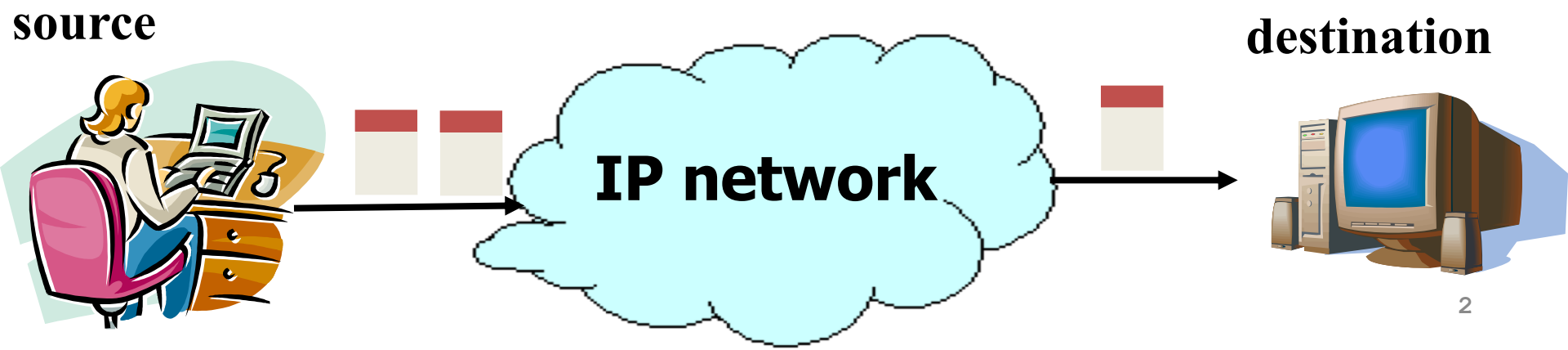
Middleboxes
ou Appliances

Slides by Jennifer Rexford. Used with permission.

Internet Ideal: Modelo de Rede Simples

- Identificadores globais únicos
  - Cada nó tem um endereço IP único e fixo
  - … alcançavel por todos e de todo lugar
- Encaminhamento simples de pacote
  - Nós de rede simplesmente encaminham pacotes
  - … ao invés de modificá-los ou filtrá-los



Realidade da Internet

- Mobilidade de hosts
  - Host muda de endereço conforme ele move
- Esgotamento de endereços IP
  - Múltiplos hosts usando o mesmo endereço
- Problemas de segurança
  - Detectar e bloquear tráfego indesejável
- Serviços replicados
  - Balanceamento de carga em replicas de servidor
- Problemas de desempenho
  - Alocação de LB, caching de conteúdo, …
- Implantação incremental
  - Novas tecnologias implantadas em estágios

Middleboxes

- Middleboxes são intermediárias
  - Colocada entre hosts que se comunicam
  - Geralmente sem o conhecimentos das partes
- Vários usos
  - Tradutores de endereço
  - Firewalls
  - Traffic shapers
  - Detecção de intrusão
  - Proxy transparente
  - Aceleradores de aplicação

"Uma aberração!"

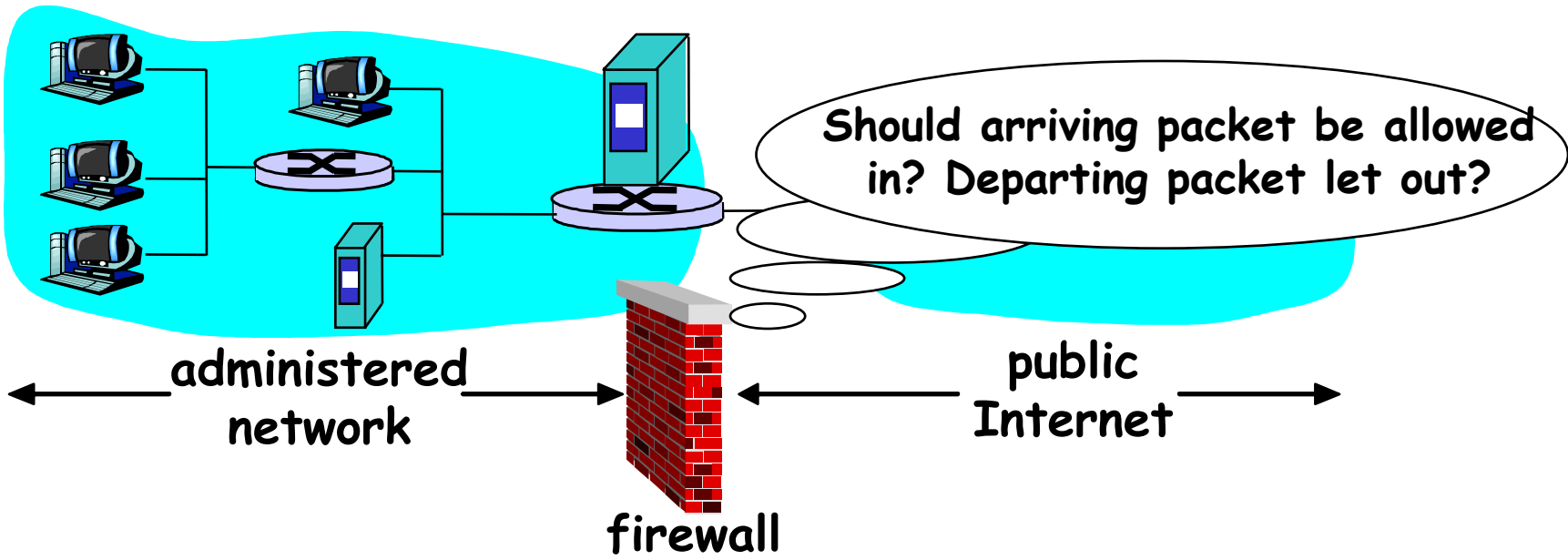
- **Viola modelo de camadas**
- **Difícil de modelar**
- **Responsável por bugs sutis**

"Uma necessidade prática!"

- **Resolve problemas reais**
- **Necessidades não vão desaparecer**

Firewalls

Firewalls



- Firewall filtra pacote-por-pacote, baseado em:
  - Endereços IP de origem e destino e números de porta
  - TCP SYN e ACK bits; Tipo de mensagem ICMP
  - Inspeção profunda em pacotes (DPI - Deep Packet Inspection) olha para o conteúdo do pacote

Exemplos de Filtragem de Pacote

- Bloquear todos os pacotes com campo IP protocol = 17 ou portas de origem ou destino = 23.
  - Todos os fluxos UDP de entrada e saída bloqueados
  - Todas as conexões Telnet bloqueadas
- Bloquear pacotes de entrada com SYN mas sem ACK
  - Previne que clientes externos estabeleçam conexões TCP com hosts internos
  - Mas permite que clientes internos se conectem com hosts de fora
- Bloquear todos os pacotes com porta TCP ou UDP do Quake

Configuração de Firewall

- Firewall aplica um conjunto de regras em cada pacote
  - Para decidir se permite (*allow*) ou nega (*deny*) o pacote
- Cada regra é um teste no pacote
  - Comparando campos dos cabeçalhos IP e TCP/UDP
  - … e decidindo se permite ou nega
- A ordem é importante
  - A primeira regra satisfeita determina a decisão

Exemplo de Configuração Firewall

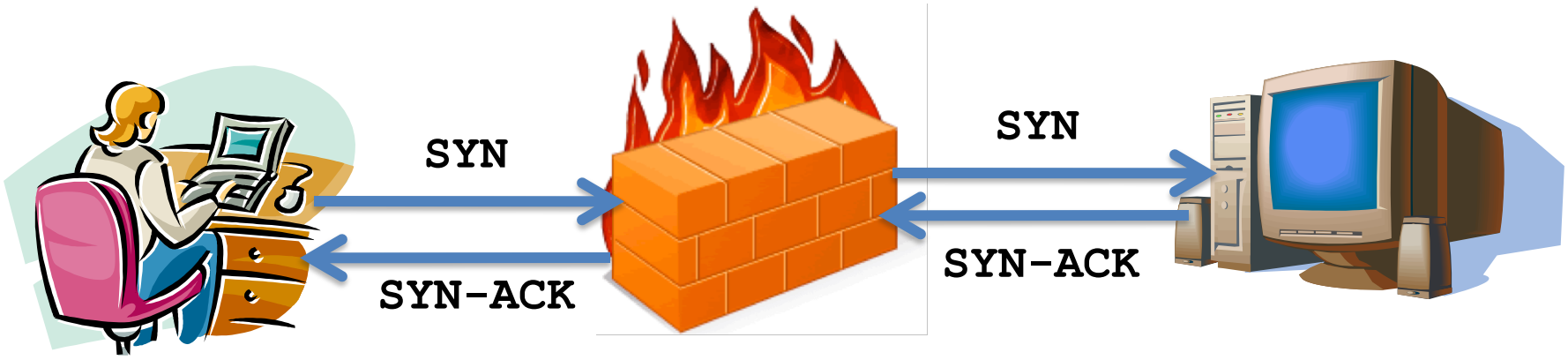
- Alice gerencia uma rede 222.22.0.0/16
- Quer permitir que a escola de Bob acesse alguns hosts
  - Bob está na rede 111.11.0.0/16
  - Hosts especiais de Alice estão em 222.22.22.0/24
- Alice não confia em Trudy, que está na rede de Bob
  - Trudy está em 111.11.11.0/24
- Alice não quer nenhum outro tipo de tráfego Internet

Firewall Configuration Rules

- #1: Nega as máquina de Trudy
  - Deny (src = 111.11.11.0/24, dst = 222.22.0.0/16)
- #2: Permite acesso da rede de Bob aos hosts especiais
  - Permit (src=111.11.0.0/16, dst = 222.22.22.0/24)
- #3: Bloqueia o resta do mundo
  - Deny (src = 0.0.0.0/0, dst = 0.0.0.0/0) ou
  - Deny (src=*, dst=*)

Stateful Firewall

- Stateless firewall (sem estado):
  - Trata pacote independentemente
- Stateful firewall (com estado)
  - Mantém informações sobre conexões
  - E.g., cliente iniciando conexão com um servidor
  - … permite que o servidor envie tráfego de retorno



Uma Variação: Gerenciamento de Tráfego

- Permit vs. deny é uma decisão binária
  - Classifica o tráfego baseado em regras
  - … e lida com cada classe de forma diferente
- Traffic shaping (rate limiting – Limitação de tráfego)
  - Limita quantidade de largura de banda de certo tráfego
- Filas separadas
  - Usa regras para agrupar pacotes relacionados
  - E então escalona os grupos de acordo com pesos específicos (*weighted fair scheduling*)

Usuários Podem Burlar um Firewall

- Exemplo: filtrar acesso de uma subrede a um servidor
  - Regra de Firewall baseada nos endereços da subrede
  - … e endereço IP e número da porta do servidor
  - Problema: usuários podem acessar a partir de outra máquina
- Exemplo: filtrar P2P com base em #s de porta
  - Regra de Firewall baseada em números de portas TCP/UDP
    - E.g., permitir apenas porta 80 (e.g., tráfego Web)
  - Problema: software usando porta não tradicional
    - E.g., cliente P2P usando porta 80

Network Address Translation

Históra de NATs

- Esgotamento do espaço de enderaçamento IP
  - Claro no início da década de 80 que 2^{32} endereços não seriam suficientes
  - Trabalho começou em um protocolo successor de IPv4
- Ao mesmo tempo…
  - Compartilhamento de endereços entre vários dispositivos
  - … sem necessidade de mudanças nos hosts existentes
- Pensado como um remédio de curto prazo
  - Agora: NAT é amplamente utilizado, muito mais do que IPv6

Network Address Translation

10.0.0.1

Outbound: Rewrite the src IP addr

Inbound: Rewrite the dest IP addr

Problem: Local address not globally addressable

NAT

outside

10.0.0.2

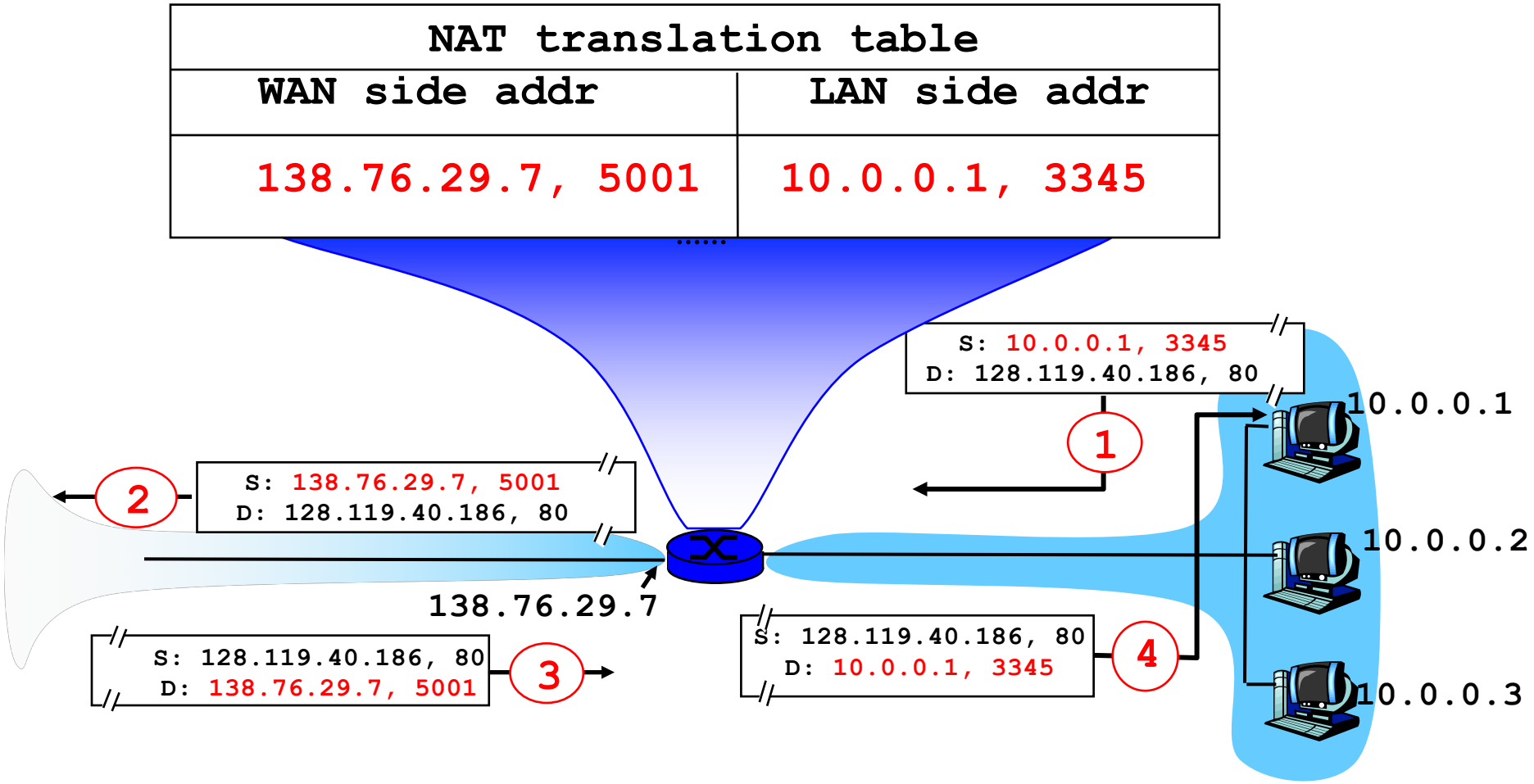
NAT rewrites the IP addresses

- Make “inside” look like single IP addr
- Change header checksums accordingly

NAT com Tradução de Portas

- Dois hosts se comunicando com o mesmo destino
  - O destino precisa diferenciar os dois
- Mapeia pacotes na saída
  - Muda endereço e porta de origem
- Mantém uma tabela de tradução
  - Mapeia (src addr, port #) para (NAT addr, new port #)
- Mapeia pacotes na entrada
  - Mapeia o endereço/porta de destino para o host local

Exemplo de NAT



Mantendo a Tabela de Mapeamento

- Crie uma entrada ao ver um pacote na saída
  - Pacote com um par (source addr, source port) novo
- Eventualmente, precisa apagar entradas para liberar espaço
  - Quando? Se nenhum pacote chegar antes de um timeout
  - (Corre o risco de interromper uma conexão temporariamente ociosa)
- Exemplo de “soft state”
  - I.e., remover estado se não atualizado durante um interval de tempo

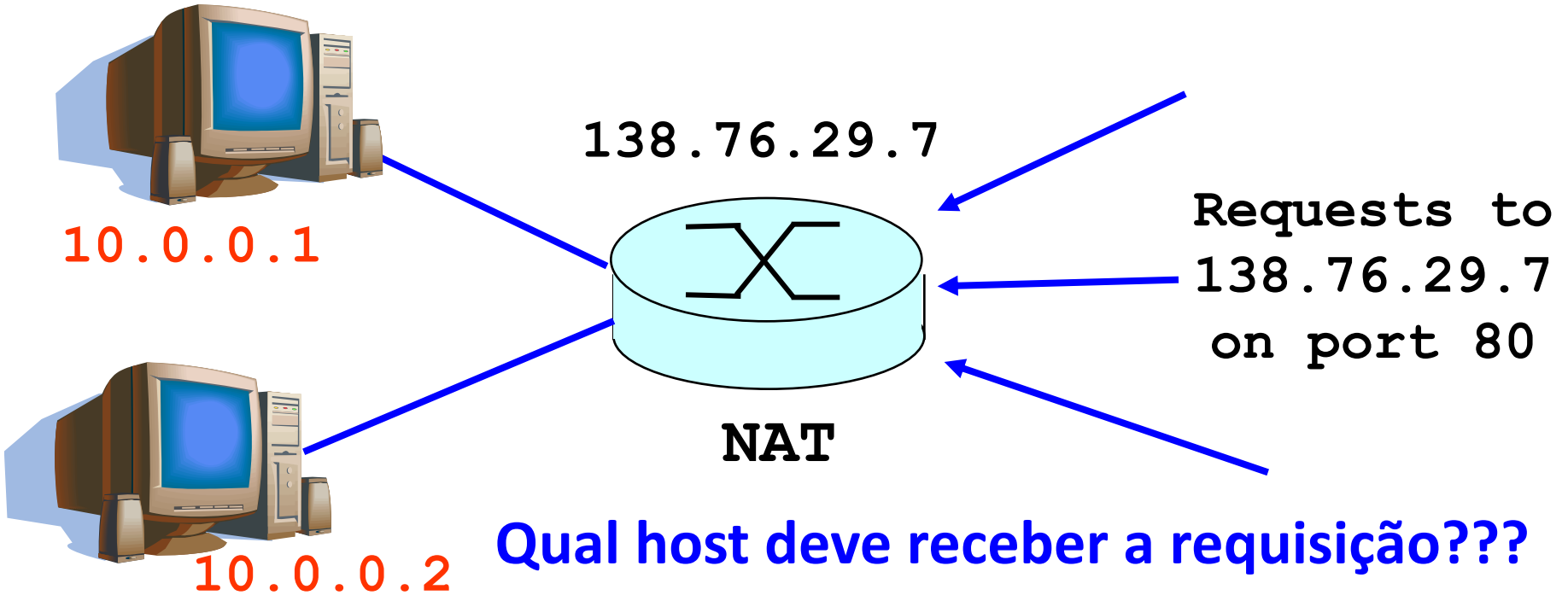
Onde NAT é Implementado?

- Roteador doméstico (e.g., Linksys box)
  - Integra roteador, servidor DHCP, NAT, etc.
  - Usa um único endereço IP do provedor de serviços

- Rede de câmpus ou corporativa
  - NAT na conexão com a Internet
  - Compartilha uma coleção de endereços IP públicos
  - Evita a complexidade de renumerar hosts/roteadores quando troca de provedor

Objeções Práticas Contra NAT

- Número de porta foi projetado para identificar sockets
  - Mas, NAT usa para identificar hosts
  - Torna difícil rodar um servidor atrás de um NAT



Qual host deve receber a requisição???

- **Configuação explicita no NAT para novas conexões**

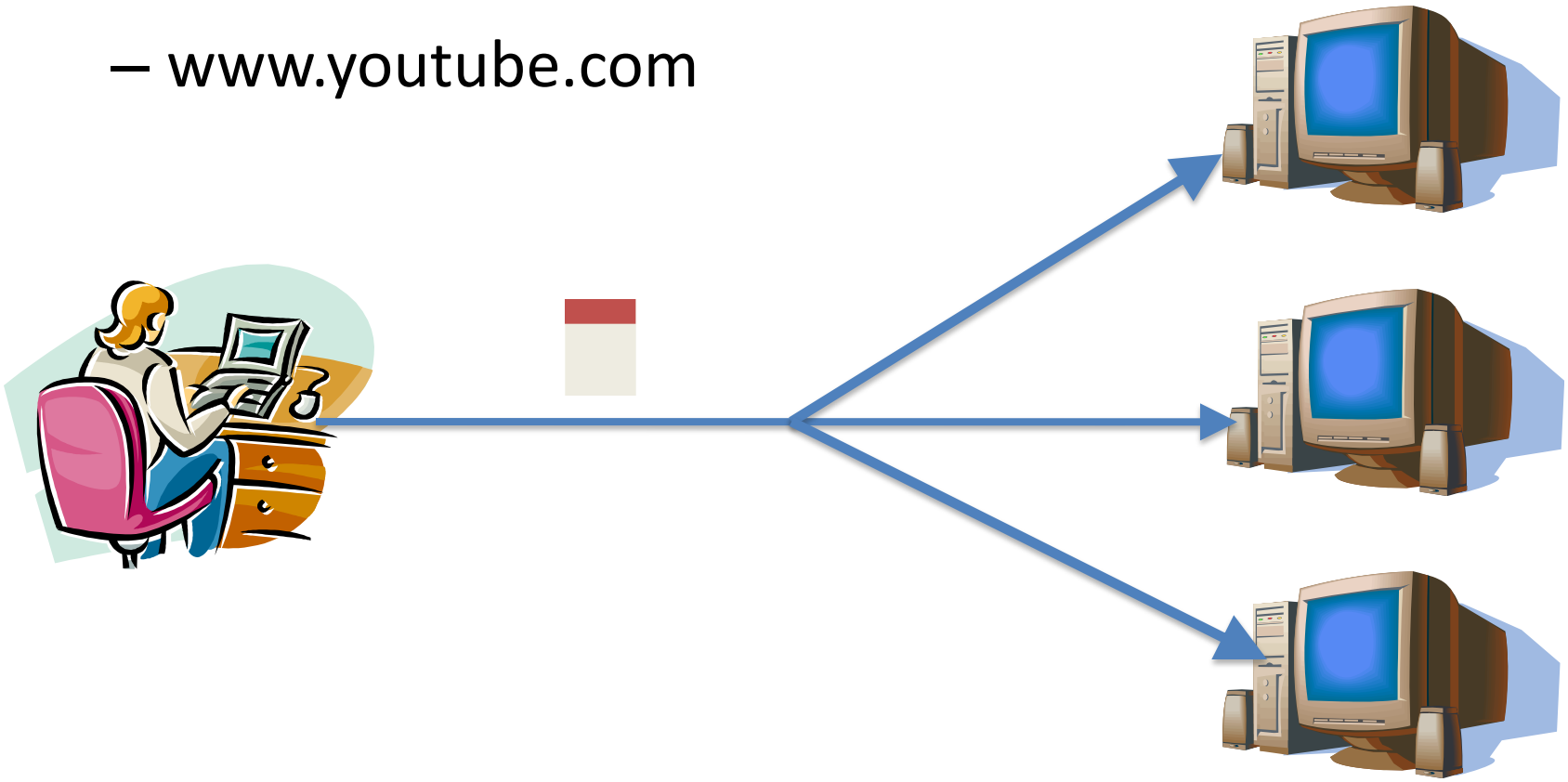
Objeções Fundamentais Contra NAT

- Roteadores não devem olhar em #s de porta
  - Camada de rede deveria se preocupar apenas com cabeçalho IP
  - … e não olhar em números de porta
- NAT viola o princípio fim-a-fim (*end-to-end argument*)
  - Nós de rede não deveriam modificar pacotes
- IPv6 é uma solução mais limpa
  - Melhor migrar do que continuar com uma gambiarra

Balanceadores de Carga
Load Balancers

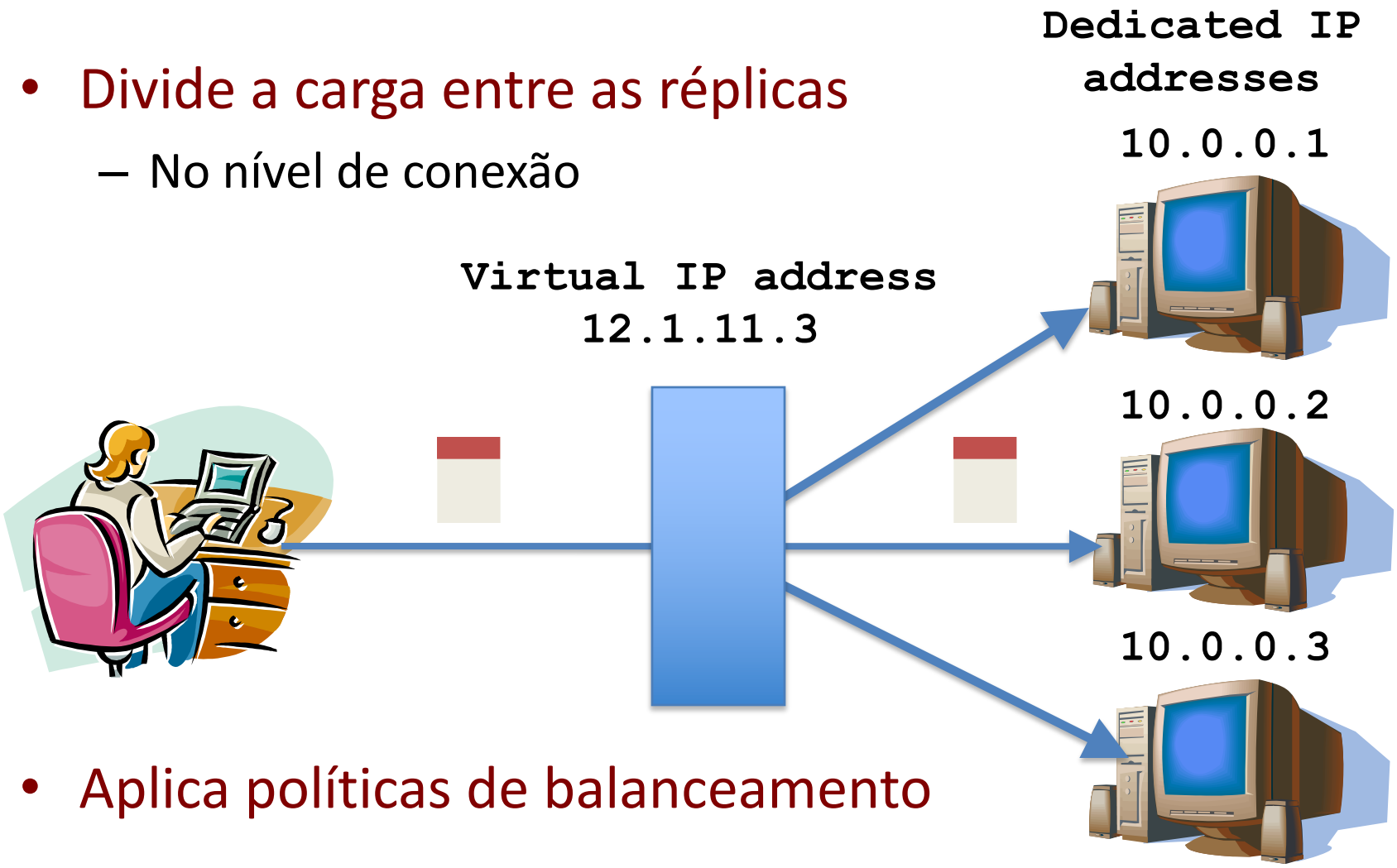
Servidores Replicados

- Um site, vários servidores
  - www.youtube.com



Balanceador de Carga

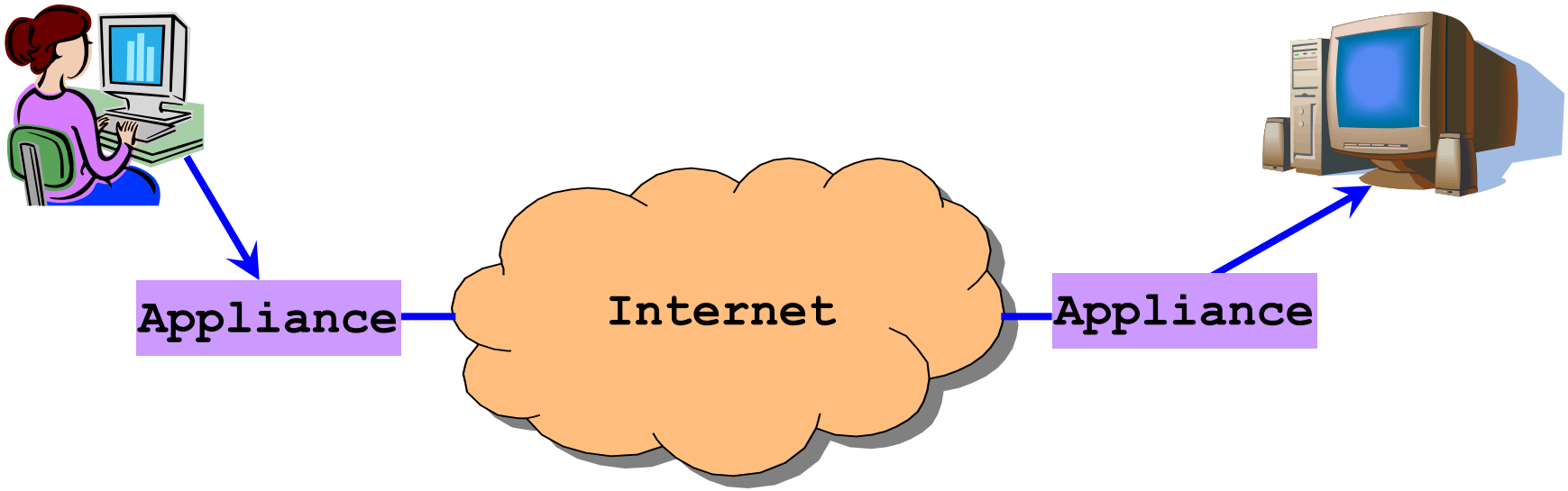
- Divide a carga entre as réplicas
  - No nível de conexão



- Aplica políticas de balanceamento

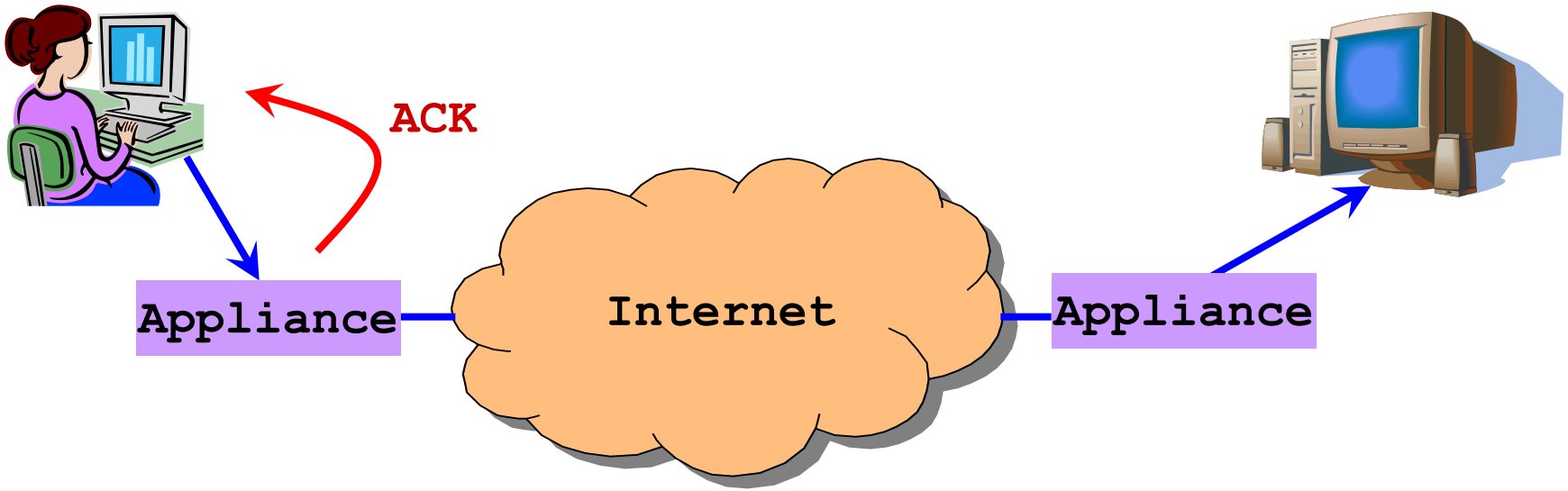
Acelaradores WAN
Wide-Area Accelerators

No Ponto de Conexão com a Internet



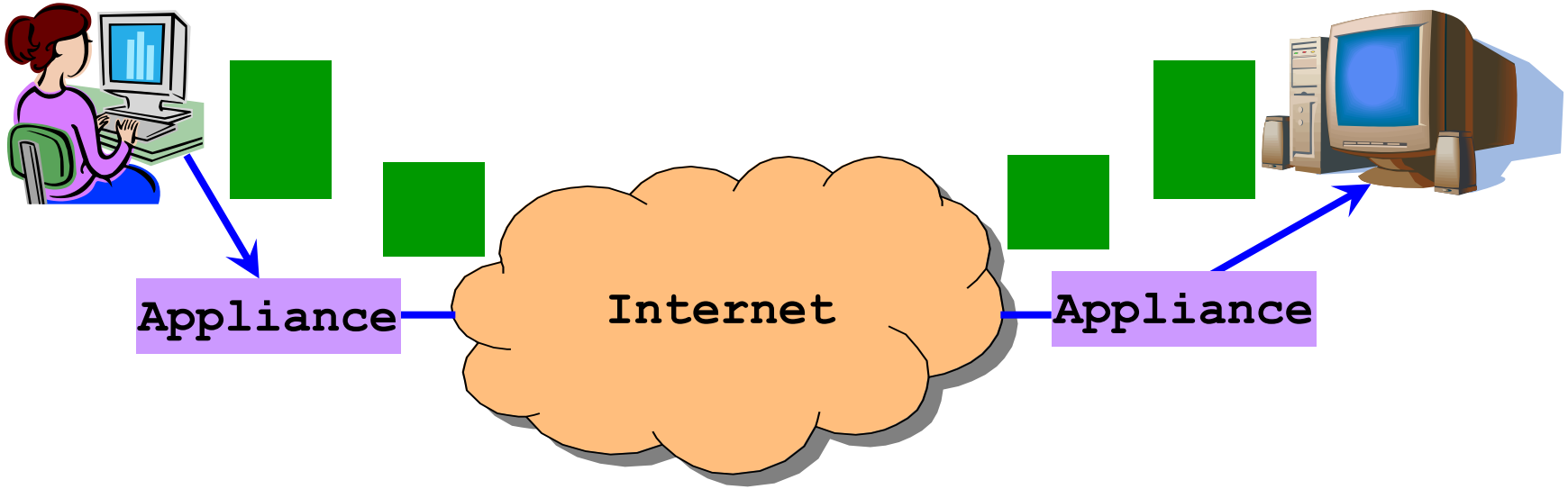
- Melhora desempenho fim-a-fim
  - Via compressão, buferização, caching, …
- Implantação incremental
  - Não precisa mudra os hosts ou o resto da Internet

Exemplo: Melhoria da Vazão do TCP



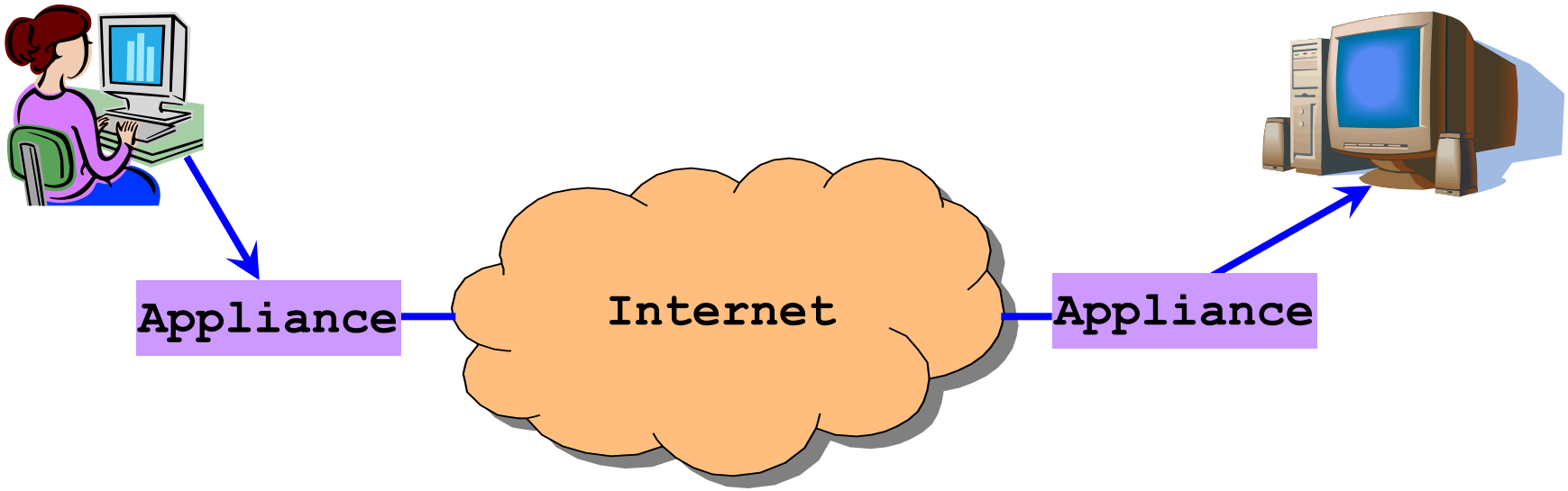
- Appliance com muita memória local
- Envia ACK rapidamente para o transmissor
- Modifica a receiver window com um valor grande
- Ou, até mesmo roda uma versão nova e melhorada de TCP

Exemplo: Compressão



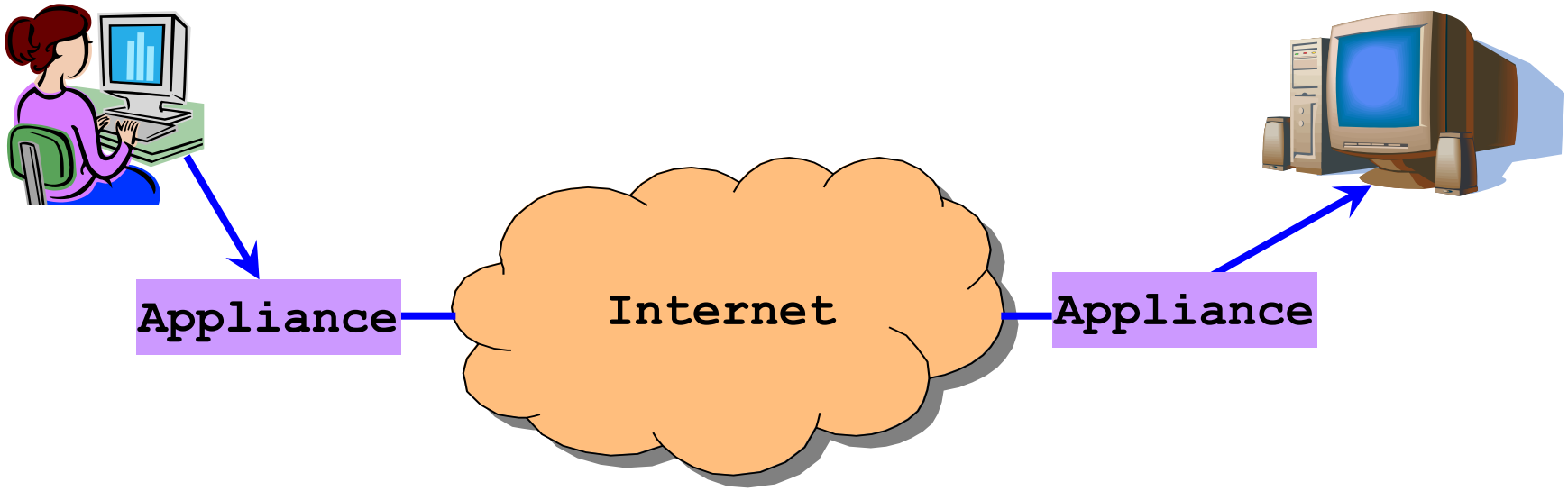
- Compacta os pacotes
- Envia os pacotes compactados
- Descompacta no outro lado
- Pode até fazer compressão entre pacotes

Exemplo: Caching



- Armazena cópias de pacotes em cache
- Procura por sequências de byte que casam com dados passados
- Envia apenas um ponteiro para dados passados
- E o outro lado reconstrói os dados originais

Exemplo: Criptografia

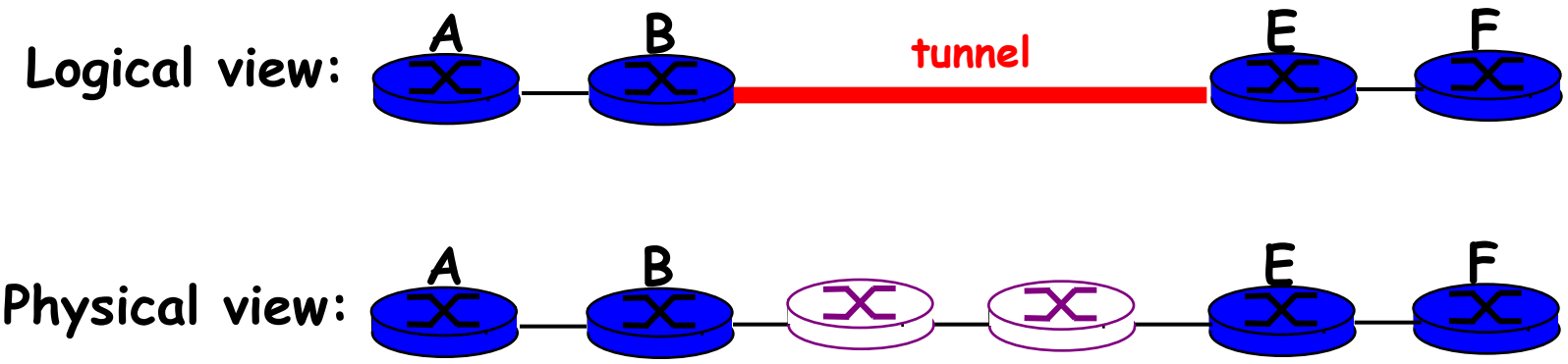


- Dois sites compartilham chaves para criptografar os dados
- Appliance transmissor criptografa os dados
- Appliance receptor descriptografa os dados
- Protege os sites de bisbilhoteiros na Internet

Tunelamento
Tunneling

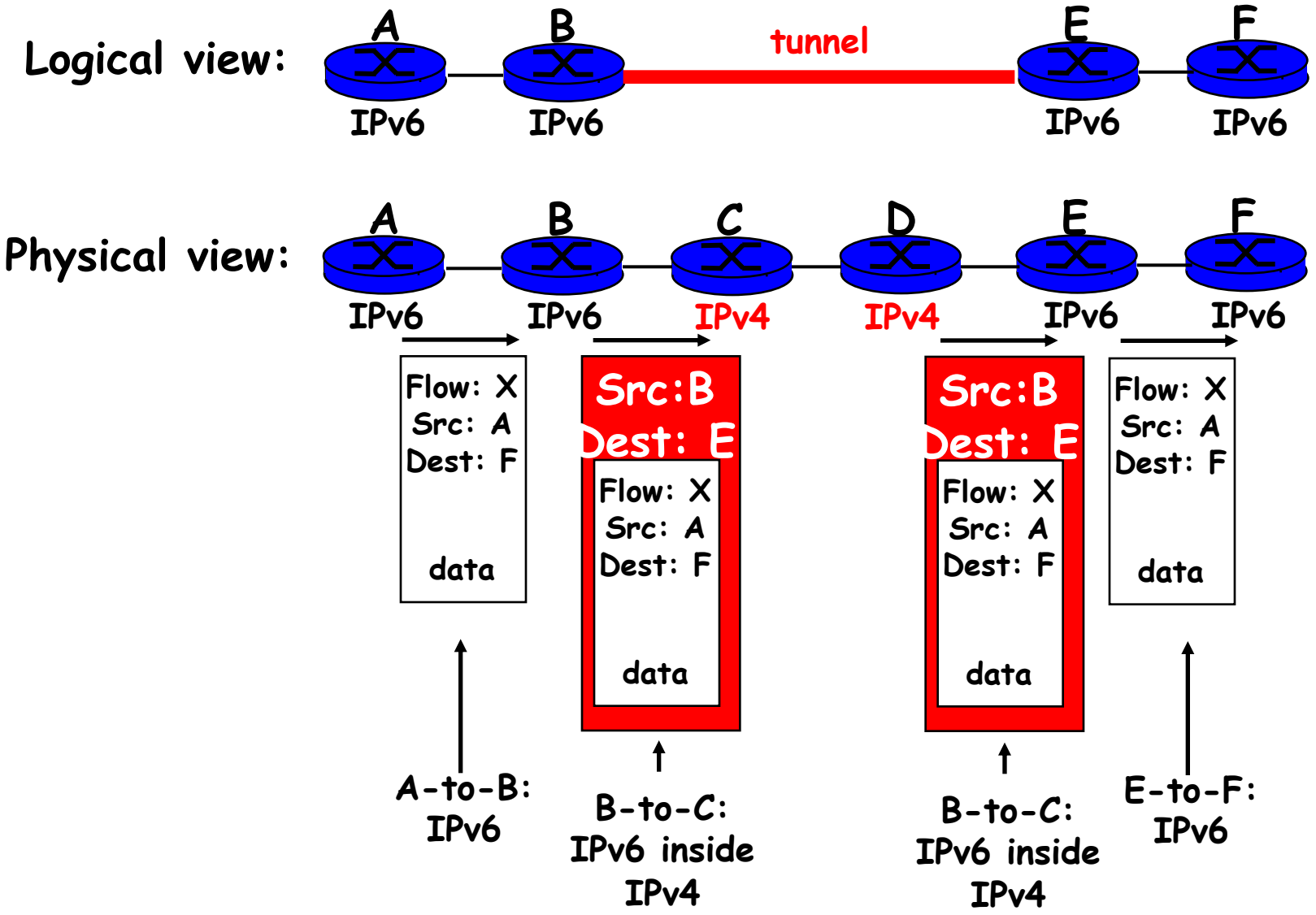
Tunelamento IP

- Túnel IP é um enlace virtual ponto-a-ponto
  - Ilusão de um enlace direto entre dois nós

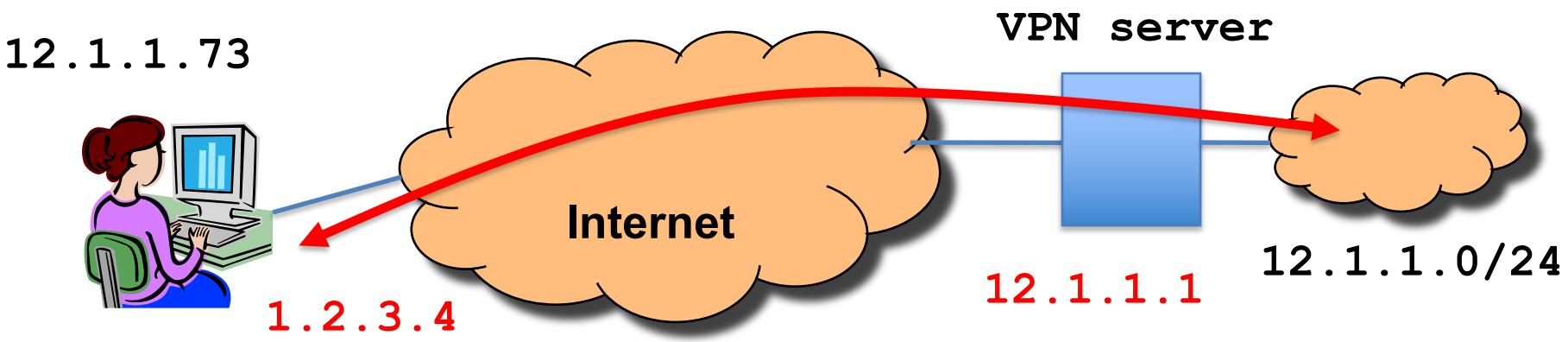


- Encapsulamento de pacotes dentro de um datagrama IP
  - Nó B envia um pacote para o nó E
  - … contendo um outro pacote no payload

6Bone: Implantação de IPv6 usando IPv4



VPN: Virtual Private Network



- Túnel da máquina do usuário até o servidor VPN
  - Um “link” via Internet até a rede local
- Encapsula pacotes do/para o usuário
  - Pacote de 12.1.1.73 para 12.1.1.100
  - Dentro de um pacote de 1.2.3.4 para 12.1.1.1

Conclusões

- Middleboxes/Appliances resolvem problemas importantes
  - Configurações com menos endereços IP públicos
  - Bloqueio de tráfego indesejável
  - Uso mais eficiente/justo de recursos de rede
  - Melhora de desempenho fim-a-fim
- Middleboxes/Appliances introduzem novos problemas
  - Endereços IP não são mais únicos globalmente
  - Não pode assumir que a rede simplesmente entrega pacotes