UNICARIOCA 25 anos
Centro Universitário

Pós Graduação em Projeto e Gerencia de Redes de Computadores

Cadeira de Projeto de Redes

Prof. Dr. Eng. Frederico Sauer

Apresentação do Curso

Objetivos do Curso

- Apresentar ao aluno os desafios da tarefa do projeto de redes;
- Relembrar e/ou conhecer alguns aspectos teóricos, fundamentais para o entendimento das técnicas apresentadas;
- Apresentar o conteúdo da ementa de uma forma gradativa e autocontida em exposições de soluções que usem as tecnologias a discutir;
- Exercitar Projeto de Redes, de acordo com a metodologia apresentada;

Organização do Curso

- Módulo I
  - Introdução ao Projeto de Redes
  - Projeto de LAN
  - Projeto TCP/IP
- Módulo II
  - Projeto Desktop
  - Projeto WAN
  - Documentação
  - Projeto de uma Rede com o uso da Metodologia
- Bônus: elaboração de orçamentos

UNICARIOCA 25 anos
Centro Universitário

Cadeira de Projeto de Redes

Módulo I

Introdução ao Projeto de Redes

Sumário

- Introdução ao Projeto de Redes
  - Visão Geral de um Projeto de Redes
  - Projeto Hierárquico
- Projeto de LAN
  - Visão Geral de um Projeto de LAN
  - Tecnologia de LAN
  - Modelos de Projeto de LAN
- Projeto TCP/IP
  - Visão Geral de um Projeto TCP/IP
  - Projeto de Endereçamento
  - Projeto de Roteamento

Introdução ao Projeto de Redes

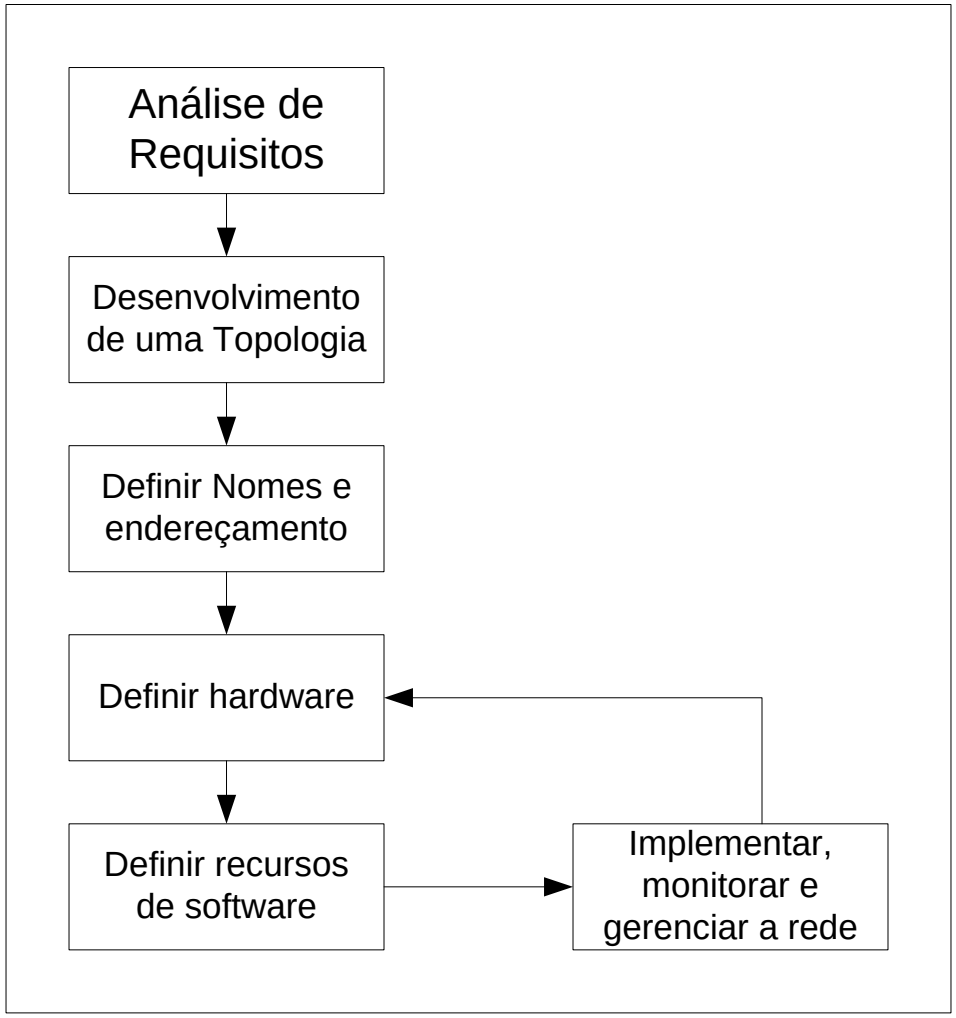
Visão Geral de um Projeto de Redes

- Há diretrizes básicas comuns a todos os projetos
- O objetivo deve ser reunir as informações relevantes para atender ao cliente
- Metas do Projeto
  - ✓ **Funcionalidade** – funciona como planejada
  - ✓ **Escalabilidade** – cresce com a organização
  - ✓ **Adaptabilidade** – não limitada às tecnologias atuais (ex. deve ser capaz de suportar outras tecnologias, como VoIP e multicast, caso ainda não estejam no projeto)
  - ✓ **Capacidade de Gerenciamento** – ação proativa
  - ✓ **Eficácia de Custos** – compensa o investimento e atende às restrições orçamentárias do cliente[1]

1 – O MELHOR projeto é aquele que ATENDE aos requisitos do cliente com o MENOR CUSTO possível.

Metodologia de Projeto

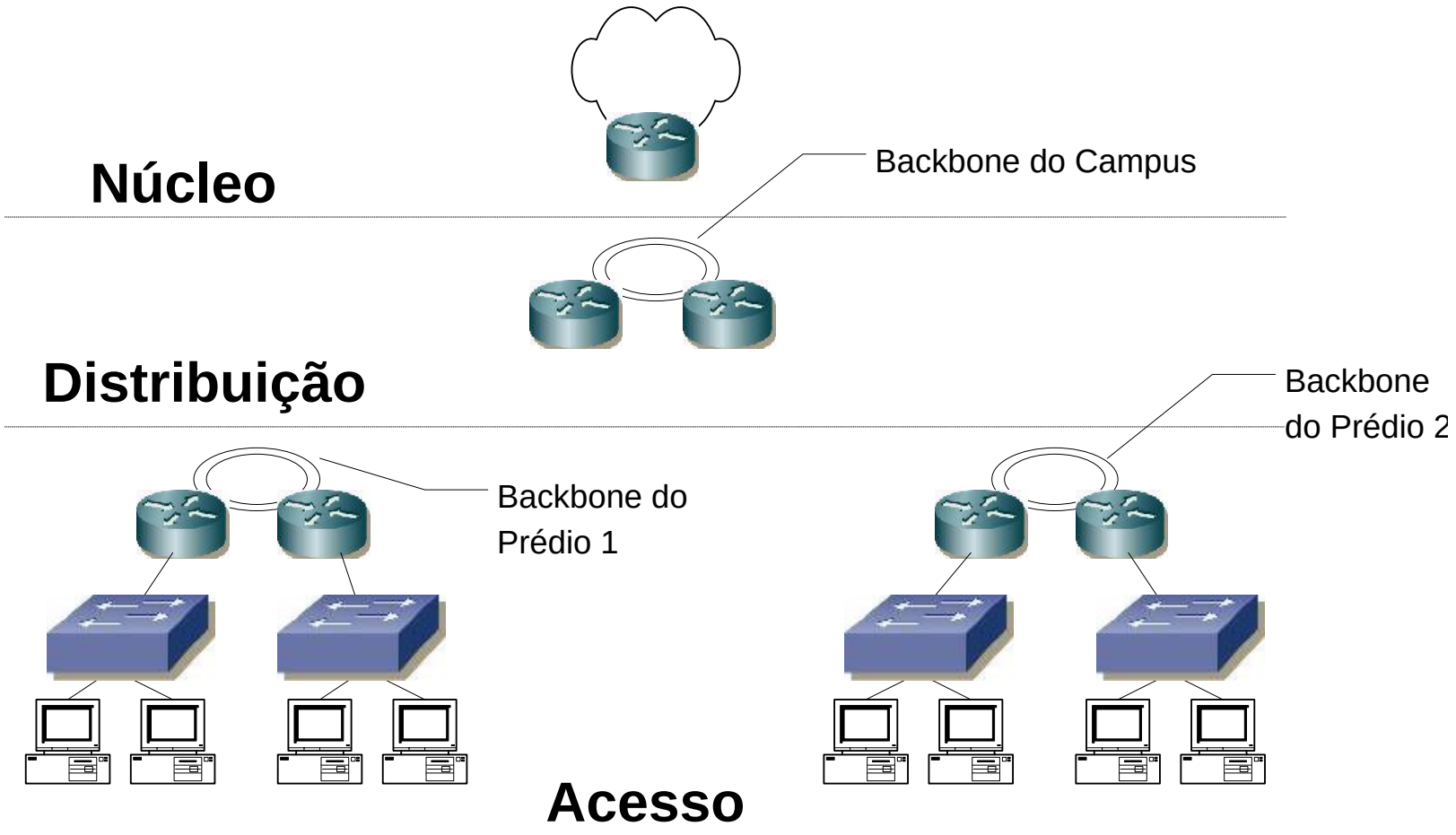
- Análise de Requisitos – da rede e dos usuários
- Topologia – Modelo hierárquico
- Nomes e Endereçamento – busca organização e escalabilidade
- Hardware – de acordo com recursos, expansibilidade, gerenciamento e custo
- Software – recursos do SO dos equipamentos



Metodologia de Projeto

- Três primeiras etapas únicas e sequenciais, as três seguintes são um ciclo recorrente
- Na Análise de Requisitos deve-se observar que a rede deve poder se adaptar para atender um aumento da demanda por banda de novas aplicações
- A topologia deve implementar um modelo hierárquico de três camadas
  - **Núcleo** – enlaces remotos – forma a WAN. Normalmente usa serviços contratados de terceiros (E1, FR, MPLS, LPCD, xDSL, etc)
  - **Distribuição** – Serviços de rede às várias LANs do Campus – É onde se implementa a PolSeg da empresa.
  - **Acesso** – Uma LAN onde os *hosts* são conectados à rede

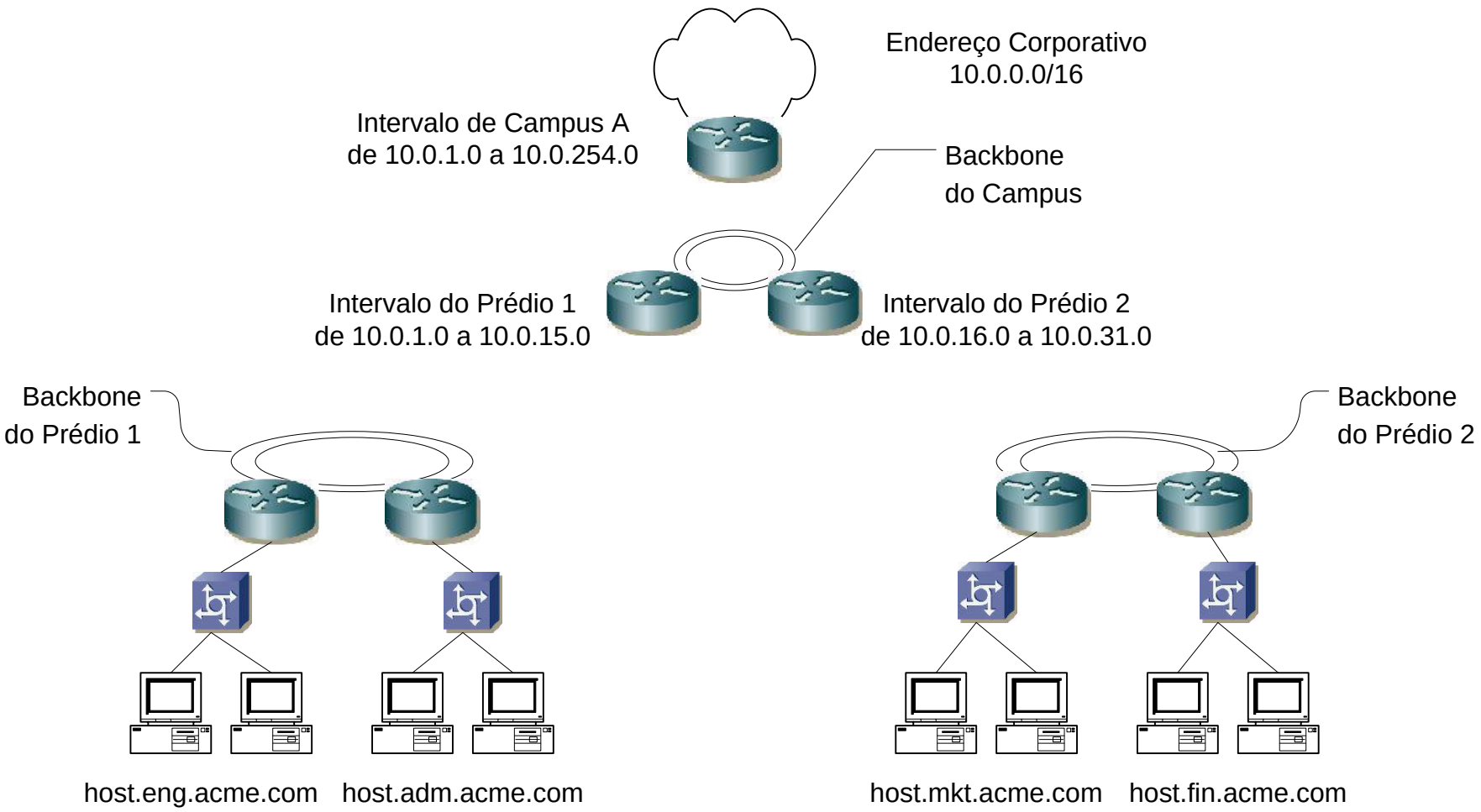
Modelo Hierárquico



Convenções de Nomes e Endereçamento

- Atribuição de blocos de endereços com foco na administração simplificada e escalabilidade
- Atribuição de nomes sistêmica, visando facilitar o gerenciamento pela fácil identificação
- Efetuar ambos planejamentos de forma hierárquica, compatível com o modelo definido na etapa anterior
- Ambas as tarefas contribuem para a eficácia da documentação da rede

Convenções de Nomes e Endereçamento



Especificação do Hardware

- Consultar a documentação dos fabricantes em busca das características desejadas
- Cada dispositivo possui funções e recursos peculiares
- Capacidade de expansão e gerenciamento é vital
- O custo deve compensar o benefício e estar dentro das limitações do cliente
- Deve-se tomar cuidado com questões de interoperabilidade, principalmente entre equipamentos de fabricantes diferentes

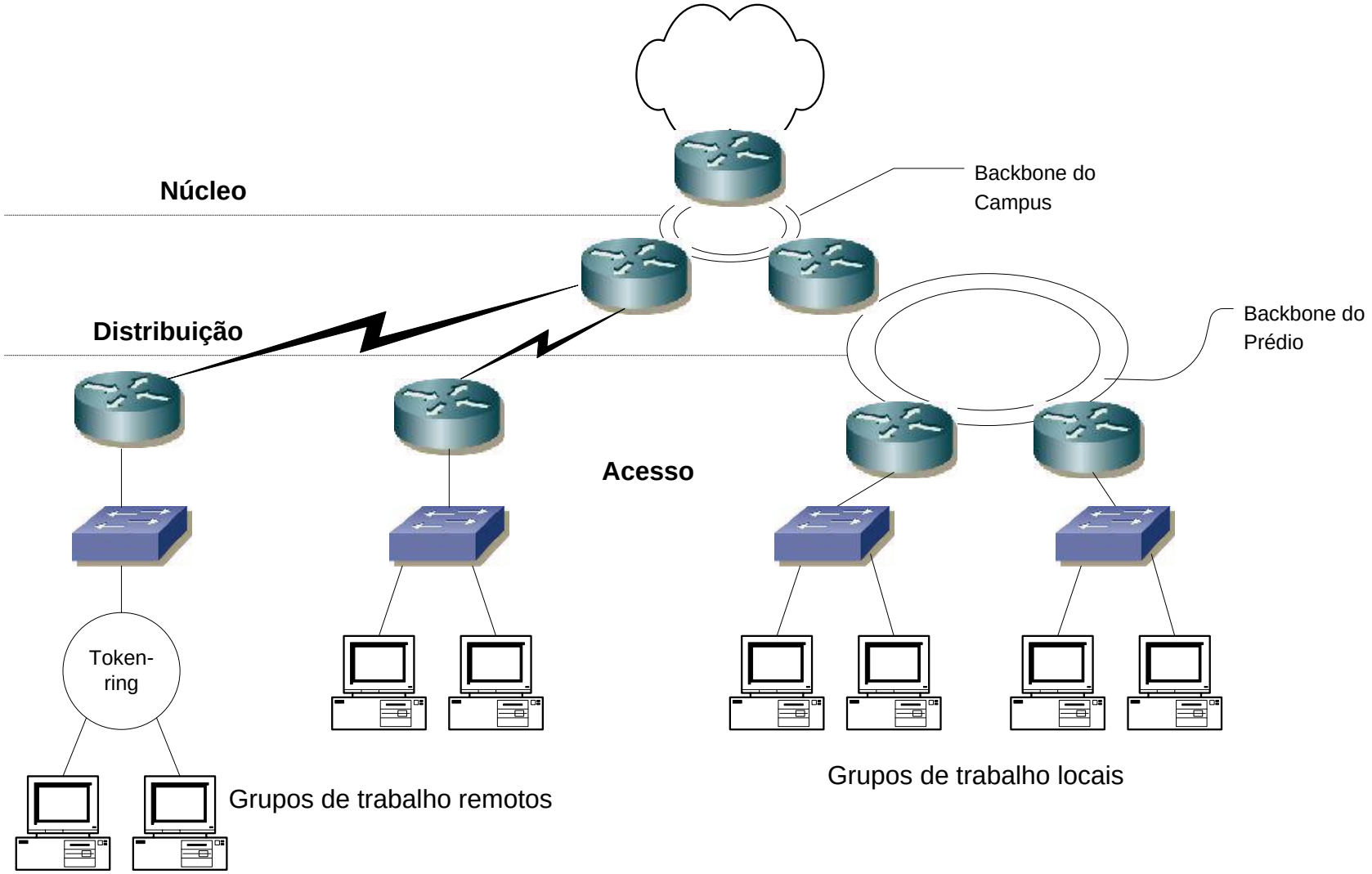
Especificação do Software

- Recursos como listas de acesso, proxy, controle de tráfego e filas, QoS, compactação, balanceamento de carga e NAT são dependentes de versões específicas de software (SO) do equipamento
- Os serviços desejados devem ser planejados hierarquicamente
  - Acesso – Servidores de arquivos, captação de estatísticas
  - Distribuição – compactação, controle de congestionamento, segurança, Servidores empresariais (e-mail, DMZ), proxy de internet, firewall
  - Núcleo – QoS, balanceamento de carga

Implementar e Monitorar a Rede

- De preferência, prototipar os elementos escolhidos e testar antes de adquirir tudo
- Colocar a rede em atividade
- Fazer a implementação em fases para reduzir o impacto para os usuários
- Monitorar o tráfego e agir proativamente para ajustar as necessidades da rede
- Importante: Contingências !!!!

Projeto Hierárquico



Projeto Hierárquico - Camadas

- **Camada Núcleo**
  - Missão: concentrar na redundância e na confiabilidade
  - Cada componente deve ser examinado para avaliação da relação do custo *versus* confiabilidade, à luz do custo do *downtime*
- **Camada de Distribuição**
  - Acondiciona a Política da rede (Segurança – políticas de acesso, filtros, firewall, ACLs, Convenções de nomes e endereços, criptografia, etc.)
  - Deve funcionar em taxas mais altas, como 10Gbps, ATM ou, no mínimo, Gigabit Ethernet full duplex.
- **Camada de Acesso**
  - Meio de acesso diretamente disponível para os hosts clientes e servidores
- As camadas devem ser projetadas para serem totalmente compatíveis e complementares às demais camadas.

Projeto Hierárquico – Funções das Camadas

- Camada Núcleo
  - Transporte adequado entre sites remotos
  - Normalmente implementada como uma WAN de alta velocidade
  - Deve priorizar a redundância e resistência às falhas
  - Devido ao custo das tarifas dos provedores, deve-se usar eficientemente a banda disponível, com priorização de tráfego

Regra de Projeto: Transporte otimizado na Camada Núcleo

Projeto Hierárquico – Funções das Camadas

- Camada de Distribuição
  - Deve proporcionar conectividade baseada em política

Regra de Projeto: A Política deve ser implementada na Camada de Distribuição

- Camada de Acesso
  - Deve conectar Grupos de Trabalho à camada de distribuição
    - ✓ Segmenta a rede lógica
    - ✓ Isola o broadcast de acordo com os Workgroups
    - ✓ Distribui serviços entre as CPU
  - Se baseia tipicamente em divisões organizacionais (marketing, finanças, produção, etc.)

Regra de Projeto: Mova servidores e serviços de usuários para a camada de acesso

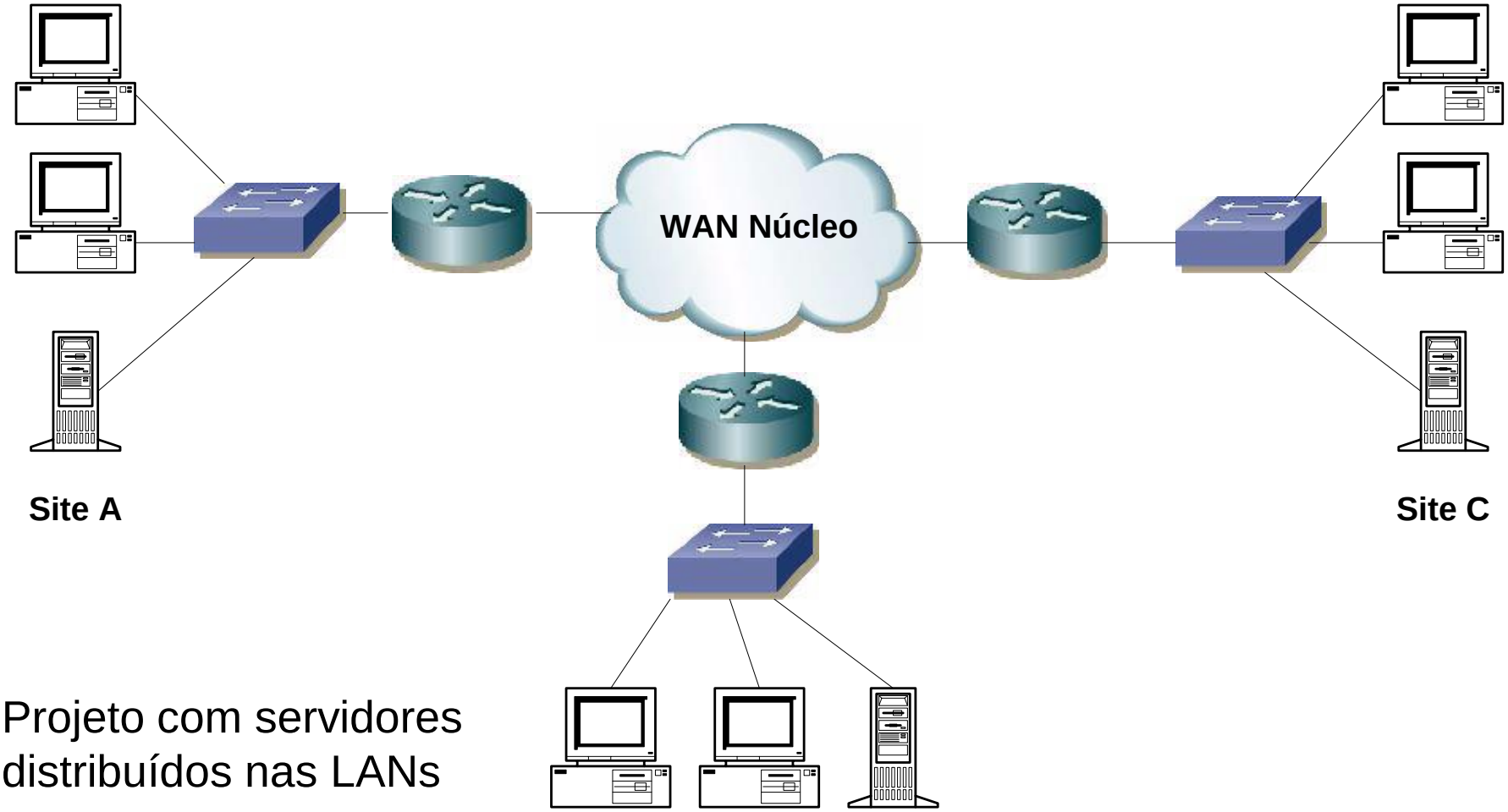
Projeto Hierárquico – Funções das Camadas

- Vantagens do Projeto Hierárquico
  - **Escalabilidade**
    - ✓ Crescer sem sacrifício do gerenciamento
  - **Facilidade de Implementação**
    - ✓ Top-down (núcleo → distribuição → acesso)
  - **Facilidade de Resolução de Problemas**
    - ✓ “Dividir e conquistar” na resolução dos problemas
  - **Previsibilidade**
    - ✓ Monitoramento de cada camada independente das demais, permitindo planejamento racional da capacidade de crescimento
  - **Suporte à Protocolos**
    - ✓ Devido à modularidade do modelo hierárquico
  - **Capacidade de Gerenciamento**
    - ✓ Implementada de forma hierárquica, de acordo com o modelo

Variações do Modelo Hierárquico

- Pode-se manter a estrutura hierárquica com uma ou duas camadas, com expansibilidade em caso de necessidade
- **Projeto de uma camada – Distribuído** → redes pequenas
  - Decisão Crítica → inserção de servidores corporativos
    - ✓Distribuídos pelas LANs ou num *server farm* central?
  - Benefícios
    - ✓Capacidade de sobrevivência
    - ✓Baixos requisitos de banda
  - Desvantagens
    - ✓Perda do controle centralizado
      - *Backups* e documentação são delegadas ao site de acesso

Projeto de uma Camada - Distribuído

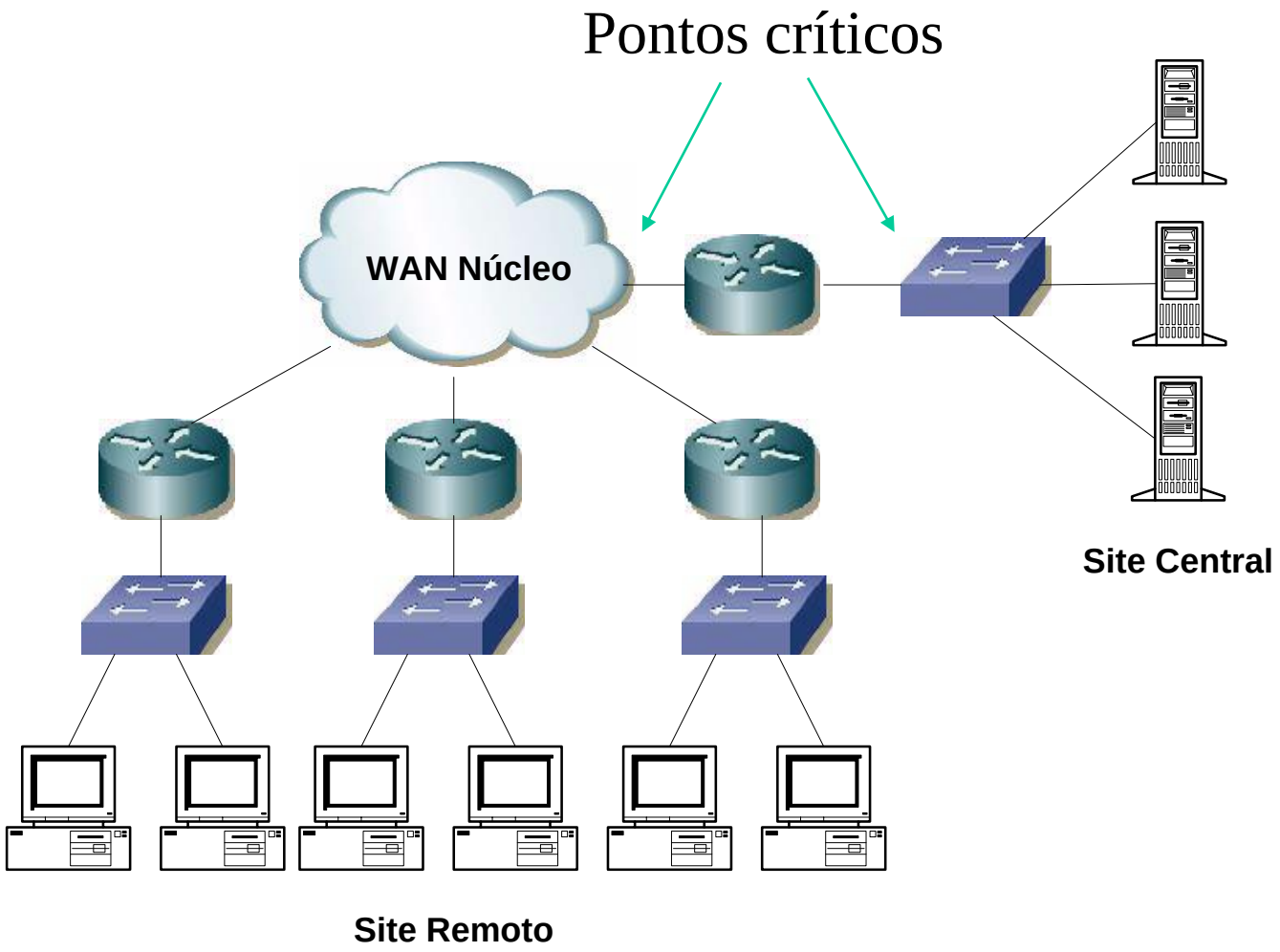


Projeto com servidores distribuídos nas LANs

Projeto de uma Camada – Hub-and Spoke

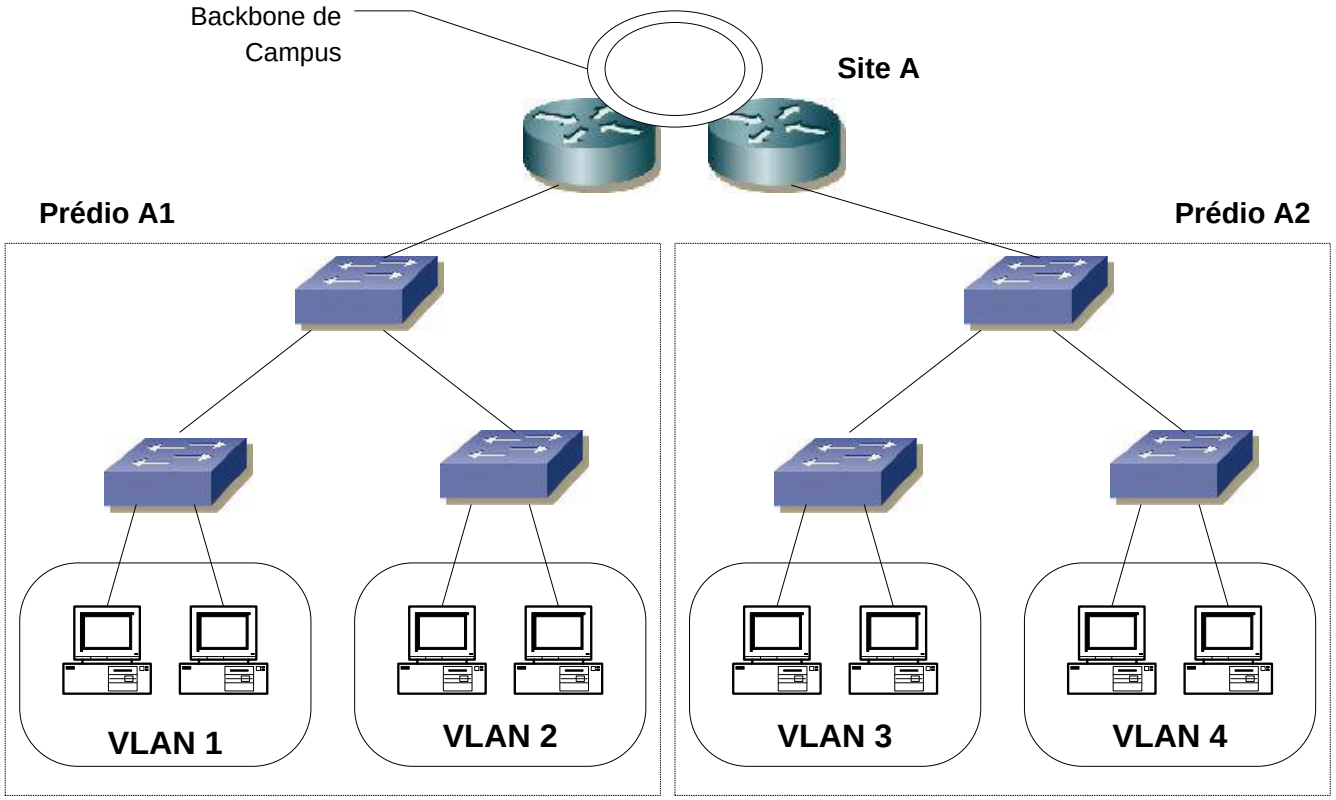
- Servidores são concentrados em *server farms,* o que não ocorre no distribuído
- Benefício
  - Maior controle de gerenciamento
  - Simplicidade de estrutura
- Contrapartida
  - Ponto único de falha e agregação de largura de banda

Projeto de uma Camada – Hub-and Spoke



Projeto de Duas Camadas

- Um *backbone* interliga prédios separados
- Em cada prédio, pode-se ter uma única rede lógica ou *bridges* entre redes lógicas (ex. VLANs)



Diretrizes para o Projeto Hierárquico

- Usar o modelo adequado para os requisitos
  - Isolamento de *broadcasts* e controle (segurança) da rede
- Não conectar as camadas da rede em malha
  - Roteadores do acesso e/ou distribuição ligados diretamente → devem ser usados *backbones*
  - Já o núcleo deve ficar em malha, para redundância
- Não colocar estações em *backbones*
  - Reduz confiabilidade e dificulta o gerenciamento
- *Workgroups* devem manter cerca de 80% do seu tráfego confinado – Regra 80/20 para LANs
- Usar recursos de acordo com o nível de hierarquia

UNICARIOCA 25 anos
Centro Universitário

Cadeira de Projeto de Redes

Módulo I

Projeto de LANs

Projeto de LAN

- Visão Geral de um projeto de LAN
  - Etapa preliminar do projeto: determinar as características do problema a solucionar
- Aspectos Técnicos do projeto:
  - estações cliente
  - estações servidoras
  - infraestrutura da rede
  - *cabling*
  - gerenciamento da rede
  - aspectos comerciais

Aspectos sobre a Estação Cliente

- **Abrangência**
  - Suporte à aplicações
    - ✓Demanda de banda
    - ✓QoS desejada e necessária
  - Atualizações de plataformas
  - NICs
- **Aspectos de software e de hardware**
  - Software → nível de dependência de *broadcasts* pelo SO; demanda de banda dos aplicativos; QoS necessária para as aplicações (ex. tráfego de voz e vídeo)
  - Hardware → Atualização de plataformas podem agregar mais demanda

Aspectos sobre a Estação Servidora

- **Os mesmos dos clientes, acrescidos de:**
  - Concorrência no acesso (maiores requisitos de banda)
  - SO de rede é peculiar (*broadcasts*)
  - Atendimento às demandas de QoS
  - Colocação dos servidores → fisicamente continuamente acessíveis
  - Tolerância à falhas → disponibilidade x risco

Aspectos sobre Infraestrutura

- Decisão sobre o modelo hierárquico (*backbone* distribuído ou colapsado ?)
  - Distribuído – um roteador por andar diretamente conectados ao backbone central
    - ✓Boa tolerância a falhas, mas maior custo
  - Colapsado – cabos dos andares são todos ligados a um único roteador
- Banda do *backbone* ? qual tecnologia empregar ?
- *Switching, Route-switching* ou *Routing* ?

Decisão sobre o modelo hierárquico (*backbone* distribuído ou colapsado ?)

- **Distribuído**
  - roteadores em cada prédio conectados diretamente ao backbone central
    - ✓ demanda uso de portas extras no backbone → custo
    - ✓ falhas podem ser rapidamente corrigidas pelo isolamento
    - ✓ melhor tolerância à falhas
- **Colapsado**
  - único ponto de concentração para o tráfego de todos os usuários
    - ✓ localização do problema é dificultada
    - ✓ ponto único de falhas
    - ✓ fácil de implementar alterações e menor custo

Banda do *backbone* ? qual tecnologia empregar ?

- Alta velocidade e Confiabilidade são requisitos comuns
- Passo inicial é a determinação dos requisitos de largura de banda para depois classificar as tecnologias disponíveis
- Essa classificação é feita através de uma matriz com os requisitos do projeto e as características de cada tecnologia

Switching ou Routing ?

- “Roteie onde puder, crie bridges onde forem necessárias”
- Separação lógica de domínio de *broadcasts* deve ser um objetivo

Projeto de Cabling

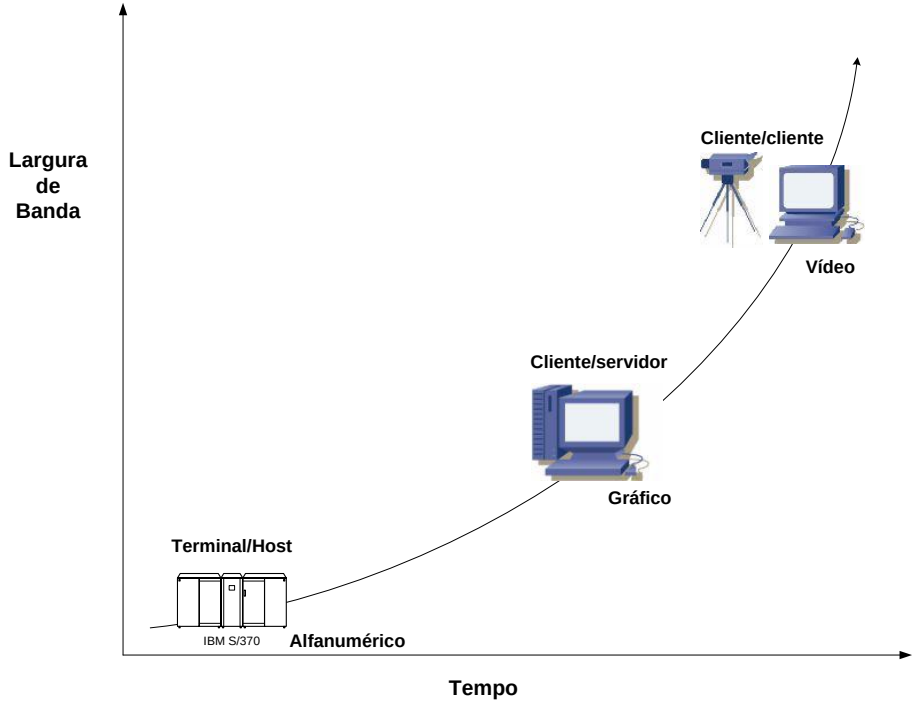
- Mais de 50% das paralisações de rede estão relacionadas ao cabeamento
- Deve-se observar as distâncias máximas e pontos fortes e fracos de cada topologia de fiação
- Veja especificações em: http://www.hp.com/rnd/pdfs/10gig_cabling_technical_brief.pdf

Aspectos sobre Gerenciamento de Rede

- Abrangência:
  - Plataforma de Gerenciamento
    - ✓ Centralizado (menores redes, devido ao custo do pooling) ou distribuído (mantido regionalmente, administração e diagnósticos mais complexos)
    - ✓ SNMP, RMON
  - Ferramentas de Gerenciamento
  - Administração de usuários finais e preparação para crescimento da rede
    - ✓ Previsão de VLANs, estratégias pré-definidas para mudanças, inclusões e alterações
- Aspectos Comerciais
  - Considerações orçamentárias são críticas no projeto

Projetando LANs de Campus

- Evolução das Redes



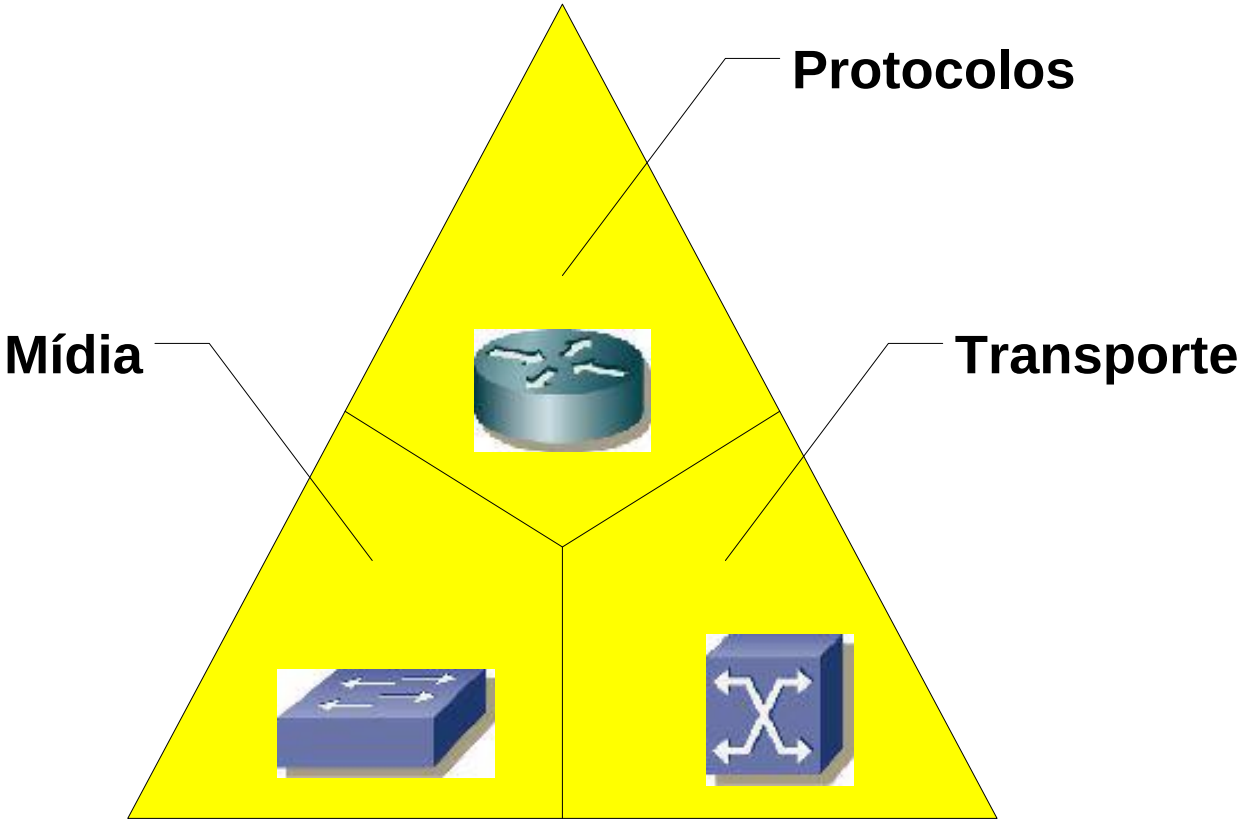
- Além de novas aplicações, as CPU evoluem, e as organizações crescem. A escalabilidade deve ser planejada

Determinando o “Problema” da Rede

- A escolha de um dispositivo de conectividade depende do problema do cliente
  - Contenção de mídia – excesso de colisões por excesso de nós, excesso de *broadcasts* devido aos protocolos usados
  - Falta de pessoal qualificado para configurar e gerenciar
  - Necessidade de transportar novas mídias
  - Necessidade de estar dentro de um orçamento limitado

Categorizando e Propondo Soluções

- São três as categorias de problemas:

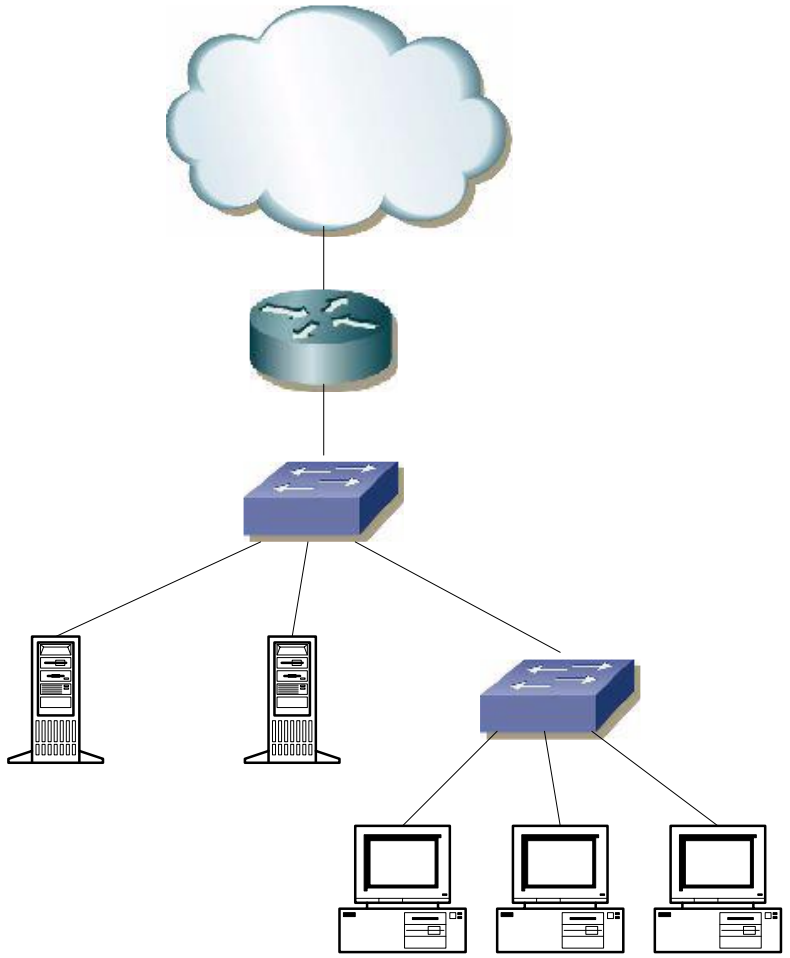


Categorias de Problemas

- **Mídia**
  - Carga de rede alta → congestionamento
  - Solução: comutador de LAN e VLANs
    - ✓ Analisar a quantidade de portas, escalabilidade e eficácia de custos de acordo com a dimensão do problema
- **Protocolos**
  - Grande dependência de *broadcasts* (NetBIOS, ARP) → congestionamento
  - Solução: Comutador de LAN com VLANs ou Roteamento
    - ✓ Divisão da rede em segmentos
    - ✓ Analisar a taxa de tráfego requerida, recursos necessários, escalabilidade e eficácia de custos de acordo com a dimensão do problema
- **Transporte**
  - Necessidade de Alta largura de banda e baixa latência → degradação do serviço
  - Solução: Comutação ATM ou 10 Gigabit Ethernet
    - ✓ Analisar os requisitos de tráfego requeridos (característica do fluxo, velocidade), recursos necessários (QoS), escalabilidade e eficácia de custos de acordo com a dimensão do problema

Problemas de Mídia

- Microsegmentação: uso de switches em full-duplex para melhor desempenho de um *backbone* ou *Workgroup*
- O uso de VLANs melhora bastante o cenário
- Servidores devem ser conectados à portas de comutação dedicadas



Problemas de Mídia

- Tempestades de *Broadcasts* - há limites teóricos para uma LAN (ou VLAN):

Protocolo	**Número Máx. Estações**
IP	500
IPX	300
AppleTalk	200
NetBIOS	200
Rede híbrida	200

- Regra básica: 80% do tráfego deve ser local e apenas 20% para outra LAN (servidores ou *hosts* de outras VLAN)
- Com o surgimento dos *WEB services*, esta regra pode ser quebrada com cuidado para evitar gargalos

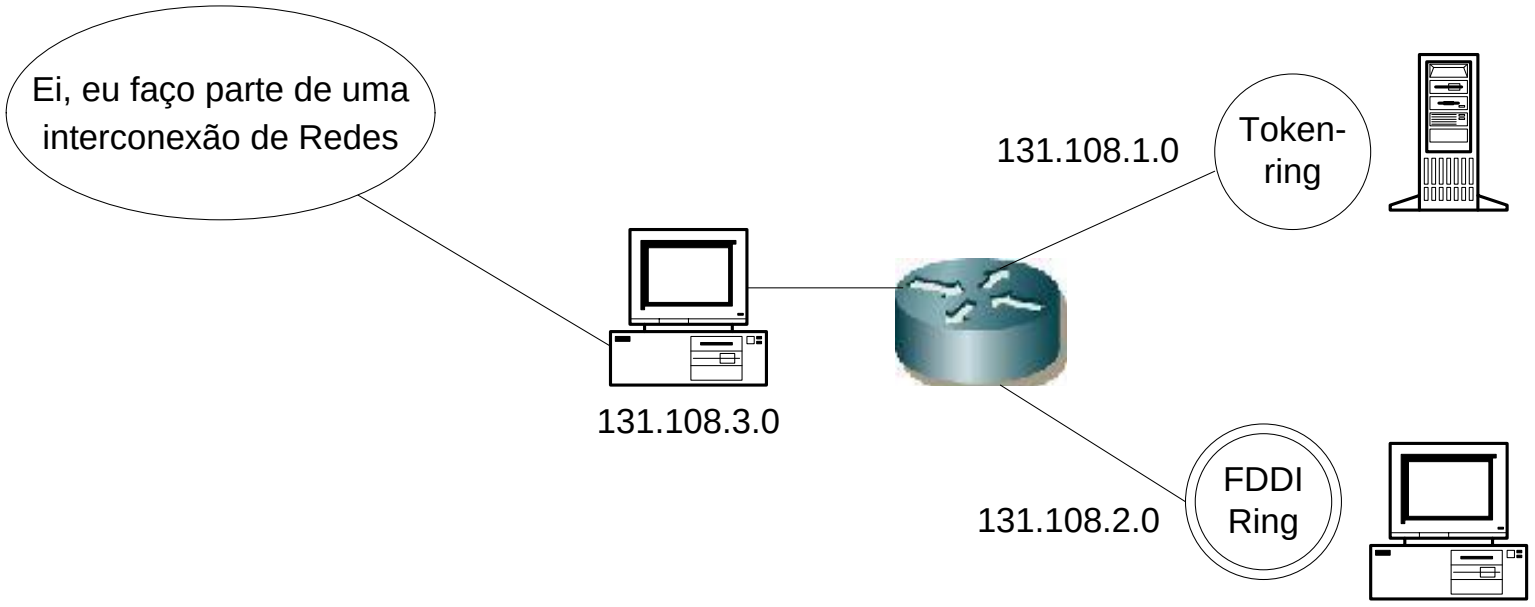
Regras de Projeto

- Regra 1: Use roteadores para interconexão de redes
  - Com isso, filtra-se os *broadcasts* e multicasts, e converte-se mídia[2], quando necessário
  - Recursos dos roteadores:
    - ✓ Comunicação entre LANs de diferentes padrões
    - ✓ Endereçamento hierárquico
    - ✓ Políticas de roteamento
    - ✓ Roteamento com QoS
    - ✓ Segurança
    - ✓ Filtro de broadcasts e multicasts
    - ✓ Redundância e balanceamento de carga
    - ✓ Gerenciamento de fluxo de tráfego
    - ✓ Associação à grupos multimídia (multicast)

2 – Esta conversão é L2, ou seja, ethernet para ATM, por exemplo.

Regras de Projeto

- Regra 2: use roteadores impondo uma estrutura lógica
  - Com comutadores, endereços desconhecidos são “espalhados” para todas as portas se não estiverem com VLANs configuradas

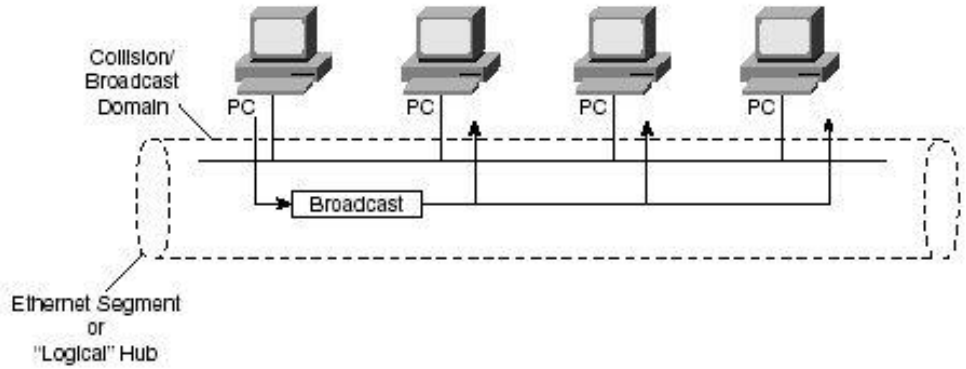


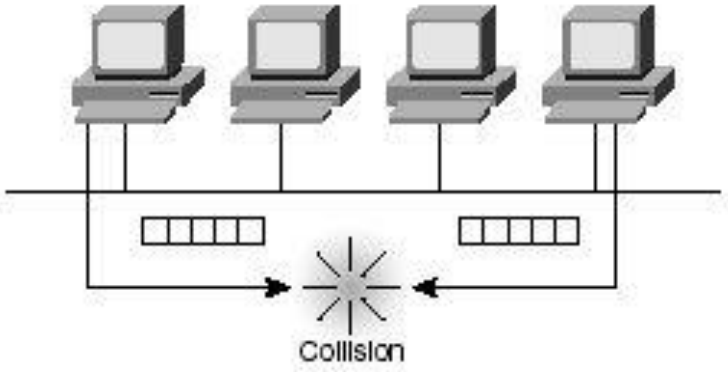
Tecnologia de LAN

- Opções de Tecnologia de LAN atuais:
  - ***Ethernet*** – simples e de baixo custo (10, 100, 1000 Mbps ou 10Gbps)
- Legadas:
  - **Token-ring** – pouco usada, opera a 4 ou 16 Mbps
  - **FDDI** – tecnologia estável, oferece 100 Mbps com redundância
  - **ATM** – flexível e excelente desempenho (OC-48 – 2,4 Gbps), permite implementação de garantia de requisitos de QoS, mas é cara

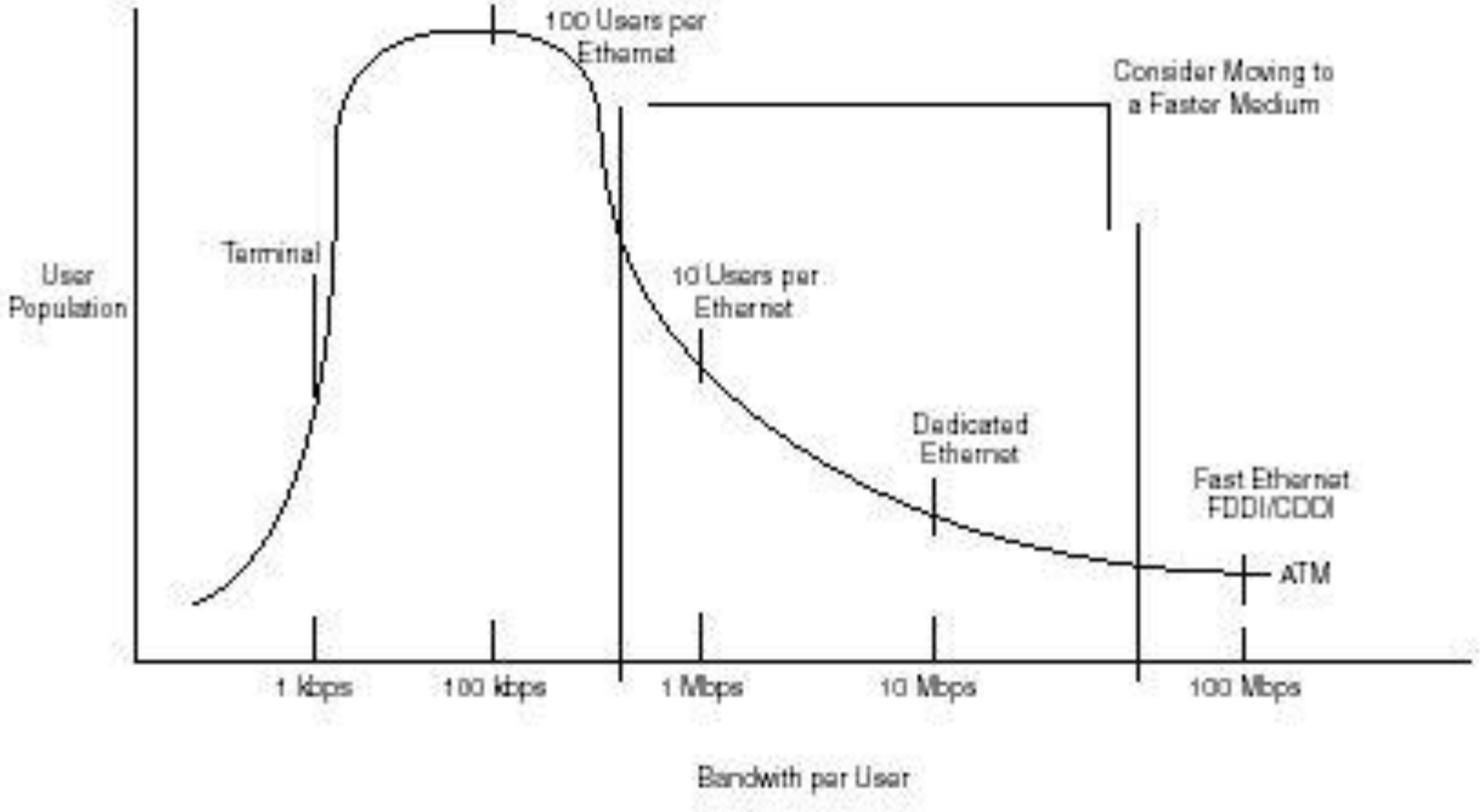
Ethernet

- Em cabos coaxiais e hubs, usava colisões para controle de acesso
- Comutadores segmentam os domínios de colisão, mas não os de *broadcast*
- Devido a isso, apenas 35% a 40% da banda fica disponível para aplicações



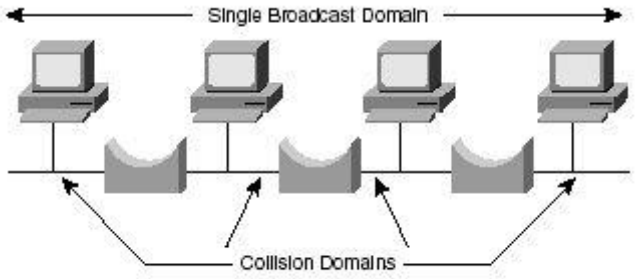


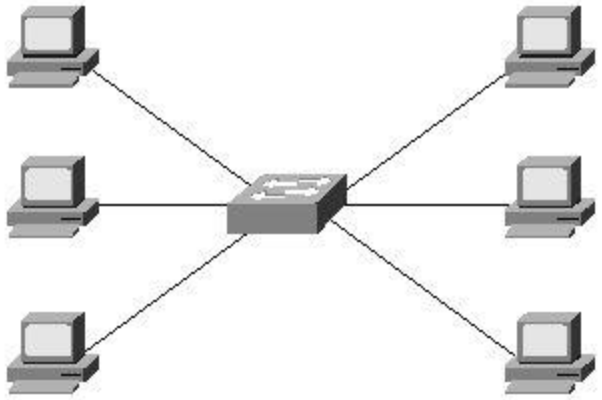
Ethernet – Demanda de Banda



Ethernet - Segmentação

- Comutadores segmentam domínios de colisão, dedicando toda a banda (10, 100 ou 1000 Mbps) em cada sentido do fluxo em cada uma de suas portas
- Em full-duplex o *throughput* é o dobro que half-duplex
- Há três tipos de comutação:
  - *Cut-through* – comutador lê apenas os primeiros 48 bits (MAC destino – DA), sem verificação erro e despacha → é rápida mas não filtra os erros
  - Fragment-free – lê os primeiros 64 bytes sem verificação de erro
  - *Store-and forward* – Comutador lê todo o quadro, verifica erro e só então encaminha-o para o destino





Ethernet - Evoluções

- Fast Ethernet
  - 100Mbps num menor diâmetro de rede em *half-duplex,* considerando os cabos coaxiais em 10Mbps
  - Operação em *full-duplex* elimina colisões
- Gigabit Ethernet
  - A tecnologia Fibre Channel possibilitou esse upgrade
  - Também reduz o diâmetro de rede
- 10Gbit Ethernet
  - Já disponível principalmente para portas de uplink, tipicamente através de módulos SPF
  - Só opera em full-duplex

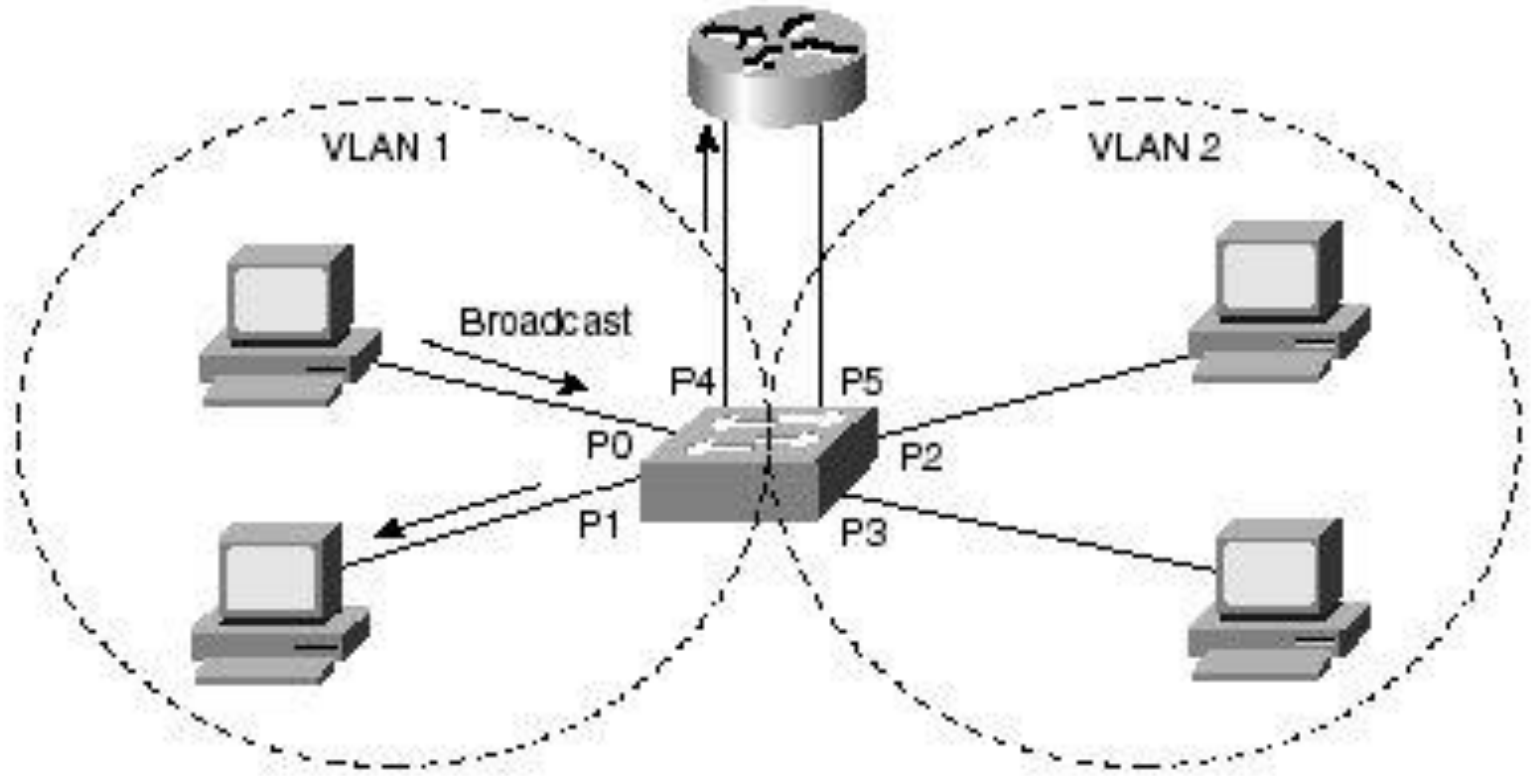
Legadas: Token-Ring, FDDI e ATM

- Token-Ring
  - Não há colisões, permite alcance de 90% da banda disponível
- FDDI
  - É uma tecnologia de anel lógico de fibra onde o anel redundante permanece inoperante até que ocorra um problema
  - É considerado legado por ser preterido pelo ATM e Gigabit Ethernet
- ATM
  - Combina as vantagens da comutação de circuitos (taxa e retardos garantidos) com a de pacotes (eficiência no tráfego de rajadas)
  - Aceita opções de QoS com largura de banda alta

Escalando uma Rede Comutada

- A escalabilidade de uma rede comutada depende dos protocolos em uso
- Estações NetBIOS enviam broadcasts até para saberem seu próprio nome
- Redes IP podem ter até mais de 1000 estações, com a desativação de serviços desnecessários e o uso de VLANs
- A criação de VLANs representa domínios de broadcasts logicamente separados, e o despacho pode ser feito de acordo com uma associação de porta física, endereço MAC, endereço de rede ou até mesmo características de quadro. Para interligar VLANs, é necessária comutação de nível 3 ou um roteador

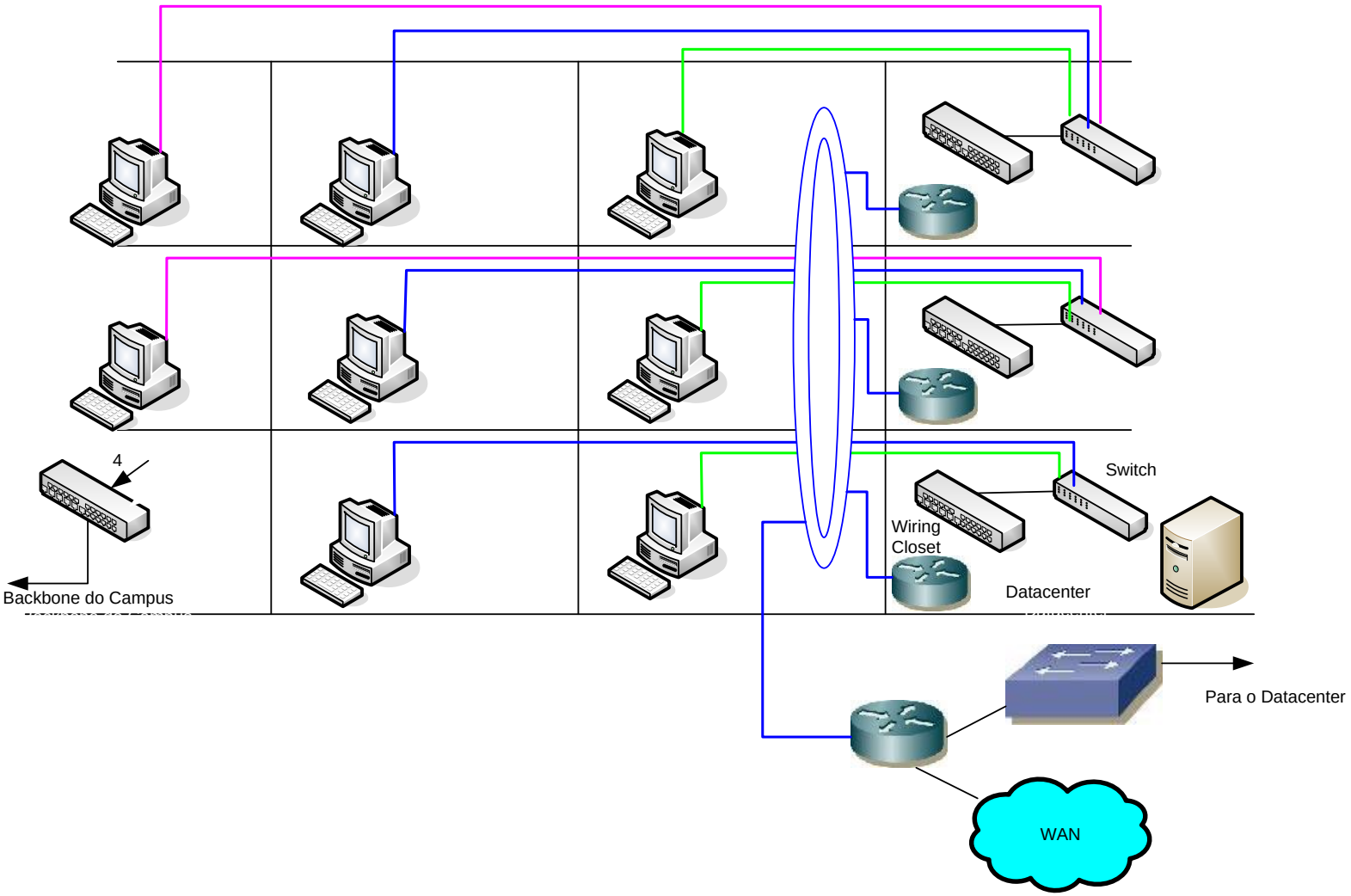
VLANs



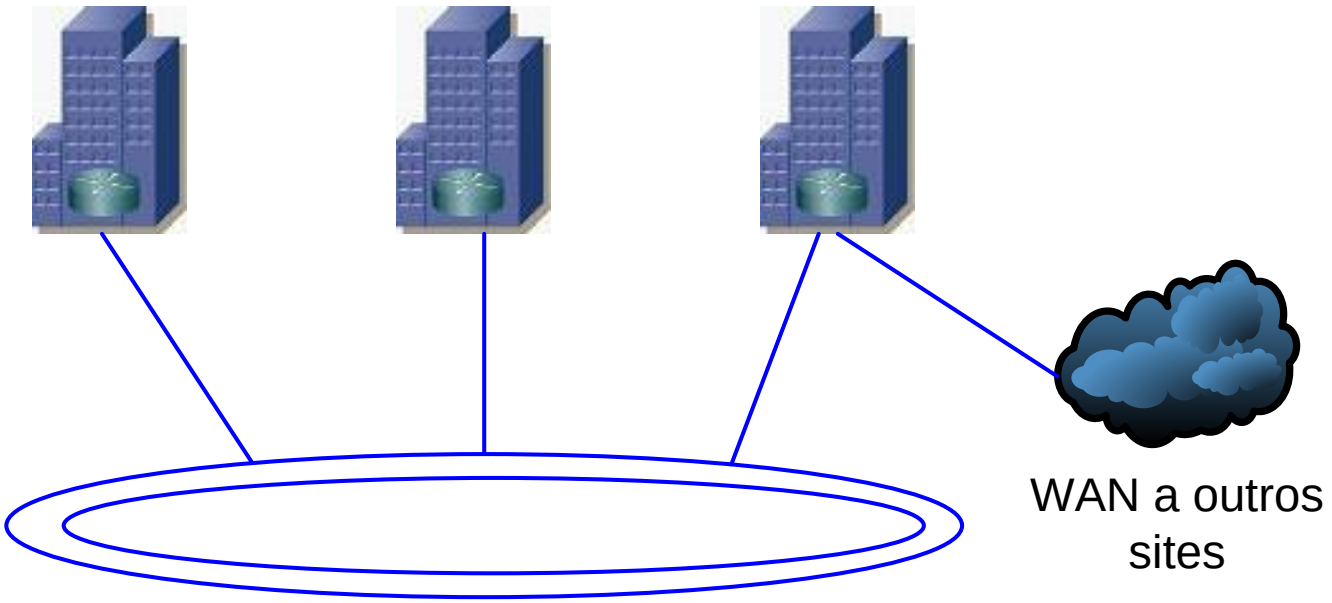
Modelos de Projeto de LAN

- ***Backbones* Distribuídos**
  - Evitam o ponto único de falha
  - Menos flexíveis, dificultando inclusões, migrações e alterações de usuários
  - Mais caros e dependentes de esquemas detalhados de endereçamento
  - O *backbone* deve ser apenas um caminho de trânsito entre as LANs dos andares
  - Num Campus, pode-se usar um único roteador por prédio, com comutadores oferecendo acesso interno a cada estação do prédio

Backbone Distribuído em um Prédio



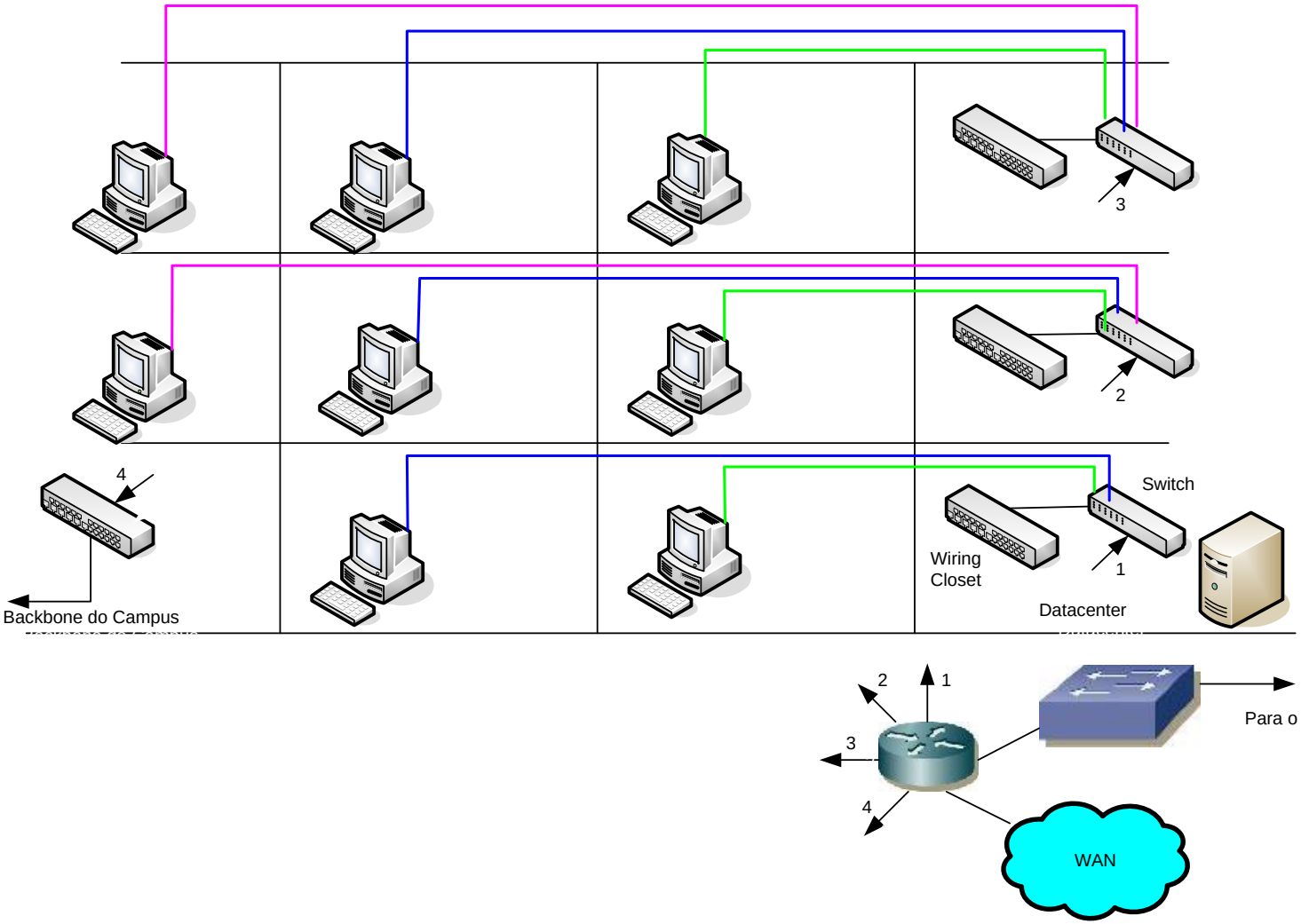
Backbone Distribuído no Campus



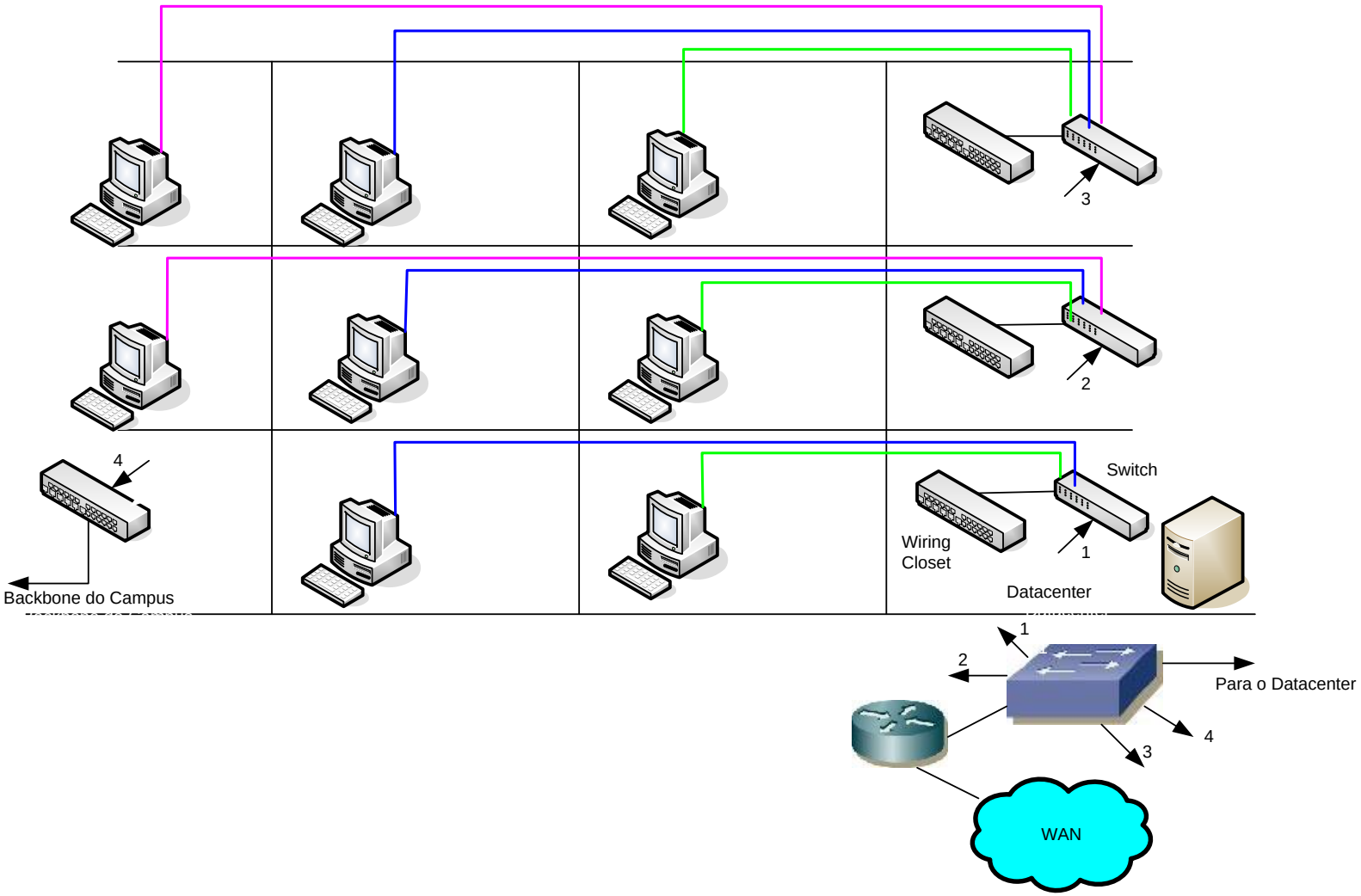
Modelos de Projeto de LAN

- **Backbone Colapsado**
  - Mais flexível e eficaz
  - Roteador é ponto único de falha e gargalo para a rede
  - Pode ser facilmente estendido para acomodar VLANs

Backbone Colapsado roteador - comutador

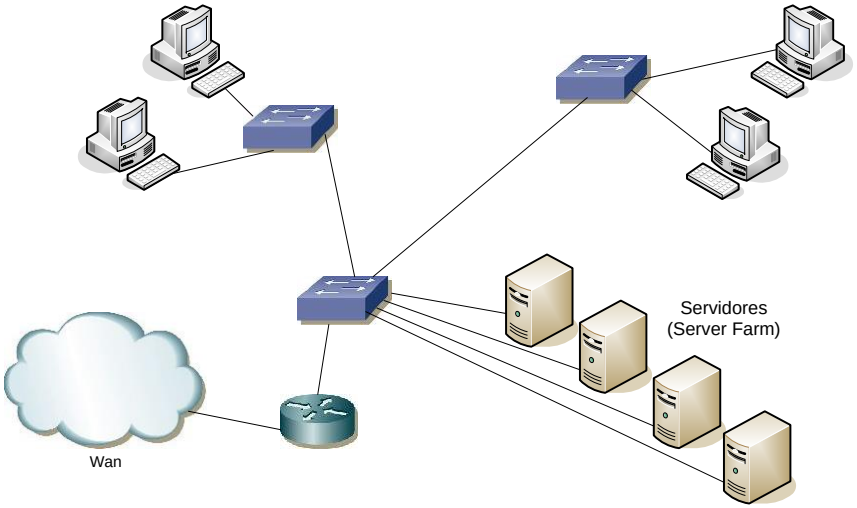


Backbone Colapsado - VLAN

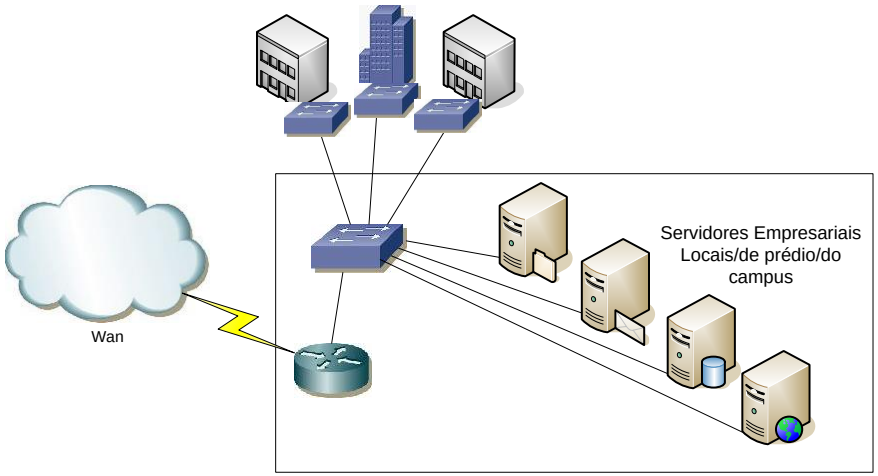


Empregando VLANs

- Independente de localização física
- Os atributos de VLAN devem objetivar a regra 80/20



Backbone Colapsado – VLAN de prédio



Backbone Colapsado – VLAN de Campus

Endereçamento - DHCP

- O uso do DHCP no projeto de LAN simplifica o processo de migrar/incluir/alterar na rede
- Oculta totalmente a complexidade da estrutura de endereçamento
- Deve ser adotado, sempre que possível

UNICARIOCA 25 anos
Centro Universitário

Cadeira de Projeto de Redes

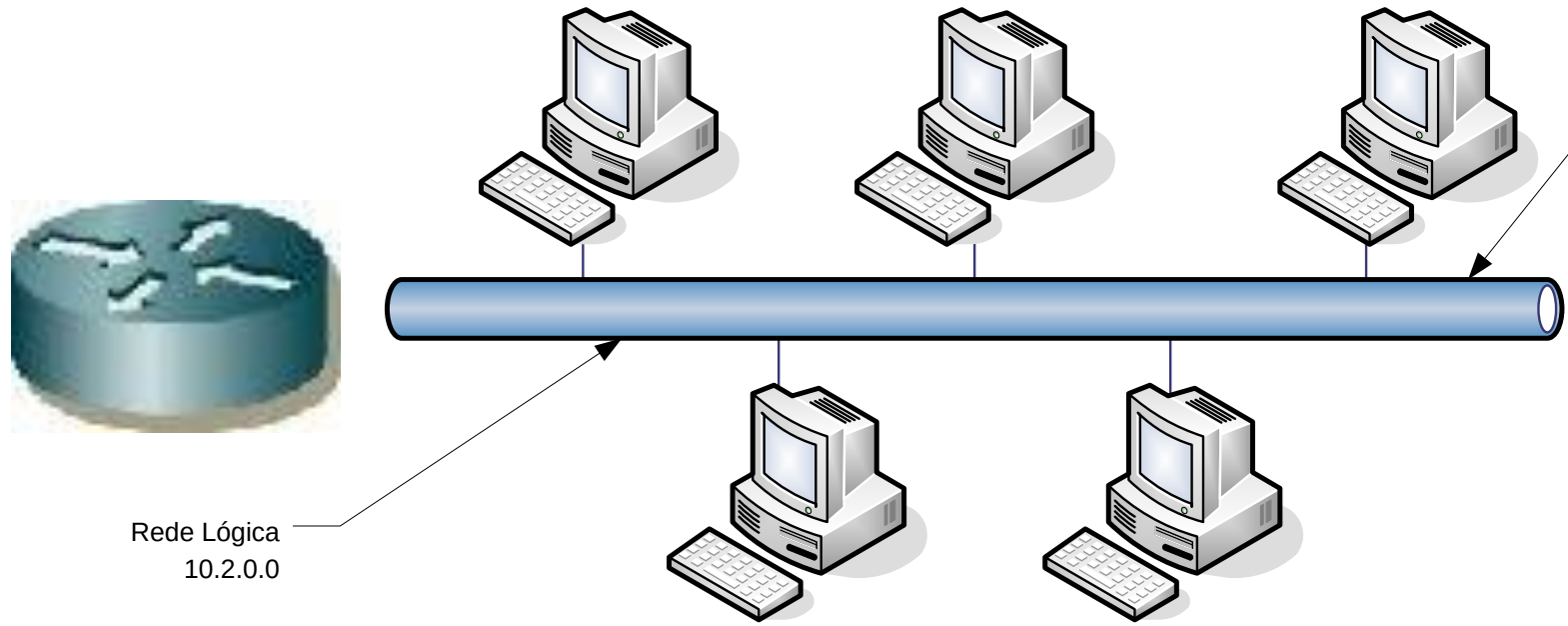
Módulo I

Projeto TCP/IP

Visão Geral de um Projeto TCP/IP

- Decisão mais importante: como manipular o endereçamento IP
- Um estratégia eficaz permitirá escalabilidade capaz de absorver uma nova tecnologia como telefonia IP sem traumas
- Redes IP
  - Característica Física
    - ✓ Definida como um único domínio de broadcasts
  - Característica Lógica
    - ✓ Possui um número particular específico do protocolo
    - ✓ Uma parte fundamental do projeto da rede lógica é o endereçamento IP e o esquema de sub-redes

Visão Geral de um Projeto TCP/IP



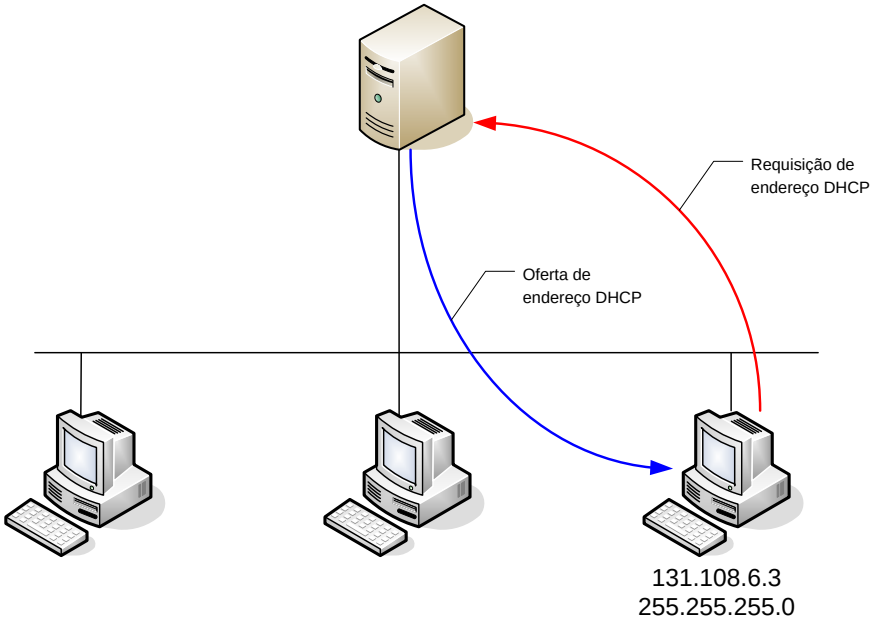
Endereçamento IP e Sub-Redes

- Há endereços IP públicos, que devem ser licenciados, e IPs privados que são disponíveis universalmente
- Cada endereço IP possui uma parte que identifica univocamente uma rede e outra um host
- Essas informações podem ser manipuladas através das máscaras de sub-rede, visando um uso mais eficaz do espaço de endereçamento

Endereço	Máscara	Rede	Host
10.16.127.104	255.255.0.0	10.16.0.0	127.104
131.16.82.97	255.255.255.0	131.16.82.0	97

Considerações sobre Endereçamento

- Primeira decisão: onde usar endereços públicos e privados
  - O uso de endereços privados depende do NAT
  - Por oferecer maior escalabilidade e menor custo, o uso interno do endereçamento privado é o mais indicado
  - Apenas hosts da DMZ devem possuir endereços públicos
- O uso do DHCP facilita alterações ágeis



Considerações sobre Roteamento

- Por tratar-se de uma estratégia que não demanda manutenção permanente, convém consultar especialistas
- São usados protocolos de dois grupos:
  - Interior Gateway Protocols (IGPs)
    - ✓ Propagam rotas para redes em uma área de controle de gerenciamento (pertencentes a um mesmo Sistema Autônomo – AS)
  - Exterior Gateway Protocols (EGPs)
    - ✓ Conexão aos Sistemas Autônomos (como é o caso da Internet)
- Podem ainda ser categorizados como:
  - Link-state
    - ✓ Anunciam apenas redes interconectadas a elas
  - Distance-Vector
    - ✓ Anunciam redes remotas apuradas por anúncios recebidos de outros roteadores
- Os roteadores podem ser configurados estaticamente (redes pequenas) ou com o uso de um protocolo de roteamento

Considerações sobre Roteamento

	IGPs	EGPs
Protocolos Link-State	OSPF, IS-IS	Nenhum
Protocolos Distance Vector	RIP, RIPv2, IGRP, EIGRP	BGP, EGP

- O BGP é o EGP mais usado na Internet, bem como o RIP é o IGP mais usado, apesar de ser obsoleto (é classfull)

Considerações sobre Segurança

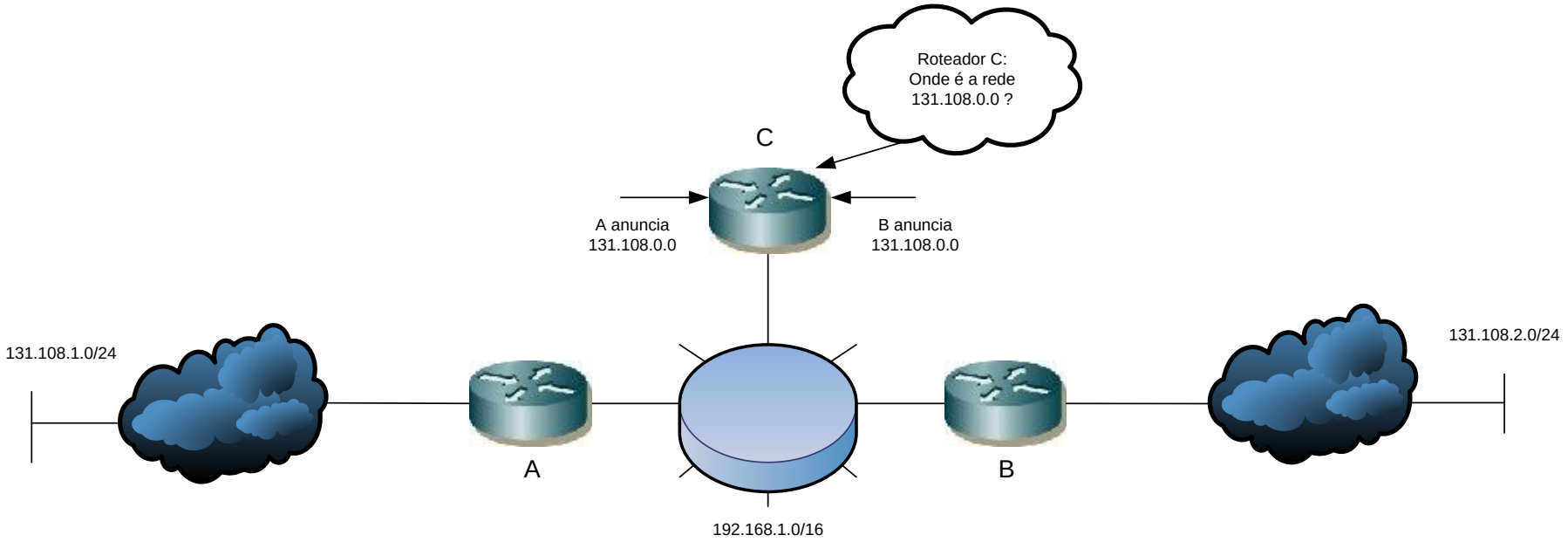
- Primeiro passo é definir a Política de Segurança (PS)
- Sistemas Firewall devem implementar as regras da PS
  - NAT
  - Proxy
  - Filtro de Pacotes
  - Registro de auditoria
  - Proteção de Login

Projeto de Endereçamento

- Decisões
  - Endereçamento hierárquico
    - ✓ Determinará sua escalabilidade

Projeto de Endereçamento

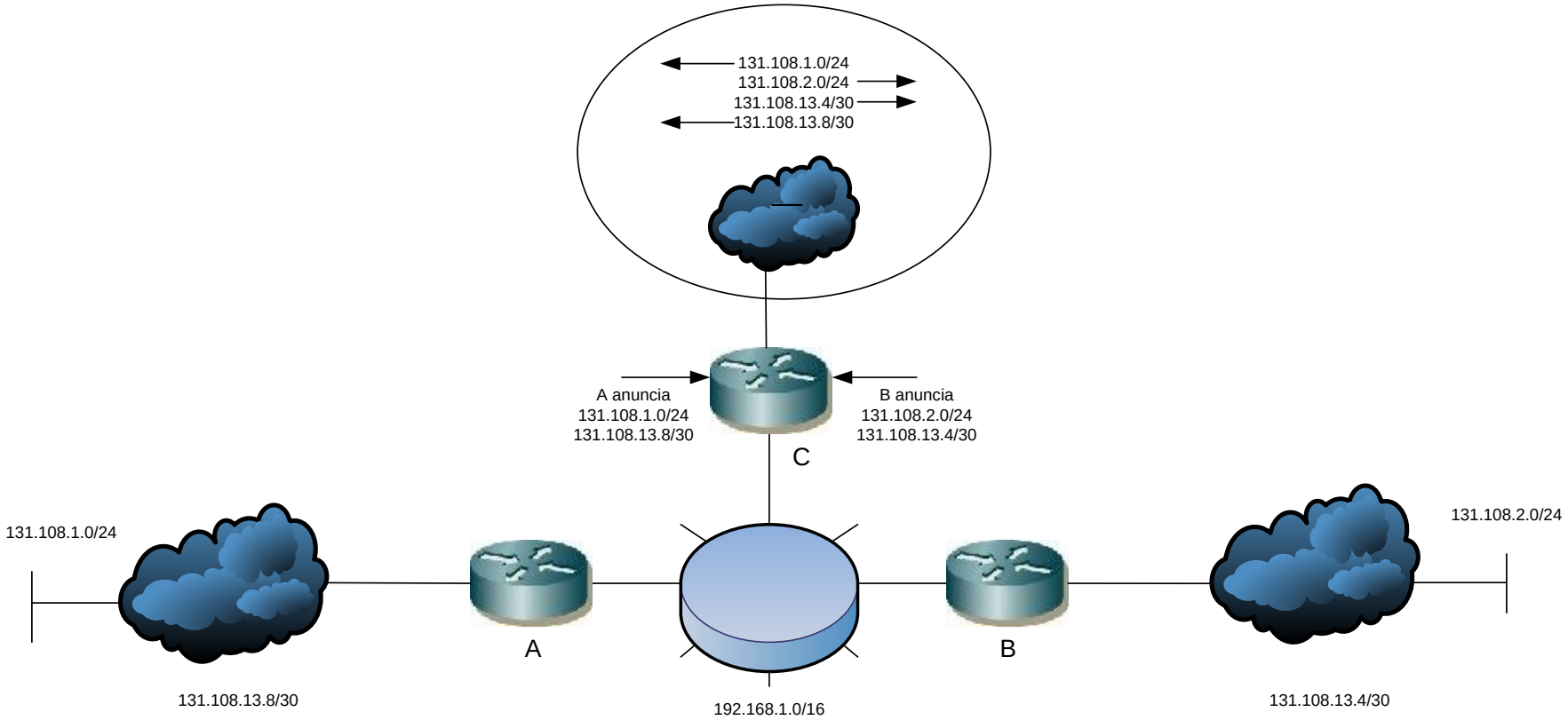
- Decisões (continuação)
  - Roteamento por Prefixo
    - ✓ O suporte ao endereçamento *classless* é diferencial
    - ✓ Nesse caso, a máscara acompanha as atualizações de roteamento



Roteamento Classfull

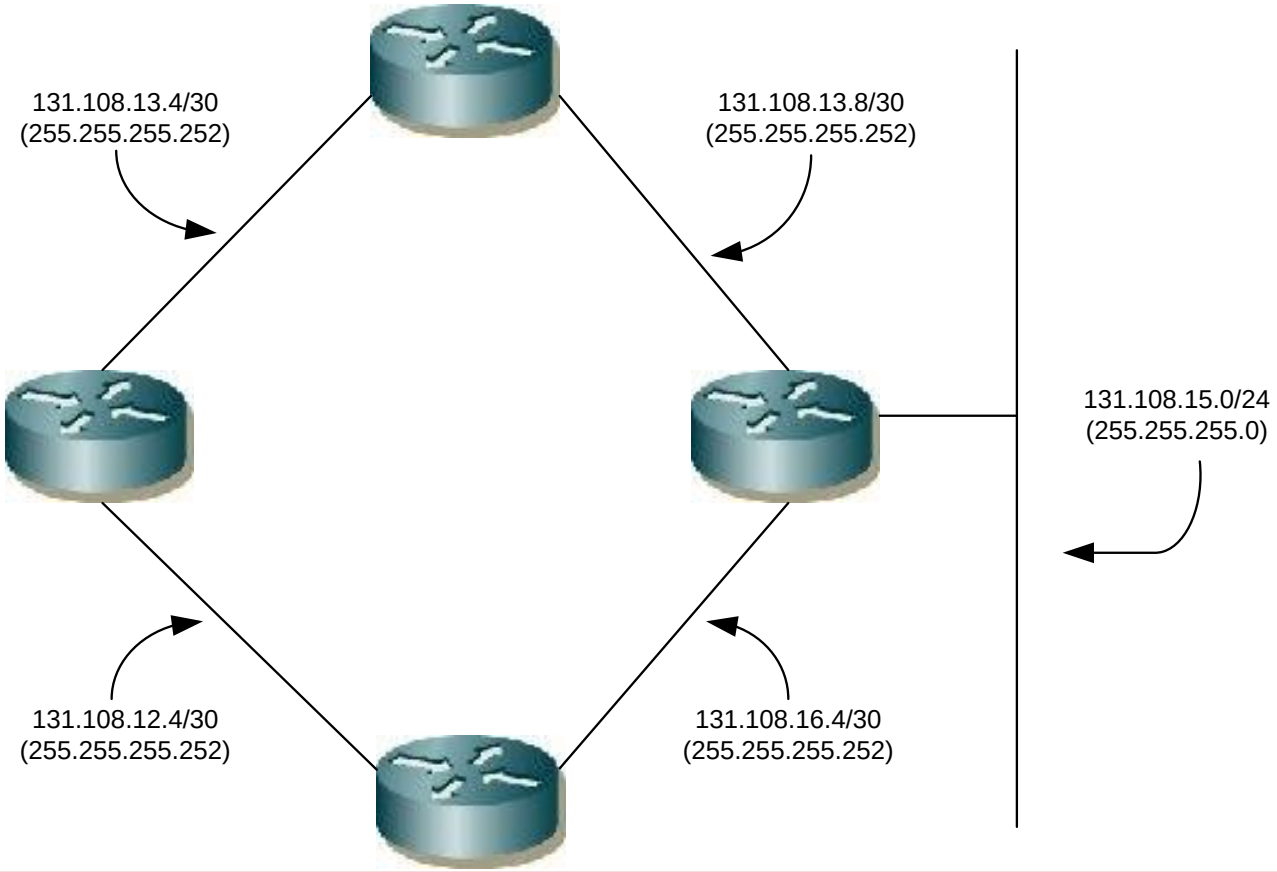
Projeto de Endereçamento

- O EIGRP, IS-IS, OSPF e RIPv2 suportam roteamento classless



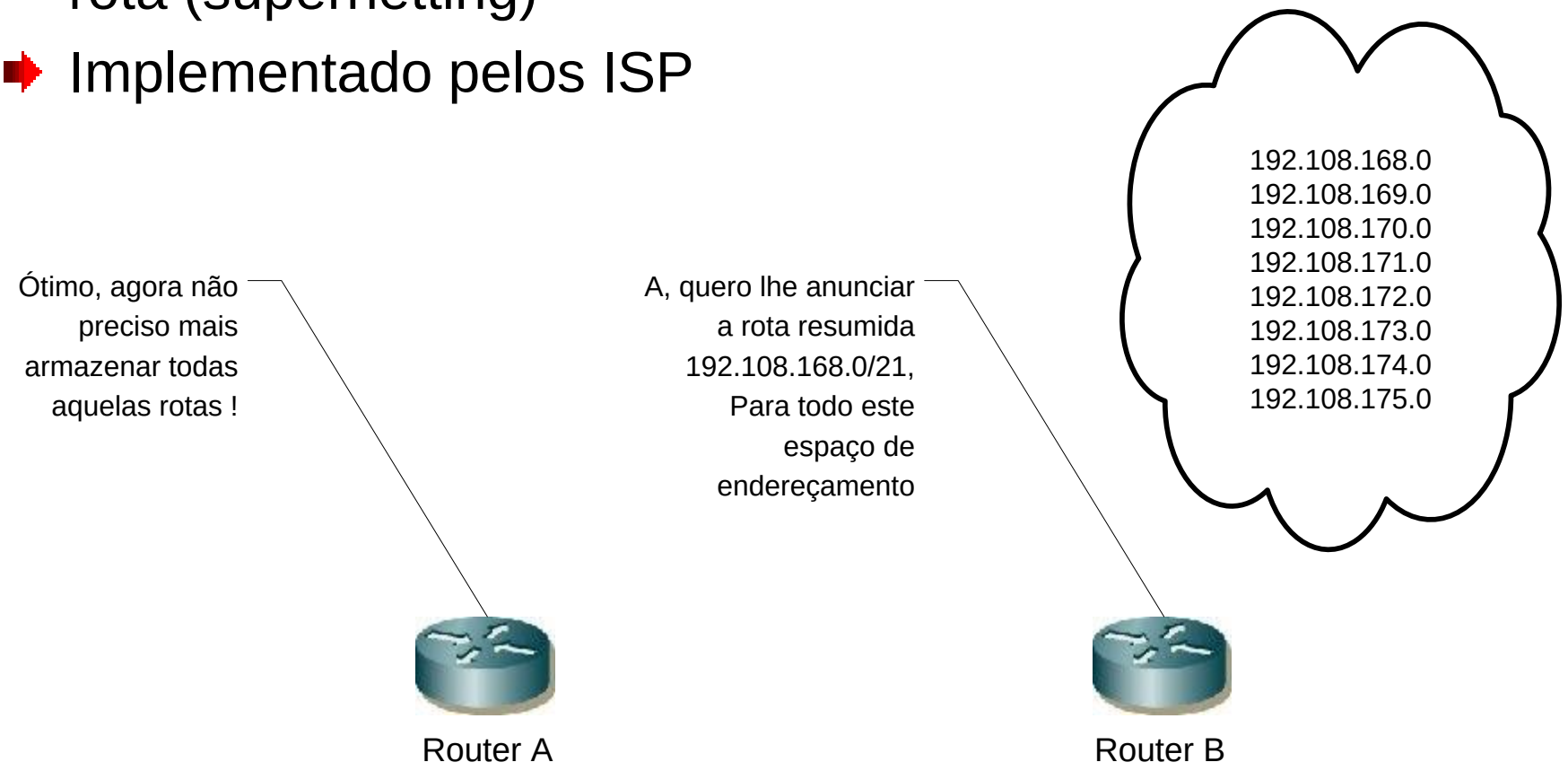
Projeto de Endereçamento

- O VLSM (*Variable Lenght Subnet Mask*) é ideal para numerar enlaces ponto-a-ponto sem desperdício de IPs



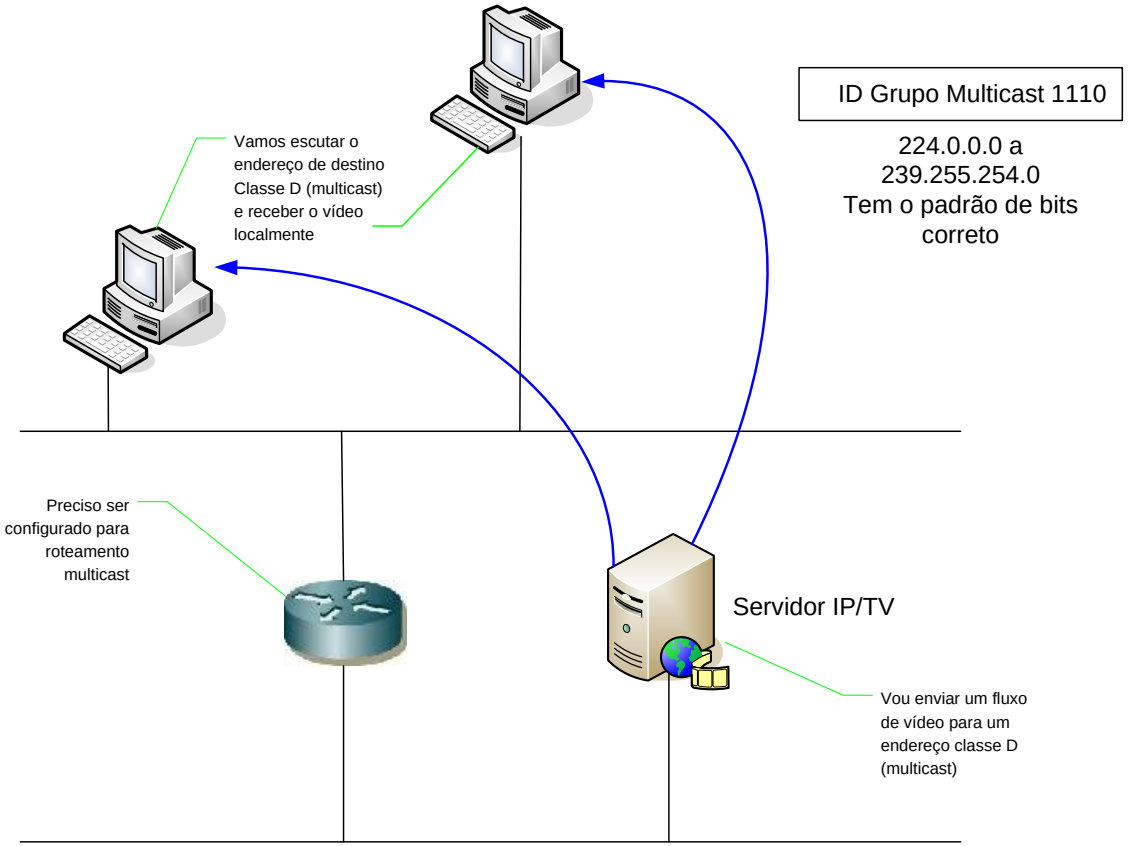
Projeto de Endereçamento

- O CIDR permite agregar blocos de redes em uma única rota (supernetting)
- Implementado pelos ISP



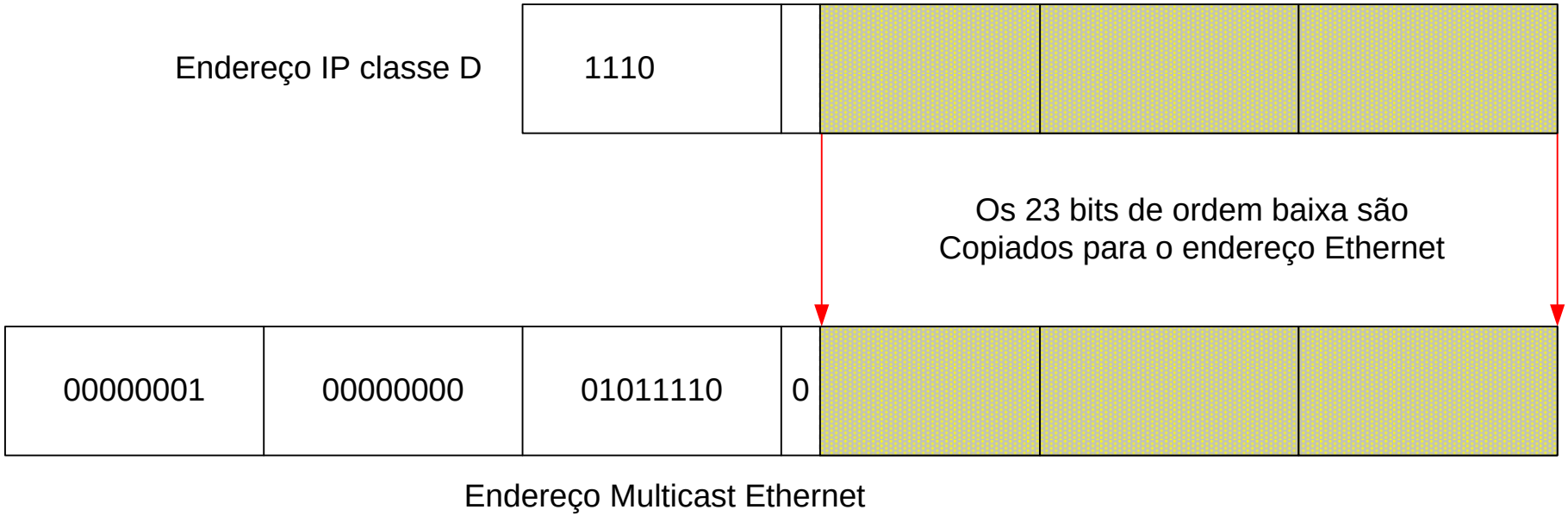
Projeto de Endereçamento

- Aspectos sobre Multicast
  - O IGMP (*Internet Group Management Protocol*) deve ser configurado nos comutadores para evitar *flooding*



Projeto de Endereçamento

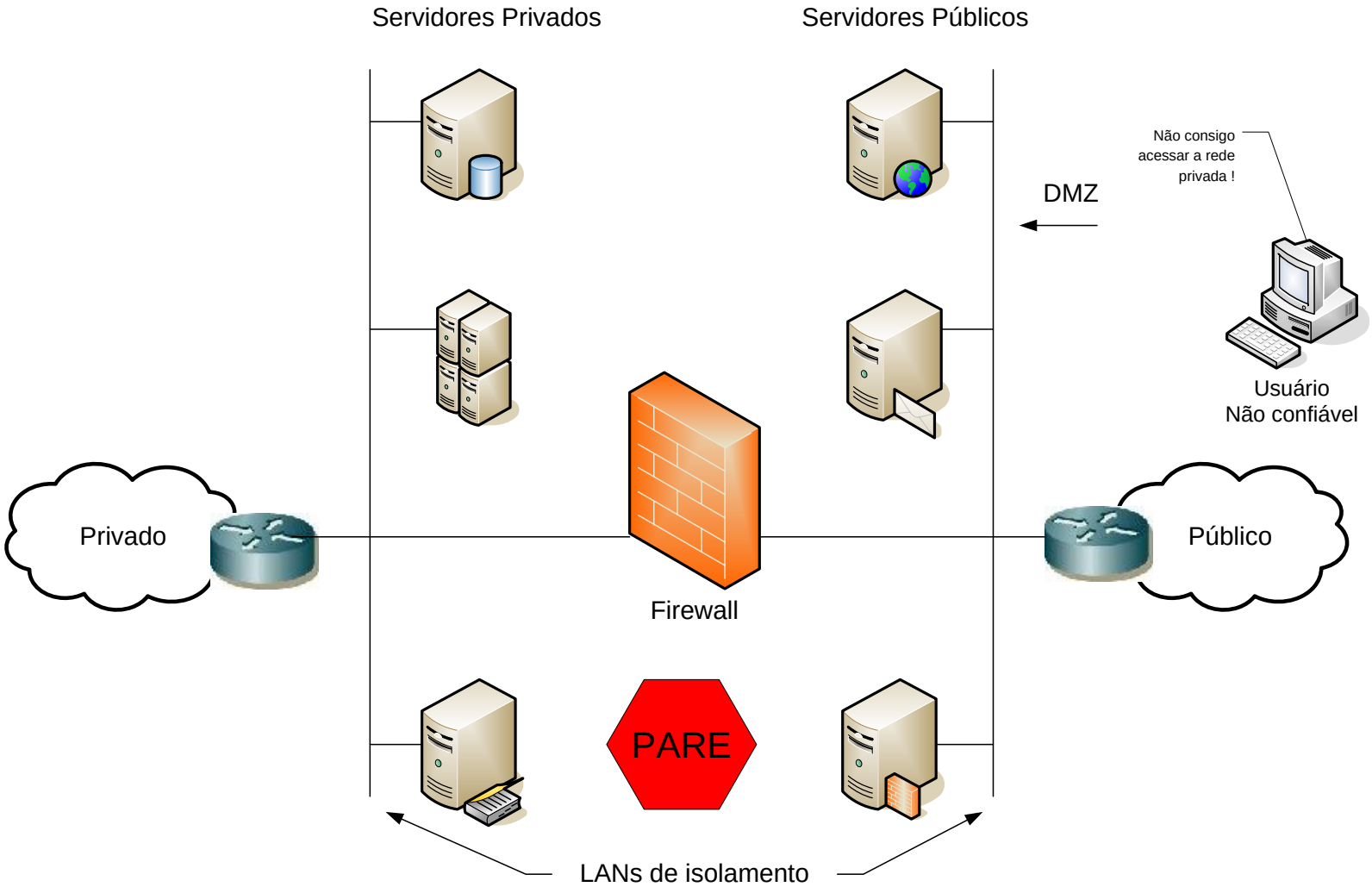
- Os endereços Multicast (classe D) são mapeados em MAC



Segurança TCP/IP

- Etapas do Projeto de Segurança:
  - Metas (objetivos) e Política de Segurança
    - ✓ Negar tudo que não é permitido ou apenas auditar a rede ?
  - Que nível de monitoramento, redundância e controle se deseja ?
    - ✓ O que deverá ser monitorado, permitido e negado ?
  - Quanto custará a solução desejada ?

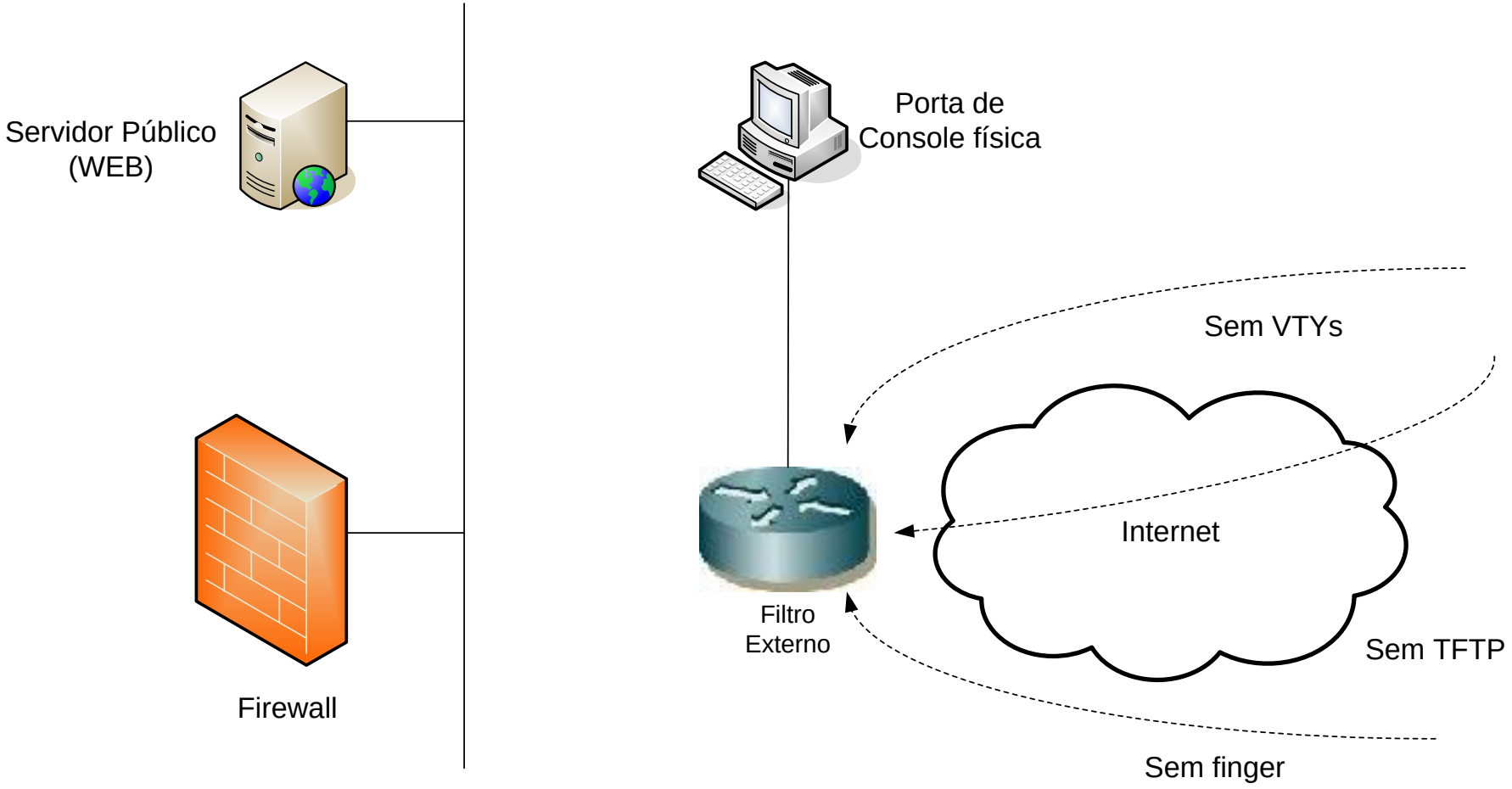
Sistema Firewall



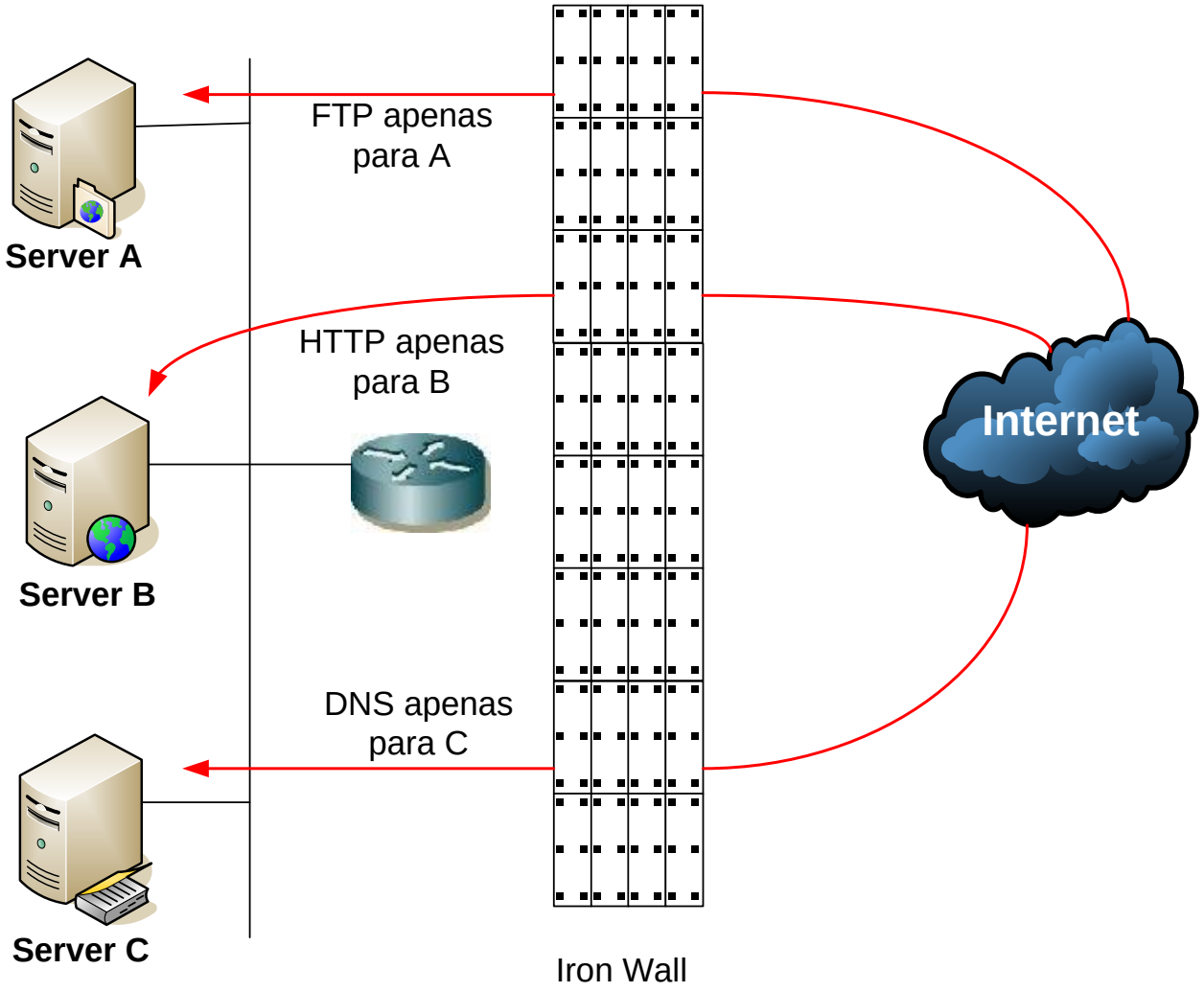
Sistema Firewall

- Serviços disponíveis ao mundo exterior na DMZ
  - FTP Server
  - Web Server
  - DNS Server
  - SMTP Server
- Funcionalidades de um Firewall
  - NAT
  - Proxy
  - Filtro de Pacotes
  - Logs
  - Proteção para logins

Sistema Firewall - Roteador



Sistema Firewall – Abordagem Iron Wall



Sistema Firewall – Evitar Spoofing