

Projeto Lógico da Rede

Projeto da Topologia da Rede

- Uma topologia é um mapa de uma rede que indica:
 - segmentos de rede (redes de camada 2)
 - pontos de interconexão
 - comunidades de usuários
- Queremos projetar a rede logicamente e não fisicamente
 - Identificam-se redes, pontos de interconexão, o tamanho e alcance das redes e o tipo de dispositivos de interconexão
 - Não lidamos (ainda) com tecnologias específicas, dispositivos específicos, nem considerações de cabeamento
- Nosso objetivo é projetar uma rede segura, redundante e escalável

Projeto hierárquico de uma rede

- Um modelo hierárquico ajuda a desenvolver uma rede em pedaços, cada pedaço focado num objetivo diferente
- Um exemplo de uma rede hierárquica aparece a seguir
- As 3 camadas mostradas:
 - Camada **núcleo**: roteadores e comutadores de alto desempenho e disponibilidade
 - Camada de **distribuição**: roteadores e comutadores que implementam políticas
 - Camada de **acesso**: conecta usuários aos pontos de acesso (comutadores e wifi)

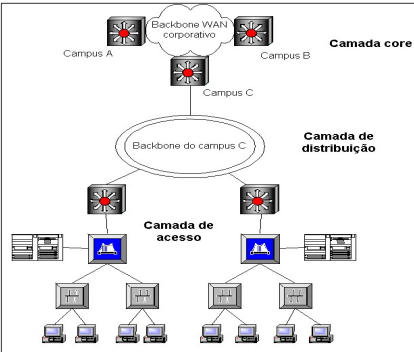


Fig. 3-1: Backbone com projeto hierárquico

Por que usar um modelo hierárquico?

- Uma rede não estruturada (espaguete) cria muitas adjacências entre equipamentos
 - Ruim para propagação de rotas (R1 --- R2 --- . . . --- Rn)
- Uma rede achatada (camada 2) não é escalável devido ao broadcast
- Minimiza custos, já que os equipamentos de cada camada serão especializados para uma determinada função
 - Exemplo: Usa comutadores rápidos no núcleo, sem recursos adicionais
- Mais simples de entender, testar e consertar
- Facilita mudanças, já que as interconexões são mais simples
- A replicação de elementos se torna mais simples
- Permite usar protocolos de roteamento com "sumarização de rotas"
- Comparação de estrutura hierárquica com achatada para a WAN
 - OK para redes pequenas
 - Para redes grandes, o tráfego cruza muitos nós (atraso mais alto)
 - Qualquer quebra é fatal (embora se possa usar um loop de roteadores para minimizar o problema)

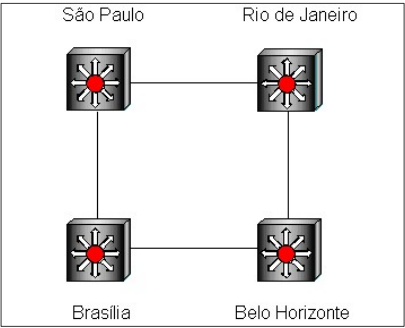


Fig. 3-2: Anel de roteadores

Roteadores redundantes numa hierarquia dão:

- Mais escalabilidade
- Mais disponibilidade
- Atraso mais baixo

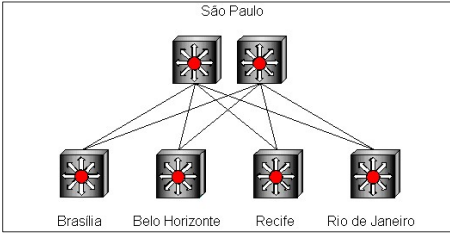


Fig. 3-3: Roteadores redundantes

Comparação de estrutura hierárquica com achatada para a LAN

- O problema básico é que um domínio de broadcast grande reduz significativamente o desempenho
- Com uma rede hierárquica, os equipamentos apropriados são usados em cada lugar
 - Roteadores (ou VLANs e comutadores de camada 3) são usados para delimitar domínios de broadcast
 - Comutadores de alto desempenho são usados para maximizar banda passante
 - Switches simples são usados onde o acesso barato é necessário

Topologias de full-mesh e mesh hierárquica

- A full-mesh oferece baixo atraso e alta disponibilidade, mas é muito cara
- Uma alternativa mais barata é uma mesh parcial
- Um tipo de mesh parcial é a mesh hierárquica, que tem escalabilidade, mas limita as adjacências de roteadores
- Para pequenas e médias empresas, usa-se muito a topologia hub-and-spoke

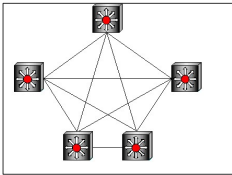


Fig. 3-4a: Full mesh

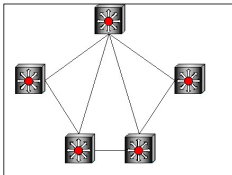


Fig. 3-4b: Partial mesh

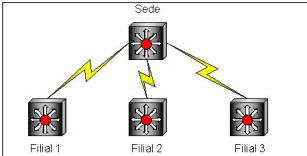


Fig. 3-4c: Hub-and-spoke

O modelo hierárquico clássico em 3 camadas

- Permite a agregação (junção) de tráfego em três níveis diferentes
- É um modelo mais escalável para grandes redes corporativas
- Cada camada tem um papel específico
 - Camada núcleo: provê transporte rápido entre sites
 - Camada de distribuição: conecta as folhas ao núcleo e implementa políticas
 - Segurança
 - Roteamento
 - Agregação de tráfego
 - Camada de acesso
 - Numa WAN, são os roteadores na borda das redes campus
 - Numa LAN, provê acesso aos usuários finais

• A camada de núcleo

- Backbone de alta velocidade
- A camada deve ser projetada para minimizar o atraso
- Dispositivos de alta vazão devem ser escolhidos, sacrificando outros recursos (filtros de pacotes, etc.)
- Deve possuir componentes redundantes devido à sua criticidade para a interconexão
- O diâmetro deve ser pequeno (para ter baixo atraso)
 - LANs se conectam ao núcleo sem aumentar o diâmetro
- A conexão à Internet é feita na camada de núcleo

• A camada de distribuição

- Tem muito papéis
 - Controla o acesso aos recursos (segurança)
 - Controla o tráfego que cruza o núcleo (desempenho)
 - Delimita domínios de broadcast
 - Isso pode ser feito na camada de acesso também
 - Com VLANs, a camada de distribuição roteia entre VLANs
 - Interfaceia entre protocolos de roteamento que consomem muita banda passante na camada de acesso e protocolos de roteamento otimizados na camada de núcleo (no caso de WAN)
 - Exemplo: sumariza rotas da camada de acesso e as distribui para o núcleo
 - Exemplo: Para o núcleo, a camada de distribuição é a rota default para a camada de acesso
 - Pode fazer tradução de endereços, se a camada de acesso usar endereçamento privativo
 - Embora o núcleo também possa usar endereçamento privativo

• A camada de acesso

- Provê acesso à rede para usuários nos segmentos locais
- Frequentemente usa apenas comutadores

Guia para o projeto hierárquico de uma rede

- Controle o diâmetro da topologia inteira, para ter atraso pequeno
- Mantenha controle rígido na camada de acesso
 - É aqui que departamentos com alguma independência implementam suas próprias redes e dificultam a operação da rede inteira
 - Em particular, deve-se evitar:
 - **Chains** (adicionando uma quarta camada abaixo da camada de acesso)
 - Causam atrasos maiores e dependências maiores de tráfego
 - Chains podem fazer sentido para conectar mais um país numa rede corporativa
 - **Portas-dos-fundos** (conexões entre dispositivos para mesma camada)
 - Causam problemas inesperados de roteamento
- Projete a camada de acesso primeiro, depois a camada de distribuição, depois o core
 - Facilita o planejamento de capacidade

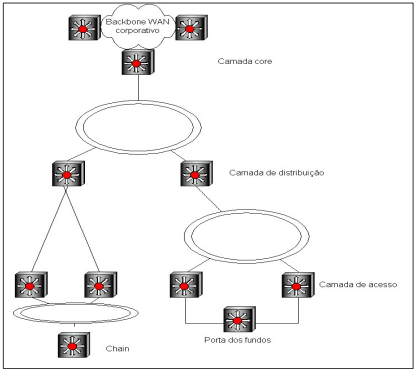


Fig. 3-5: Chain e Porta dos fundos

Topologias redundantes no projeto de uma rede

- A disponibilidade é obtida com a redundância de enlaces e dispositivos de interconexão
- O objetivo é eliminar pontos únicos de falha, duplicando qualquer recurso cuja falha desabilitaria aplicações de missão crítica
- Pode duplicar enlaces, roteadores importantes, uma fonte de alimentação
 - Em passos anteriores, você deve ter identificado aplicações, sistemas, dispositivos e enlaces críticos
- Para dispositivos muito importantes, pode-se considerar o uso de componentes "hot-swappable"
- A redundância pode ser implementada tanto na WAN quanto na LAN
- Há obviamente um tradeoff com o custo da solução

Caminhos alternativos

- Para prover alternativas aos enlaces primários
- Três aspectos são importantes
 - Qual deve ser a capacidade do enlace redundante?
 - É frequentemente menor que o enlace primário, oferecendo menos desempenho
 - Pode ser um acesso ADSL, por exemplo
 - Em quanto tempo a rede passa a usar o caminho alternativo
 - Se precisar de reconfiguração manual, os usuários vão sofrer uma interrupção de serviço
 - "Failover" automático pode ser mais indicado
 - Lembre que protocolos de roteamento descobrem rotas alternativas e comutadores também (através do protocolo de spanning tree)
 - O caminho alternativo deve ser testado!
 - Não espere que uma catástrofe ocorra para descobrir que o caminho alternativo nunca foi testado e não funciona!
 - Faça testes (simulações) de falhas!!

Considerações especiais para o projeto de uma topologia de rede de campus

- Os pontos principais a observar são:
 - Manter domínios de broadcast pequenos (VLANs podem/devem ser usadas)
 - Incluir segmentos redundantes na camada de distribuição
 - Usar redundância para servidores importantes
 - Incluir formas alternativas de uma estação achar um roteador para se comunicar fora da rede de camada 2

LANs virtuais

- Uma LAN virtual (VLAN) nada mais é do que um domínio de broadcast configurável
- VLANs são criadas em um ou mais comutadores
- Usuários de uma mesma comunidade são agrupados num domínio de broadcast independentemente do cabeamento físico
 - Isto é, mesmo que estejam em segmentos físicos diferentes
- Esta flexibilidade é importante em empresas que crescem rapidamente e que não podem garantir que quem participa de um mesmo projeto esteja localizado junto
- Uma função de roteamento (normalmente localizada dentro dos comutadores) é usada para passar de uma VLAN para outra
 - Lembre que cada VLAN é uma "rede de camada 2" e que precisamos passar para a camada 3 (rotear) para cruzar redes de camada 2
- Há várias formas de agrupar os usuários em VLANs, dependendo dos switches usados
 - Baseadas em portas do switches
 - Baseadas em endereços MAC
 - Baseadas em subnet IP
 - Baseadas em protocolos (IP, NETBEUI, IPX, ...)
 - VLAN para multicast
 - VLAN criada dinamicamente pela escuta de pacotes IGMP
 - VLANs baseadas em políticas gerais (com base em qualquer informação que aparece num quadro)
 - Baseadas no nome dos usuários
 - Com ajuda de um servidor de autenticação

Segmentos redundantes de LAN

- Enlaces redundantes entre comutadores são desejáveis para aumentar a disponibilidade
- Laços são evitados usando o protocolo Spanning Tree (IEEE 802.1d)
- Isso fornece redundância mas não balanceamento de carga
 - O protocolo Spanning Tree corta enlaces redundantes (até que sejam necessários)

Redundância de servidores

- Servidor DHCP
 - Em redes pequenas, o servidor DHCP é colocado na camada de distribuição onde pode ser alcançado por todos
 - Em redes grandes, vários servidores DHCP são colocados na camada de acesso, cada um servindo a uma fração da população
 - Evita sobrecarga de um único servidor
 - DHCP funciona com broadcast
 - Somos obrigados a colocar um servidor DHCP para cada domínio de broadcast?
 - Não, se utilizar uma função do roteador de encaminhar broadcast DHCP para o servidor de DHCP (fazer DHCP relay)
- Servidor DNS
 - O servidor DNS é crítico para mapear nomes de máquinas a endereços IP
 - Por isso, é frequentemente duplicado

Redundância estação-roteador

- Para obter comunicação fora da rede de camada 2 imediata, uma estação precisa conhecer um roteador (roteador default)
- Como implementar redundância aqui?
- O problema básico é que o IP do roteador que a estação conhece é freqüentemente configurado manualmente ("parafusado") em cada estação
- Há algumas alternativas:
 - Alternativa 1: DHCP
 - DHCP pode informar mais coisas do que apenas o endereço IP da estação
 - Pode informar o roteador a usar (ou até mais de um roteador)
 - Alternativa muito usada

- Alternativa 2: Virtual Router Redundancy Protocol (VRRP)
 - VRRP cria um roteador fantasma (que não existe de verdade) entre vários roteadores reais, um dos quais está ativo, os outros em standby
 - Os roteadores reais conversam entre si para saber qual é o roteador ativo
 - O roteador fantasma tem um endereço MAC e os roteadores reais podem aceitar quadros de um bloco de endereços MAC, incluindo o endereço MAC do fantasma
 - O roteador fantasma (que nunca quebra!) é o roteador default das estações
 - Quando uma estação usa ARP para descobrir o MAC do gateway, o roteador ativo, responde (com o MAC do fantasma)
 - Se o roteador ativo mudar, nada muda para a estação (continua conversando com o roteador fantasma)

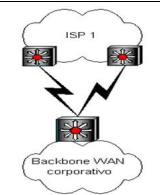
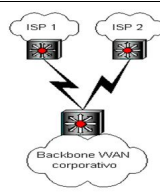
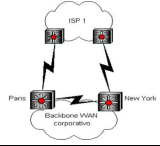
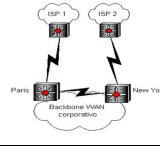
Considerações especiais para o projeto de uma topologia de rede corporativa

Segmentos redundantes de WAN

- Uso de uma mesh parcial é normalmente suficiente
- Cuidados especiais para ter [diversidade de circuito](#)
 - Se os enlaces redundantes usam a mesma tecnologia, são fornecidos pelo mesmo provedor, passam pelo mesmo lugar, qual a probabilidade da queda de um implicar na queda de outro?
 - Discutir essa questão com o provedor é importante

Conexões múltiplas à Internet

- Há 4 alternativas básicas para ter acesso múltiplo à Internet

	<p>Opção A</p> <p><u>Vantagens</u></p> <ul style="list-style-type: none">- Backup na WAN- Baixo custo- Trabalhar com um ISP pode ser mais fácil do que trabalhar com ISPs múltiplos <p><u>Desvantagens</u></p> <ul style="list-style-type: none">- Não há redundância de ISPs- Roteador é um ponto único de falha <p>Supõe que o ISP tem dois pontos de acesso perto da empresa</p>
	<p>Opção B</p> <p><u>Vantagens</u></p> <ul style="list-style-type: none">- Backup na WAN- Baixo custo- Redundância de ISPs <p><u>Desvantagens</u></p> <ul style="list-style-type: none">- Roteador é um ponto único de falha- Pode ser difícil trabalhar com políticas e procedimentos de dois ISPs diferentes
	<p>Opção C</p> <p><u>Vantagens</u></p> <ul style="list-style-type: none">- Backup na WAN- Bom para uma empresa geograficamente dispersa- Custo médio- Trabalhar com um ISP pode ser mais fácil do que trabalhar com ISPs múltiplos <p><u>Desvantagens</u></p> <ul style="list-style-type: none">- Não há redundância de ISPs
	<p>Opção D</p> <p><u>Vantagens</u></p> <ul style="list-style-type: none">- Backup na WAN- Bom para uma empresa geograficamente dispersa- Redundância de ISPs <p><u>Desvantagens</u></p> <ul style="list-style-type: none">- Alto custo- Pode ser difícil trabalhar com políticas e procedimentos de dois ISPs diferentes

- As opções C e D merecem mais atenção
- * O desempenho pode freqüentemente ser melhor se o tráfego ficar na rede corporativa mais tempo antes de entrar na Internet
 - * Exemplo: pode-se querer que sites europeus da empresa acessem a Internet pelo roteador de Paris, mas acessem sites norte-americanos da empresa pelo roteador de New York
 - * A configuração de rotas default nas estações (para acessar a Internet) pode ser feita para implementar essa política
 - * Exemplo mais complexo: Queremos que sites europeus da empresa acessem sites norte-americanos da Internet pelo roteador de New York (idem para o roteador de Paris sendo usado para acessar a Internet européia pelos sites norte-americanos da empresa)
 - * Fazer isso é mais complexo, pois os roteadores da empresa deverão receber rotas do ISP
 - * Exemplo mais complexo ainda: tráfego que vem da Internet para sites norte-americanos da empresa devem entrar na empresa por New York (idem para Paris)
 - * Neste caso, a empresa deverá anunciar rotas para a Internet
 - * Observe que, para evitar que a empresa se torne um *transit network*, apenas rotas da própria empresa devem ser anunciadas!

Redes privativas virtuais

- * Redes privativas virtuais (VPN) permitem que um cliente utilize uma rede pública (a Internet, por exemplo) para acessar a rede corporativa de forma segura
 - * Toda a informação é criptografada
- * Muito útil para montar uma extranet (abrir a intranet para parceiros, clientes, fornecedores, etc.)
- * Muito útil para dar acesso a usuários móveis da empresa
- * Solução muito usada quando a empresa é pequena e tem restrições de orçamento para montar a rede corporativa
- * A técnica básica é o [tunelamento](#)
- * Vários protocolos podem ser usados:
 - * Mais simples: Point to Point Tunelling Protocol (PPTP)
 - * Mais recente e mais seguro: IP Security Protocol (IPsec)

Topologias de rede para a segurança

- * Falaremos mais de segurança adiante
- * Por enquanto, queremos ver os aspectos topológicos da questão

Planejamento da segurança física

- * Verificar onde os equipamentos serão instalados
- * Prevenção contra acesso não autorizado, roubo físico, vandalismo, etc.

Topologias de firewalls para alcançar requisitos de segurança

- * Um **firewall** é um sistema que estabelece um limite entre duas ou mais redes
- * Pode ser implementado de várias formas
 - * Simples: um roteador com filtro de pacote
 - * Mais complexo: software especializado executando em um hardware proprietário (muitas vezes uma caixa preta LINUX)
- * Serve para separar a rede corporativa da Internet
- * A topologia mais básica usa um roteador com filtro de pacote
 - * Só é suficiente para uma empresa com política de segurança muito simples

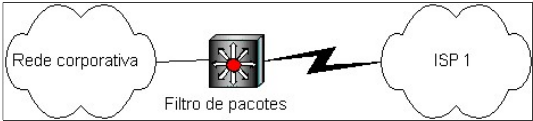


Fig. 3-7: Firewall básico

- * A tabela de filtragem de pacotes poderia ser como segue
 - * A primeira regra que casa com cada pacote examinado é aplicada

Host remoto	Porta remota	Host local	Porta local	Ação
mau.ladrao.com	*	*	*	Nega
*	*	mailserver	25	Permite
*	25	*	*	Permite
*	*	*	*	Nega

- * Para melhorar as coisas, pode-se usar endereçamento privativo na rede corporativa
 - * Uso de Network Address Translation (NAT) implementada no roteador para acessar a Internet
 - * Uso de um proxy para certos serviços (web, ftp, etc.)

- * Para empresas que precisam publicar informação na Internet (Web, DNS, FTP, etc.), pode-se ter algumas máquinas na Internet, numa área chamada Demilitarized Zone (DMZ)
 - * Os hospedeiros têm que ser muito bem protegidos contra invasões (*Bastion Hosts*)
- * Um firewall especializado pode ser incluído
 - * Fornece uma boa GUI e ações especiais para implementar a política de segurança
- * Há duas topologias básicas
 - * Com um roteador
 - * Com dois roteadores

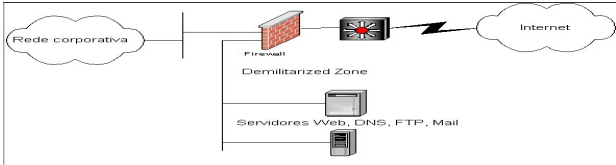


Fig. 3-8a: Topologia com 1 roteador e firewall dedicado

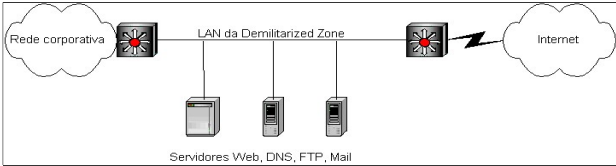


Fig. 3-8b: Topologia com 2 roteadores filtrando pacotes