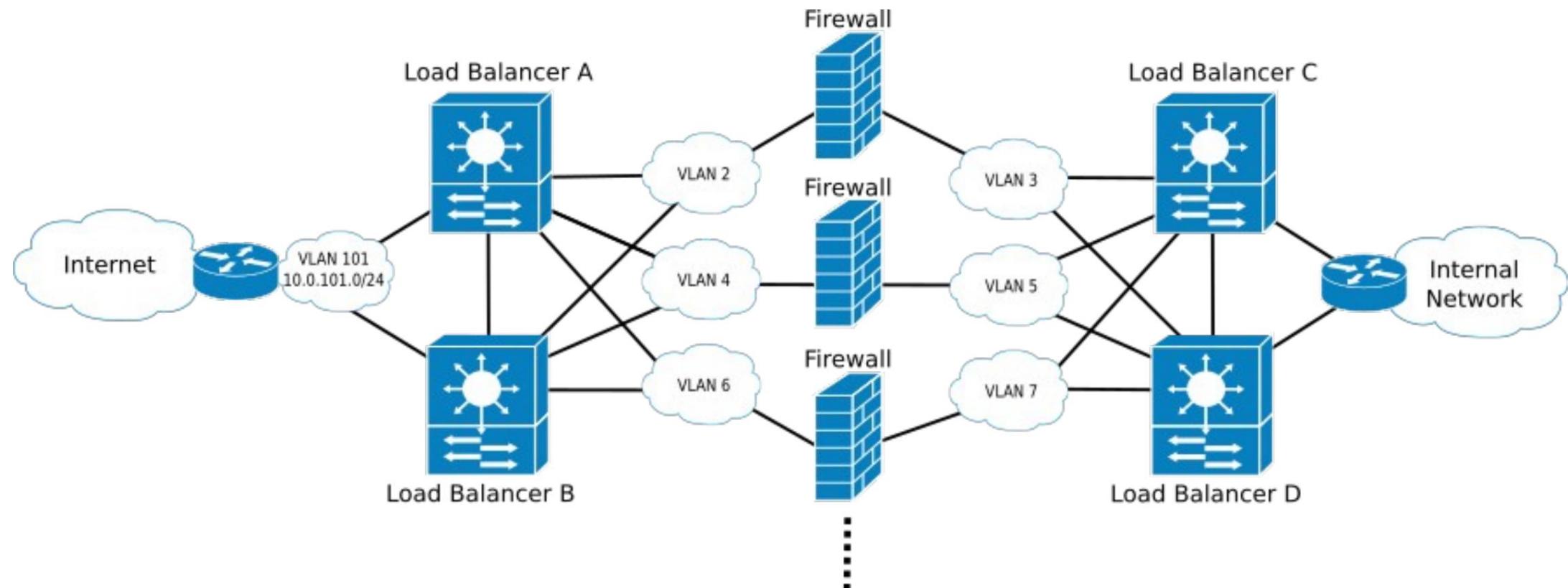


- Para evitar a sincronização do estado do FW, os balanceadores de carga devem enviar pacotes do mesmo fluxo sempre para o mesmo firewall.
 - Deve diminuir a chance de sobrecarga de memória do FW.
- Os balanceadores de carga que usam algoritmos IP Hash LB não exigem sincronização do histórico de roteamento (entre LB).
 - Usando outros algoritmos LB, eles devem compartilhar o histórico de roteamento.

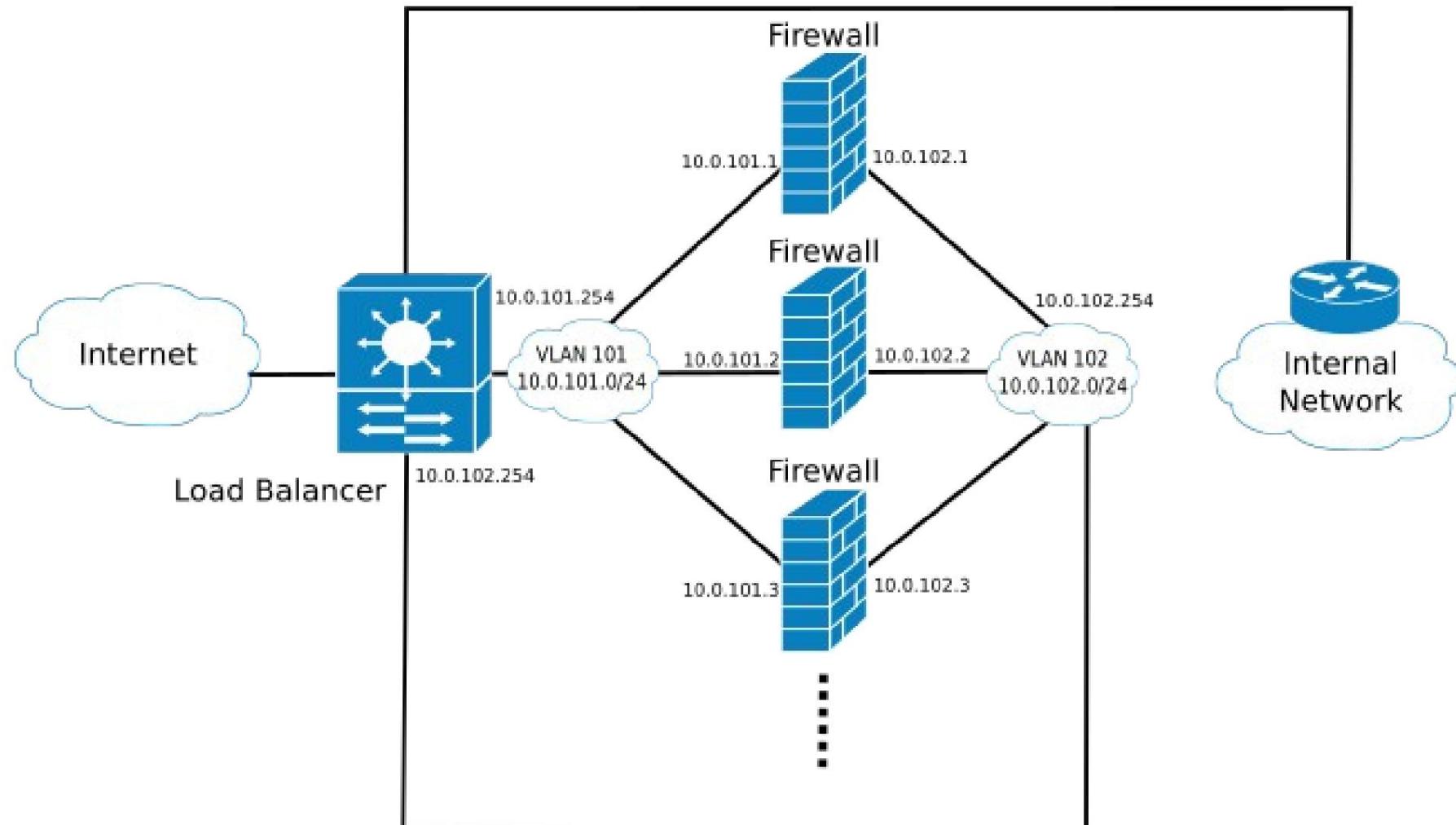


Balanceadores de carga redundantes

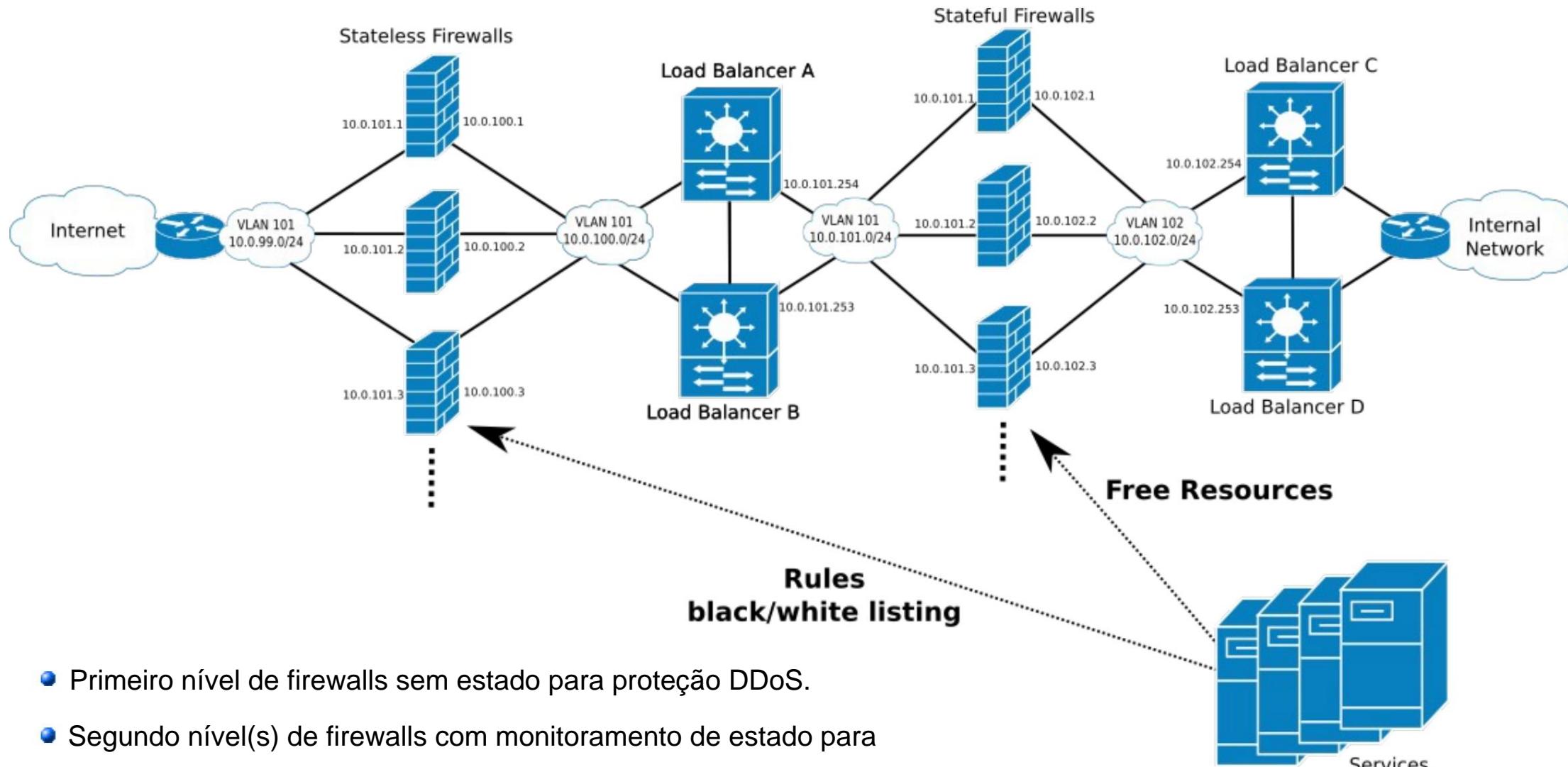
Firewalls furtivos



Balanceador de carga único



Múltiplos Níveis de Defesa



- Primeiro nível de firewalls sem estado para proteção DDoS.
- Segundo nível(s) de firewalls com monitoramento de estado para proteção geral.
- As informações dos serviços podem ser usadas para
 - ◆ liberar recursos nos firewalls com estado.
 - ◆ Para configurar regras de listas negras/brancas nos firewalls sem estado.

Regras

- As regras de firewall devem ser especificadas com base na origem, destino e tipo de tráfego.
 - ◆ Origem e destino podem ser endereços IP, portas, zonas, etc...
 - ◆ O tipo pode ser definido em termos de protocolo ou especificidades de protocolo.
- As regras podem ser especificadas com base no estado de uma conexão (requer um firewall com estado) após a observação de um pacote:
 - ◆ NOVO
 - O pacote observado está iniciando uma nova conexão ou está associado a uma conexão que não gerou pacotes em ambas as direções.
 - ◆ ESTABELECIDO
 - O pacote observado está associado a uma conexão que gerou pacotes em ambas as direções.
 - Normalmente, uma regra específica permite apenas o tráfego de uma direção, uma regra ESTABELECIDA deve ser definida para permitir dinamicamente a resposta da outra direção.
 - ◆ RELACIONADO
 - O pacote observado está iniciando uma nova conexão, mas está associado a uma conexão existente, como um erro ICMP (por exemplo, porta inacessível relacionada a uma conexão UDP)



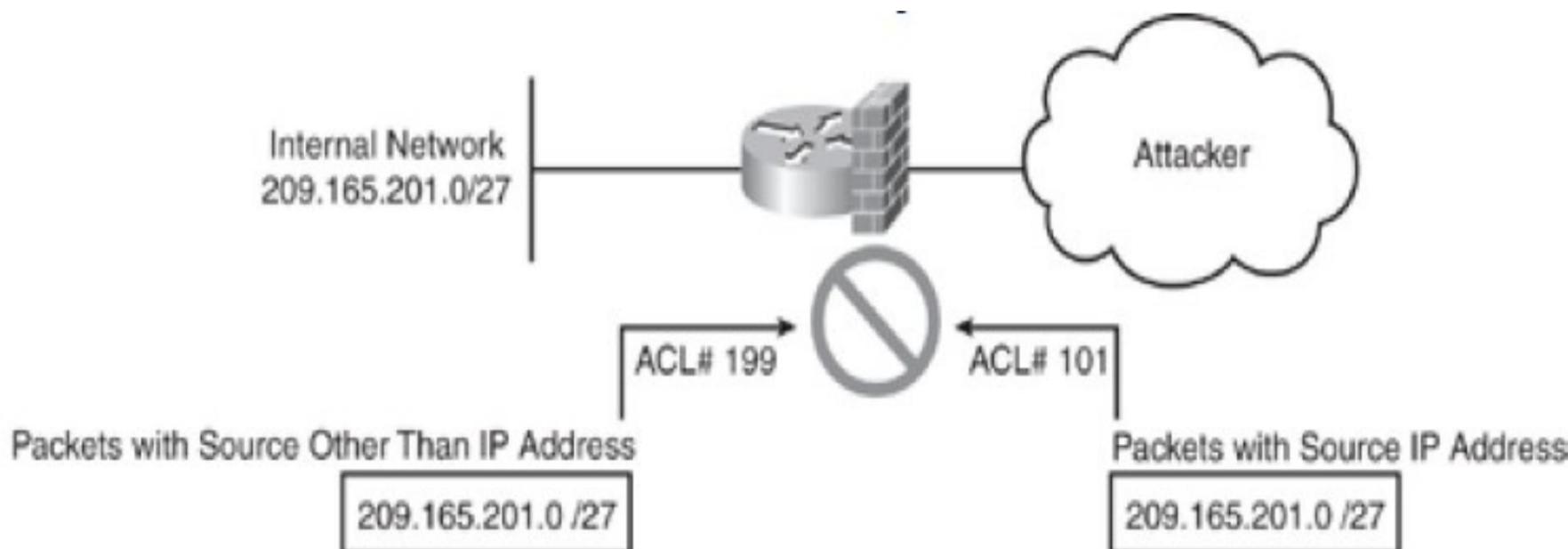
Melhores práticas e recomendações

- Padronize suas políticas de segurança.
 - ◆ Inclui firewalls, relações de zonas de rede, dispositivos e perfis de usuários, serviços ativos, etc.
- Bloqueando todo o tráfego por padrão.
 - ◆ Remova as regras “Aceitar tudo”.
- Adicione exceções "Aceitar".
 - ◆ Geralmente clientes para direção de serviço.
 - ➡ Ex: Interno para Internet, Internet para DMZ, etc...
 - ➡ Adicionar base de regra reversa em conexões estabelecidas/relacionadas.
- Manter a documentação das regras de firewall:
 - ◆ Objetivo, relação com as políticas de segurança, dispositivos e usuários afetados, datas de implantação e expiração, identificação do gerente.
- Manutenção e acompanhamento de regras.
 - ◆ Verifique periodicamente a validade das regras dentro das políticas de segurança atuais.
 - ◆ Analise as estatísticas de uso/correspondência de cada regra.
- Integre o controle de fluxo com políticas e serviços existentes de rotting, switching e balanceamento de carga.

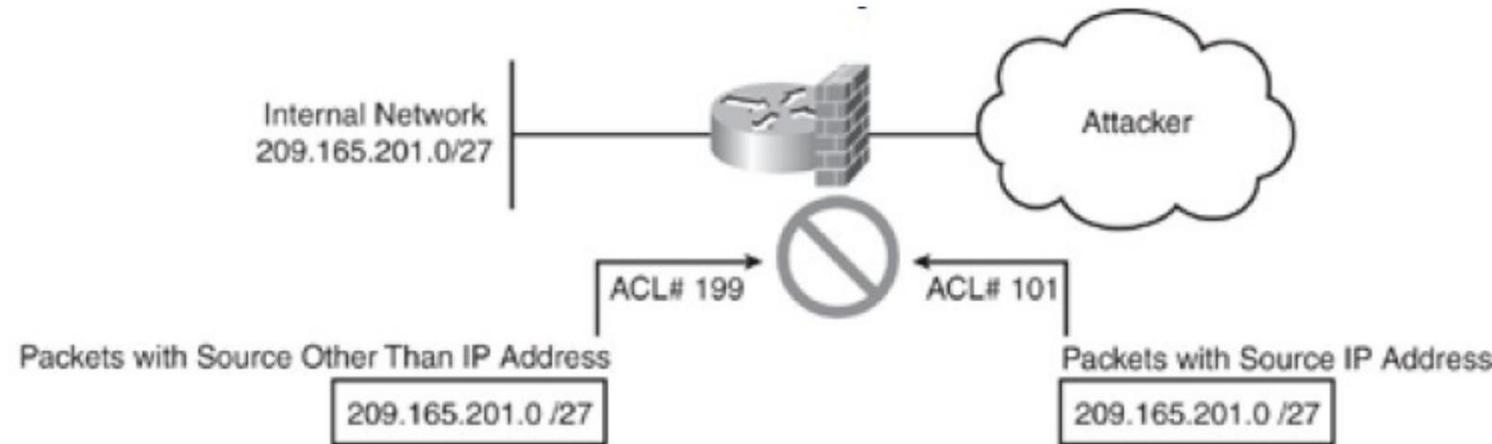


Falsificação de IP

- A falsificação de IP refere-se à criação de pacotes IP com um endereço IP de origem forjado.
 - ◆ Para ocultar a identidade do remetente ou representar outro sistema de rede.
 - ◆ A falsificação de datagramas IP é um problema bem conhecido.
 - ◆ A maioria das falsificações é feita para fins ilegítimos.



Evitando falsificação de IP na camada 3

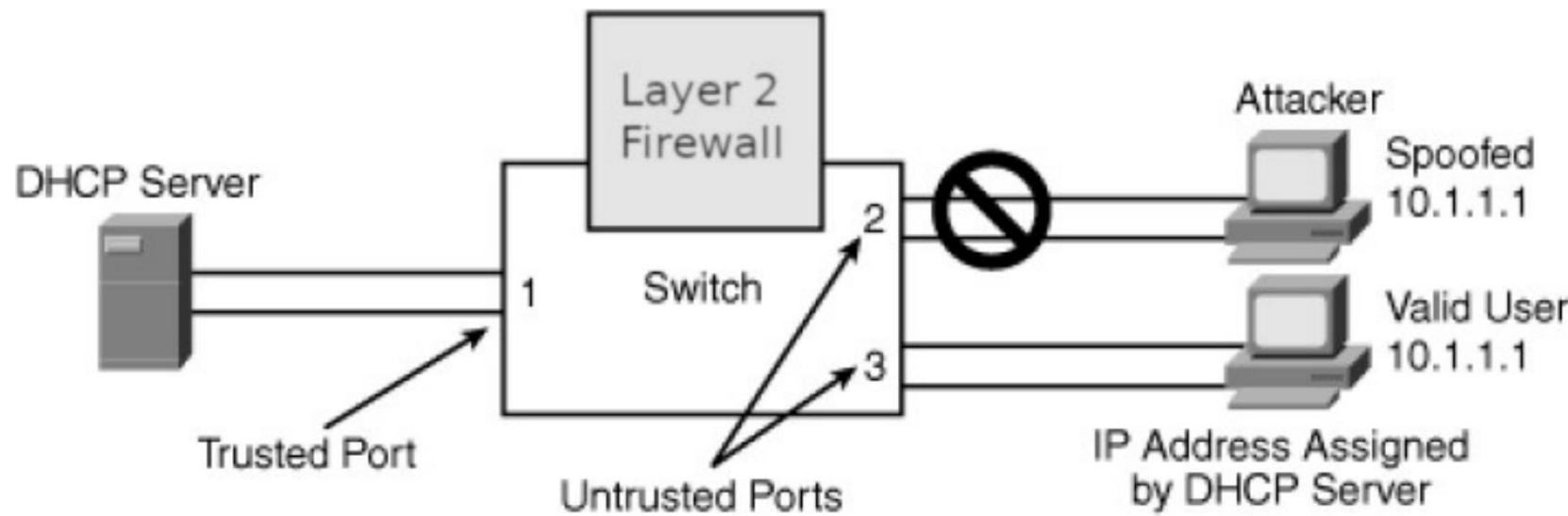


- Negar tráfego externo com
 - ◆ origem IP igual a intervalos de IP de rede protegidos.
 - ◆ Origem IP igual a endereços privados.
 - ◆ Destinos multicast.
- Verificação de caminho reverso
 - ◆ Nega o tráfego onde a rede IP de origem não pode ser acessada usando a interface onde o pacote chegou.

```
Interface interface-name
  ip access-group 101 in
  ip access-group 199 out
!
access-list 101 deny ip 209.165.201.0 0.0.0.31 any
access-list 101 deny icmp any any redirect
access-list 101 deny ip 224.0.0.0 31.255.255.255 any
access-list 101 deny ip 240.0.0.0 15.255.255.255 any
access-list 101 deny ip 127.0.0.0 0.255.255.255 any
access-list 101 deny ip host 0.0.0.0 any
access-list 101 deny ip 10.1.1.0 0.0.0.255 any
access-list 101 deny ip 172.16.0.0 0.15.255.255 any
access-list 101 deny ip 192.168.0.0 0.0.255.255 any
access-list 101 permit ip any any
!
access-list 199 permit ip 209.165.201.0 0.0.0.31 any
access-list 199 deny ip any any
```



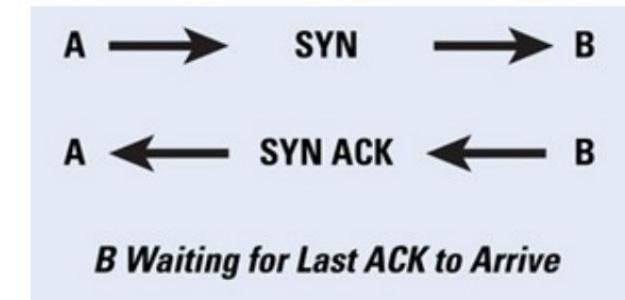
Evitando falsificação de IP na camada 2



- Para evitar ataques de falsificação de IP, restringindo o tráfego de IP em portas não confiáveis da Camada 2 para clientes com um endereço IP atribuído.
- Funciona filtrando o tráfego IP com um endereço IP de origem diferente daquele atribuído por meio do Protocolo de Configuração de Host Dinâmico (DHCP) ou configuração estática nas portas não confiáveis da Camada 2.
- Funciona em combinação com o DHCP e é ativado em portas não confiáveis da Camada 2.

Problema de conexão TCP semi-aberta

- Um ataque DoS geralmente usa conexões TCP semi-abertas.
 - O firewall mantém o estado da sessão TCP na memória.
 - Múltiplas conexões TCP semi-abertas podem ultrapassar firewalls.
 - Defina valores de tempo limite para sessões TCP semi-abertas:
 - Normal: valores pequenos/médios.
 - Sob ataque (com base nos limites de tráfego): valores muito pequenos.
 - Pode ser necessário usar meios externos para “limpar” o firewall.
 - Redefinir conexões (semi-abertas) do interno servidores.



Avaliação de desempenho do firewall

• Firewall básico

- ◆ Rendimento IP
 - ➡ Capacidade bruta do firewall para passar o tráfego de interface para interface
- ◆ Latência
 - ➡ Tempo de atraso de tráfego no firewall
 - ➡ Deve ser medido e relatado quando o firewall estiver em sua carga operacional

• Firewall empresarial tradicional

- ◆ Taxa de Estabelecimento de Conexão
 - ➡ Velocidade na qual os firewalls podem configurar conexões
- ◆ Capacidade de conexão simultânea
 - ➡ Número total de conexões abertas pelo firewall em um determinado momento
- ◆ Taxa de Desativação de Conexão
 - ➡ Velocidade na qual os firewalls podem derrubar conexões e liberar recursos

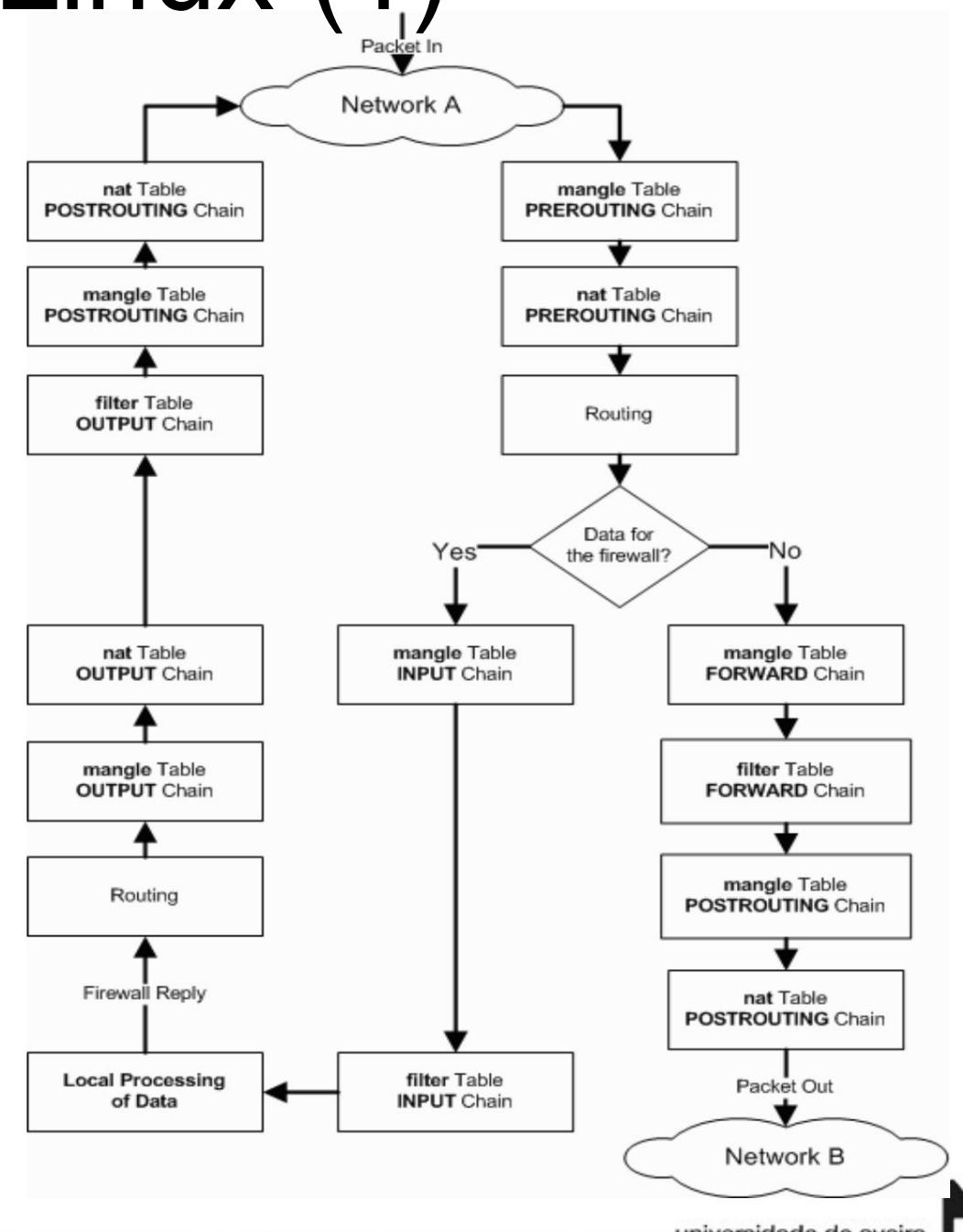
• Firewall de Próxima Geração

- ◆ Taxa de transação do aplicativo
 - ➡ Capacidade do firewall de proteger transações discretas da camada de aplicativos contidas em uma conexão aberta
 - ➡ Pode incluir gateways de camada de aplicativo, prevenção de intrusão ou tecnologia de inspeção profunda
 - ➡ A taxa de transação do aplicativo é altamente dependente de dados



iptables Linux (1)

- Nome da ferramenta de espaço do usuário pela qual os administradores criam regras para filtragem de pacotes e módulos NAT.
- Usado para configurar, manter e inspecionar as tabelas de regras de filtragem de pacotes IP no kernel do Linux.
- Tem 5 cadeias padrão:
 - ◆ ENTRADA, SAÍDA, AVANÇO
 - ◆ PRÉ-ENCAMINHAMENTO
 - ◆ POSTROUTING
- Tem 3 tabelas padrão,
 - ◆ Filtro, nat e mangle
- decisões básicas
 - ◆ ACEITAR, DEIXAR, ENCARAR E RETORNAR
- Decisões estendidas
 - ◆ LOG, MARK, REJECT, TOS, SNAT, DNAT, MASQUERADE, REDIRECT, etc...
- Múltiplas máquinas de estado
 - ◆ Conntrack (rastreador de conexão).



IPTables do Linux (2)

- Além das cadeias integradas, o usuário pode criar qualquer número de cadeias definidas pelo usuário dentro de cada tabela, o que permite agrupar as regras logicamente.
- Cada cadeia contém uma lista de regras,
 - ◆ Quando um pacote é enviado para uma cadeia, ele é comparado com cada regra da cadeia em ordem.
- A regra especifica quais propriedades o pacote deve ter para que a regra corresponda (como o número da porta ou o endereço IP).
- Se a regra não corresponder, o processamento continua com a próxima regra.
- Se, no entanto, a regra corresponder ao pacote, as instruções de destino da regra serão seguidas (e o processamento posterior da cadeia geralmente será abortado).
- Algumas propriedades de pacotes só podem ser examinadas em certas cadeias,
 - ◆ Por exemplo, a interface de rede de saída não é válida na cadeia INPUT.
- Alguns alvos só podem ser usados em certas cadeias e/ou certas mesas,
 - ◆ Por exemplo, o destino SNAT só pode ser usado na cadeia POSTROUTING da tabela NAT.
- O destino de uma regra pode ser o nome de uma cadeia definida pelo usuário ou um dos destinos integrados (ACCEPT, DROP, RETURN, DNAT, SNAT e MASQUERADE).
- Você pode pensar em um destino da mesma forma que uma sub-rotina.



Linux nftables

- nftables substitui iptables.
- Fornece uma nova estrutura de classificação de pacotes no kernel baseada em uma máquina virtual (VM) específica da rede.
- Usa uma nova ferramenta de linha de comando nft userspace.
 - ◆ Ferramenta de linha de comando do espaço do usuário, sem necessidade de atualizações de kernel.
- Alta performance através de mapas e concatenações.
- Base de código do kernel menor. A inteligência é colocada na ferramenta de linha de comando nft do espaço do usuário.
- Sintaxe unificada e consistente para cada família de protocolo de suporte.



Controle por Análise de Camadas Superiores

- O controle de fluxo de tráfego baseado em dados/protocolos de camada superior funciona apenas com tráfego não cifrado.
- Alguns firewalls fornecem descriptografia e inspeção do tráfego SSL/TLS.
- A decifração do tráfego pode ser realizada usando um certificado raiz em máquinas clientes, atuando como Autoridade de Certificação para solicitações SSL.
 - ◆ Os firewalls devem emitir certificados para clientes em nome dos servidores da Web aos quais estão se conectando.
 - ◆ Os firewalls interceptam o handshake SSL/TLS.
 - ◆ Requer alterações no nível do dispositivo cliente.
- A implementação dessa técnica exige muito do processador.
 - ◆ Resulta na degradação do desempenho.
 - ◆ Pode ser evitado descarregando a descriptografia SSL/TLS para dispositivos dedicados.
- Pode violar leis e direitos de privacidade/confidencialidade em alguns países.



Listas de controle de acesso (ACL) da Cisco

- Uma lista de acesso é uma coleção sequencial de condições **de permissão e negação**.
- O software testa os pacotes em relação às condições de uma lista de acesso, um por um.
- A primeira correspondência determina se o software aceita ou rejeita o pacote.
 - Como o software para de testar as condições após a primeira correspondência, a ordem das condições é crítica.
- Se nenhuma condição corresponder, o software rejeita o pacote.
- Pode ser aplicado ao tráfego de entrada ou saída.



Tipos de ACL

● Padrão

- ◆ Controle o tráfego pela análise do endereço de origem dos pacotes IP.
- ◆ Numerado de 1 a 99
 - Exemplo: lista de acesso 1 permissão 10.1.1.0

● 0.0.0.255 Estendida

- ◆ Controle o tráfego pela análise dos endereços de origem e destino e protocolo dos pacotes IP.
- ◆ Numerado de 100 a 199
 - Exemplo: access-list 101 permit ip any 10.1.1.0 0.0.0.255 Named

● Permite

- ◆ que ACLs padrão e estendidas recebam nomes em vez de números. Identifica intuitivamente uma ACL usando um nome alfanumérico.
- ◆ Elimine os limites de número que existem em ACLs padrão e estendidas.
- ◆ As ACLs nomeadas fornecem a capacidade de modificar as ACLs sem excluí-las e, em seguida, reconfigurá-las.
 - Exemplo: lista de acesso ip {extended | padrão} nome

● Reflexivo

- ◆ Permite que os pacotes IP sejam filtrados com base nas informações da sessão da camada superior.
- ◆ A comunicação em uma direção abre portas na direção oposta.
- ◆ Geralmente usado para permitir o tráfego de saída e limitar o tráfego de entrada em resposta a sessões originadas dentro da rede.

● Controle de acesso baseado em contexto (CBAC)

- ◆ Inspeciona o tráfego para descobrir e gerenciar informações de estado para sessões TCP e UDP
- ◆ Essas informações de estado são usadas para criar aberturas temporárias nas listas de acesso do firewall



Comunicações seguras

**Segurança em Redes de Comunicações
Mestrado em Cibersegurança**

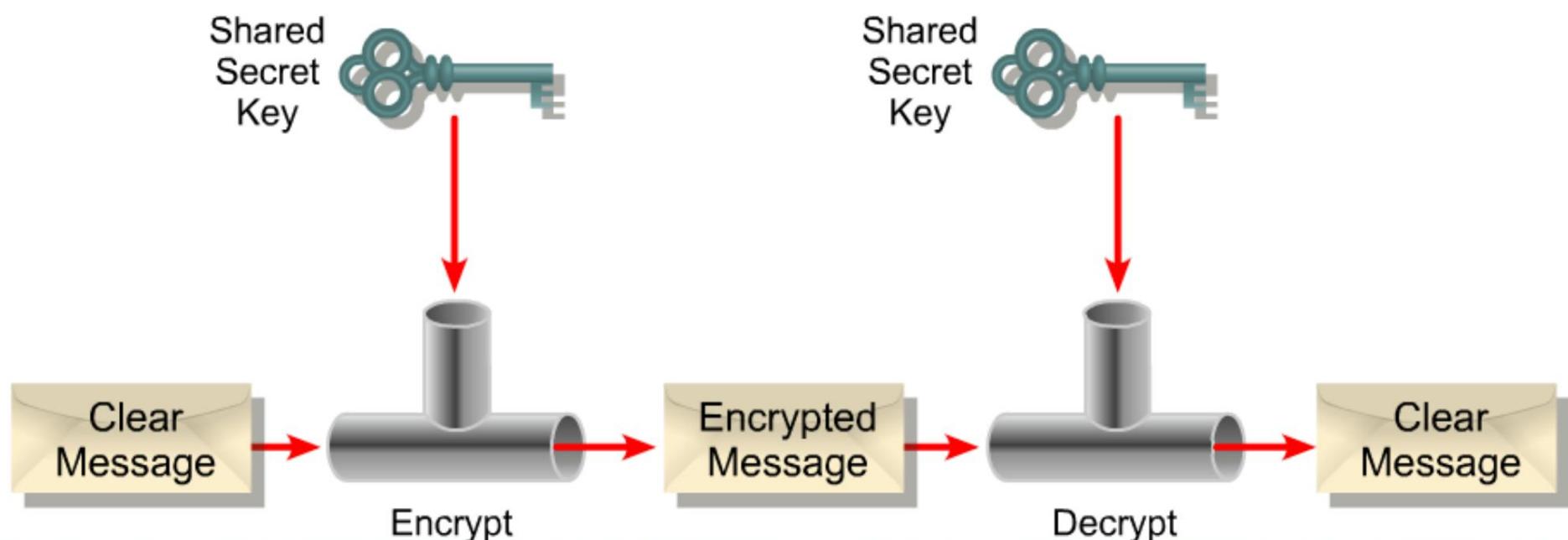
**Mestrado em Engenharia de Computadores e
telemática**

DETI-UA



Criptografia de chave simétrica

- Dois requisitos para uso seguro de criptografia simétrica:
 - ◆ Algoritmo de criptografia forte
 - ◆ Chave secreta conhecida apenas pelo remetente/destinatário
- Suponha que o algoritmo de criptografia seja conhecido
- Implica um canal seguro para distribuir a chave



Criptografia de chave pública

- A criptografia de chave pública envolve um par de chaves

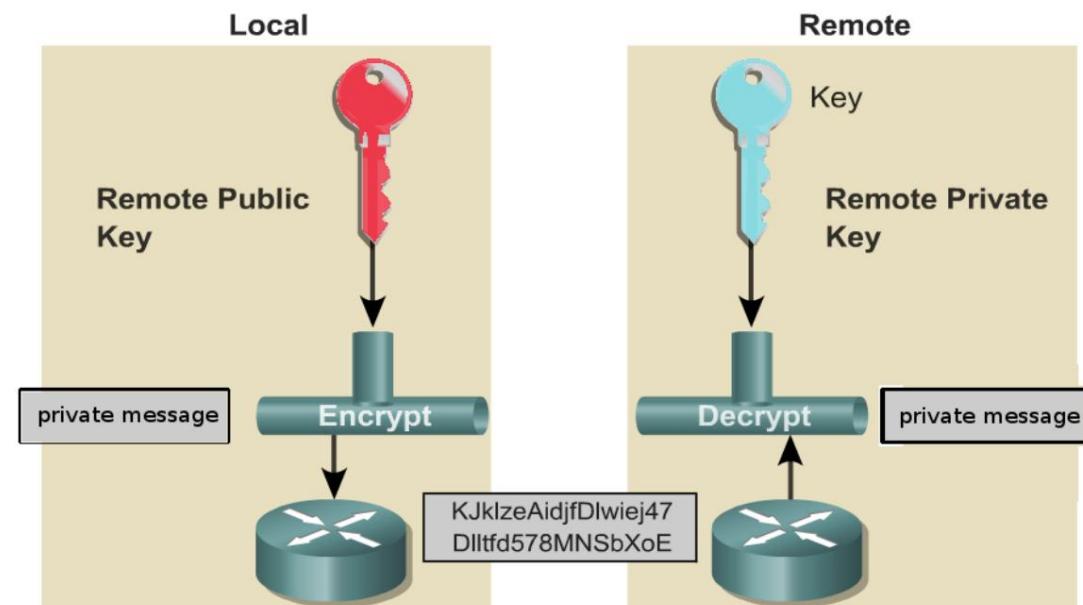
- **Uma chave pública**

- ◆ Pode ser conhecido por qualquer pessoa e pode ser usado para criptografar mensagens e verificar assinaturas

- **Uma chave privada**

- ◆ Conhecido apenas pelo destinatário, usado para descriptografar mensagens e assinar (criar) assinaturas

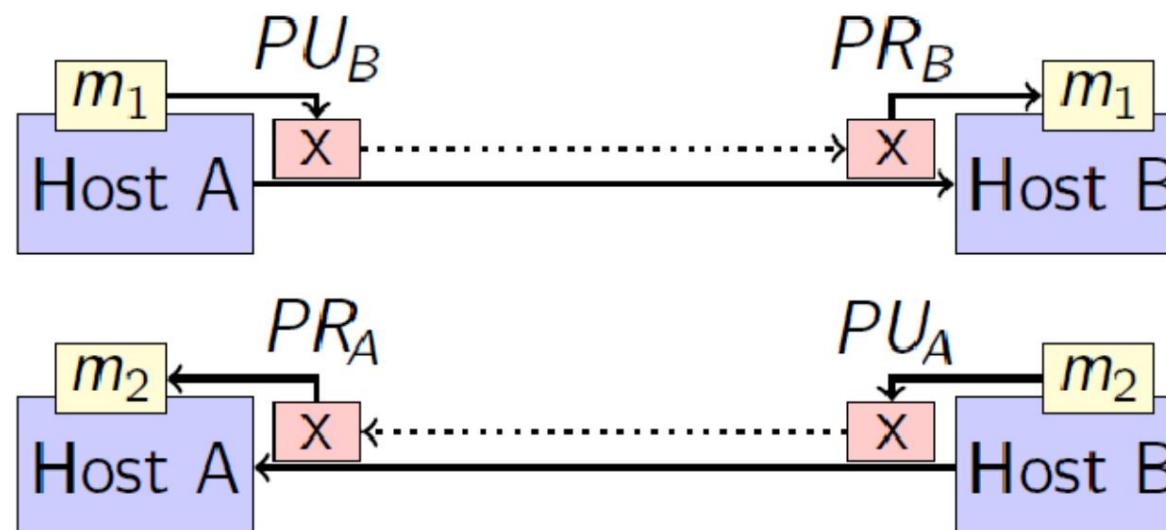
- Cada chave pública é publicada e a chave privada correspondente é mantida em segredo
- É assimétrico porque aqueles que criptografam mensagens ou verificam assinaturas não podem descriptografar mensagens ou criar assinaturas



Chave pública

Criptografia para confidencialidade

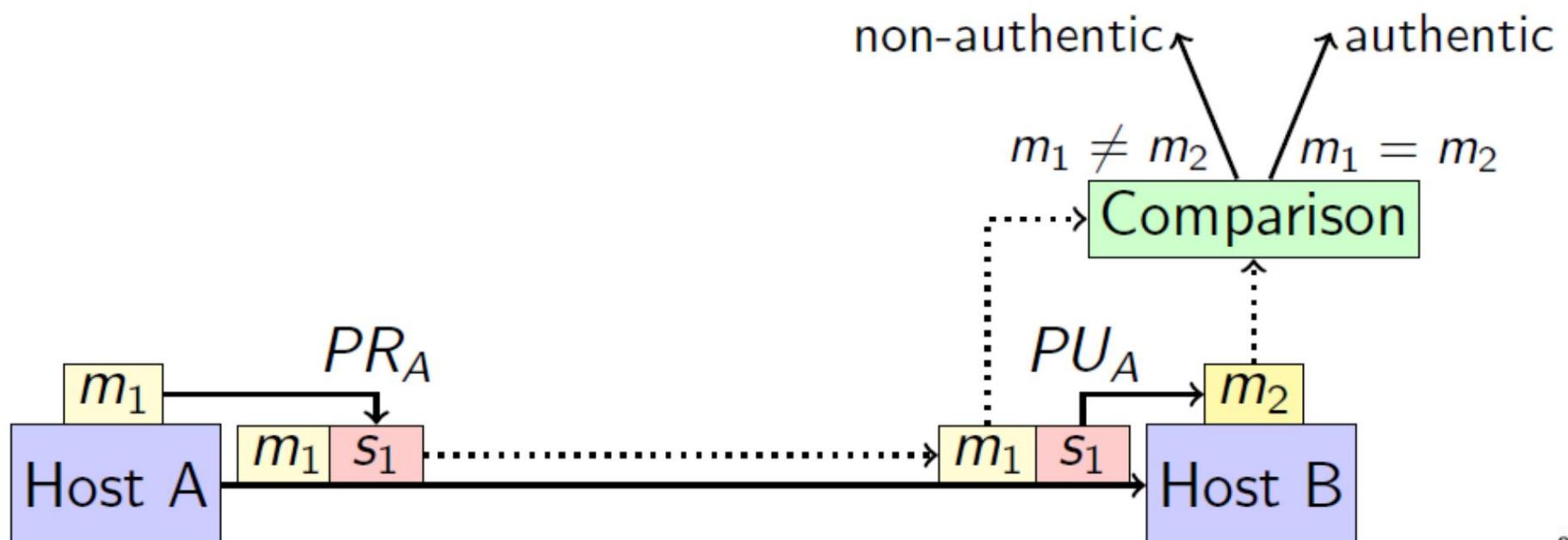
- Para enviar uma mensagem criptografada de A para B
 - ◆ Host A criptografa dados com chave pública Host B (PUB)
 - ◆ Host B descriptografa dados com chave privada Host B (PRB)
- Para enviar uma mensagem criptografada de B para A
 - ◆ Host B criptografa dados com chave pública Host A (PUA)
 - ◆ Host A descriptografa dados com chave privada Host A (PRA)
- Esse método é computacionalmente ineficiente para criptografar grandes quantidades de dados.
- Comumente usado para criar canais de comunicação seguros onde uma chave simétrica temporária pode ser negociada e usada para criptografar grandes quantidades de dados.



Chave pública

Assinaturas digitais para autenticação

- Para enviar uma mensagem autenticada de A para B
 - O Host A cria uma assinatura criptografando os dados com a chave privada (PRA) do Host A
 - Host A envia dados e assinatura para host B
 - O Host B verifica a data descriptografando a assinatura com a chave pública (PUA) do Host A e compara com a mensagem recebida



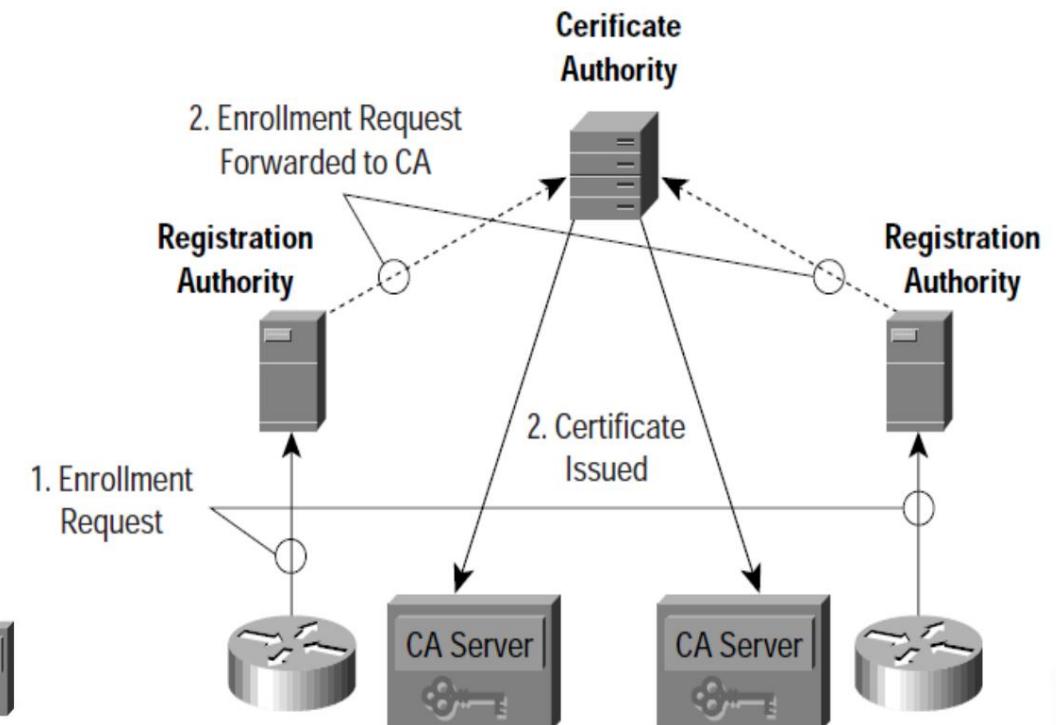
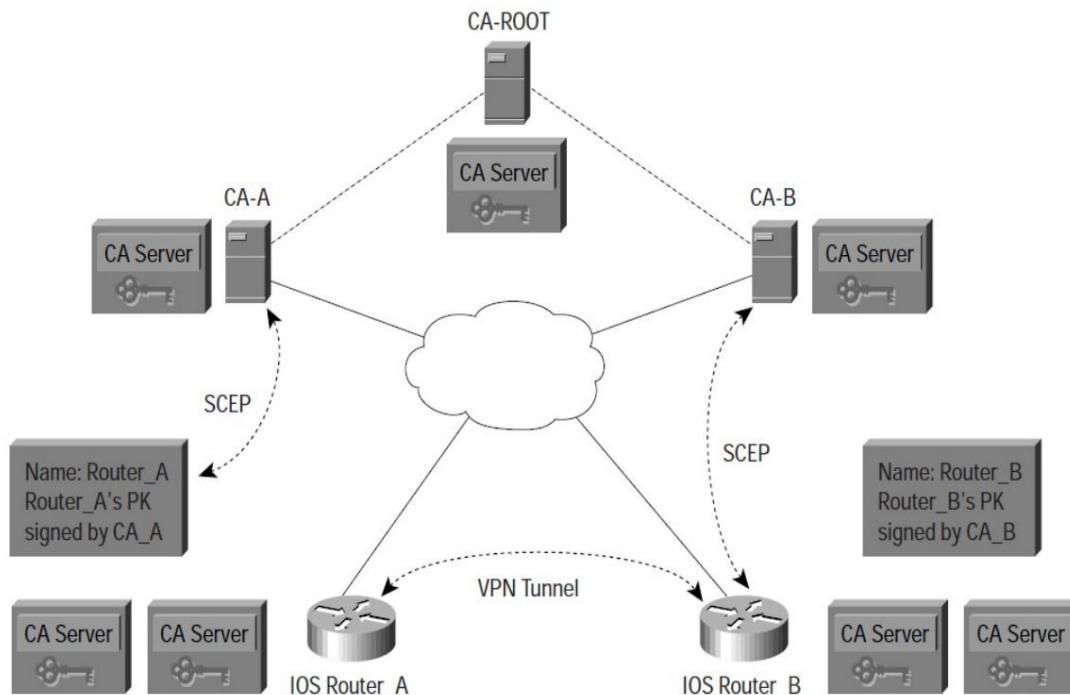
RSA (Rivest, Shamir e Adleman)

- Nomeado após seus inventores - Rivest, Shamir e Adleman
- É um algoritmo de chave pública (criptografia e descriptografia)
- O comprimento da chave é variável
 - ◆ Comprimentos de chave comuns: 512, 1024 e 2048 bits
- O tamanho do bloco é variável, mas deve ser menor que o comprimento da chave
- O comprimento do texto cifrado será o comprimento da chave
- Mais lento que DES, AES e IDEA
 - ◆ Normalmente não usado para criptografar mensagens grandes
 - ◆ Usado para criptografar a chave secreta e a chave secreta usada para criptografar mensagens



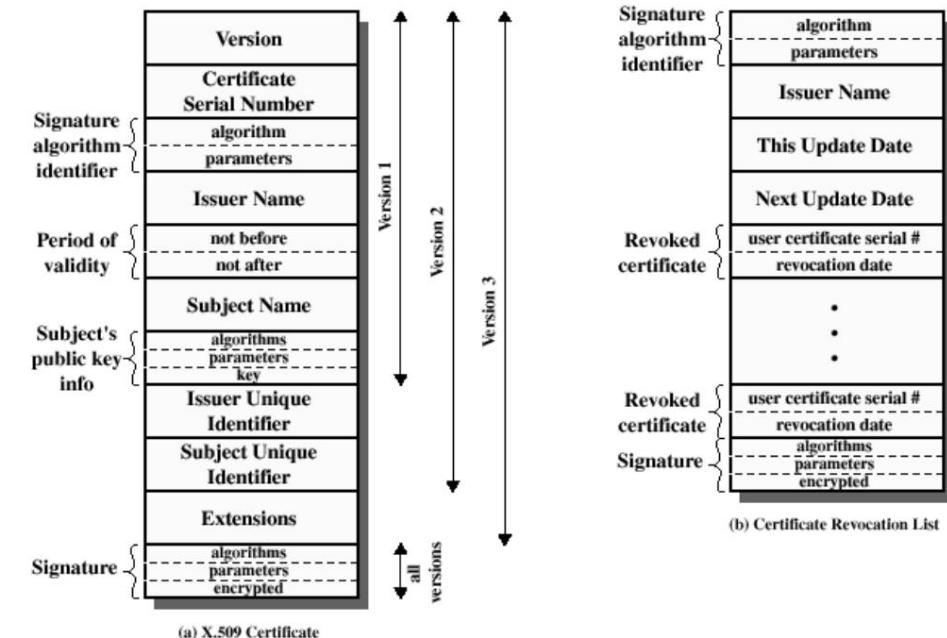
Infraestrutura de chave pública (PKI)

- PKIs são de natureza hierárquica
- Cada participante da PKI possui um certificado digital emitido por uma Autoridade de Certificação (CA)
 - ◆ A CA pode ser uma CA raiz ou uma CA subordinada
 - ◆ Cadeia de confiança.
- A PKI pode usar hosts adicionais chamados Autoridades de Registro (RA) para aceitar solicitações de inscrição na PKI



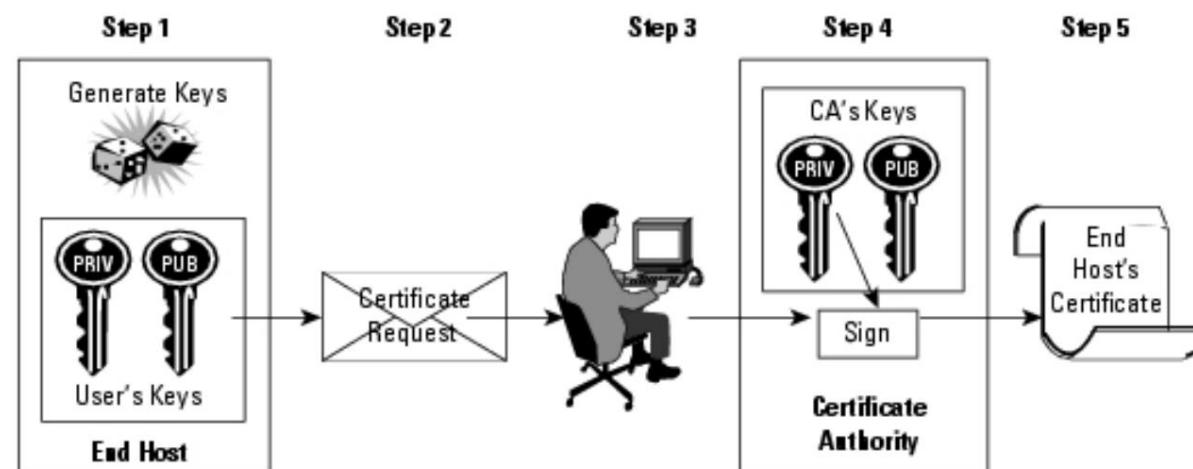
conteúdo do certificado X.509

- Versão
- Número de série
- Algoritmo de Assinatura
- Nome do emissor
- Período de Validade
- Nome do Assunto
 - ◆ Nome Distinto (DN) da entidade CN=Java
 - ◆ Duke, OU=Java Software Division, O=U.Aveiro, C=PT Informação da Chave
- Pública do Assunto Algoritmo da Chave
 - ◆ Pública do Assunto
 - ◆ Algoritmo de
- Assinatura do Certificado de Chave Pública
- do Assunto Assinatura do Certificado



Inscrição na autoridade de certificação

- O Simple Certificate Enrollment Protocol (SCEP) é usado para o transporte seguro de informações importantes e certificados
- Inscrevendo-se em uma autoridade de certificação
 - 1.Host final gera um par de chaves públicas-privadas
 - 2.Host final gera uma solicitação de certificado, que encaminha para a CA
 - 3.Manual, intervenção humana é necessária para aprovar a inscrição solicitar,
 - 4.Após a aprovação, a CA assina o certificado com sua chave privada e retorna o certificado completo para o host final
 5. O host final armazena o certificado

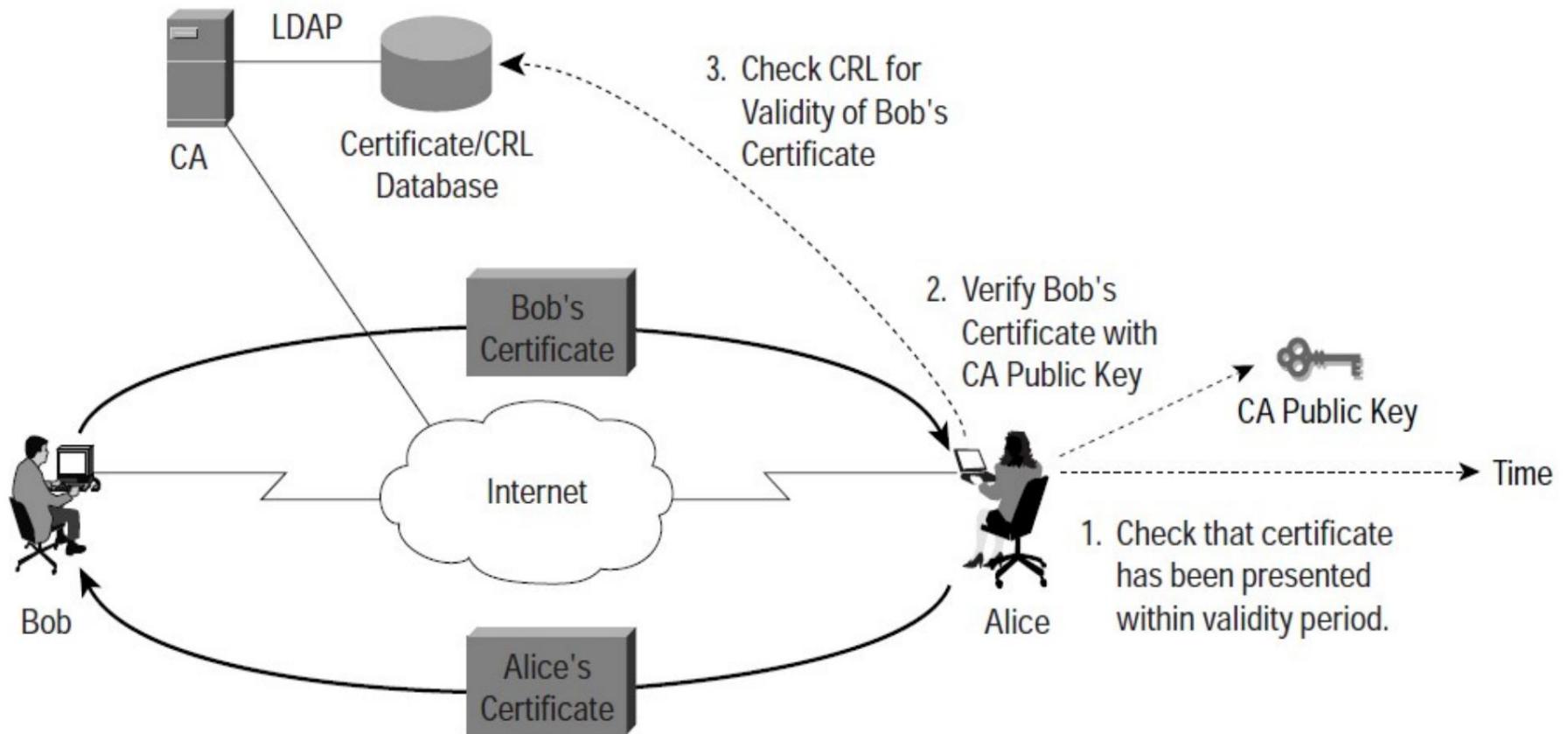


Listas de certificados revogados (CRL)

- A CRL é outro componente crucial da PKI
- É uma lista de certificados que eram anteriormente válidos dentro do PKI, mas foram revogados por algum motivo
- Esses motivos podem incluir qualquer um dos seguintes:
 - ◆ Compromisso de chaves dentro do certificado
 - ◆ Perda de privilégios de acesso para usuário/dispositivo
 - ◆ Alteração da estrutura da PKI exigindo reemissão do certificado



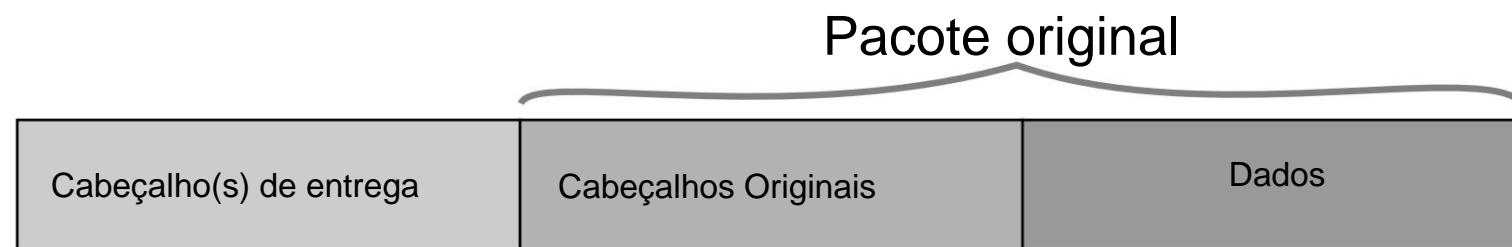
Verificação de uso e validade do certificado



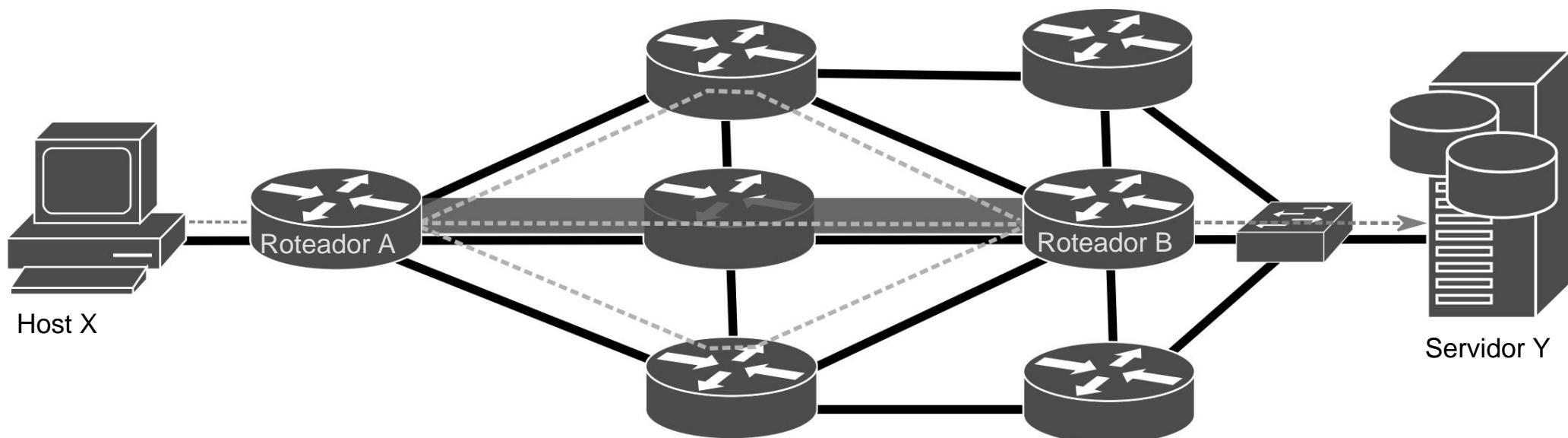
- O certificado está sendo apresentado dentro do prazo de validade
- A CA que assinou o certificado é conhecida e confiável
- O certificado não está em uma lista de revogação (opcional em alguns cenários)

Conceito de Túnel de Tráfego

- Objetivos principais
 - ◆ Garantir que um pacote que chega a um nó da rede chegará a um nó da rede secundária específico independentemente dos processos de roteamento dos nós
 - ◆ intermediários, Garantir a entrega de um pacote a um nó remoto quando os nós intermediários não suportam o protocolo de rede do pacote original
 - ◆ e , Defina um canal virtual que adicione recursos adicionais de transporte de dados para fornecer QoS diferenciado, requisitos de segurança e/ou roteamento otimizado.
- Obtido pela adição, no ponto de entrada do túnel, de um ou mais cabeçalhos de protocolo aos pacotes originais para lidar com sua entrega ao ponto de saída do túnel.



Pontos Finais do Túnel



Protocolo(s) de entrega

Fonte: Um endereço
Destino: Endereço B

Protocolos originais

Fonte: Endereço X
Destino: Endereço Y

Dados

Interface de túnel virtual (VTI)

- Construção lógica que cria uma interface de rede virtual que pode ser tratada como qualquer outra interface de rede dentro de um equipamento de rede.
- Um túnel não requer nenhum endereço de rede além daqueles já vinculados ao roteador de ponto final.
- No entanto, a maioria das implementações impõe que um endereço de rede deve ser vinculado a uma interface de túnel para permitir o processamento de IP na interface.
 - ◆ A interface do túnel pode ter um endereço de rede vinculado explicitamente ou reutilizar um endereço de outra interface já configurada no roteador.

```
1 #interface Tunnel 1
2 #ip address 10.1.1.1 255.255.255.252
3 #ipv6 address 2001:A::A:1/64
4 #ip unnumbered FastEthernet0/0
5 #ipv6 unnumbered FastEthernet0/0
6 #ip ospf cost 10
7 #ipv6 ospf 1 area 0
8 #tunnel mode ipip
9 #tunnel source FastEthernet0/0
10 #tunnel destination 200.2.2.2
```



Requisitos VTI

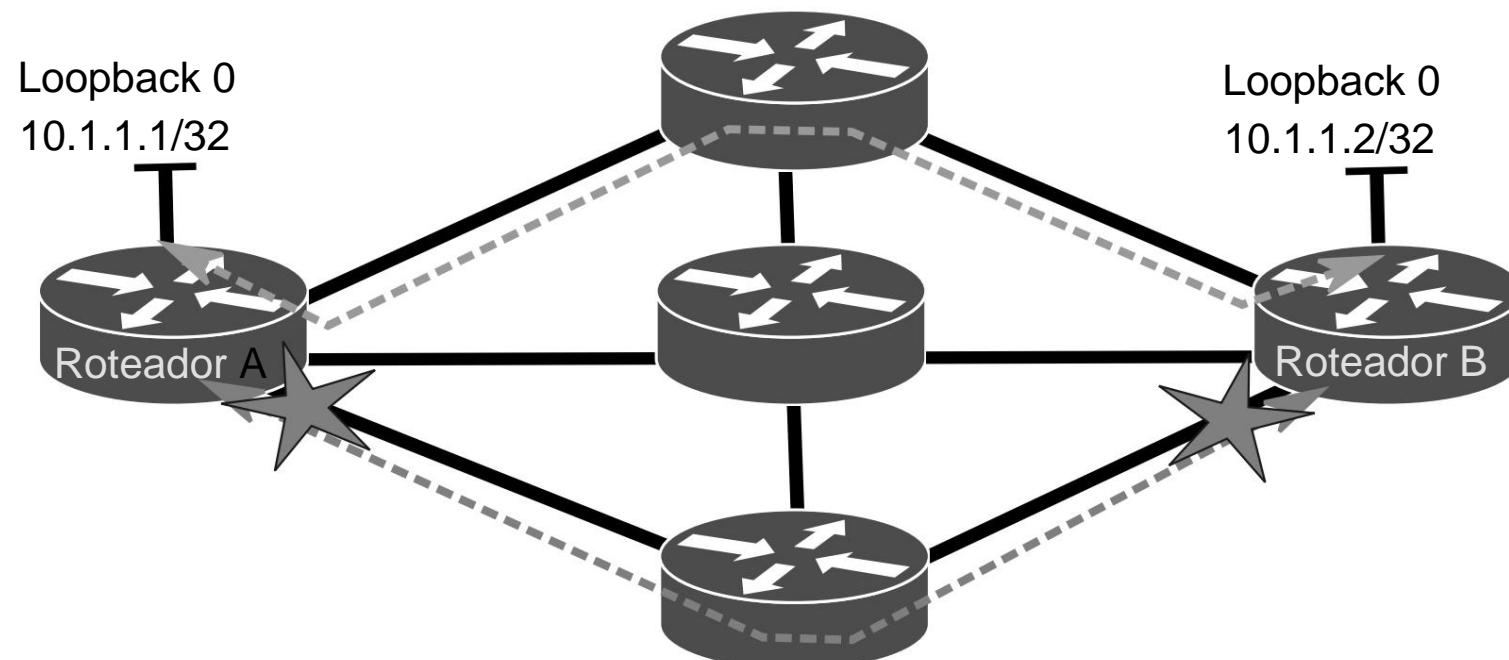
- Um identificador numérico,
- Um endereço IP limitado, isso permitirá o processamento de IP,
 - ◆ Adicione a interface de túnel à tabela de roteamento e permita o roteamento por meio da interface,
- Um modo ou tipo de túnel definido. A
 - ◆ disponibilidade dos modelos de túnel depende do modelo do roteador, do software operacional e das licenças
- Fonte do túnel,
 - ◆ Definido como o nome da interface local ou endereço IPv4/IPv6 dependendo do tipo de túnel.
- Destino do túnel,
 - ◆ definido como um nome de domínio ou endereço IPv4/IPv6, dependendo do tipo de túnel.
 - ◆ Esta definição não é obrigatória para todos os tipos de túneis porque, em alguns casos, o ponto final do túnel é determinado dinamicamente.
- Pode opcionalmente ter configurações adicionais para propósitos de roteamento, segurança e QoS.

```
1 #interface Tunnel 1
2 #ip address 10.1.1.1 255.255.255.252
3 #ipv6 address 2001:A::A:1/64
4 #ip unnumbered FastEthernet0/0
5 #ipv6 unnumbered FastEthernet0/0
6 #ip ospf cost 10
7 #ipv6 ospf 1 area 0
8 #tunnel mode ipip
9 #tunnel source FastEthernet0/0
10 #tunnel destination 200.2.2.2
```



Interfaces de loopback como pontos finais

- A interface de loopback é outra construção lógica que cria uma interface de rede virtual completamente independente das demais interfaces de rede do roteador físico e lógico.
- O principal objetivo de uma interface de loopback é fornecer um endereço de rede para servir como identificador de roteador em configurações de rede remota e distribuir algoritmos.
- A principal vantagem de usar interfaces de loopback como endpoints de túnel é a criação de um túnel não limitado a nenhuma placa/link de rede individual que pode falhar.



Tipos de túnel IP

- IPv4-IPv4

- ◆ Os pacotes IPv4 originais são entregues usando IPv4 como protocolo de rede.

- GRE IPv4

- ◆ O protocolo de pacotes originais (qualquer protocolo de rede) é definido pelo cabeçalho GRE e entregue usando IPv4 como protocolo de rede.

- IPv6-IPv6

- ◆ Os pacotes IPv6 originais são entregues usando IPv6 como protocolo de rede.

- GRE IPv6

- ◆ O protocolo de pacotes originais (qualquer protocolo de rede) é definido por um cabeçalho GRE e entregue usando IPv6 como protocolo de rede.

- IPv6-IPv4

- ◆ Os pacotes IPv6 originais são entregues usando IPv4 como protocolo de rede.

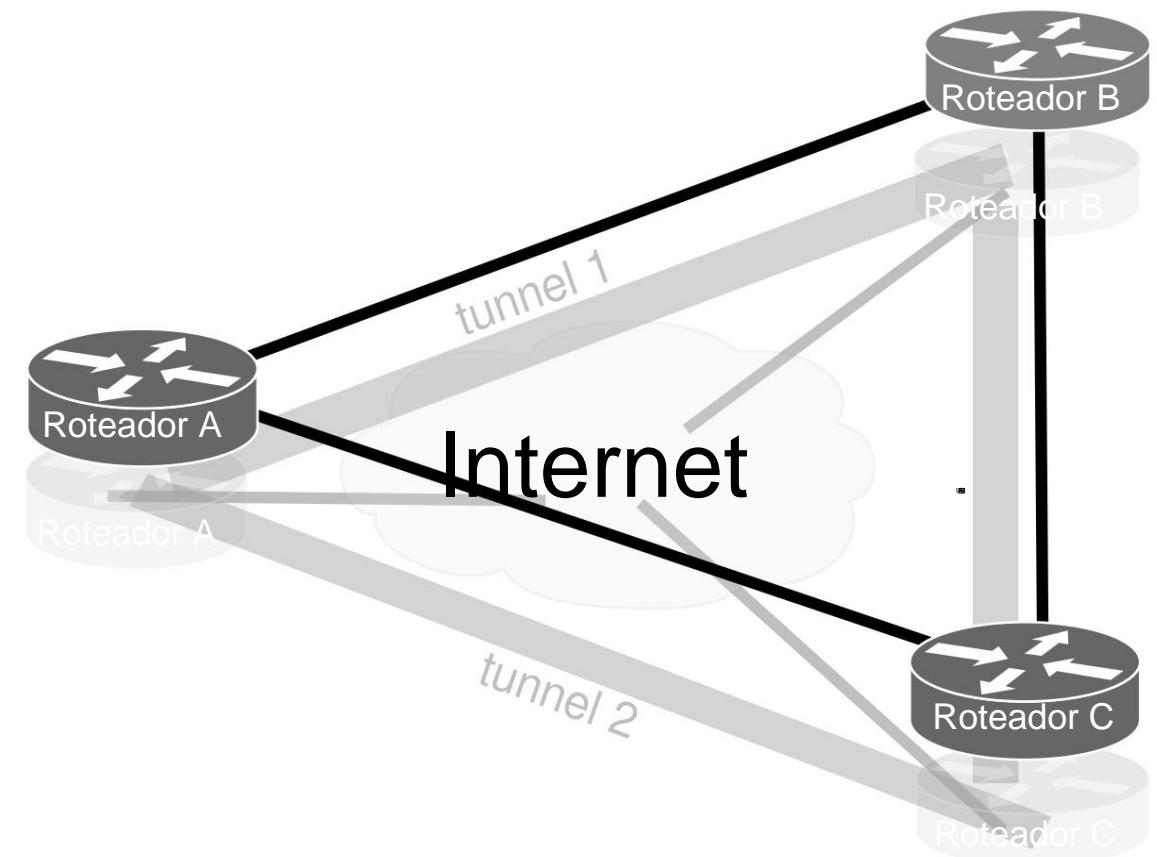
- IPv4-IPv6

- ◆ Os pacotes IPv4 originais são entregues usando IPv6 como protocolo de rede.

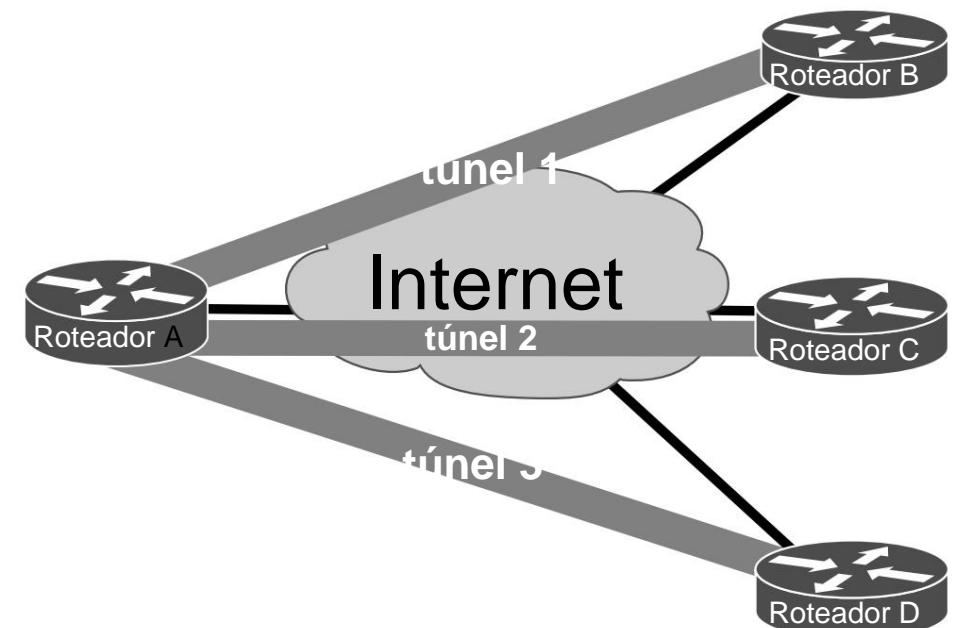
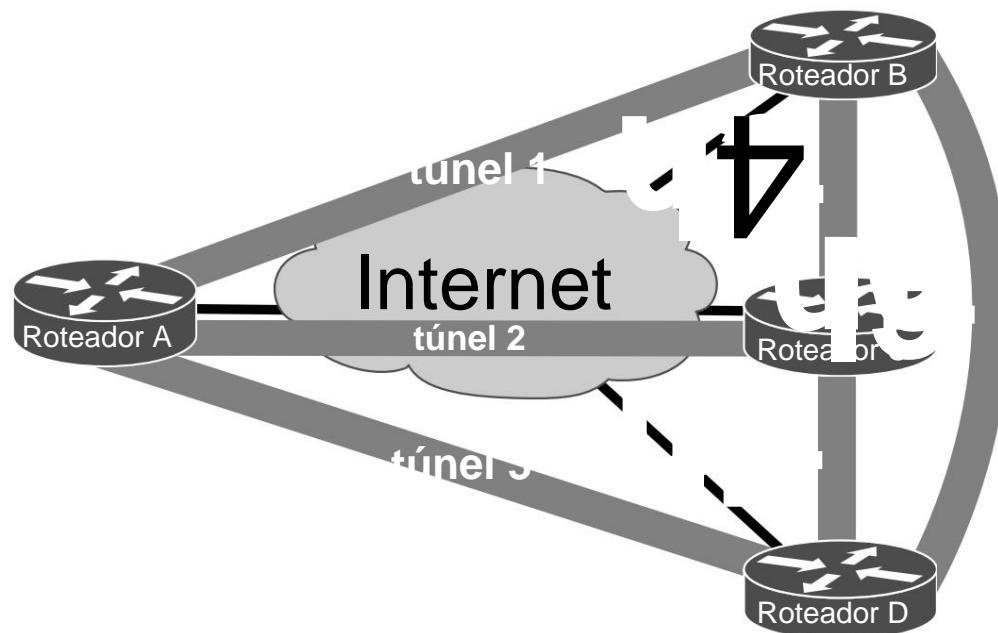


Rede de sobreposição

- Uma rede de sobreposição pode ser definida como uma rede virtual definida sobre outra rede.
 - ◆ Para uma finalidade específica, como políticas de roteamento/transporte privado, QoS, segurança.
- A rede subjacente pode ser física ou também virtual.
 - ◆ Pode resultar em várias camadas de redes de sobreposição.
- Quando qualquer nível de protocolo de privacidade está presente em uma rede de sobreposição, é designado por Virtual Private Network (VPN).



Malha de sobreposição total/parcial



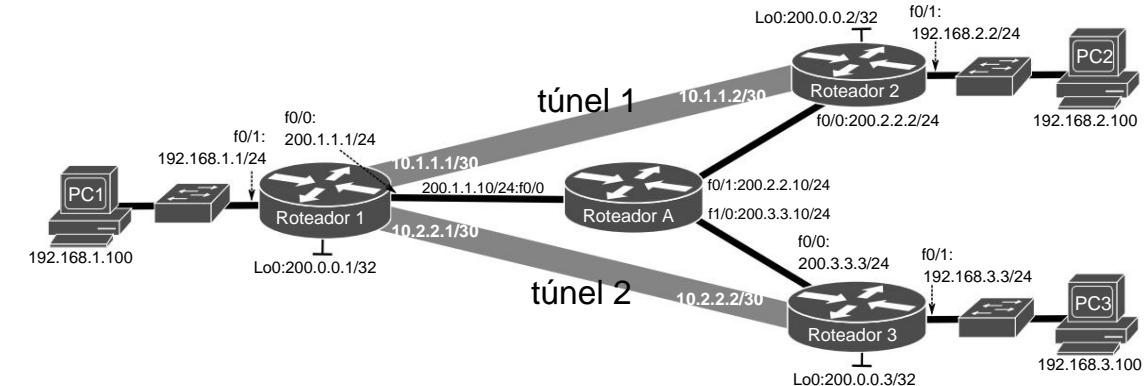
Roteamento através/entre túneis

- Rotas Estáticas

```

1 #ip route 192.168.2.0 255.255.255.0 Tunnel1
2 #ip route 192.168.2.0 255.255.255.0 10.1.1.2
3 #ipv6 route 2001:A::1:/64 Tunnel1
4 #ipv6 route 2001:A::1:/64 2001:0:0::2
5 #ip route 192.168.2.100 255.255.255.255 10.1.1.2
6 #ipv6 route 2001:A::100/128 2001:0:0::2

```



- Roteamento baseado em políticas (mapas de rotas)

```

1 #access-list 100 permit ip host 192.168.1.100 192.168.2.0 255.255.255.0
2 #route-map routeT1
3 #match ip address 100
4 #set ip next-hop 10.1.1.2
5 #interface FastEthernet0/1
6 #ip policy route-map routeT1

```

- Roteamento Dinâmico

- Múltiplos (distintos) processos de roteamento.
 - Um por rede de sobreposição
 - e um para a rede subjacente.

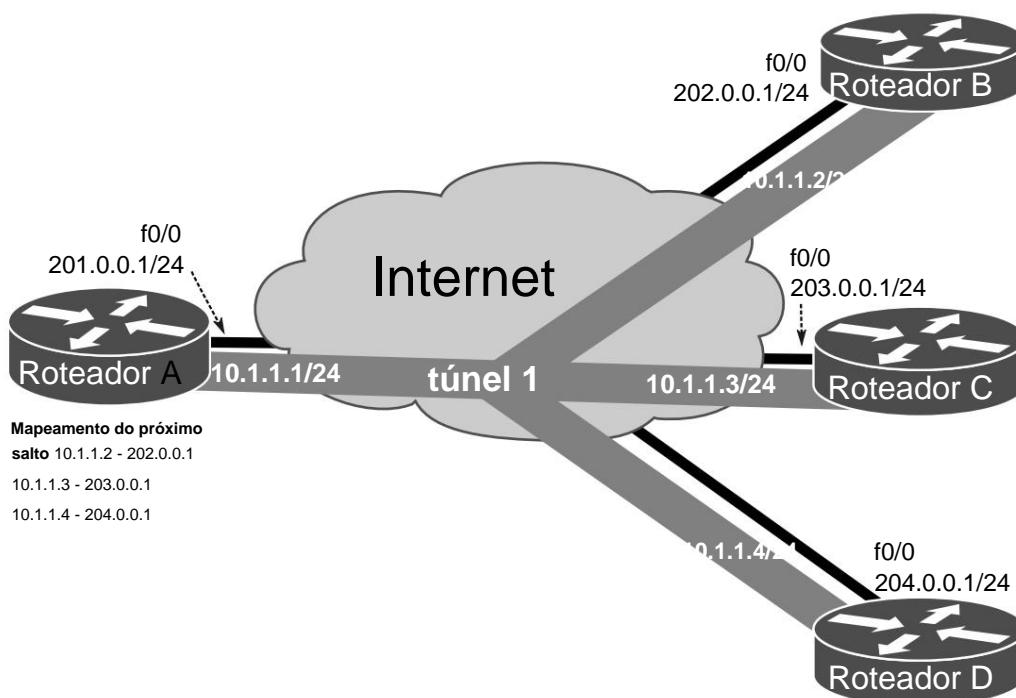
```

1 #router ospf 1
2 #network 200.1.1.0 0.0.0.255 area 0
3 #network 200.0.0.1 0.0.0.0 area 0
4 !
5 #router ospf 2
6 #network 10.0.0.0 0.255.255.255 area 0
7 #network 192.168.0.0 0.0.255.255 area 1

```



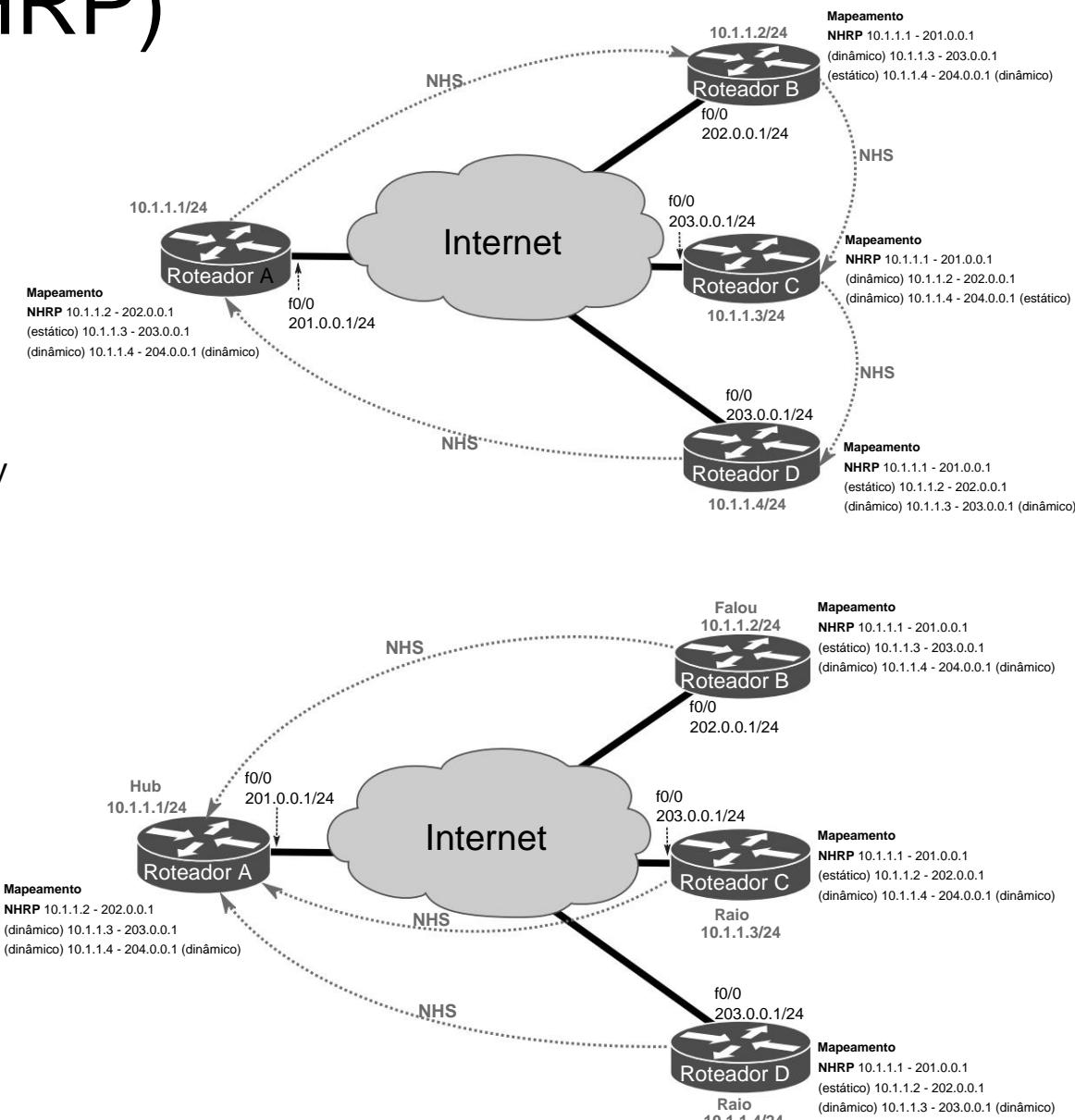
túneis multiponto



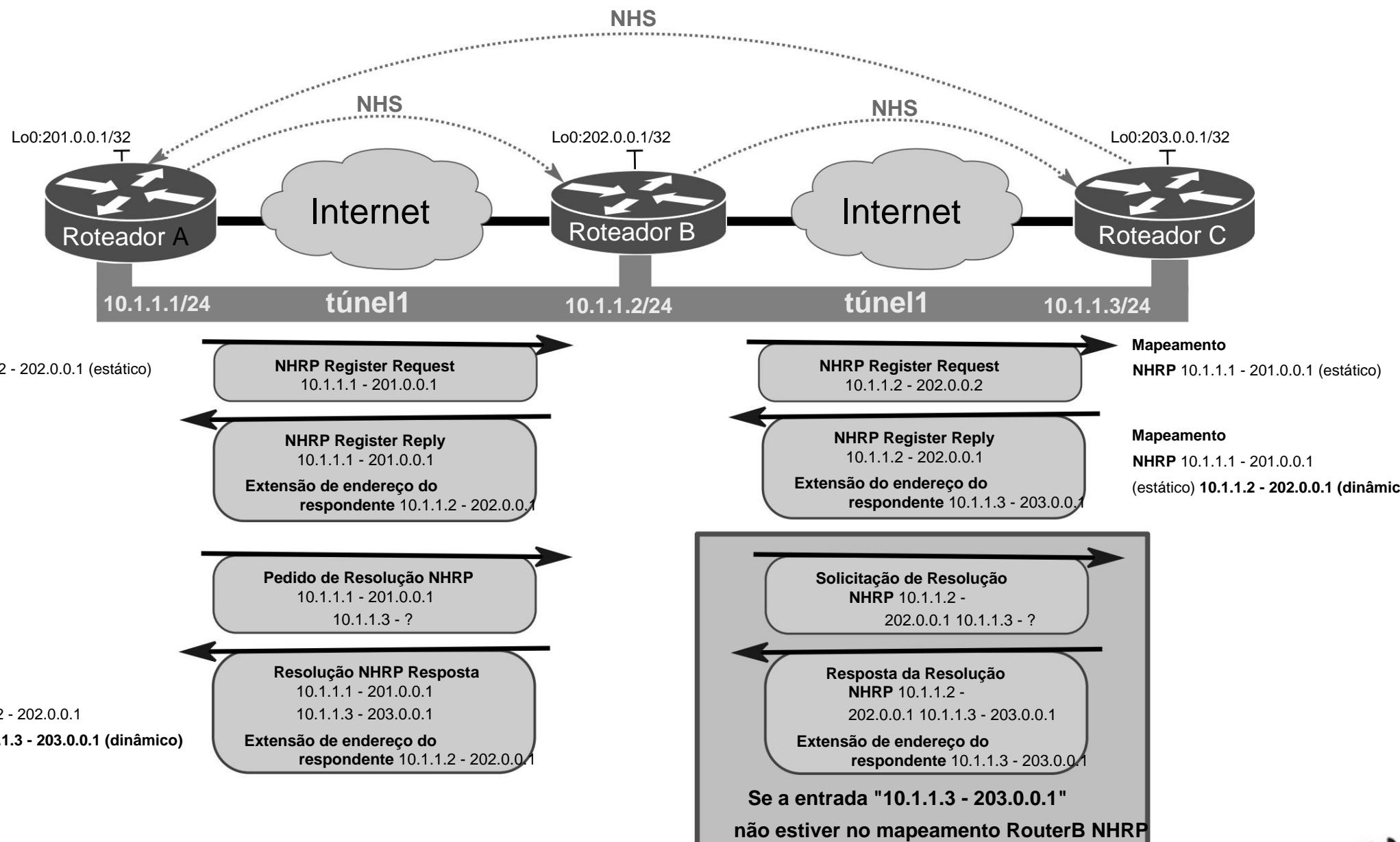
- Em um cenário com muitos nós para interconectar, a abordagem mais simples e eficiente é ter um único túnel que interconecta vários nós - um túnel multiponto.
 - Conecte-se diretamente usando uma única rede IP de sobreposição virtual, definida em um túnel multiponto.
 - Em um cenário de túnel multiponto, o endereço do cabeçalho de entrega é determinado com base no endereço do próximo salto dentro da rede de sobreposição.
 - O mapeamento de endereços entre a sobreposição e os endereços de rede subjacentes pode ser definido estaticamente ou obtido dinamicamente.

Protocolo de resolução do próximo salto (NHRP)

- O NHRP permite mapear um endereço IP de interface de túnel (rede de sobreposição) para o respectivo endereço IP de interface de rede subjacente.
- O túnel NHRP requer que todos os nós intervenientes sejam capazes de encontrar um caminho para qualquer um dos outros nós.
- Cada nó deve conhecer pelo menos um outro nó overlay (e respectivos endereços overlay e underlaying) através do qual ele tentará encontrar os mapeamentos de endereço dos outros nós.
 - ◆ Servidor do próximo salto (NHS).
- Além disso, todos os nós devem ser configurados de forma que todos os nós tenham pelo menos um caminho válido para todos os outros nós - formando uma malha parcial.



Intercâmbio de Informações do NHRP



Hub-Spoke vs. Spoke-Spoke

- Hub-Spoke
 - ◆ Cada site remoto é conectado com um túnel GRE ponto a ponto a um nó central pré-definido (Hub).
 - ◆ Hub aceita novas conexões de túnel de Spokes (nós de ramificação).
 - ◆ A comunicação de dados (pela rede de sobreposição) entre Spokes é retransmitida por meio do Hub.
 - ◆ Vários hubs podem existir para fornecer redundância.
- Spoke-Spoke
 - ◆ Os nós individuais das filiais podem iniciar dinamicamente conexões de túnel entre si, ignorando o nó Hub.
 - ◆ A comunicação de dados (pela rede overlay) pode ser direta entre os Spokes.
 - ◆ Os protocolos de roteamento IGP dinâmico podem operar entre Spoke e Hubs, mas não entre Spokes.
 - ◆ Sem interoperabilidade com roteadores IOS não Cisco. (?)



IPSec

- Estrutura de protocolos de segurança e algoritmos usados para proteger dados na camada de rede
- Cabeçalho de Autenticação (AH)
 - ◆ Garante a integridade dos dados
 - ◆ Não fornece confidencialidade
 - ◆ Fornece autenticação de origem
 - ◆ Usa mecanismos de hash com chave
- Encapsulando Security Payload (ESP)
 - ◆ Fornece confidencialidade de dados (criptografia)
 - ◆ Integridade de dados
 - ◆ Não protege o cabeçalho IP
- AH e ESP usam algoritmos de chave secreta simétrica, embora algoritmos de chave pública sejam viáveis



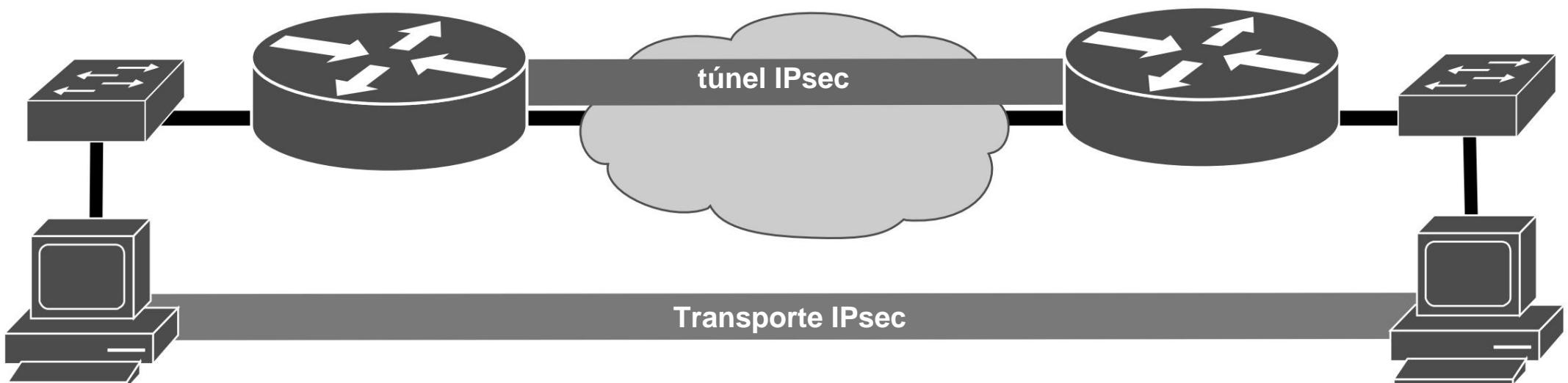
Modos IPsec

- Túnel

- Os gateways IPsec fornecem serviços IPsec para outros hosts em túneis peer-to-peer Os hosts finais não estão cientes de que o IPsec está sendo usado para proteger seu tráfego Os gateways IPsec fornecem proteção transparente sobre redes não

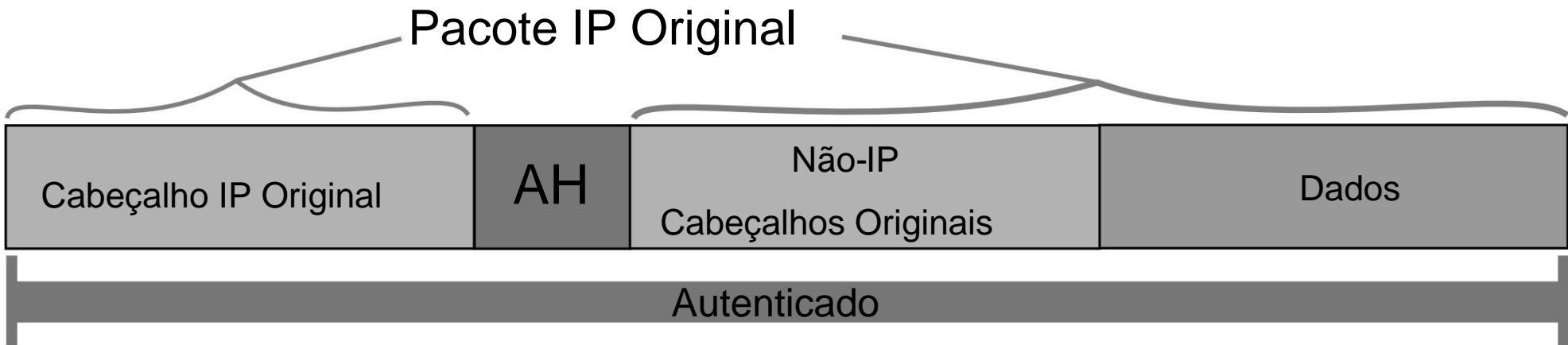
- confiáveis

- Transporte Cada host final faz o encapsulamento IPsec de seus próprios dados , host -to-host.
- O IPsec deve ser implementado nos hosts finais O endpoint do aplicativo também deve ser o endpoint IPsec

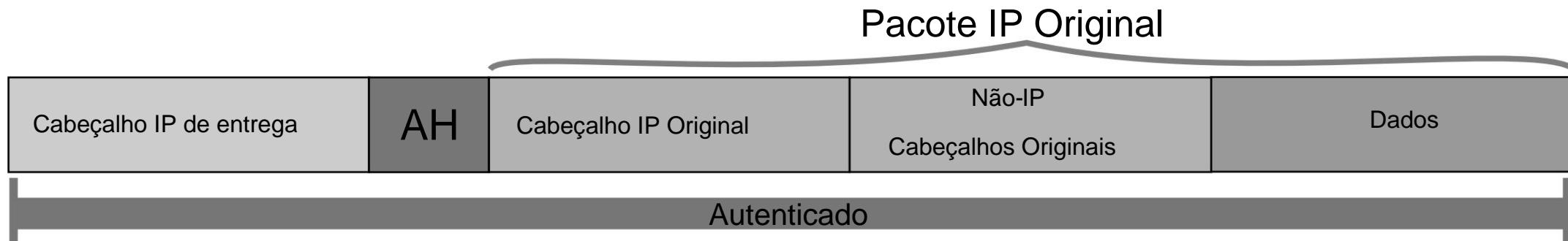


IPSec - Posicionamento do cabeçalho AH

- Modo de transporte

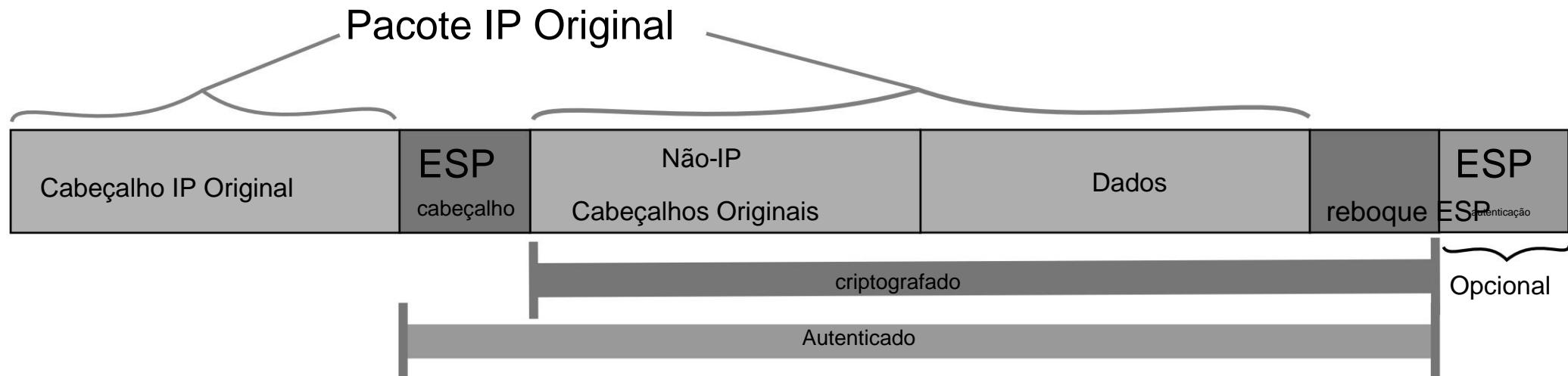


- modo túnel

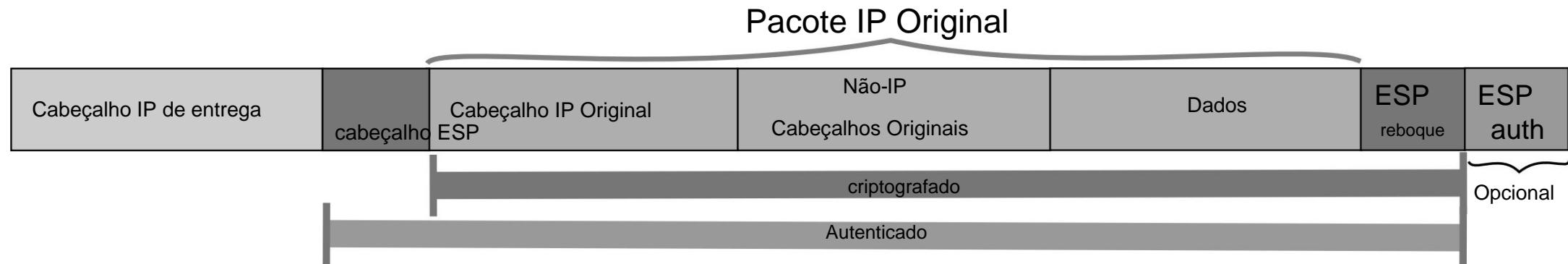


IPSec - Posicionamento do cabeçalho ESP

- Modo de transporte



- modo túnel



Cabeçalho IPsec AH

- Contém cinco campos obrigatórios:

- O campo Next Header é um campo de 8 bits que identifica o tipo da próxima carga após o AH.
- O Payload Length é um campo de 8 bits que especifica o comprimento do cabeçalho (excluindo os primeiros 8 bytes) em unidades de 4 bytes.
- O campo SPI contém o SPI IPsec de saída negociado e é usado pelo ponto remoto para identificar o SA ao qual o pacote pertence.
- O campo Sequence Number é um campo de 32 bits que contém um valor de contador que aumenta em um para cada pacote enviado (usando o mesmo IPsec SA de saída).
- O campo ICV possui um comprimento variável (múltiplo de 32 bits) que contém a saída da função hash de autenticação (ou HMAC baseada em algoritmos de criptografia simétrica) aplicada aos dados/cabeçalhos sob proteção.
 - Pode incluir preenchimento para garantir que o comprimento total do cabeçalho AH seja um múltiplo de 32 bits em IPv4 ou 64 bits em IPv6.



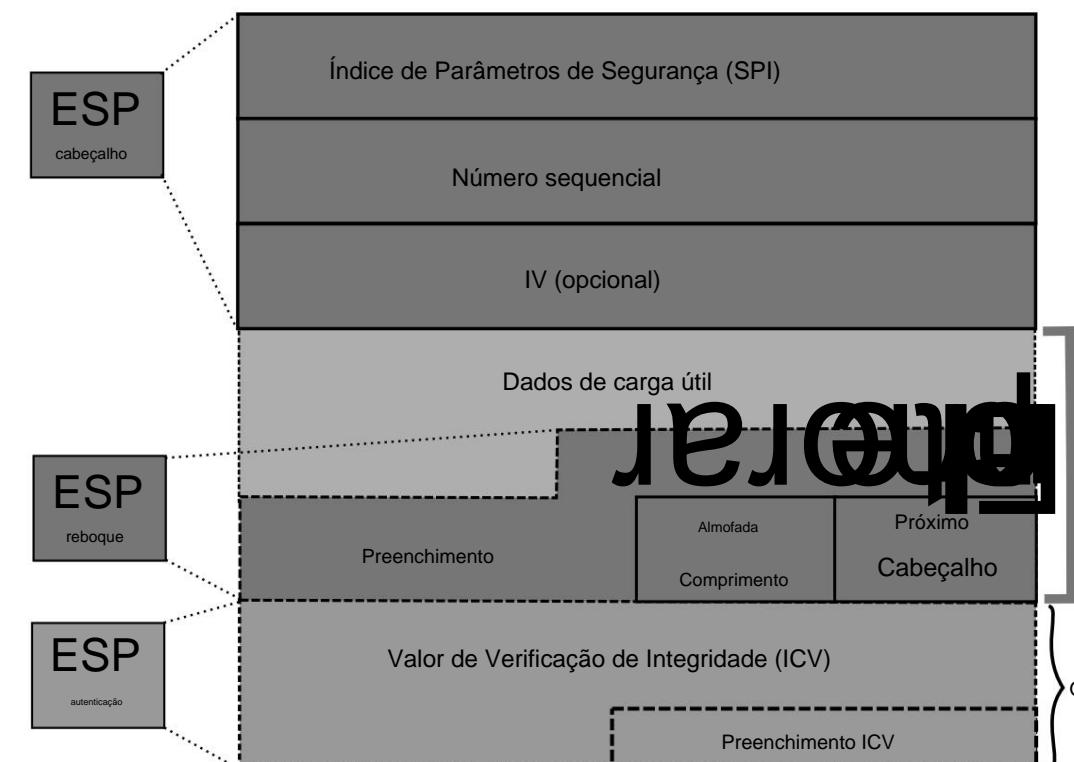
Cabeçalho e trailer do IPsec ESP

- Contém cinco campos obrigatórios:

- O campo SPI contém o SPI IPsec de saída negociado e é usado pelo ponto remoto para identificar o SA ao qual o pacote pertence.
- O campo Sequence Number é um campo de 32 bits que contém um valor de contador que aumenta em um para cada pacote enviado (usando o mesmo IPsec SA de saída).
- O campo Padding pode conter de 0 a 255 zero bytes para garantir: (i) um tamanho de carga útil específico imposto pelo algoritmo de criptografia (por exemplo, tamanho múltiplo do tamanho da cifra de bloco) e (ii) que os campos Pad Length e Next header estão alinhados à direita dentro de uma palavra de 4 bytes.
- O Pad Length é um campo de 8 bits que indica o número de bytes de preenchimento no campo Padding.
- O próximo cabeçalho é um campo de 8 bits que identifica o tipo de dados contidos nos dados de carga útil.

- Pode conter dois campos opcionais:

- Quando o algoritmo de criptografia requer um vetor de inicialização (IV) explícito, esse valor é enviado usando o campo IV.
 - Alguns modos de algoritmo combinam criptografia e integridade em uma única operação.
- O campo do campo ICV tem um comprimento variável que contém a saída da função hash de autenticação (ou HMAC com base em algoritmos de criptografia simétrica) aplicada aos campos de cabeçalho ESP, dados de carga útil e trailer ESP.
 - O campo ICV pode incluir preenchimento.



IPSec - Associações de Segurança

- SAs representam um contrato de política entre dois pares ou hosts
- Descrever como os pares usarão os serviços de segurança IPSec para proteger o tráfego de rede
- Uma SA contém os seguintes parâmetros de segurança:
 - ◆ Algoritmo de autenticação/criptografia, comprimento da chave e outros parâmetros de criptografia (por exemplo, tempo de vida da chave, ...)
 - ◆ Chaves de sessão para autenticação, ou HMACs, e criptografia, que podem ser inseridas manualmente ou negociadas automaticamente Uma especificação do
 - ◆ tráfego de rede ao qual o SA será aplicado (por exemplo, tráfego IP ou apenas sessões TELNET)
 - ◆ Protocolo de encapsulamento IPSec AH ou ESP e túnel ou modo de transporte



Estabelecimento de SA e Criptografia

Chaves

- ISAKMP - Associação de Segurança da Internet e Protocolo de Gerenciamento de Chaves
 - ◆ Usado para estabelecer associações de segurança (SA) e chaves criptográficas
 - ◆ Separe os detalhes do gerenciamento de associações de segurança (e gerenciamento de chaves) dos detalhes da troca de chaves
 - ◆ Fornece uma estrutura para autenticação e troca de chaves, mas não as define
- Protocolo de Determinação de Chave da Oakley
 - ◆ Protocolo de acordo de chave
 - ◆ Permite que pares autenticados troquem material de chave através de uma conexão insegura
 - ◆ Usa Diffie-Hellman
- ESQUEMA
 - ◆ Protocolo de troca de chaves
- IKE - Internet Key Exchange
 - ◆ É um protocolo híbrido
 - ◆ Usa parte da Oakley e parte da SKEME em conjunto com ISAKMP



IKE/ISAKMP e IPsec

- Aprimora o IPSec fornecendo recursos adicionais e flexibilidade
- Fornece autenticação dos pares IPSec, negocia chaves IPSec e negocia associações de segurança IPSec O túnel
- IKE protege as negociações SA. Depois que as SAs estão em vigor, o IPSec protege as vantagens da
 - ◆ Elimina a necessidade de especificar manualmente os parâmetros de segurança IPSec em ambos os pares
 - ◆ Permite que os administradores especifiquem um tempo de vida para a associação de segurança IPSec
 - ◆ Permite que as chaves de criptografia mudem durante as sessões IPSec
 - ◆ Permite que o IPSec forneça serviços anti-replay
 - ◆ Permite suporte à autoridade de certificação (CA) para uma implementação IPSec gerenciável e escalável
 - ◆ Permite autenticação dinâmica de pares
- IKE/ISAKMP fornece três métodos para autenticação bidirecional:
 - ◆ Chave pré-compartilhada
 - ◆ (PSK), Assinaturas digitais (RSA-SIG),
 - ◆ Criptografia de chave pública (RSA-ENC).



ISAKMP e IPsec – Fases/Modos

- Os modos ISAKMP controlam uma compensação entre eficiência e segurança durante a troca inicial de chaves
- Fase 1

- Os pares concordam com um conjunto de parâmetros a serem usados para autenticar os pares e criptografar uma parte das trocas da fase 1 e todas as trocas da fase 2, autenticar os pares e gerar chaves para serem usadas como material de geração de chaves.

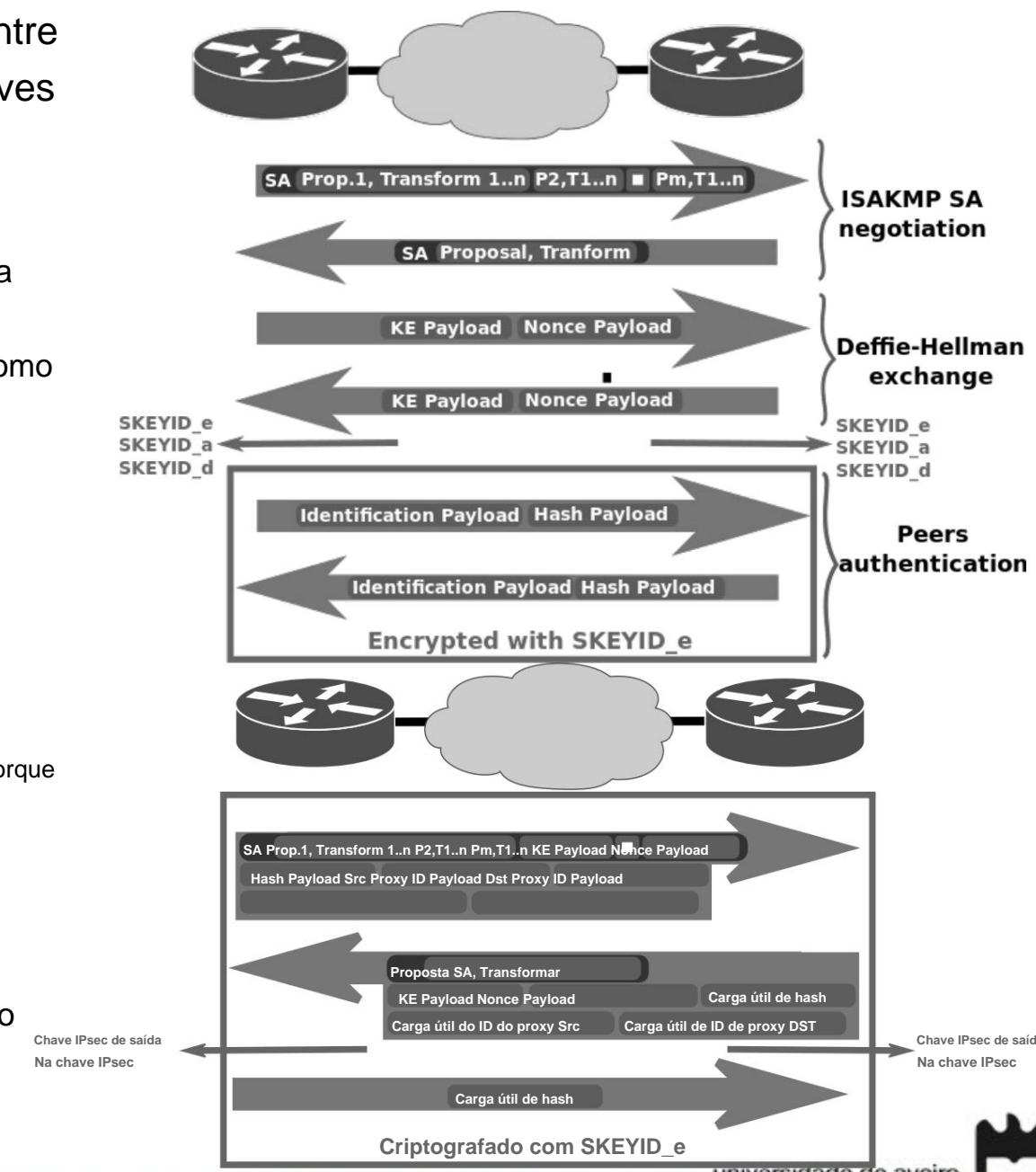
- Modo principal

- Requer seis pacotes de ida e volta
- Fornece segurança completa durante o estabelecimento de uma conexão IPsec
- O modo agressivo é uma alternativa ao modo principal

- Usa metade das trocas, mas oferece menos segurança porque algumas informações são transmitidas em texto não criptografado

- Fase 2 - Modo rápido

- Os pares negociam e concordam com os parâmetros necessários para estabelecer um serviço de comunicação IPsec totalmente funcional.



Troca de pacotes IPsec

No.	Time	Source	Destination	Protocol	Length	Info
12	12.259744000	2001:a:a::2	2001:a:a::1	ISAKMP	146	Identity Protection (Main Mode)
13	12.293700000	2001:a:a::1	2001:a:a::2	ISAKMP	146	Identity Protection (Main Mode)
14	12.330320000	2001:a:a::2	2001:a:a::1	ISAKMP	298	Identity Protection (Main Mode)
15	12.364351000	2001:a:a::1	2001:a:a::2	ISAKMP	318	Identity Protection (Main Mode)
16	12.481540000	2001:a:a::2	2001:a:a::1	ISAKMP	170	Identity Protection (Main Mode)
17	12.496192000	2001:a:a::1	2001:a:a::2	ISAKMP	138	Identity Protection (Main Mode)
18	12.542122000	2001:a:a::2	2001:a:a::1	ISAKMP	250	Quick Mode
19	12.556571000	2001:a:a::1	2001:a:a::2	ISAKMP	250	Quick Mode
20	12.582568000	2001:a:a::2	2001:a:a::1	ISAKMP	114	Quick Mode
21	15.425134000	2001:a:a::2	2001:a:a::1	ESP	322	ESP (SPI=0xb26693bc)
22	15.440166000	2001:a:a::1	2001:a:a::2	ESP	202	ESP (SPI=0x328b3017)

```

▶ Frame 21: 322 bytes on wire (2576 bits), 322 bytes captured (2576 bits) on interface 0
▶ Ethernet II, Src: c2:04:62:06:00:00 (c2:04:62:06:00:00), Dst: ca:06:73:90:00:08 (ca:06:73:90:00:08)
▶ Internet Protocol Version 6, Src: 2001:a:a::2 (2001:a:a::2), Dst: 2001:a:a::1 (2001:a:a::1)
▽ Encapsulating Security Payload
  ESP SPI: 0xb26693bc (2993066940)
  ESP Sequence: 10

```

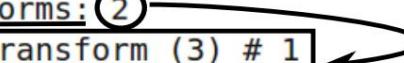


ISAKMP (fase 1) Primeira mensagem

```

▷ Internet Protocol Version 4, Src: 200.2.2.2 (200.2.2.2), Dst: 200.1.1.1 (200.1.1.1)
▷ User Datagram Protocol, Src Port: 500 (500), Dst Port: 500 (500)
▽ Internet Security Association and Key Management Protocol
    Initiator SPI: 06ba66b161c0b75d
    Responder SPI: 0000000000000000
    Next payload: Security Association (1)
▷ Version: 1.0
    Exchange type: Identity Protection (Main Mode) (2)
▷ Flags: 0x00
    Message ID: 0x00000000
    Length: 204
▽ Type Payload: Security Association (1)
    Next payload: Vendor ID (13)
    Payload length: 96
    Domain of interpretation: IPSEC (1)
▷ Situation: 00000001
▽ Type Payload: Proposal (2) # 1
    Next payload: NONE / No Next Payload (0)
    Payload length: 84
    Proposal number: 1
    Protocol ID: ISAKMP (1)
    SPI Size: 0
    Proposal transforms: 2
        ▷ Type Payload: Transform (3) # 1
        ▷ Type Payload: Transform (3) # 2
    ▷ Type Payload: Vendor ID (13) : RFC 3947 Negotiation of NAT-Traversal in the IKE
    ▷ Type Payload: Vendor ID (13) : draft-ietf-ipsec-nat-t-ike-07
    ▷ Type Payload: Vendor ID (13) : draft-ietf-ipsec-nat-t-ike-03
    ▷ Type Payload: Vendor ID (13) : draft-ietf-ipsec-nat-t-ike-02\n

```




ISAKMP (fase 1) Segunda mensagem

```
▷ Internet Protocol Version 4, Src: 200.1.1.1 (200.1.1.1), Dst: 200.2.2.2 (200.2.2.2)
▷ User Datagram Protocol, Src Port: 500 (500), Dst Port: 500 (500)
▽ Internet Security Association and Key Management Protocol
    Initiator SPI: 06ba66b161c0b75d
    Responder SPI: 48aa62bdcb19e9e3
    Next payload: Security Association (1)
    ▷ Version: 1.0
        Exchange type: Identity Protection (Main Mode) (2)
    ▷ Flags: 0x00
        Message ID: 0x00000000
        Length: 104
    ▷ Type Payload: Security Association (1)
        Next payload: Vendor ID (13)
        Payload length: 56
        Domain of interpretation: IPSEC (1)
    ▷ Situation: 00000001
    ▷ Type Payload: Proposal (2) # 1
        Next payload: NONE / No Next Payload (0)
        Payload length: 44
        Proposal number: 1
        Protocol ID: ISAKMP (1)
        SPI Size: 0
        Proposal transforms: 1
            ▷ Type Payload: Transform (3) # 1
    ▷ Type Payload: Vendor ID (13) : RFC 3947 Negotiation of NAT-Traversal in the IKE
```



ISAKMP (fase 1) Terceiro e Quarto mensagens

```

    ▷ Internet Protocol Version 4, Src: 200.2.2.2 (200.2.2.2), Dst: 200.1.1.1
    ▷ User Datagram Protocol, Src Port: 500 (500), Dst Port: 500 (500)
    ▷ Internet Security Association and Key Management Protocol
        Initiator SPI: 06ba66b161c0b75d
        Responder SPI: 48aa62bdcb19e9e3
        Next payload: Key Exchange (4)
    ▷ Version: 1.0
        Exchange type: Identity Protection (Main Mode) (2)
    ▷ Flags: 0x00
    Message ID: 0x00000000
    Length: 276
    ▷ Type Payload: Key Exchange (4)
        Next payload: Nonce (10)
        Payload length: 132
        Key Exchange Data: 6b90894c1593b8ddda8d321a05af8075
    ▷ Type Payload: Nonce (10)
        Next payload: Vendor ID (13)
        Payload length: 24
        Nonce DATA: 21edc1d7ee9a9a51d9d8a0fcccl012ff9d58a348
    ▷ Type Payload: NAT-D (RFC 3947) (20)
    ▷ Type Payload: NAT-D (RFC 3947) (20)

    ▷ Internet Protocol Version 4, Src: 200.1.1.1 (200.1.1.1), Dst: 200.2.2.2
    ▷ User Datagram Protocol, Src Port: 500 (500), Dst Port: 500 (500)
    ▷ Internet Security Association and Key Management Protocol
        Initiator SPI: 06ba66b161c0b75d
        Responder SPI: 48aa62bdcb19e9e3
        Next payload: Key Exchange (4)
    ▷ Version: 1.0
        Exchange type: Identity Protection (Main Mode) (2)
    ▷ Flags: 0x00
    Message ID: 0x00000000
    Length: 296
    ▷ Type Payload: Key Exchange (4)
        Next payload: Nonce (10)
        Payload length: 132
        Key Exchange Data: 820d0eafec6260bc958a60d1d086e6ec823032774f16c316...
    ▷ Type Payload: Nonce (10)
        Next payload: Vendor ID (13)
        Payload length: 24
        Nonce DATA: 0f37423fb10f422983fcf0d9dcab26a5b8be59aa
    ▷ Type Payload: NAT-D (RFC 3947) (20)
    ▷ Type Payload: NAT-D (RFC 3947) (20)

```

ISAKMP (fase 1) Quinto e Sexto mensagens

- ▷ Internet Protocol Version 4, Src: 200.2.2.2 (200.2.2.2), Dst: 200.1.1.1
- ▷ User Datagram Protocol, Src Port: 500 (500), Dst Port: 500 (500)
- ▽ Internet Security Association and Key Management Protocol
 - Initiator SPI: 06ba66b161c0b75d
 - Responder SPI: 48aa62bdcb19e9e3
 - Next payload: Identification (5)
 - ▷ Version: 1.0
 - Exchange type: Identity Protection (Main Mode) (2)
 - ▷ Flags: **0x01**
 - Message ID: 0x00000000
 - Length: 92
 - Encrypted Data (64 bytes)**

- ▷ Internet Protocol Version 4, Src: 200.1.1.1 (200.1.1.1), Dst: 200.2.2.2
- ▷ User Datagram Protocol, Src Port: 500 (500), Dst Port: 500 (500)
- ▽ Internet Security Association and Key Management Protocol
 - Initiator SPI: 06ba66b161c0b75d
 - Responder SPI: 48aa62bdcb19e9e3
 - Next payload: Identification (5)
 - ▷ Version: 1.0
 - Exchange type: Identity Protection (Main Mode) (2)
 - ▷ Flags: **0x01**
 - Message ID: 0x00000000
 - Length: 68
 - Encrypted Data (40 bytes)**



Mensagem ISAKMP (fase 2)

- ▷ User Datagram Protocol, Src Port: 500 (500), Dst Port: 500 (500)
- ▽ Internet Security Association and Key Management Protocol
 - Initiator SPI: 06ba66b161c0b75d
 - Responder SPI: 48aa62bdcb19e9e3
 - Next payload: Hash (8)
 - ▷ Version: 1.0
 - Exchange type: Quick Mode (32)
 - ▷ Flags: 0x01
 - Message ID: 0x5277ae21
 - Length: 220
 - Encrypted Data

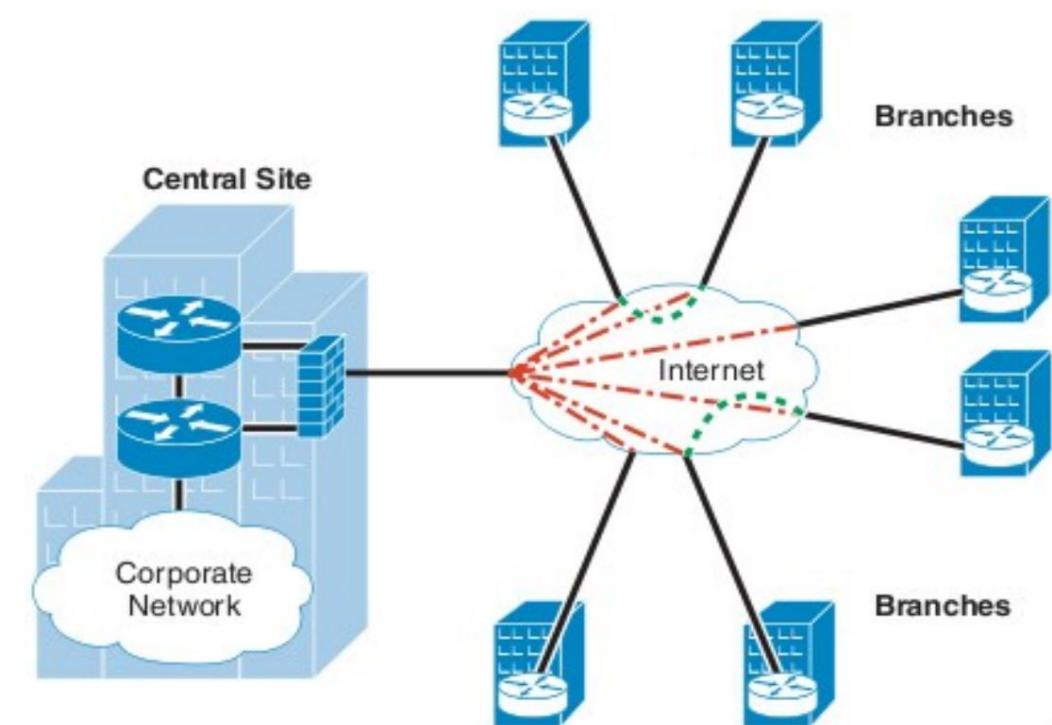
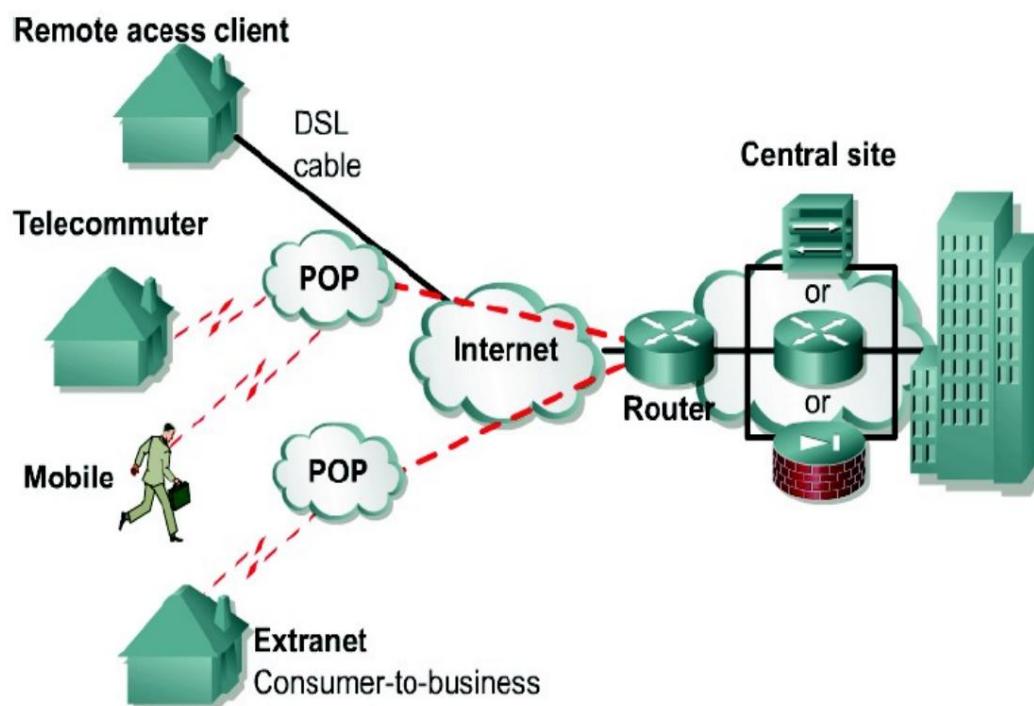


Redes Privadas Virtuais (VPN)



VPN - Redes Privadas Virtuais

- É uma conexão criptografada entre redes privadas em uma rede pública



- VPN de acesso remoto

- VPN site a site



tipos de VPN

- VPN de acesso remoto
 - ◆ PPTP
 - ◆ L2TP/IPsec
 - ◆ VPN SSL/TLS
 - Web VPN (SSL VPN sem cliente) – o cliente VPN pode ser um navegador padrão
 - ◆ VPN SSH
 - ◆ VPN aberta
- VPN site a site
 - ◆ VPN IPsec
 - Com configuração estática ou dinâmica
 - ◆ IPsec + GRE VPN
 - VPN Multiponto Dinâmica



VPN de acesso remoto - VPN PPTP

- Baseado em PPTP
 - ◆ Dados de pacotes PPTP dentro de pacotes PPP
 - ◆ Encapsula os pacotes PPP dentro dos pacotes IP
- Usa uma forma de encapsulamento de roteamento geral (GRE) para obter dados de e para seu destino final
- Suporta autenticação baseada em protocolos PAP, EAP, CHAP, MS CHAPv1 e MS-CHAPv2
- Usa MPPE como cifra
 - ◆ Tem duas chaves diferentes (uma para cada direção)
 - ◆ Requer autenticação MS-CHAPv2
 - ◆ Chaves derivadas do hash de senha e desafios do MS-CHAPv2
- O PPTP cria uma conexão de controle TCP entre o cliente VPN e Servidor VPN para estabelecer um túnel
 - ◆ Usa a porta TCP 1723 para essas conexões
- O PPTP pode suportar apenas um túnel por vez para cada usuário



VPN de acesso remoto - L2TP/IPSec VPN

- Autenticação pode ser realizada com Certificados Digitais (RSA) ou com os mesmos mecanismos de autenticação PPP que PPTP
- Fornece integridade de dados, autenticação de origem e proteção de replay
- Criptografia fornecida por IPSec (protocolo ESP)
- Pode suportar vários túneis simultâneos para cada usuário
- Desempenho mais lento que PPTP



Outros tipos de VPN de acesso remoto

- **VPN SSL/TLS**

- O protocolo SSL/TLS lida com a criação do túnel VPN
- SSL/TLS é muito mais fácil de implementar do que IPSec e fornece uma plataforma simples e bem testada
- O handshake RSA (ou DH) é usado exatamente como IKE no IPSec

- **VPN SSH**

- VPN sobre uma conexão SSH
- Tunelamento SSH - encaminhamento de porta

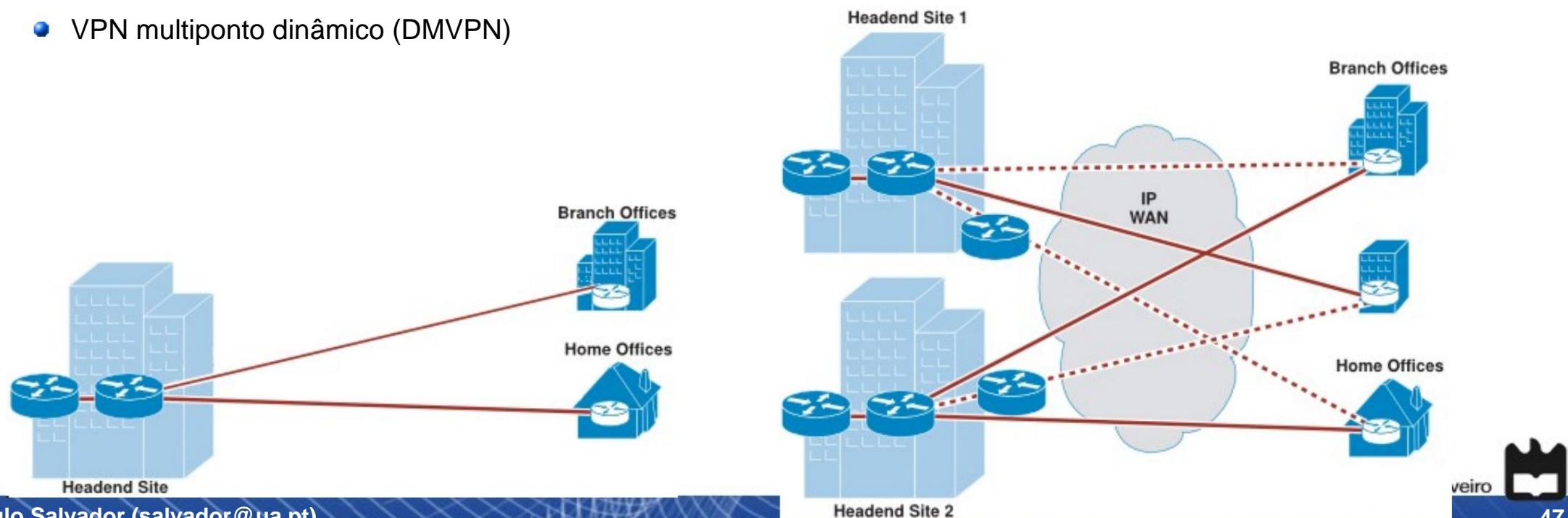
- **OpenVPN**

- Implementa uma VPN SSL/TLS
- Permite PSK, certificado e autenticação baseada em login/senha
- Criptografia fornecida por OpenSSL (pode usar todas as cifras disponíveis)
- Compatível com endereços dinâmicos e NAT



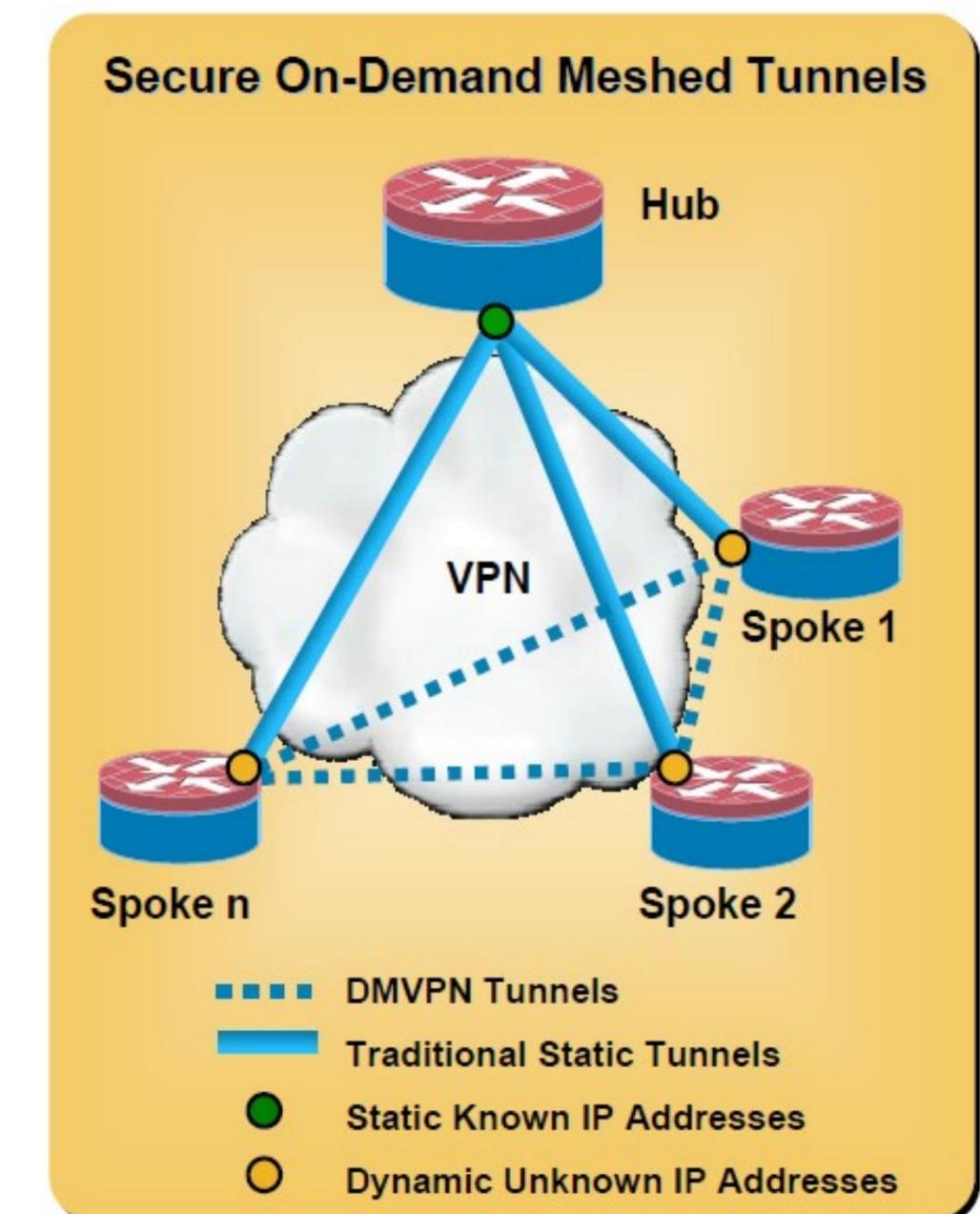
Variantes de VPN IPsec Site-to-Site

- Túneis IPsec com configuração estática
 - ◆ Requer o conhecimento de todos os pares (endereços IP e parâmetros de segurança)
 - ◆ Alta sobrecarga de configuração
- Túneis IPsec com configuração dinâmica (no headend/hub)
 - ◆ Hub + configuração de raios
 - ◆ Configuração genérica no headend/hub
 - ◆ Fácil de adicionar novos raios
- ⇒ Um túnel IPsec básico não pode proteger o tráfego multicast.
- Túneis IPsec + GRE
 - ◆ Generic Routing Encapsulation (GRE) permite a proteção do tráfego multicast sobre IPsec
- VPN multiponto dinâmico (DMVPN)

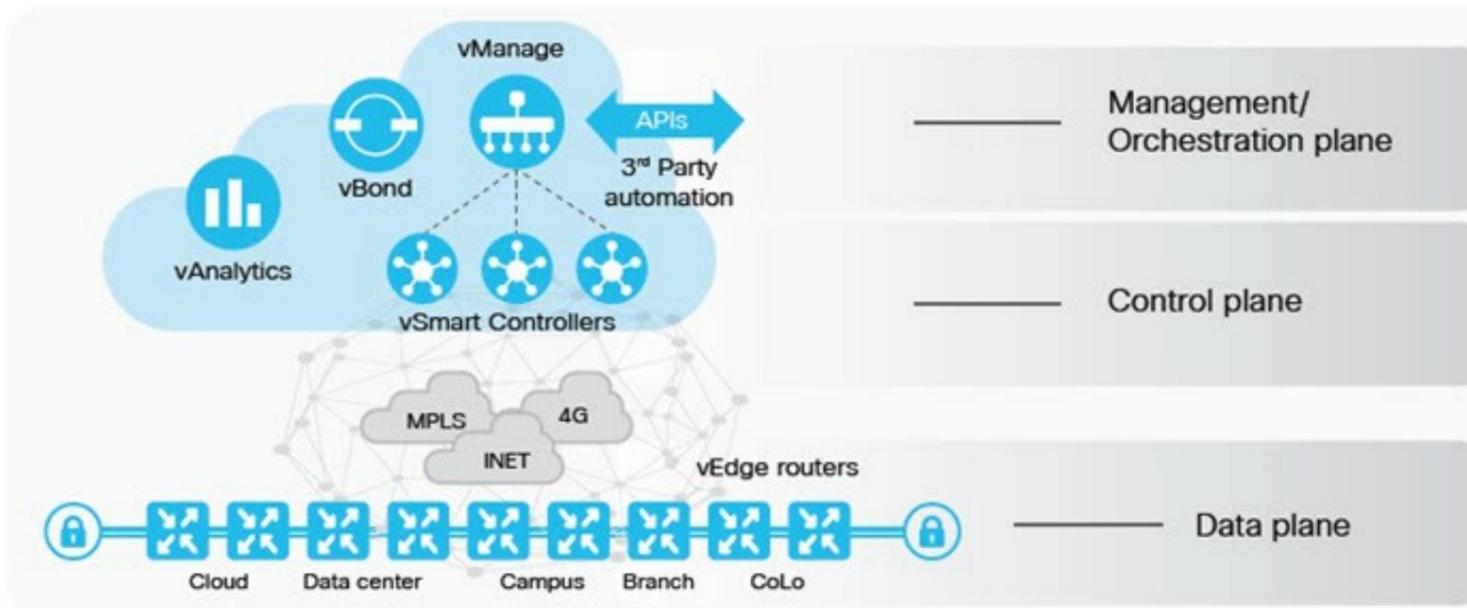


VPN Multiponto Dinâmica

- Depende do NHRP para criar uma rede de sobreposição
- Fornece conectividade em malha completa com configuração simples de hub e spoke
- Suporta raios endereçados dinamicamente
- Facilita a configuração sem toque para adição de novos raios
- Apresenta acionamento automático de IPsec para construir um túnel IPsec



SD-WAN



• WAN definida por software

- ◆ Abstração de Conectividade de Borda.
- ◆ Virtualização WAN.
- ◆ Gerenciamento centralizado e orientado por políticas.
- ◆ Gerenciamento de tráfego elástico.
- ◆ Vantagens: Fácil implantação e gerenciamento.
- ◆ Desvantagens: Dependência total (presente e futura) de provedores externos.



Acesso remoto

Segurança em Redes de Comunicações

Mestrado em Cibersegurança

**Mestrado em Engenharia de Computadores e
telemática**

DETI-UA



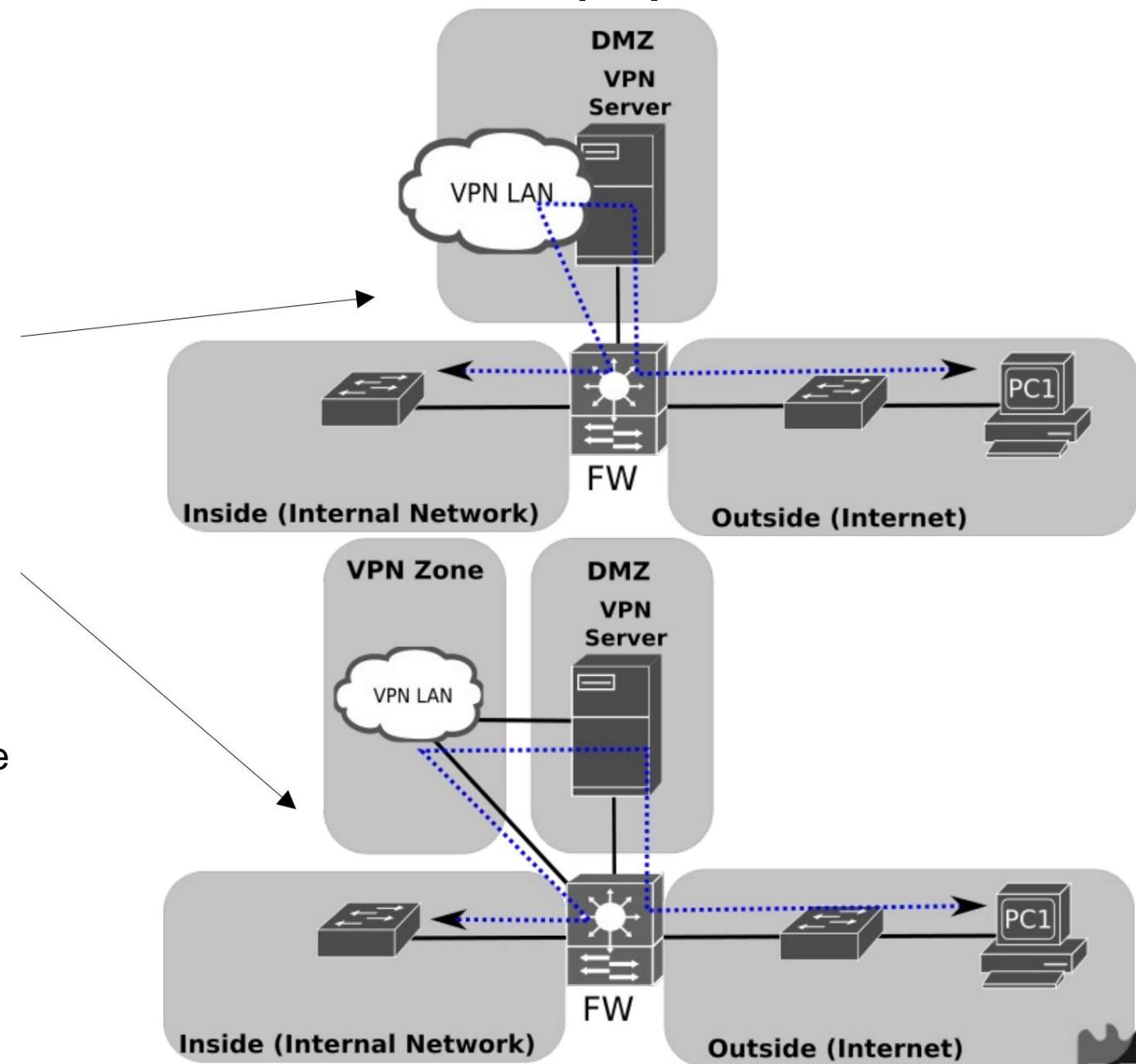
Acesso Remoto (1)

- Servidores/protocolos mais comuns
 - ◆ L2TP IPsec
 - ◆ IKE+ISAKMP+L2TP
 - ◆ OpenVPN
 - ◆ SSL
 - ◆ Baseado em
 - ◆ SSL ou IPSec proprietário .
- Autenticação
 - ◆ tipos
 - ◆ Pré-compartilhado
 - ◆ RAIO/LDAP
 - ◆ RSA com CA incorporado
 - ◆ RSA com CA externa
 - ◆ Certificados/Credenciais devem ser distribuídos com segurança
 - ◆ Web service, SSH, ...



Acesso Remoto (2)

- Servidor implantado em Firewalls.
- Servidor em DMZ.
 - ◆ Tráfego roteado de volta para o firewall usando a mesma zona.
 - ◆ Tráfego roteado de volta para o firewall usando uma interface de rede e zona diferentes.
 - ◆ Tráfego roteado diretamente para a zona privada.
 - Quebra o conceito de zona.



IPsec NAT Transversal

- Incompatibilidades de NAT/PAT com IPsec
 - ◆ O cabeçalho AH incorpora os endereços IP de origem e destino na verificação de integridade da mensagem codificada. ESP não é um problema.
 - ◆ As somas de verificação TCP e UDP podem ser atualizadas porque são protegidas por IPsec.
 - ◆ Os endereços IP podem ser usados como identificadores no Internet Key Exchange para determinar as credenciais.
- Durante a primeira fase do ISAKMP IPsec, os hosts (quando configurados e suportados) detectam que o NAT transversal deve ser ativado
 - ◆ Os pacotes subsequentes da primeira fase e da segunda fase do ISAKMP são encapsulados em pacotes UDP.
 - ◆ Normalmente porta UDP 4500.
 - ◆ O endereço IP original é enviado como cargas NAT-OA (endereço original NAT) do ISAKMP.



Integração com controle de fluxo

- Regras de serviço/protocolo OpenVPN
 - ◆ Porta UDP
 - usada.
 - Normalmente porta UDP 1194.
 - ◆ IPsec
 - Porta UDP 500 para IKE.
 - Protocolo IP número 50 (ESP).
 - Protocolo IP número 51 (AH).
 - Porta UDP 4500 para passagem NAT.
 - ◆ L2TP
 - porta UDP 1701.
 - A exceção pode não ser necessária quando o L2TP é encapsulado em pacotes IPsec.
 - Regras dos fluxos do usuário
 - ◆ Os usuários remotos recebem um endereço de rede IP.
 - ◆ Controle de fluxo baseado em endereço IP ou zona.



Detecção de Intrusão e Prevenção

Segurança em Redes de Comunicações

Mestrado em Cibersegurança

**Mestrado em Engenharia de Computadores e
telemática**

DETI-UA



Detecção e Prevenção de Intrusão

- Sistemas de Detecção de Intrusão (IDS)

- ◆ Monitoramento e identificação de acesso ou manipulação não autorizada do sistema.
- ◆ Analisa informações de várias fontes (computadores, servidores, serviços e tráfego de rede).
- ◆ Identifica:
 - ◆ Invasões, invasor fora da organização; Uso indevido,
 - ◆ comportamento incorreto de um usuário/serviço lícito.
- ◆ Não bloqueia/impede a intrusão.
- ◆ Sinaliza um alarme para:
 - ◆ Análise e intervenção humana;
 - ◆ Respostas automáticas a ameaças por firewalls ou sistemas de gerenciamento centralizado.

- Sistemas de Prevenção de Intrusão (IPS)

- ◆ No nível da rede bloqueia o tráfego; No
- ◆ nível do host mata processos, coloca um arquivo em quarentena, bloqueia o acesso ao dispositivo, etc...



Com base em host vs. com base em rede

- Para proteger servidores específicos ou dispositivos de usuários, o IDS/IPS é implantado no nível do host.
 - ◆ Monitora tráfego, processos, acesso a arquivos, acesso a dispositivos e fluxos de dados, alocações de memória, características físicas do dispositivo (temperatura, consumo de energia, movimento, etc...).
 - ◆ Hoje em dia chamado Endpoint Detection and Response (EDR).
- Para proteger uma organização (todos os dispositivos e serviços), o IDS/IPS é implantado no nível da rede.
 - ◆ Monitora o tráfego nos níveis de pacote e fluxo. Pode monitorar a rede no nível físico (rádio, sinais elétricos e ópticos).
 - ◆ Distribuídos em vários pontos da rede:
 - ◆ Acessos à Internet e WAN;
 - ◆ Links de comunicação entre
 - ◆ zonas; Sem fio.



Assinatura vs. Baseada em Anomalia

- As invasões são detectadas com base em duas abordagens diferentes: Com base em
 - ◆ assinatura: dados
 - monitorados comparados a padrões de ataque pré-configurados e predeterminados, conhecidos como
 - assinaturas; Os ataques têm assinaturas
 - conhecidas distintas; As assinaturas devem ser constantemente atualizadas para mitigar ameaças
 - As assinaturas podem conter:
 - Valores de cabeçalho de pacote individual ou padrões de dados binários,
 - Sequência de pacotes com características específicas dentro de um mesmo fluxo, ou
 - Conjunto de fluxos de dados (fluxo de dados) com características específicas (de fluxos ou pacotes/dados).
 - ◆ Baseado em
 - anomalia: Estabelece uma linha de base de comportamento (perfil) e desvio detectado desse
 - perfil; Pode contar apenas com sistemas de alto nível ou estatísticas de rede ou incluir várias fontes de
 - dados; Pode ser baseado em regras predefinidas ou em modelos de IA.



Detecção e Resposta de Endpoint (EDR)

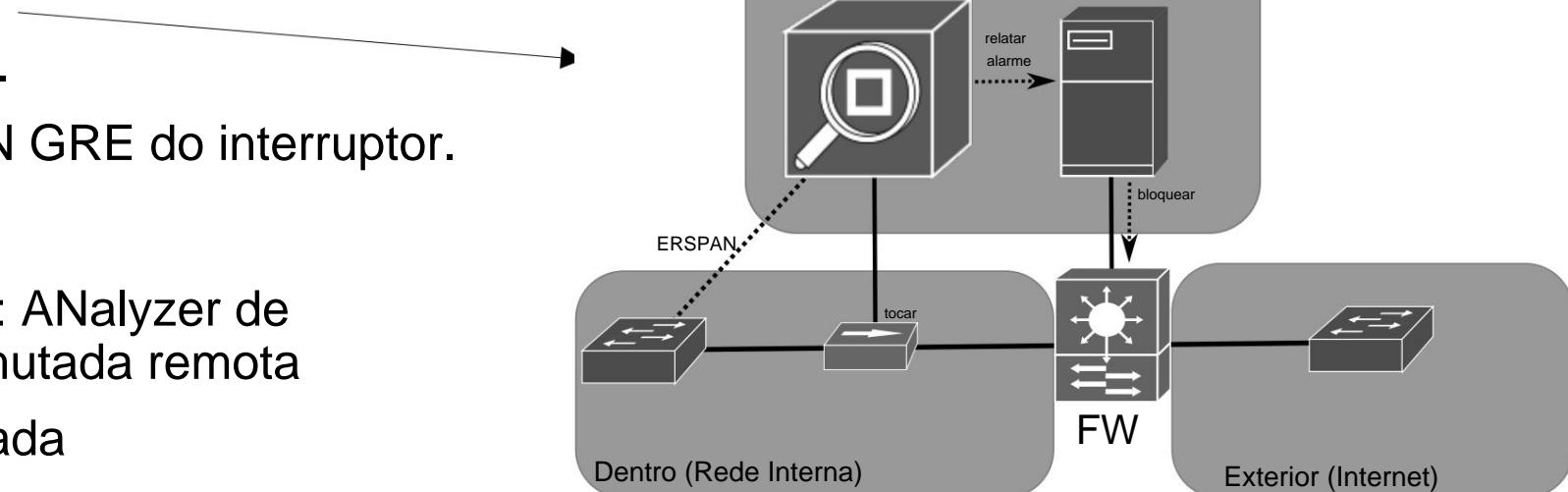
- Referido também como detecção de endpoint e resposta a ameaças (EDTR).
- Monitore, registre e analise as atividades e eventos nos dispositivos.
- Forneça visibilidade contínua e abrangente dos processos dos dispositivos e atividades do usuário.
- Permite uma resposta direta a incidentes em dispositivos/servidores.
- Pode ser totalmente implantado apenas no dispositivo ou com um agente no dispositivo e análise/armazenamento externo de dados.



Implantação de rede (1)

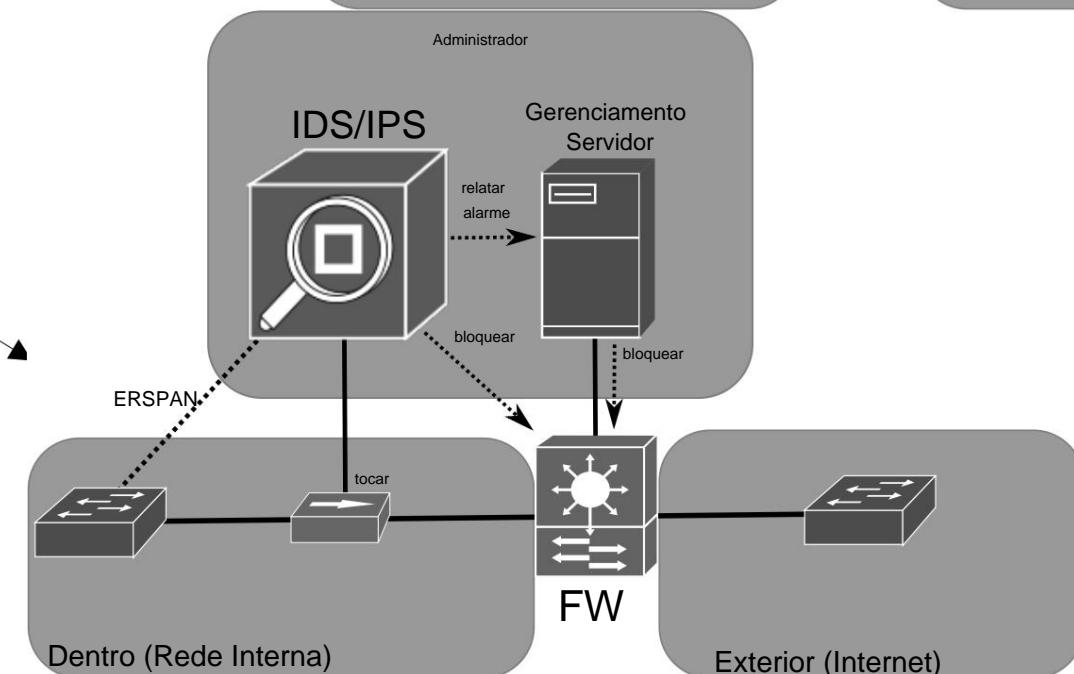
- IDS

- Toque de rede.
- Túnel ERSPAN GRE do interruptor.



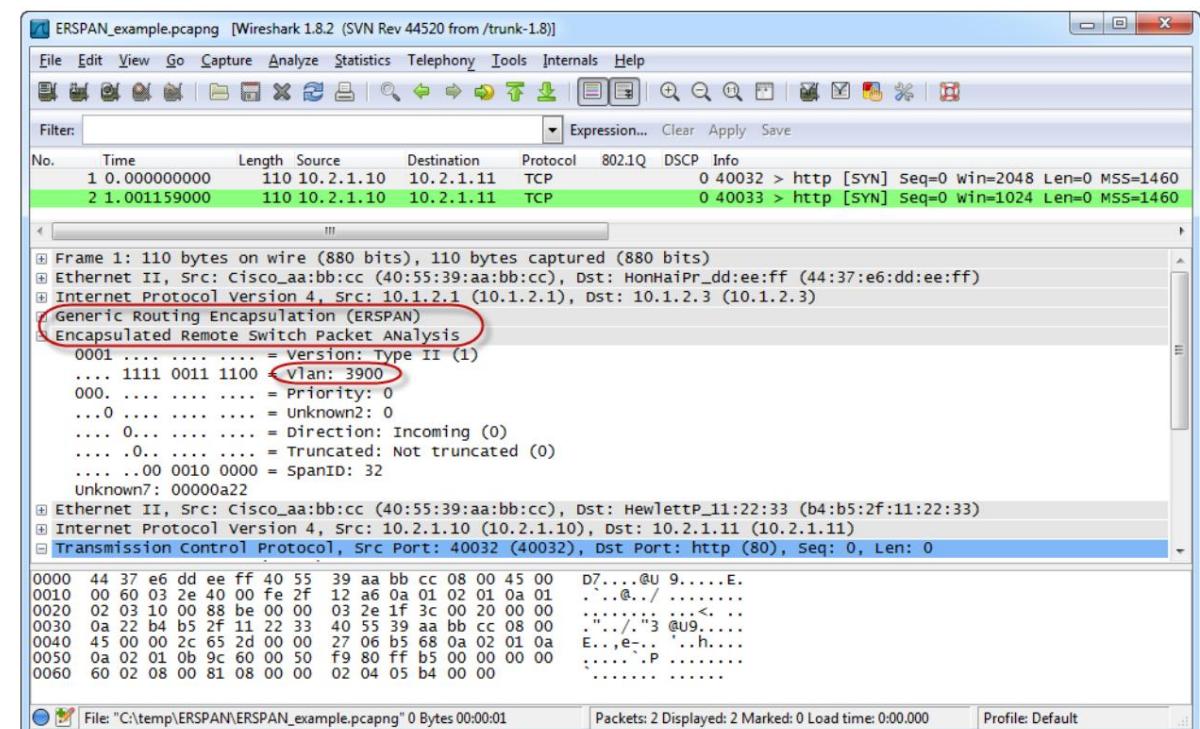
- IPS

- IDS com integração de firewall.



ERSPAN

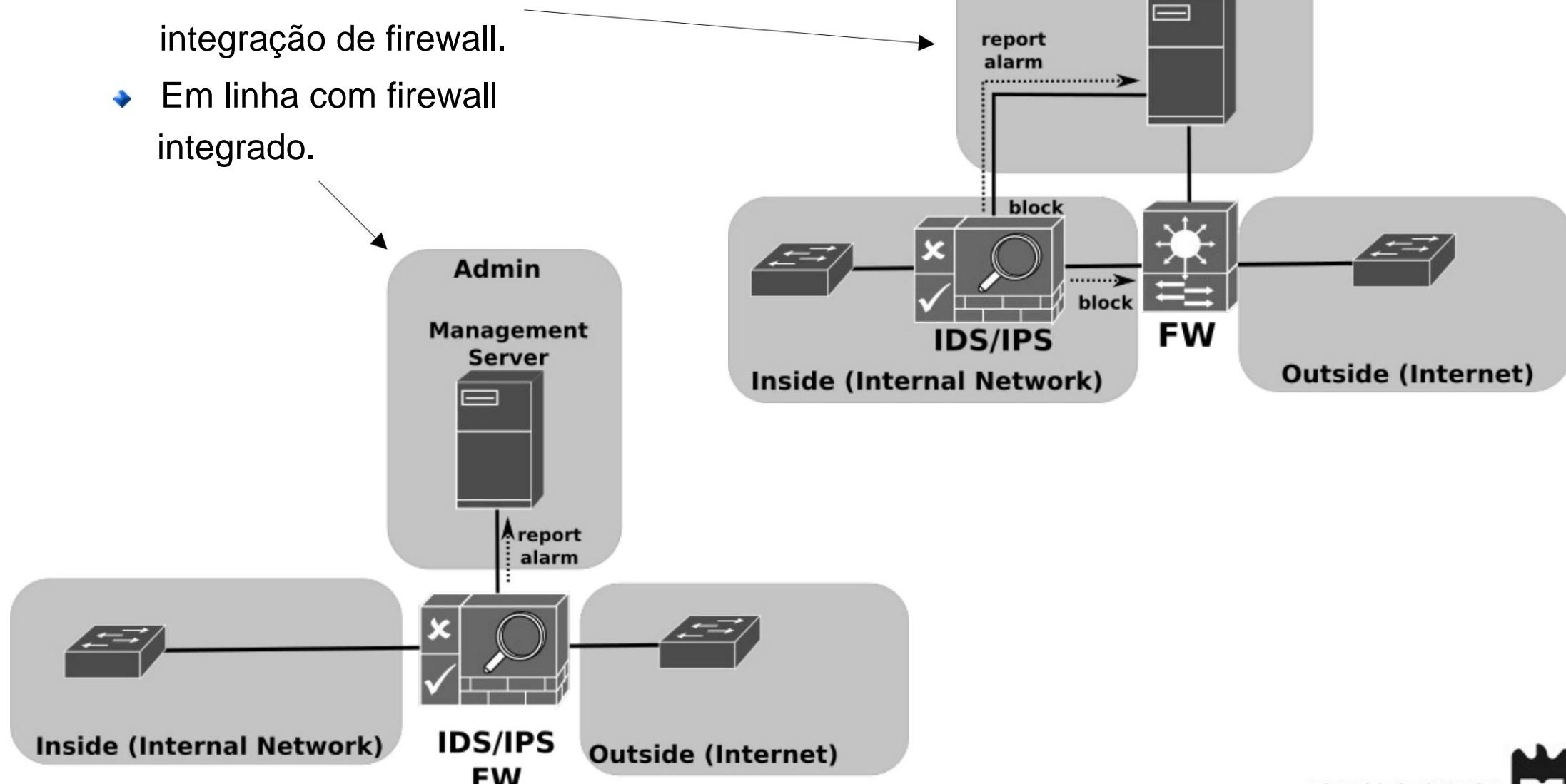
- Significa
“Encapsulated Remote
Switched Port Analyzer”.
- Espelha o tráfego de uma ou
mais portas de switch.
- Envia o tráfego
espelhado para um ou
mais destinos.
- O tráfego é
encapsulado em Generic
Routing Encapsulation (GRE).



Implantação de rede (2)

- IPS

- ◆ Em linha com integração de firewall.
- ◆ Em linha com firewall integrado.



Ações de IDS/IPS

• Suricata

- ◆ alerta - gera um alerta.
- ◆ pass - pare a inspeção adicional do pacote. drop
- ◆ - solta o pacote e gera alerta. rejeitar -
- ◆ enviar erro de não alcance RST/ICMP ao remetente do pacote correspondente.
- ◆ rejeiçãosrc - o mesmo que apenas
- ◆ rejeitar. rejeitado - envia o pacote de erro RST/ICMP para o receptor do pacote
- ◆ correspondente. rejeiçãoboth - envia pacotes de erro RST/ICMP para ambos os lados da conversa.

• bufar

- ◆ alert - gere um alerta usando o método de alerta selecionado e, em seguida, registre o pacote. log - registra
- ◆ o pacote. pass - ignore o pacote.
- ◆ pacote. drop - bloqueeie e registre o pacote.
- ◆ pacote. rejeitar - bloquear o pacote, registrá-lo e enviar uma redefinição de TCP se o protocolo for TCP ou uma mensagem de porta inacessível ICMP se o protocolo for UDP. sdrop - bloqueia o pacote, mas não o registra.



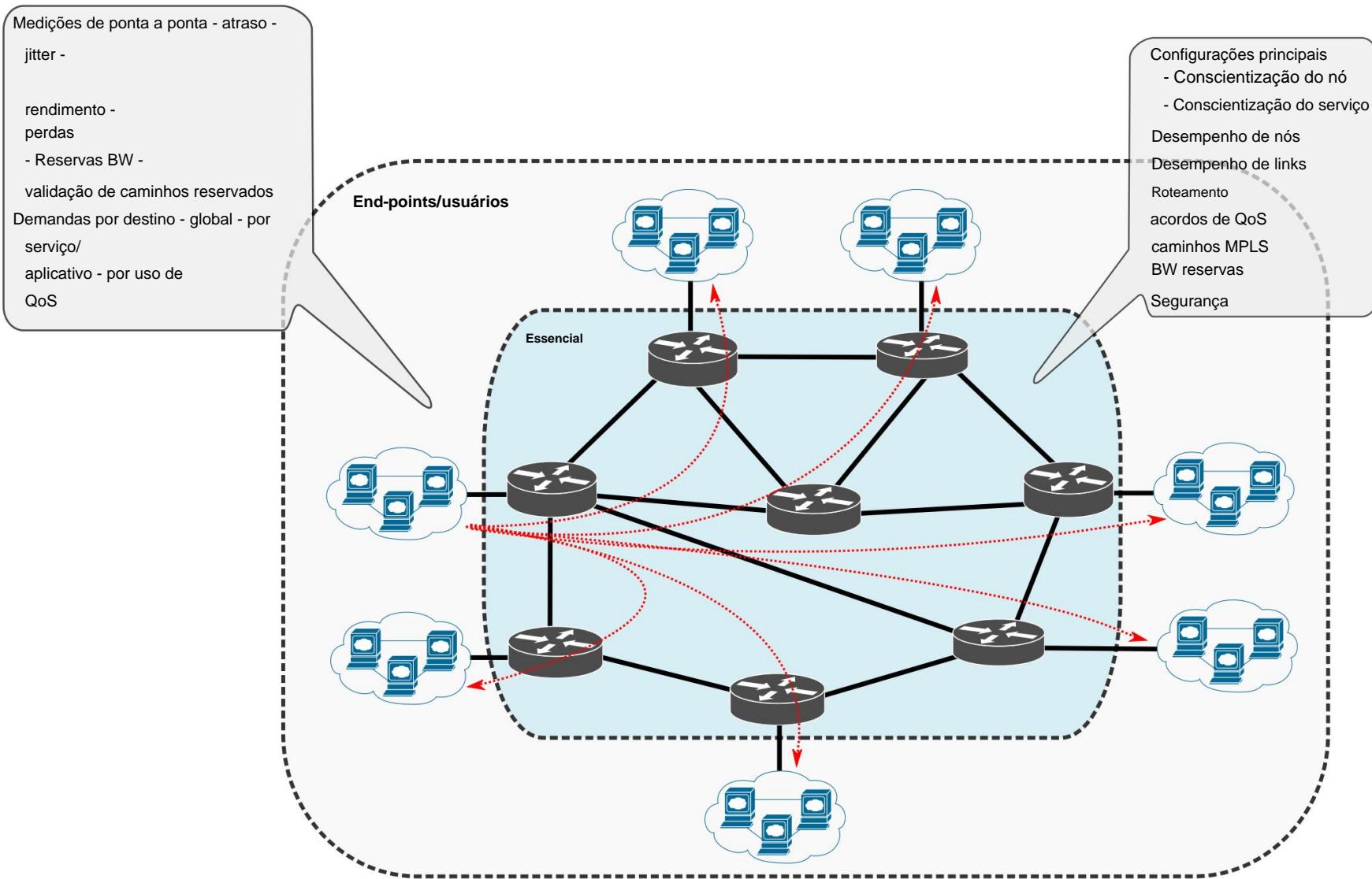
Monitoramento de rede SIEM & SOC

Segurança em Redes de Comunicações

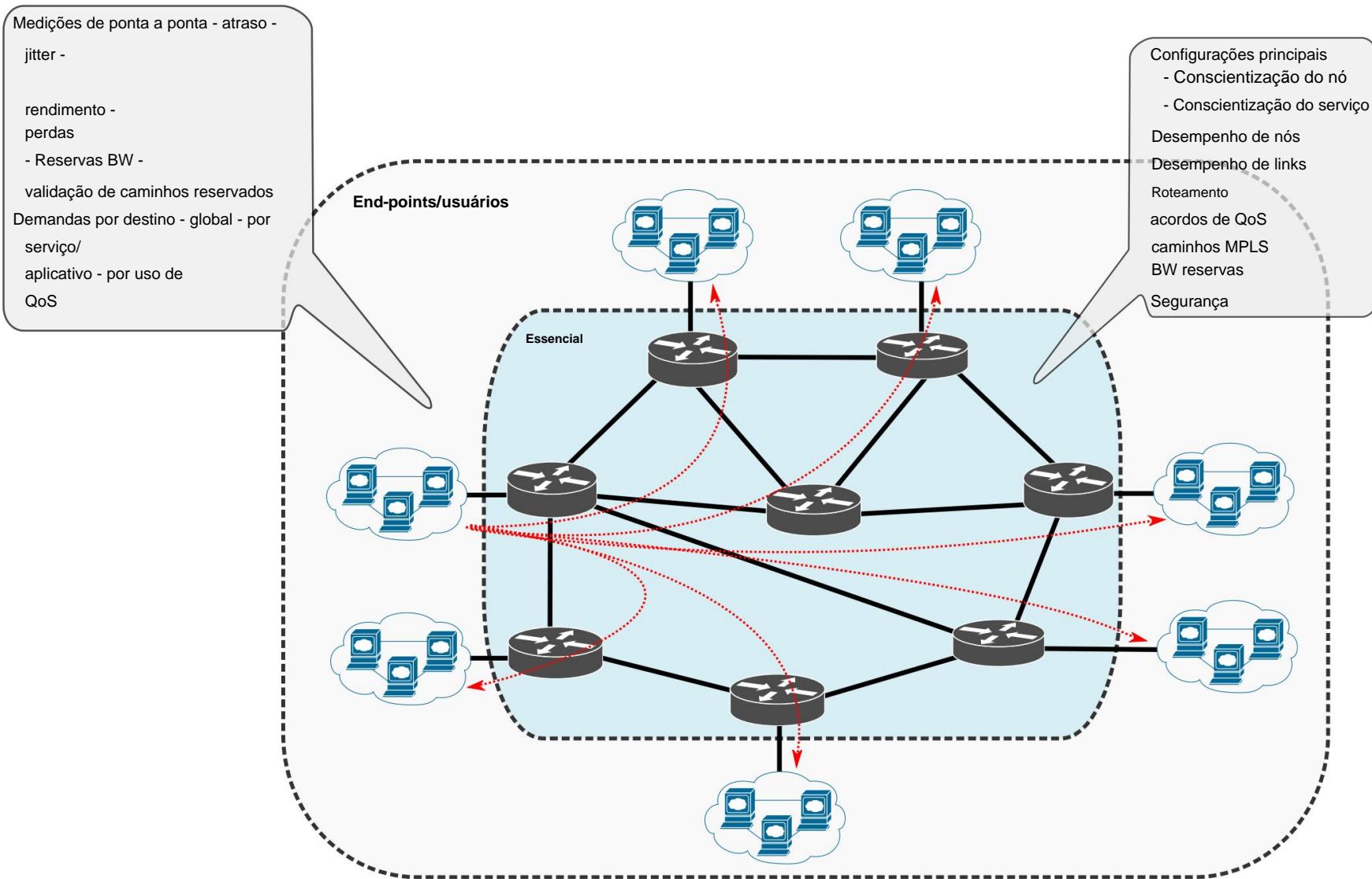
Mestrado em Cibersegurança
Mestrado em Engenharia de Computadores e
telemática
DETI-UA



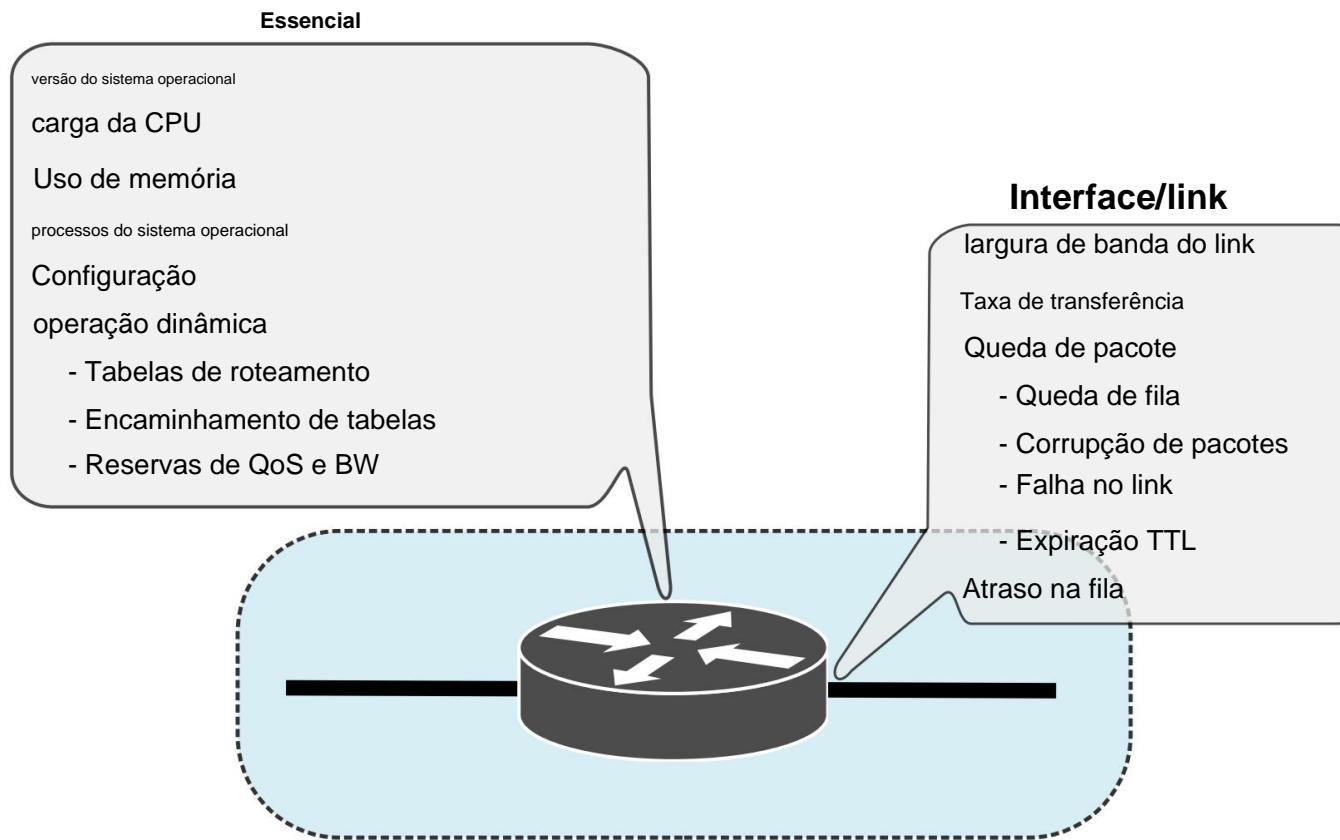
Monitoramento básico e de ponta a ponta



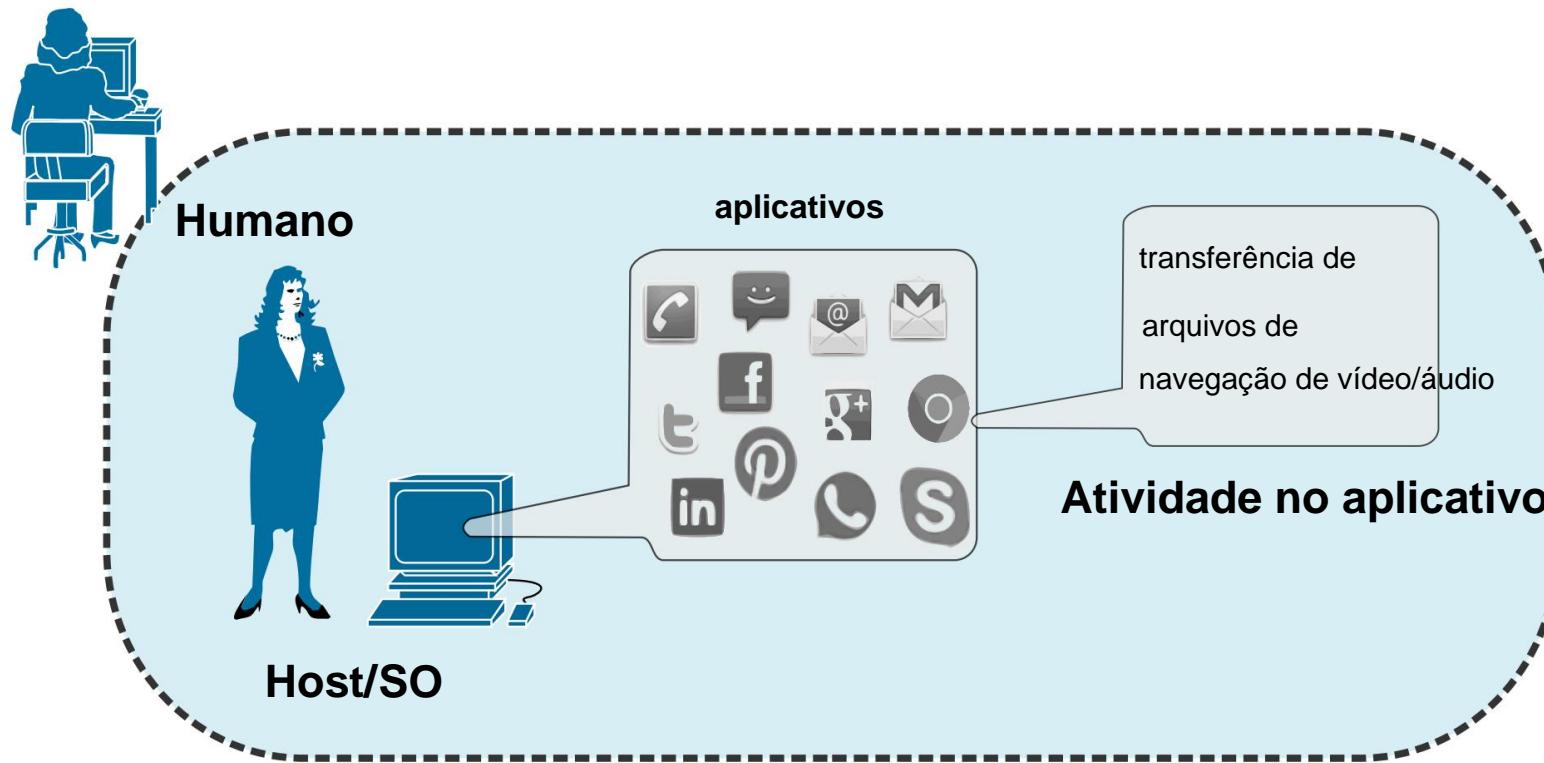
Monitoramento básico e de ponta a ponta



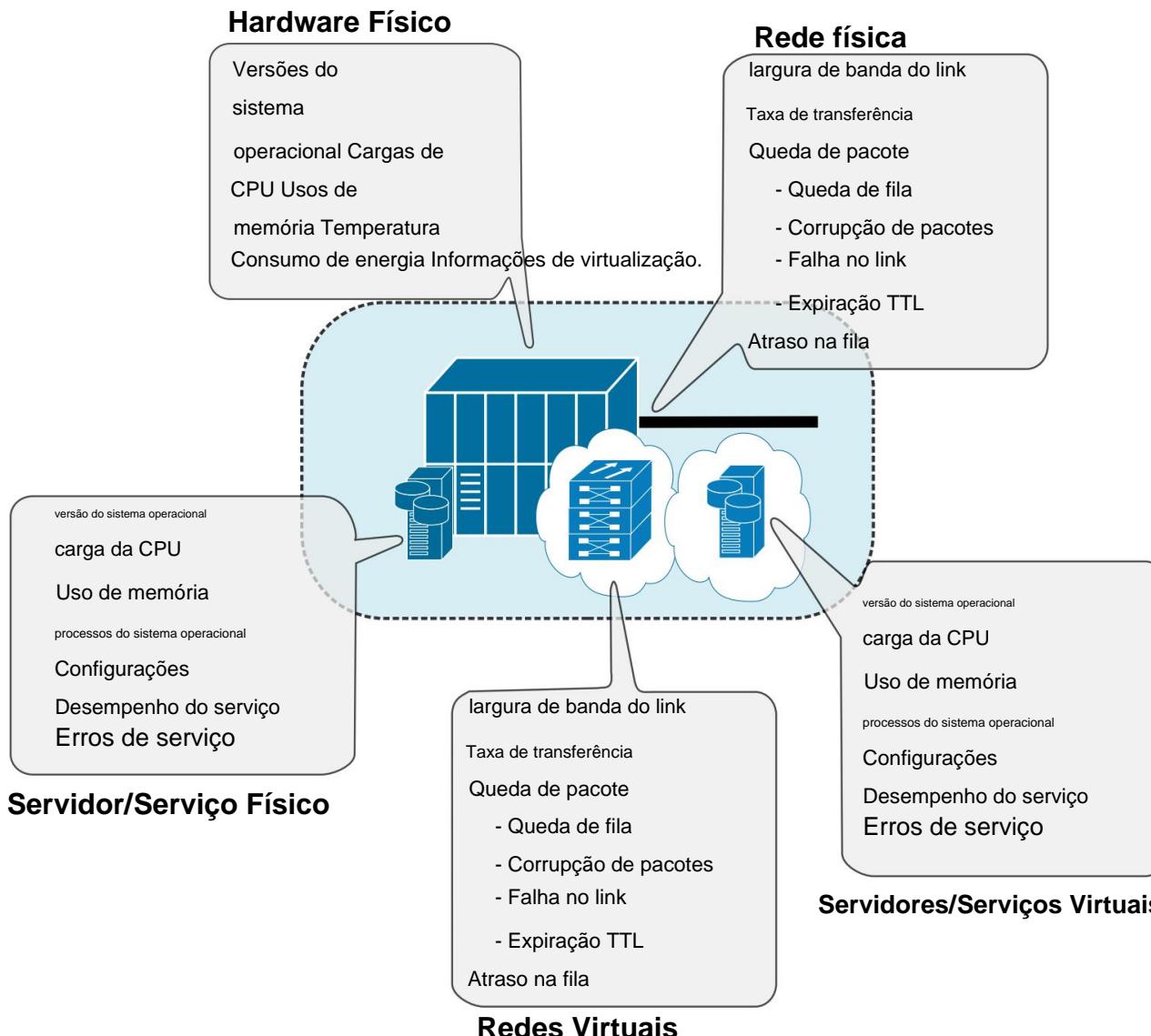
Monitoramento de nós



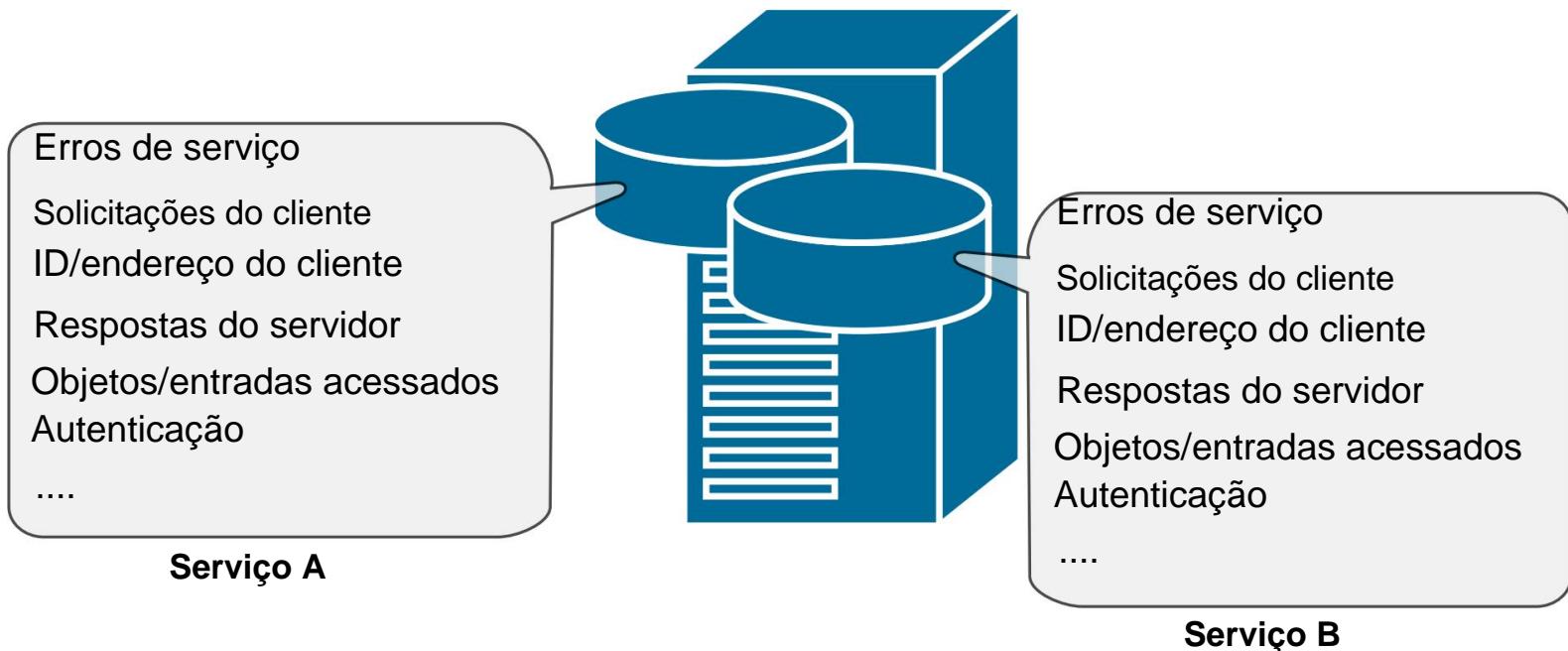
Monitoramento de usuário final/host/aplicativo



Monitoramento de servidor/serviço/nuvem



Monitoramento detalhado por serviço



Fontes de dados

- SNMP
 - ◆ Usado para adquirir conhecimento sobre os estados atuais de nós/links/servidores.
 - ◆ Informações locais. Pode ser usado para extrapolar para informações globais.
 - ◆ (Muitas vezes) Requer o uso de MIBs específicos do fornecedor.

- Exportação de fluxo
 - ◆ Usado para caracterizar usuários/serviços em termos de quantidade de tráfego e destinos de tráfego.
 - ◆ Informações de média e grande escala de tempo.
 - ◆ Protocolos: Cisco NetFlow, IPFIX – Standard, Juniper jFlow e sFlow

- Capturas de pacotes / estatísticas RAW / DPI vs. SPI
 - ◆ Usado para caracterizar usuários/serviços em pequenas escalas de tempo.
 - ◆ Requer sondas dedicadas distribuídas.

- Acessar logs do servidor/dispositivo e/ou acesso CLI.

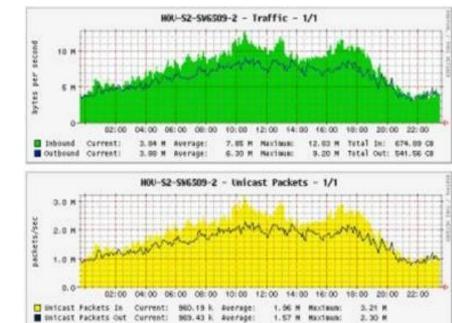
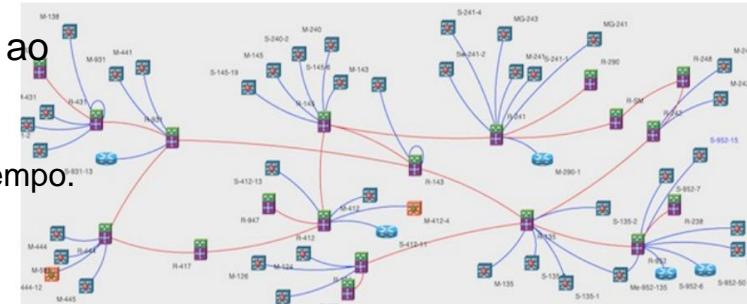
- ◆ Usado para adquirir conhecimento sobre o estado passado e atual.

- Medições ativas
 - ◆ Introduz entropia na rede e requer (para muitas medições) sincronização precisa do relógio
Por exemplo, atraso/jitter unidirecional,
 - ◆ atraso/jitter de ida e volta.



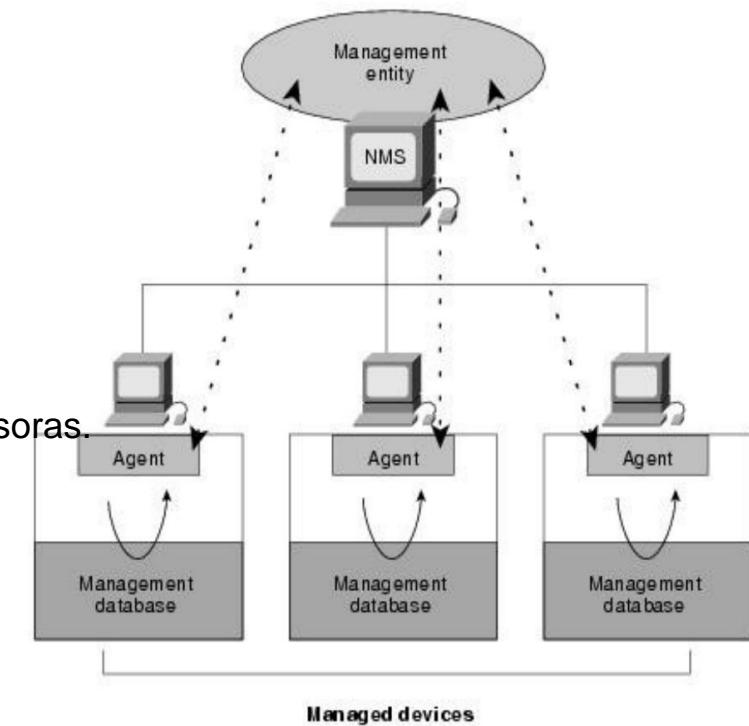
SNMP

- Usado para adquirir o status e uso de nós, links e serviços ao longo do tempo.
 - ◆ Requer extração periódica para obter informações ao longo do tempo.
- Usado para obter:
 - ◆ Elementos de rede e interconexões, serviços implantados em rede.
- Usado para estimar, caracterizar e prever: Desempenho do
 - ◆ fluxo de dados.
 - ➡ Perdas de pacotes e (por inferência indireta) atraso/jitter nos nós.
 - ➡ Permite obter informações sobre o desempenho atual e futuro do serviço ,
 - ◆ desempenho dos nós,
 - ➡ uso de memória/CPU, número de processos, etc...
 - ➡ Permite detectar pontos de falha, nós de degradação do serviço, nós instáveis.
 - ◆ Uso de link de rede,
 - ➡ bytes de entrada/saída e contagem de pacotes.
 - ➡ Permite realizar otimizações em termos de roteamento (balanceamento de carga), upgrade de link e introdução de redundância.
 - ◆ Roteamento de dados/
 - ➡ fluxo, nos níveis Layer 2, Layer 3 e MPLS.
 - ➡ Permite entender como os dados fluem e como podem reagir a eventos disruptivos.



Componentes básicos do SNMP

- Uma rede gerenciada por SNMP consiste em três componentes principais:
- Dispositivos gerenciados
 - ◆ Nó de rede que contém um agente SNMP.
 - ◆ Colete e armazene informações de gerenciamento e disponibilize essas informações usando o SNMP.
 - ◆ Podem ser roteadores e servidores de acesso, switches e pontes, hubs, hosts de computador ou impressoras.
- Agentes
 - ◆ Módulo de software de gerenciamento de rede que reside em um dispositivo gerenciado.
- Sistemas de gerenciamento de rede (NMSs)
 - ◆ Executa aplicativos que monitoram e controlam dispositivos gerenciados.
 - ◆ Fornece a maior parte dos recursos de processamento e memória necessários para o gerenciamento de rede.
 - ◆ Um ou mais NMSs devem existir em qualquer rede gerenciada.



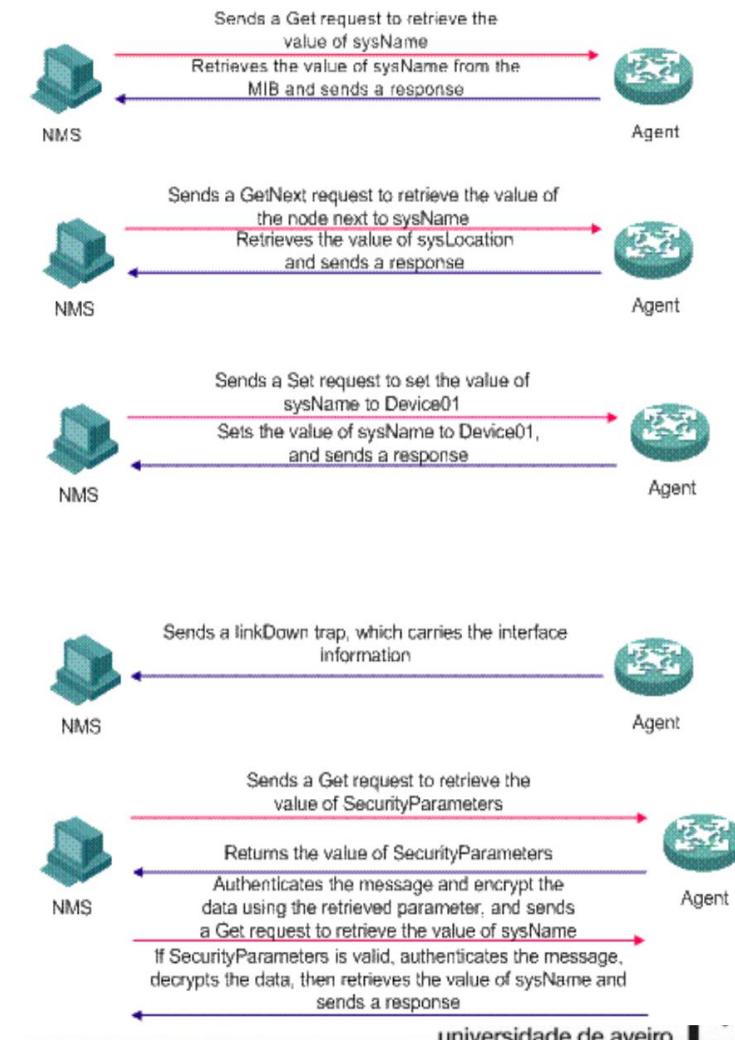
Versões SNMP

Model	Level	Authentication	Encryption	What Happens
v1	noAuthNoPriv	Community String	No	Uses a community string match for authentication.
v2c	noAuthNoPriv	Community String	No	Uses a community string match for authentication.
v3	noAuthNoPriv	Username	No	Uses a username match for authentication.
v3	authNoPriv	MD5 or SHA	No	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithm.
v3	authPriv	MD5 or SHA	DES or AES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES 56-bit or CFB128-AES-128 encryption in addition to authentication based on the CBC-DES (DES-56) standard.



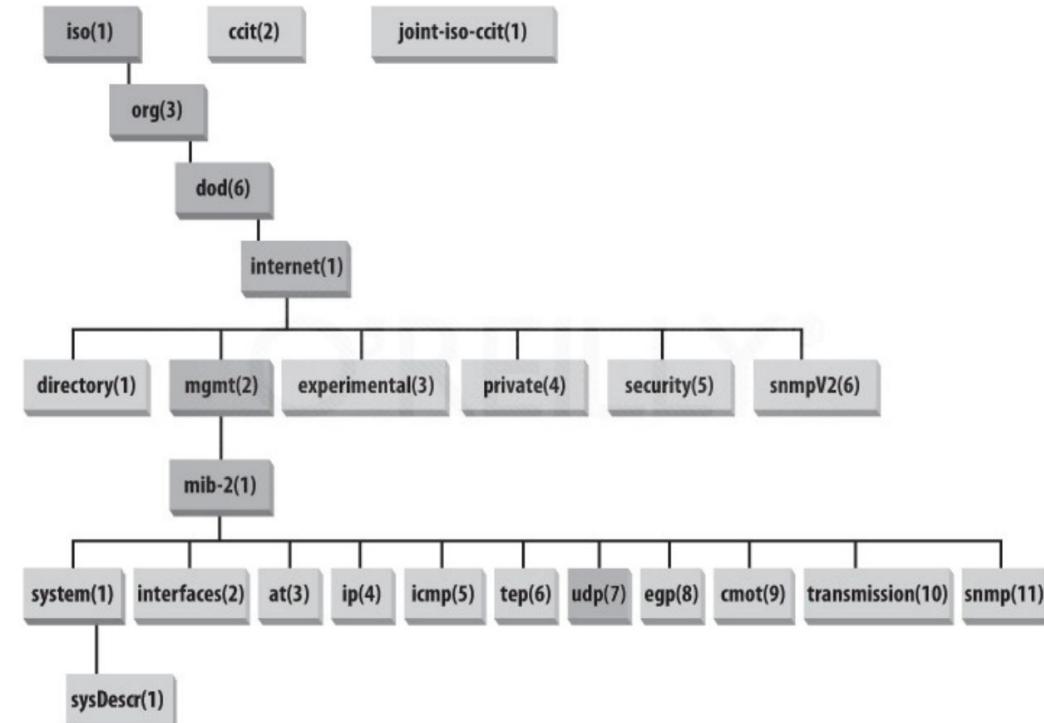
Operações SNMP

- O SNMP fornece as cinco operações básicas a seguir:
 - Get operation
 - Solicitação enviada pelo NMS ao agente para recuperar um ou mais valores do agente.
 - Operação GetNext
 - Solicitação enviada pelo NMS para recuperar o valor do próximo OID na árvore.
 - Definir operação
 - Solicitação enviada pelo NMS ao agente para definir um ou mais valores do agente.
 - Operação de resposta
 - Resposta enviada pelo agente para a NMS.
 - Operação trap
 - Resposta não solicitada enviada pelo agente para notificar a NMS sobre os eventos ocorridos.
- No SNMPv3, as operações get são executadas usando autenticação e criptografia.



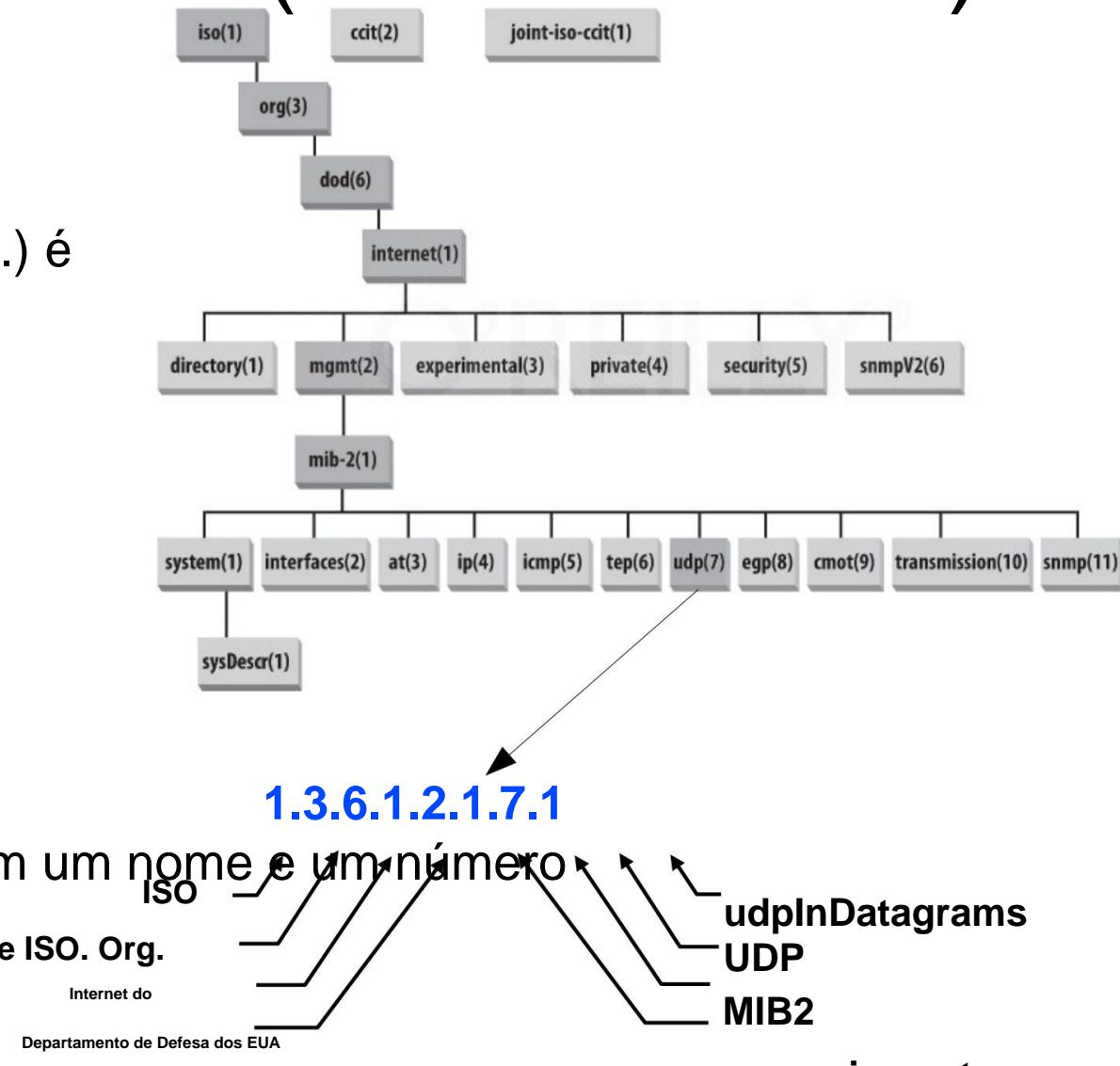
Módulos MIB e Identificadores de Objeto

- Um módulo SNMP MIB é uma especificação de informações de gerenciamento em um dispositivo
- O SMI representa a estrutura do banco de dados MIB em forma de árvore com tabelas conceituais, onde cada recurso gerenciado é representado por um objeto
- Identificadores de objeto (OIDs) identificam ou nomeiam exclusivamente variáveis MIB na árvore
 - Sequência ordenada de inteiros não negativos escritos da esquerda para a direita, contendo pelo menos dois elementos
 - Para facilitar a interação humana, os nomes com valor de string também identificam os
 - OIDs MIB-II (objeto ID 1.3.6.1.2.1)
 - MIB privado da Cisco (ID do objeto 1.3.6.1.4.1.9)
- A árvore MIB é extensível com novos módulos MIB padrão ou por ramificações experimentais e privadas Os fornecedores
 - podem definir suas próprias ramificações privadas para incluir instâncias de seus próprios produtos



Nomes SNMP (números/OID)

- Para nomear todos os objetos possíveis (protocolos, dados, etc.) é utilizada uma árvore ISO Object Identifier (OID):
- Nomenclatura
- hierárquica dos objetos Cada folha da árvore tem um nome e um número



MIB SNMP

- Management Information Base (MIB): conjunto de objetos gerenciados, utilizados para definir as informações dos equipamentos, e criados pelo fabricante
- Exemplo: módulo UDP

<u>Object ID Name</u>	<u>Tipo</u>	<u>Comentários</u>
1.3.6.1.2.1.7.1 UDPIInDatagrams	Counter32	Número de datagramas UDP entregues aos usuários.
1.3.6.1.2.1.7.2 UDPNoPorts	Counter32	Número de datagramas UDP recebidos para o qual não houve aplicação no porto de destino.
1.3.6.1.2.1.7.3 UDPIInErrors	Counter32	O número de UDP recebidos datagramas que não puderam ser entregues por outros motivos que não a falta de um aplicativo na porta de destino.
1.3.6.1.2.1.7.4 UDPOutDatagrams	Counter32	O número total de datagramas UDP enviados desta entidade.



MIBs relevantes

- Características da interface, configurações, status e estatísticas:
 - ◆ IF-MIB e IP-MIB.
 - ◆ Informações extras da Cisco: CISCO-QUEUE-MIB, CISCO-IF-EXTENSION-MIB
- Informações de gerenciamento de nós (descrição, informações gerais, status da CPU/memória, etc...):
 - ◆ SNMPv2-SMI e ENTITY-MIB.
 - ◆ Fornecedor específico: CISCO-SMI, JUNIPER-SMI, etc...
 - ◆ Cisco extra: CISCO-PROCESS-MIB, CISCO-FLASH-MIB, CISCO-ENVMON-MIB, CISCO-IMAGE-MIB, etc...
- Roteamento de nó e engenharia de tráfego: IP-MIB, IP-FORWARD-MIB
 - ◆ Informações extras da Cisco: CISCO-CEF-MIB, CISCO-PIM-MIB
 - ◆ MPLS-TE-MIB, MPLS-LSR-MIB, MPLS-VPN-MIB
- Serviços de nó:
 - ◆ Fornecedor específico: CISCO-AAA-SESSION-MIB, CISCO-SIP-UA-MIB, etc...
- Mecanismos de monitoramento de nós:
 - ◆ RMON-MIB, RMON2-MIB, CISCO-SYSLOG-MIB, CISCO-RTTMON-MIB, CISCO NETFLOW-MIB, CISCO-IPSEC-FLOW-MONITOR-MIB, etc...



NetFlow

- Os serviços Cisco NetFlow fornecem aos administradores de rede informações de fluxo IP de suas redes de dados.
 - ◆ Elementos de rede (roteadores e switches) coletam dados de fluxo e os exportam para coletores.
 - ◆ Captura dados de pacotes de entrada (entrada) e/ou saída (saída).
 - ◆ Coleta estatísticas para pacotes IP-para-IP e IP-para-MPLS.
- Um fluxo é definido como uma sequência unidirecional de pacotes com algumas propriedades comuns que passam por um dispositivo de rede.
 - ◆ Um fluxo é identificado como a combinação dos seguintes campos-chave:
 - Endereço IP de origem, Endereço IP de destino, Número da porta de origem, Número da porta de destino, Tipo de protocolo da camada 3, Tipo de serviço (ToS) e Interface lógica de entrada.
- Esses fluxos coletados são exportados para um dispositivo externo, o coletor NetFlow.
- Os fluxos de rede são altamente granulares
 - ◆ Por exemplo, os registros de fluxo incluem detalhes como endereços IP, contagens de pacotes e bytes, carimbos de data/hora, tipo de serviço (ToS), portas de aplicativos, interfaces de entrada e saída, números de sistema autônomo, etc.
- O NetFlow tem três versões principais: v1, v5 e v9. v1 é
 - ◆ recomendado apenas para dispositivos legados sem suporte para v5 ou v9.
 - ◆ V1 e v5, não suportam fluxos IPv6.

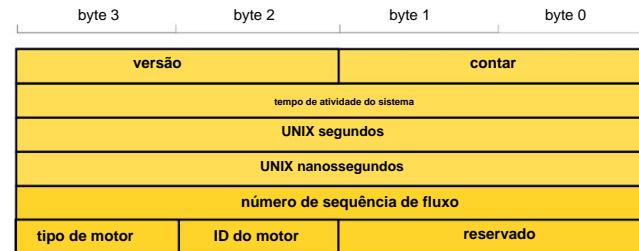


NetFlow versões 1 e 5

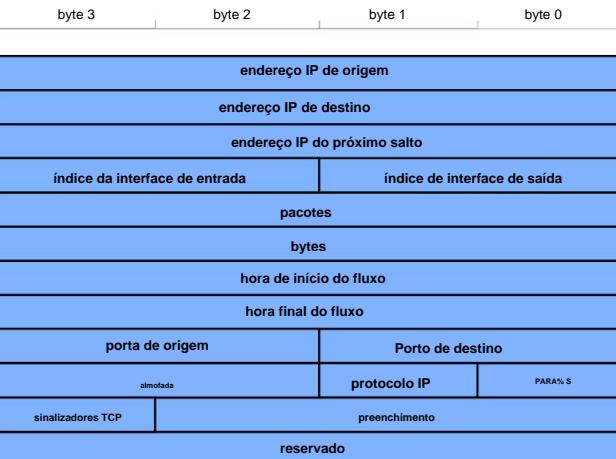
- Os pacotes NetFlow v1/v5 são pacotes UDP/IP com um cabeçalho NetFlow e um ou mais registros de dados NetFlow



Formato do
cabeçalho

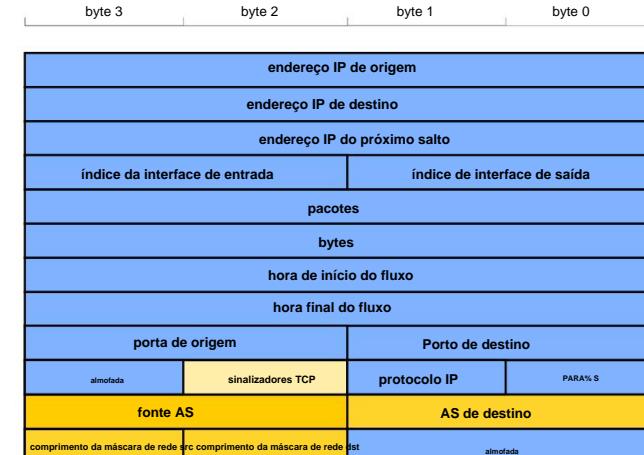


Formato
de gravação



sinalizadores TCP

Versão 1

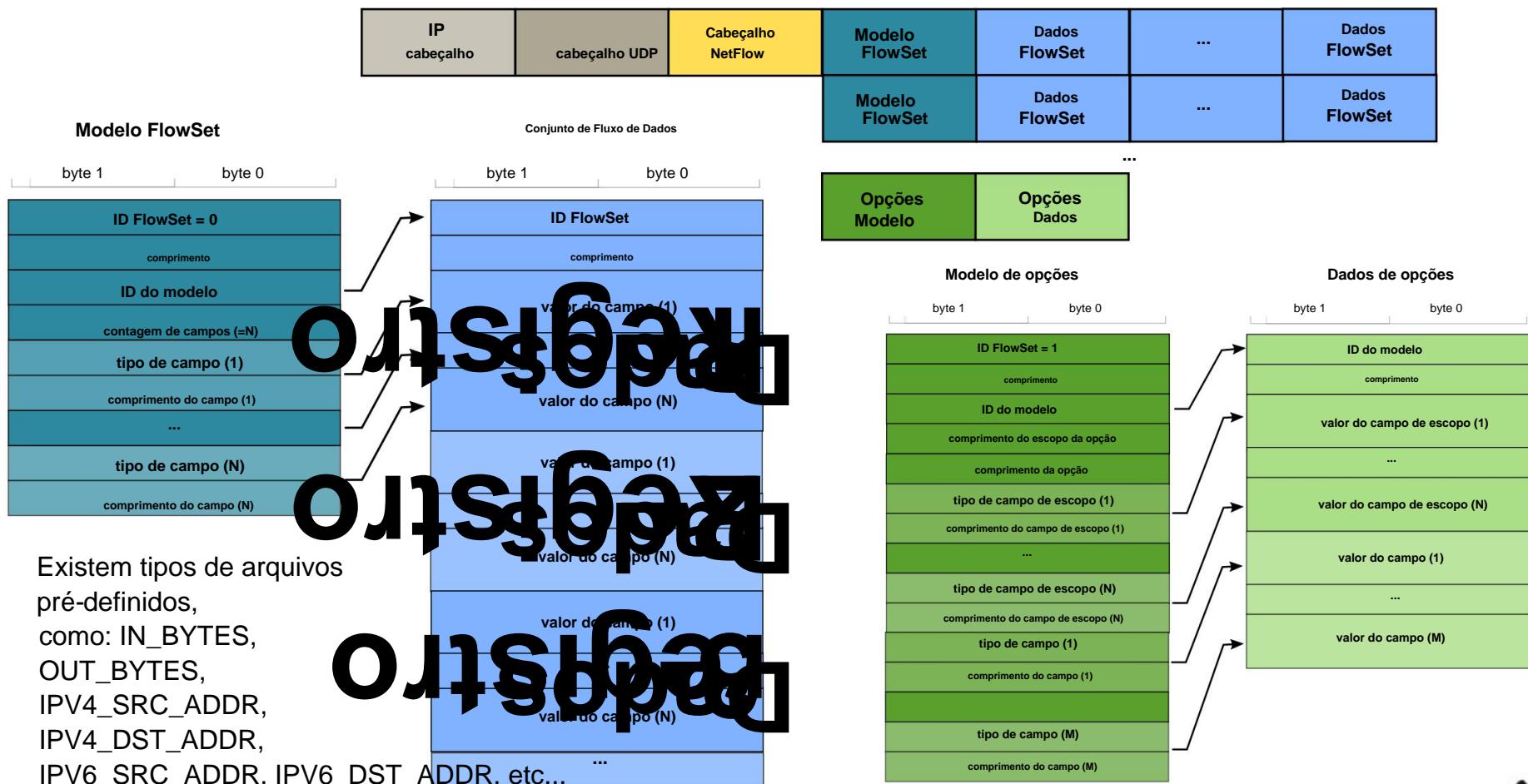


Versão 5



NetFlow versão 9

- Os pacotes NetFlow v9 são pacotes UDP/IP com um cabeçalho NetFlow, um ou mais Template FlowSets (podem ser suprimidos, se enviados anteriormente), um ou mais Data FlowSets e, opcionalmente, um Options Template e Data Record.



Uso do NetFlow

- Usado para caracterizar usuários/serviços em termos de quantidade de tráfego.
 - ◆ Usuários/Grupos (geral ou por aplicativo) → Aplicado em interfaces (V)LAN.
 - ◆ Serviços → Aplicado a interfaces de datacenter
- Usado para caracterizar destinos de tráfego (para pontos de saída) de um ponto de entrada específico em uma rede: matrizes de tráfego.
 - ◆ Os pontos de entrada/saída podem ser:
 - links de acesso à rede (camada de distribuição L3SW, roteadores de acesso à Internet, links de servidor VPN do
 - usuário), links de borda do núcleo da rede (roteadores de borda
 - do núcleo), links de emparelhamento BGP (roteadores AS Border).
- Usado para caracterizar o roteamento “na rede”.
 - ◆ Complexo para implementar e processar.



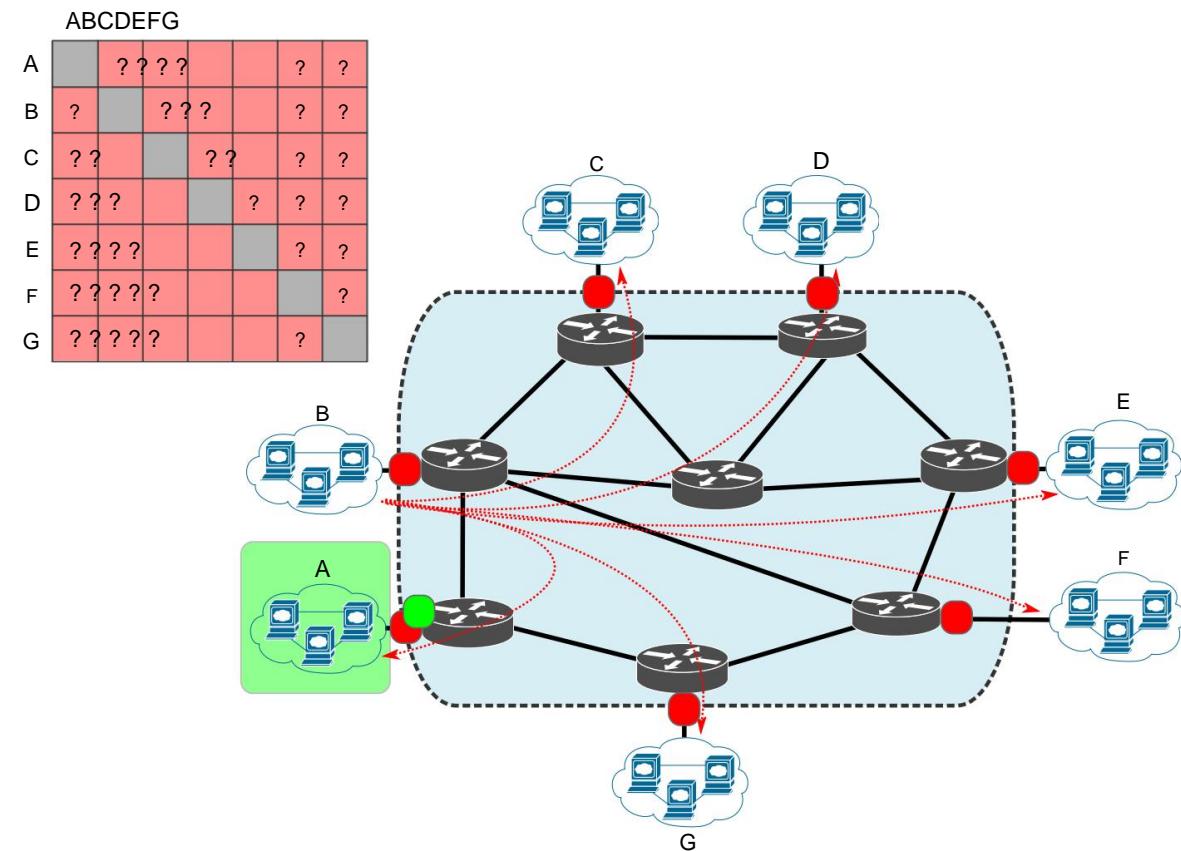
Implantação do NetFlow

- As interfaces a monitorar dependem do objetivo:

- Inferência da matriz de tráfego – todas as interfaces de borda do núcleo.
- Inferência de geração de fluxo de usuário/grupo - interface de acesso do usuário/grupo.

- Monitoramento de saída x entrada:

- Inferência da matriz de tráfego – entrada OU saída.
- Inferência de geração de fluxo de usuário/grupo – ambas as direções.



IPFIX (v10) e NetFlow Flexível

- O IPFIX é muito semelhante ao NetFlow v9. Usa
 - ◆ a versão 10 em um cabeçalho semelhante.
 - ◆ Também tem modelos e registros de dados.
 - ◆ Também possui modelos de opções e registros de dados de opções.
- O IPFIX fez provisões para o NetFlow v9 e adicionou suporte para ele.
 - ◆ IPFIX lista uma visão geral dos “identificadores de elemento de informação” que são compatíveis com os “tipos de campo” usados pelo NetFlow v9.
- O IPFIX possui mais tipos de arquivo do que os definidos para NetFlow v9.
 - ◆ Também permite que um ID de fornecedor seja especificado, o qual um fornecedor pode usar para exportar informações proprietárias/genéricas.
- O IPFIX permite campos de comprimento variável.
 - ◆ Útil para exportar strings de tamanho variável (por exemplo, URLs).
- A extensão NetFlow v9 “Flexible NetFlow” pretende ser tão flexível quanto IPFIX.



Sondagem Passiva de Rede

Captura de pacotes

- usuário para:

- Inferência de dados específicos e detalhados,
- Inferir dinâmicas de pequena e média escala de tempo.

- Tipos de sonda

- Switch mirror port, In-line,
- Network tap.

- Filtragem/amostra por usuário/

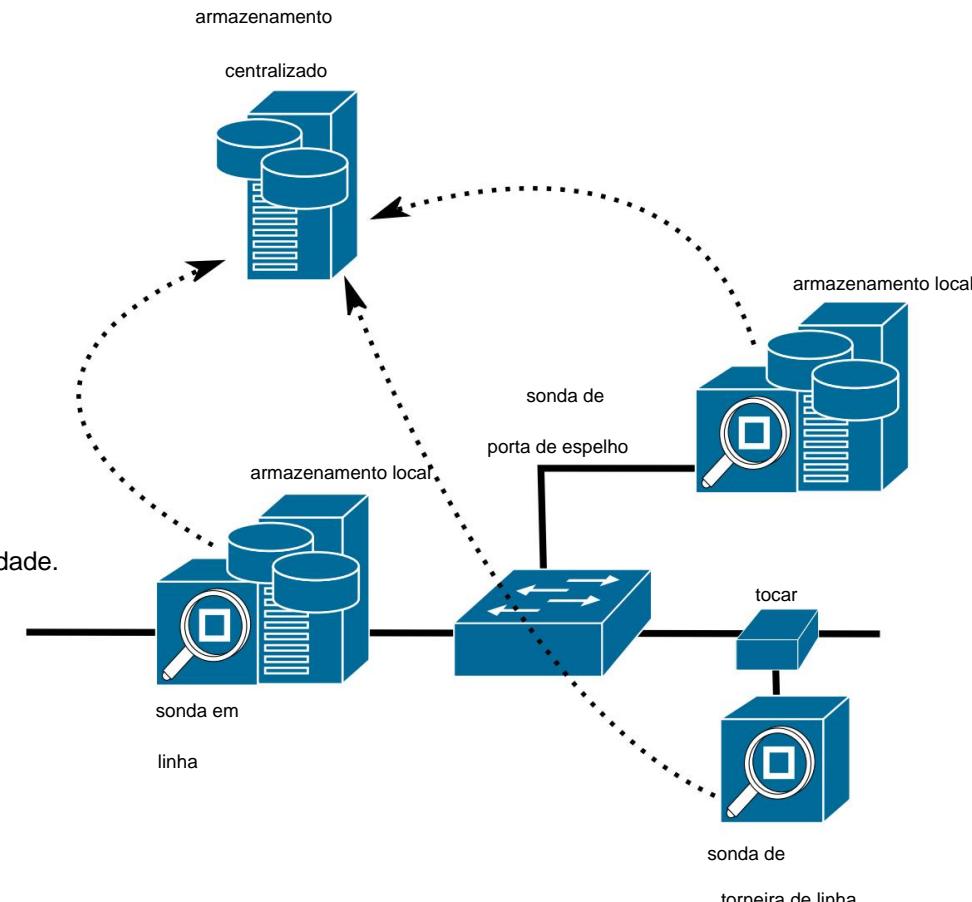
- endereço de terminal/VLAN/porta de acesso, endereço de grupo/VLAN/porta de acesso, protocolos (UDP/TCP), protocolos de camada superior, difícil de identificar devido à criptografia e restrições legais/de privacidade.
- Número/intervalo da porta UDP/TCP.

- Processamento de dados

- Contagem de pacotes/bytes, contagem de fluxo, endereços IP e distribuição de portas, estatísticas e distribuição de aplicativos/serviços.

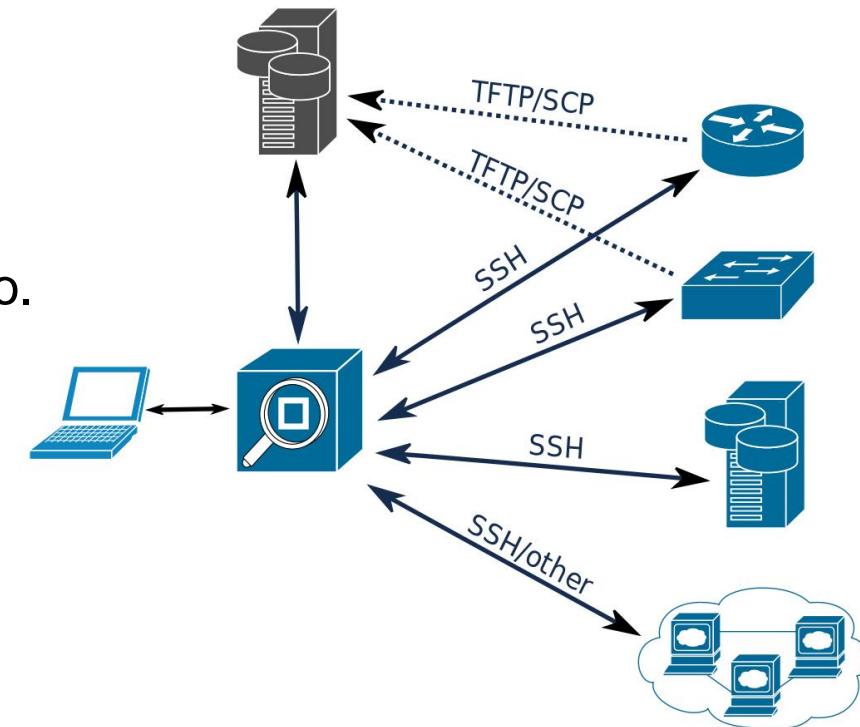
- Armazenamento e processamento local versus centralizado.

- O upload de dados para o ponto centralizado não deve ter impacto nas medições.



Acesso CLI remoto

- Usando um console remoto para dispositivos,
 - ◆ usando SSH, telnet (inseguro) ou protocolos proprietários,
 - ◆ recuperar configurações e status de processos do dispositivo.
 - ◆ Os dispositivos também podem carregar configurações para um ponto central.
 - Usando TFTP (inseguro) ou SFTP/SCP (muitos dispositivos não suportam).

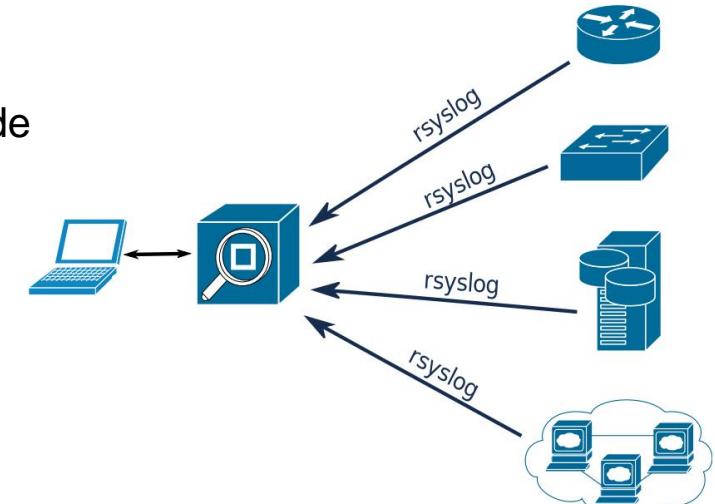


- Envie “show” como comandos CLI, recupere a saída, analise as informações.

Log de Acesso aos Arquivos

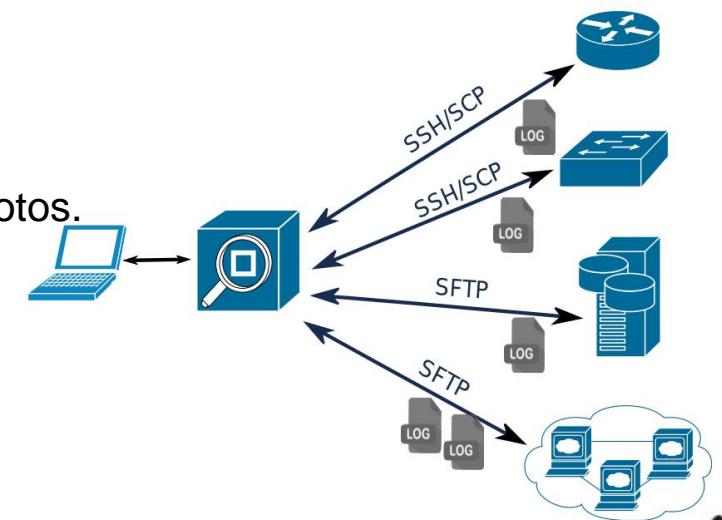
- rsyslog

- ◆ Capaz de aceitar entradas de uma ampla variedade de serviços, transformá-los e enviar os resultados para diversos destinos de rede.
- ◆ Sobre TCP e/ou SSL/TLS.
- ◆ Tempo controlado pelo nó/dispositivo monitorado.
- ◆ Muitas tarefas de processamento cruzado e pós-processamento podem ser feitas no nó/dispositivo monitorado.



- Acesso direto a arquivos de log

- ◆ Usando qualquer acesso remoto a arquivos remotos.
 - ◆ Requer permissões especiais.
- ◆ SSH/SCP, SFTP, etc...
- ◆ Tempo controlado por ponto central.
- ◆ Requer todo processamento posterior e cruzado pesado em um ponto central.



Sistemas de gerenciamento de registros (LMS)

- Sistema de software que agrupa e armazena arquivos de log de várias fontes e sistemas de rede.
- Permite que as organizações centralizem todos os seus dados de log de vários sistemas.
- Permite que os Logs sejam visualizados e correlacionados.
- Principais finalidades:
 - ◆ Detectar e responder a Indicadores de Compromisso (IoC);
 - ◆ Realizar análise forense de dados;
 - ◆ Realizar investigações sobre eventos de rede e possíveis ataques.



Informações de Segurança e Eventos Gestão (SIEM)

- Incorpora três tipos de ferramentas de segurança em um único aplicativo:
 - ◆ Security Event Management (SEM)
 - ➡ Muito semelhante ao LMS.
 - ➡ Agrega arquivos de log de vários sistemas, mas eles são mais voltados para as necessidades de analistas de segurança de TI em vez de administradores de sistema.
 - ◆ Gerenciamento de Informações de Segurança (SIM)
 - ➡ Ferramentas de software usadas para identificar, coletar e analisar dados de logs de eventos.
 - ➡ Inclua recursos e alertas automatizados que podem ser acionados quando condições predeterminadas forem satisfeitas, o que pode indicar que a rede está comprometida.
 - ➡ Ajude os analistas de segurança a automatizar o processo de resposta a incidentes e gerar relatórios mais precisos sobre a posição/passado de segurança da organização.
 - ◆ Correlação de eventos de segurança (SEC)
 - ➡ Software usado para processar e pesquisar grandes quantidades de logs de eventos e descobrir correlações e conexões entre eventos que podem indicar um problema de segurança.



LMS x SIEM

- As ferramentas LMS são mais focadas em:
 - ◆ Coleta de dados de log, retenção eficiente de dados, indexação de log e funções de pesquisa e geração de relatórios.
- As ferramentas SIEM são mais focadas em:
 - ◆ Alertas de detecção de ameaças, correlação de eventos e painel de controle (monitoramento em tempo real com visibilidade de eventos personalizados).
- A evolução dos LMS tradicionais, projetados principalmente para suporte à administração de sistemas, os tornou funcionalmente muito mais próximos das ferramentas SIEM desenvolvidas de raiz como ferramenta de segurança.



Eventos SIEM (exemplos)

● Detecção de força bruta

- ◆ Erros 404 excessivos (log do servidor HTTP) de um cliente não autenticado (log do banco de dados).
- ◆ Falhas excessivas de login (serviços ou logs de banco de dados) em um ou vários serviços.
 - De um endereço IP específico (ou conjunto de endereços IP).
 - De regiões geográficas “estranhas” ou AS.
- ◆ Credenciais não correspondentes
 - De máquinas internas com credenciais de usuário não correspondentes (RADIUS/LDAP Logs).

● Viagens impossíveis

- ◆ Vários logins do mesmo usuário de diferentes dispositivos/lokais.
- ◆ Logins consecutivos do mesmo usuário de regiões geográficas distantes dentro de uma pequena janela de tempo. O uso de VPN pode acionar esse alarme.

● Transferência de dados anômala

- ◆ Analisando por origem individual (IP ou grupo de dispositivos) e/ou destino e/ou por protocolo/porta utilizada.
- ◆ Transferência de dados excessiva/diferente não compatível com observações anteriores
 - Uso de protocolos e portas:
 - Geralmente regras de firewall resolvem isso!
 - Quantidades de download/upload, relação upload/download, número de conexões, etc...;
 - Dispositivos nunca contatados: servidores externos (IP/ASN ou país desconhecido) ou dispositivos internos;
 - Hora absoluta do dia, comportamento do tempo relativo, dispositivo final desconhecido, etc...;
- ◆ Deve ser usado para detectar exfiltração (ou propagação dentro da rede) e C&C ilícito e canais de dados.

● ataque DDoS

- ◆ Tentativas de conexão excessivas de dispositivos/endereços/regiões “nunca vistos”.
- Detecção ideal na fase inicial do ataque.

● Falha na integridade de arquivos/configurações

- ◆ Falha na soma de verificação do arquivo de configuração de dispositivo/serviço específico, não justificável por ações observadas.
- ◆ Falha de checksum de arquivo genérico, não justificável por ações observadas.

● etc...?



Centro de operações de segurança (SOC)

- Competências de um SOC em uma organização:
 - ◆ Prevenção e detecção de ataques
 - ✚ Monitorar rede e serviços (com SIEM)
 - ✚ Detectar vulnerabilidades (com ferramentas de verificação de vulnerabilidades)
 - ✚ Detectar atividades maliciosas (com SIEM)
 - ✚ Detecte comportamentos anômalos (com SIEM) –
pode não ser malicioso!
 - ◆ Investigação
 - ✚ Analisar a atividade suspeita para determinar/caracterizar a ameaça
 - ✚ Avalie o quão profundamente a ameaça penetrou na rede/sistemas
 - ◆ Resposta
 - ✚ Implante contra-medidas com base em playbooks conhecidos
 - ✚ Implante medidas de emergência quando a ameaça não corresponder a um manual de resposta conhecido
 - ◆ forense
 - ✚ Feito após um ataque
 - ✚ Reunir provas para fins judiciais
 - ✚ Reúna dados adicionais para melhorar a prevenção/detecção/resposta futura

