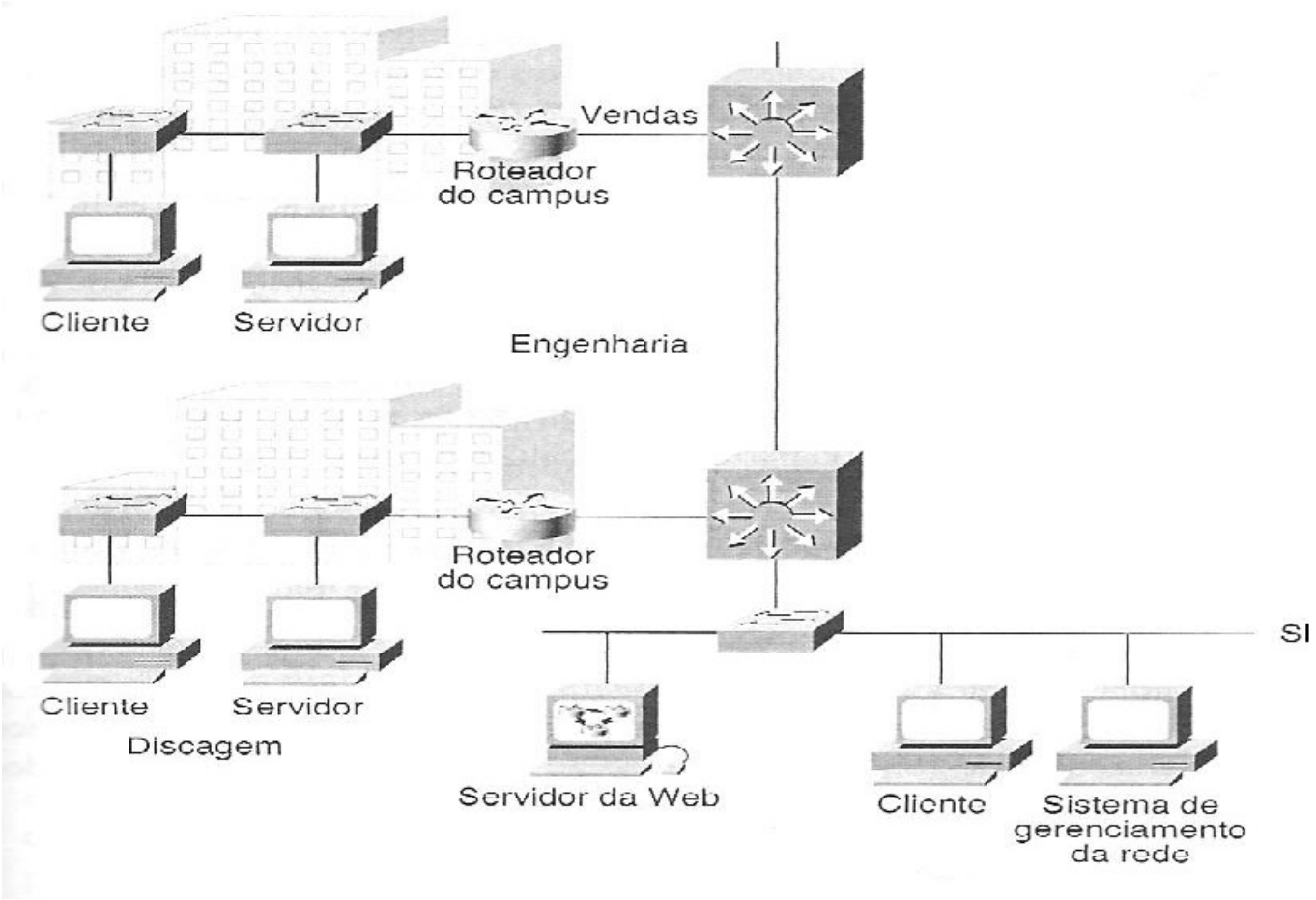
Capítulo ...

Protegendo a Infra-estrutura de Rede

Sinopse do capítulo

- Problemas de segurança para o campus.
- Soluções de segurança.
- Protegendo os dispositivos físicos.
- Protegendo a interface administrativa.
- Protegendo a comunicação entre roteadores.
- Protegendo Switches Ethernet.

Infra-estrutura de campus da Empresa XYZ
Três segmentos de rede que precisam de segurança.



Infra-estrutura de rede de campus

- Elementos de rede
  - Roteadores do campus
    - segmentos de Vendas e Engenharia
  - Switches Ethernet
    - segmento de rede SI
  - Switch-Routers
    - Backbone do campus

A rede para os usuários ...precisando de segurança

- Estações de trabalho
  - Computadores clientes
- Servidores
  - Serviços para usuários (Web, outros serviços)
  - Sistema de gerenciamento da rede

Problemas de Segurança para o campus

- Intrusos internos e externos.
- Podem usar diversas técnicas de intrusão:
  - Acesso às portas do console.
  - Acesso aos arquivos de configuração dos roteadores.
  - Acesso às configurações e conhecimento da topologia da rede via SNMP.
  - Conhecimento da topologia interna pela interceptação de atualizações de roteamento.

Problemas de Segurança para o campus

- Intrusos internos e externos.
- Podem usar diversas técnicas de intrusão:
  - Erros de roteamento do tráfego via atualizações de roteamento “disfarçadas” através de spoofing.
  - Acesso aos segmentos de redes internas.
  - Obtenção de acesso HTTP aos roteadores.
  - Acesso não-autorizado a switches Ethernet ou por intermédio desses.

Soluções de segurança

- **Configurar**, de acordo a uma **política de segurança**, os **elementos de rede da infra-estrutura**, de acordo com as vulnerabilidades conhecidas.

Objetivos

- Identificar **ameaças à rede de campus** e **métodos de segurança** para impedir essas ameaças.
- Identificar etapas para aumentar a **segurança física** dos elementos de rede.
- Identificar como proteger a **interface administrativa** dos roteadores.

Objetivos

- Identificar os métodos e comandos para proteger as **comunicações entre roteadores**.

- Identificar como **configurar os switches Ethernet** para proteger a infra-estrutura da rede.

Configuração dos elementos de rede da infra-estrutura de campus

- Proteger os dispositivos físicos.
- Proteger a interface administrativa.
- Proteger a comunicação entre roteadores.
- Proteger switches Ethernet.

Protegendo os dispositivos físicos

- Impedir acesso direto aos equipamentos de rede e às linhas de comunicação para evitar espionagem.
- Plano de segurança local e auditorias de segurança regulares.
- Salas com controles físicos de acesso.
- Alimentação reserva para o equipamento vital. Circuitos elétricos separados.

Protegendo os dispositivos físicos

- Ar condicionado suficiente.
- Armários de fiação protegidos.
- Impedir modems ligados às portas do console, sem permissão.
- Plano de contingência (recuperação) apropriado.

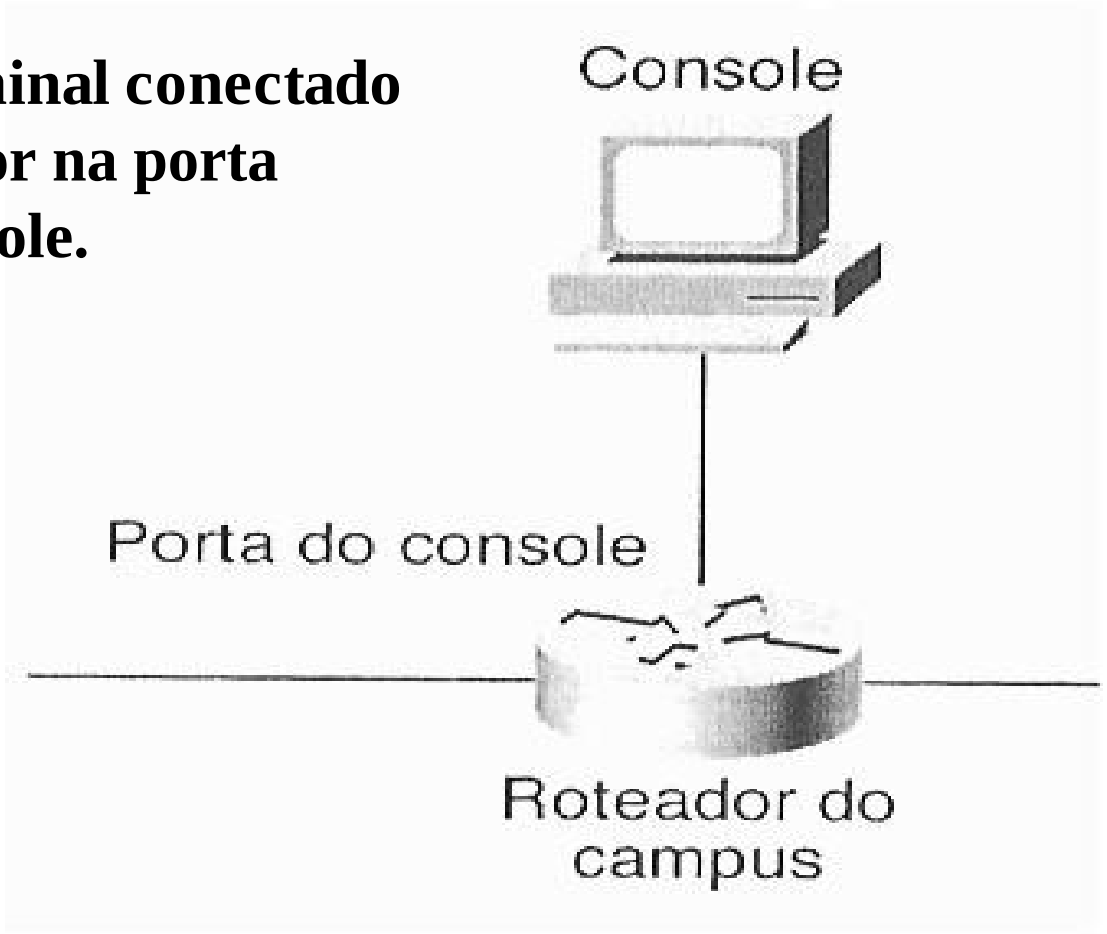
Protegendo a Interface Administrativa

- Protegendo o acesso ao console.
- Usando a criptografia de senha.
- Fazendo o ajuste dos parâmetros de linha.
- Definindo múltiplos níveis de privilégio.
- Ajustando mensagens de faixa dos dispositivos.
- Controlando o acesso Telnet.
- Controlando o acesso SNMP.

Console conectado a um Roteador

Um console é um terminal conectado diretamente ao roteador na porta designada para o console.

Intrusos não podem ter acesso físico à porta do console.



Protegendo acesso ao console

- A segurança é aplicada ao console, exigindo-se do usuário a autenticação por meio de senha.
- Na configuração padrão do roteador não há senha atribuída ao console.
- Definir senha através de comandos de configuração, diretamente no roteador.
- Modos de operação do roteador:
  - do usuário (estatísticas do roteador)
  - privilegiado (podendo alterar a configuração do roteador)
    - Definir diversos níveis de comandos para administradores.
    - Proteger os níveis do usuário e privilegiado para a segurança do roteador.

Criptografia de senha

- Para evitar senhas do console e Telnet no roteador em texto claro na configuração padrão do roteador.
- Ocultar o texto claro das senhas usando comandos para criptografia

Ajuste de parâmetros de linha

- Se a sessão do console ou *Telnet* for deixada **aberta no modo privilegiado**, qualquer um pode modificar a configuração roteador.

- Tipos de Linha:
  - tty
  - vty (portas Telnet do roteador)

- Delimitar o tempo de *login* de um console.
- Parâmetros, no roteador, para controle de segurança da linha.

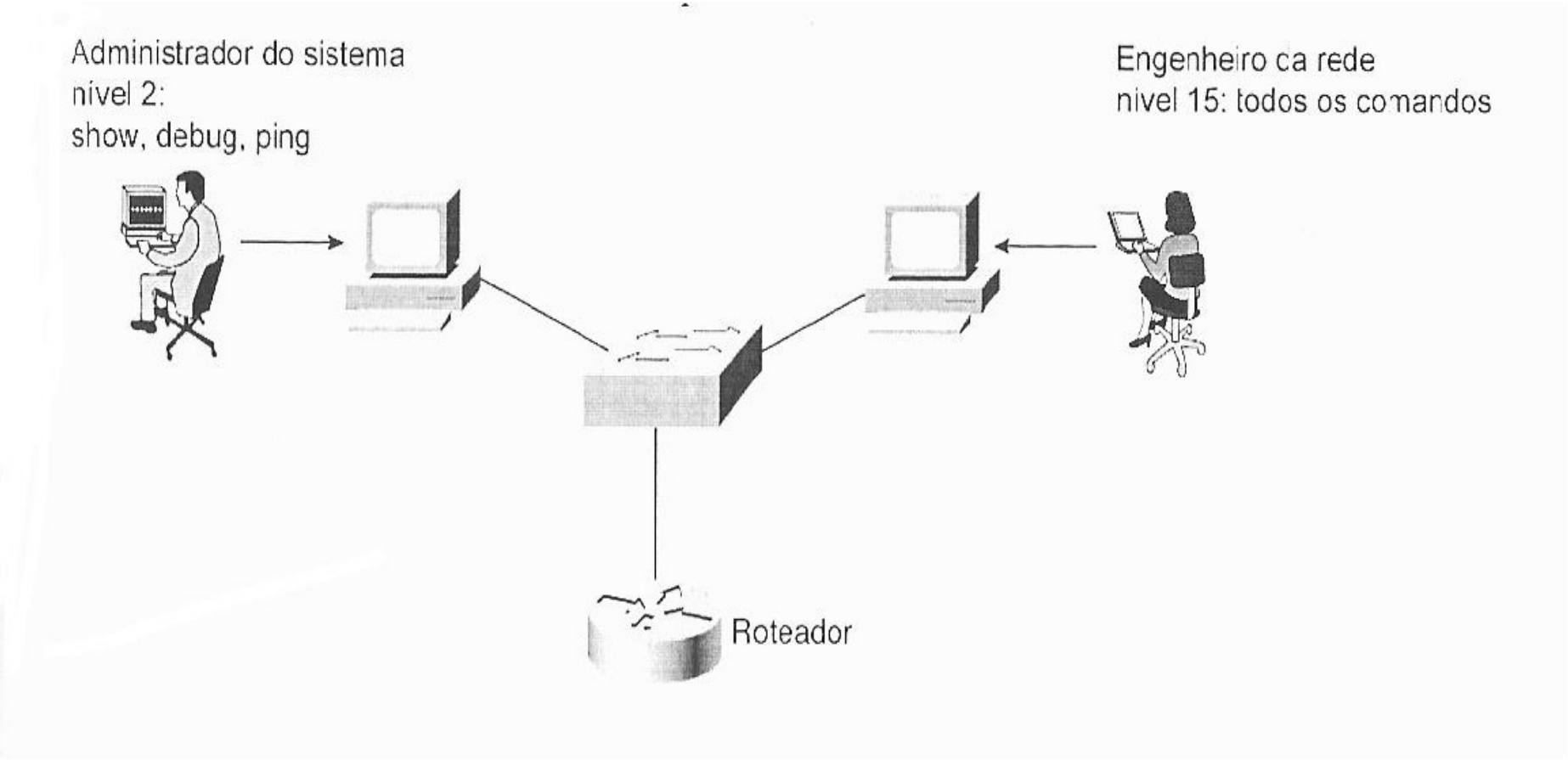
Níveis de privilégio de comandos do roteador

- O software do roteador possui, normalmente, modos de segurança para operação:
  - Modo-usuário
  - Modo-privilegiado

Níveis de privilégio de comandos do roteador

- Configurar níveis de privilégio, administrativos, hierárquicos, de comandos para cada modo.
- Os comandos do software do roteador podem ser associados a níveis de privilégio.
- Definir o nível de privilégio de cada comando.
- Nível para ativar privilégios de acesso no modo-usuário.
- Níveis para ativar privilégios personalizáveis no modo-usuário (administrador de sistema)
- Nível para ativar o acesso no modo-privilegiado (engenheiro de rede).

Administrador da Rede e o Engenheiro de Rede



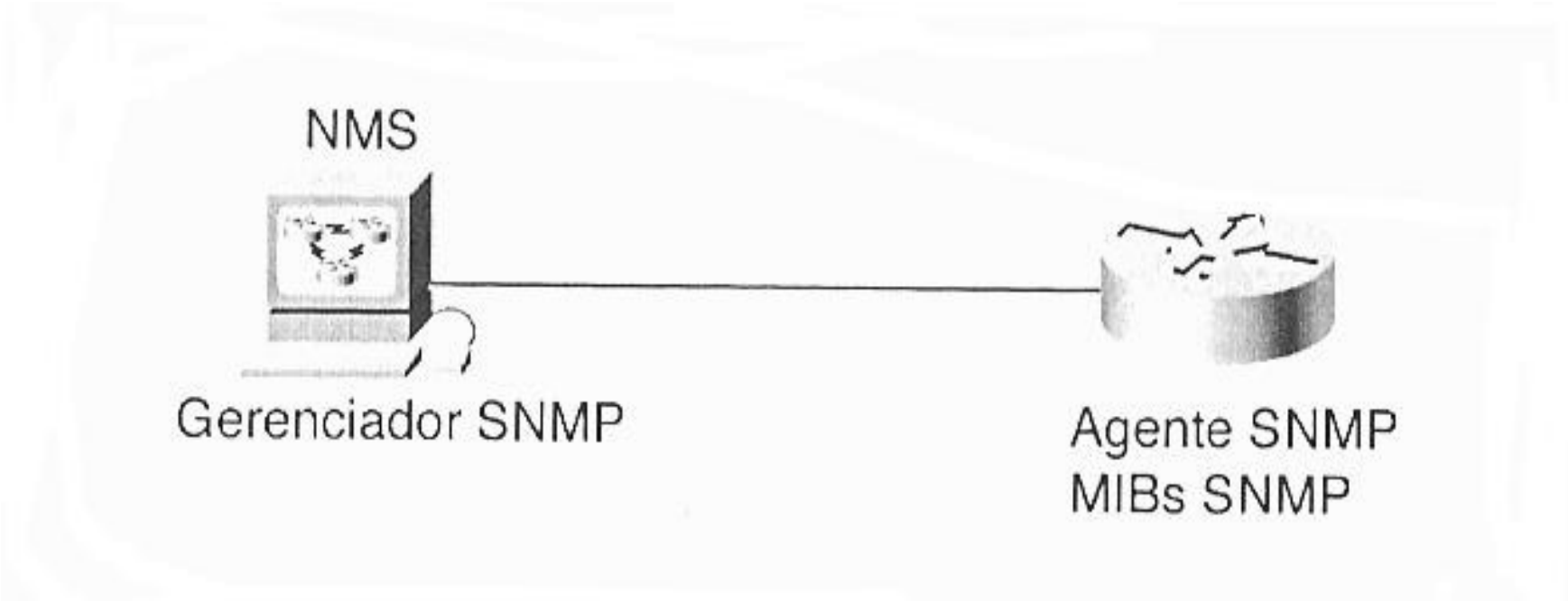
Ajustando mensagens de banner

- Para comunicar quem tem ou não permissão de entrar na rede.
- A mensagem deve refletir como a segurança é importante.
- “Esta rede é privativa da Empresa XYZ. Em caso de uso indevido, os invasores serão processados na forma da lei.”

Controlando o acesso Telnet nos roteadores

- É importante porque o acesso Telnet pode levar ao acesso privilegiado do roteador.
- Uma senha de ativação deve ser configurada para se obter acesso privilegiado.
- A porta do console é a única porta permitida para acessar o modo privilegiado, quando a senha da vty é definida.
- Restringir o acesso Telnet sobre endereços IP.
- Limitar os tipos de conexões (shell segura, RPC)

Componentes do Sistema de Gerenciamento SNMP



Controlando o acesso SNMP

- SNMP pode ser um meio para invasores da rede.
- Pode-se não saber quando uma ferramenta SNMP está acessando MIBs ou interceptando mensagens SNMP de um equipamento de rede.
- SNMP possui três níveis de acesso à MIBs através de agentes: RO, RW e W.

Controlando o acesso SNMP

- Configurar o roteador para enviar interceptações SNMP somente às estações de gerenciamento SNMP.
- Uma interceptação é uma mensagem enviada pelo agente SNMP a um gerente NMS, console ou terminal (quaisquer estações especificadas como receptores de interceptação).
- O acesso deve ser controlado para evitar que invasores observem eventos no equipamento gerenciado.

Controlando o acesso SNMP

- O acesso por NMS deve ser controlado para evitar que intrusos acessem às MIBs nos roteadores e aprendam a configuração e o status ou alterem a configuração desses.

- Controlar o acesso SNMP para a comunidade de gerentes que podem acessar uma MIB, por uma senha e lista de acesso a endereços IP de MIBs.

Protegendo Comunicações entre Roteadores

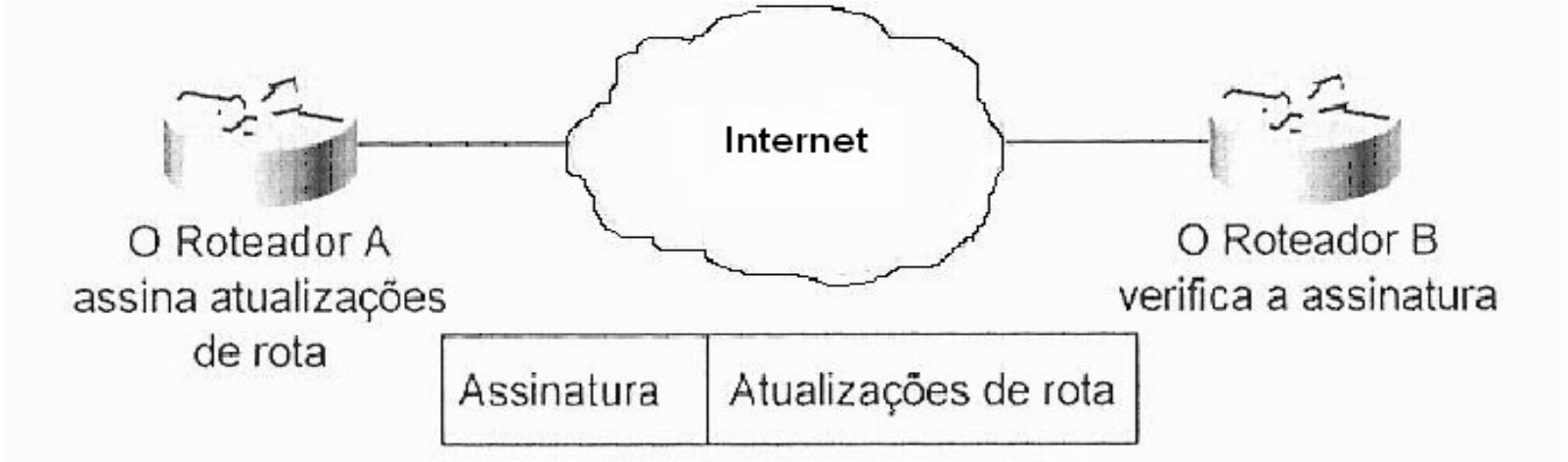
- Autenticação de protocolos de roteamento.
- Protegendo os arquivos de configuração do roteador.
- Controlando o tráfego com o uso de filtros.
- Suprimindo o processamento de rotas recebidas em atualizações.
- Filtros de rede de entrada.
- Política de segurança que controla o fluxo de tráfego.
- Controlando o acesso HTTP do roteador.

Autenticação de protocolos de roteamento

- Protocolos de roteamento são **vulneráveis a espionagem** e ***spoofing* de atualizações** de roteamento.

- O **software do roteador** pode suportar a **autenticação de atualizações** de roteamento para evitar a **introdução de pacotes** de roteamento não-autorizados e **falsificação dos endereços IP** de origem.

Autenticação de Roteador Vizinho protegendo atualizações do Protocolo de Roteamento



Autenticação de Roteador Vizinho protegendo atualizações do Protocolo de Roteamento

- Duas formas de autenticação:
  - Texto simples (Plaintext)
  - MD5 (Message Digest 5)
    (prática recomendada para proteger a infra-estrutura da rede)

Autenticação de Roteador Vizinho protegendo atualizações do Protocolo de Roteamento

- Protocolos de roteamento suportados com **autenticação de texto simples** no **Software Cisco IOS**:
  - DRP Server Agent
  - IS-IS
  - OSPF
  - RIP 2

Autenticação de Roteador Vizinho protegendo atualizações do Protocolo de Roteamento

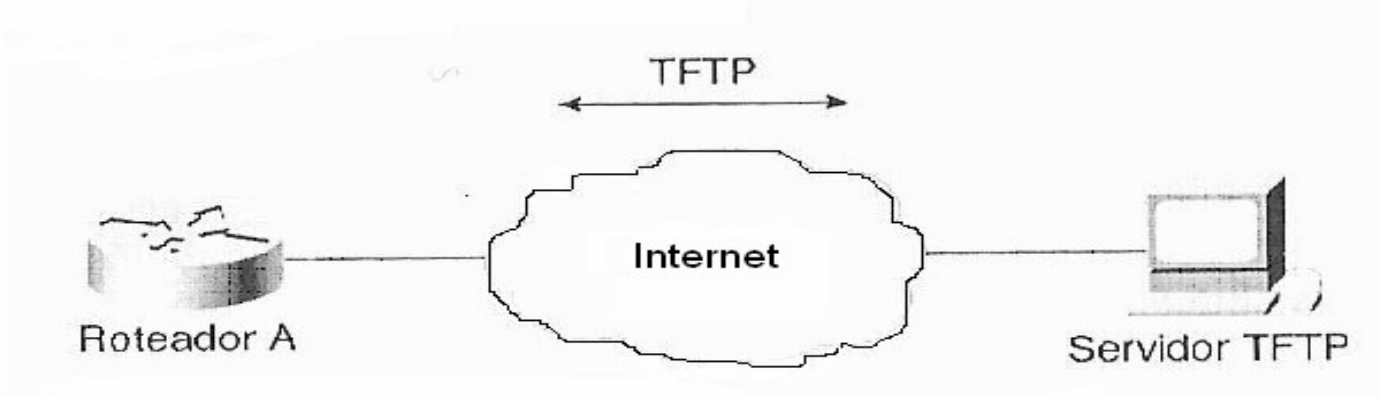
- Autenticação MD5
  - O roteador usa o algoritmo MD5 para produzir um resumo de mensagem da chave (hash).
  - O resumo é enviado no lugar da chave, e assim não se poderá espionar na linha e capturar as chaves durante a comunicação entre os roteadores, nem modificar e retransmitir a atualização de roteamento.

Autenticação de Roteador Vizinho protegendo atualizações do Protocolo de Roteamento

- Protocolos de roteamento suportados com autenticação MD5:
  - BGP (Border Gateway Protocol)
  - EIGRP (Enhanced Interior Gateway Routing Protocol)
  - IP
  - OSPF
  - RIP 2

Protegendo arquivos de configuração de Roteador

Troca de arquivos TFTP vulneráveis



Protegendo arquivos de configuração de Roteador

- Se um roteador fizer download de arquivos de configuração de um servidor TFTP (Trivial File Transport Protocol) ou MOP (Maintenance Operation Protocol), qualquer pessoa que possa acessar o servidor poderá modificar os arquivos de configuração do roteador no servidor.

Protegendo arquivos de configuração de Roteador

- A transferência de arquivos é vulnerável à espionagem e à interceptação por intrusos.
- Proteger os arquivos de configuração, significa **usar criptografia**.
- Se os servidores podem ser detectados por software de varredura de portas, pode-se **ativar e desativar manualmente o software servidor TFTP**.
- Limitar o acesso aos servidores TFTP através de uma lista de acesso SNMP.
- FTP pode ser preferível em relação ao TFTP.

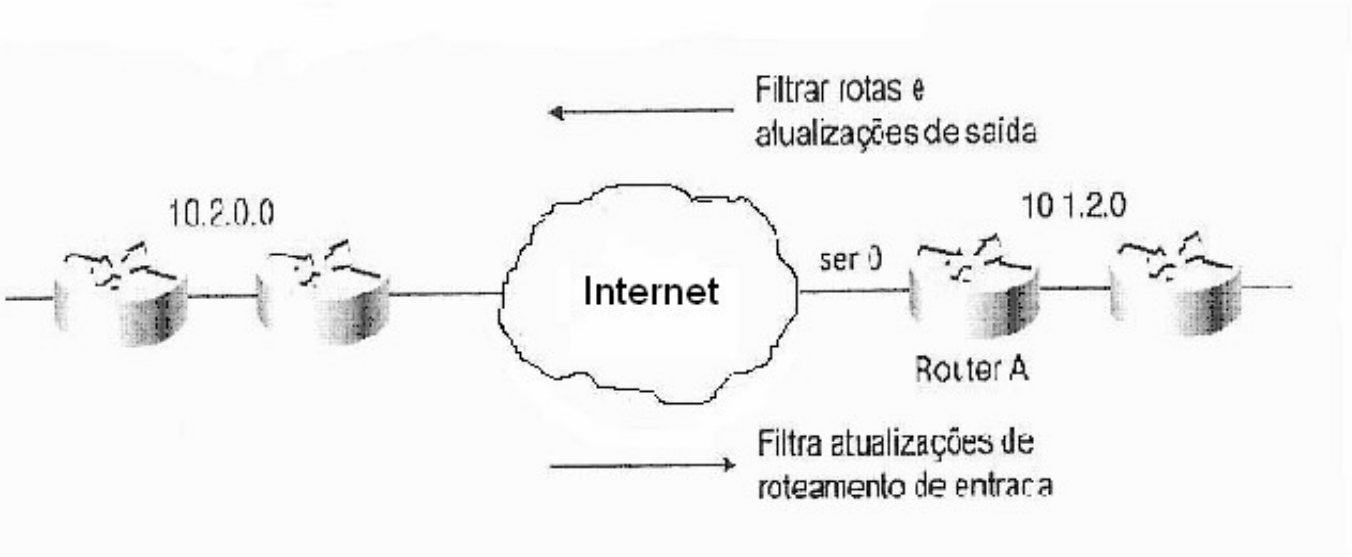
Controlando o tráfego com o uso de filtros

- **Filtros** são **listas de controle de acesso** (ACL).
- Uma ACL serve para controlar tráfego nos roteadores.
- Uma ACL filtra com base nas informações dos pacotes IP que contém, na parte dos dados, as mensagens do protocolo de roteamento.

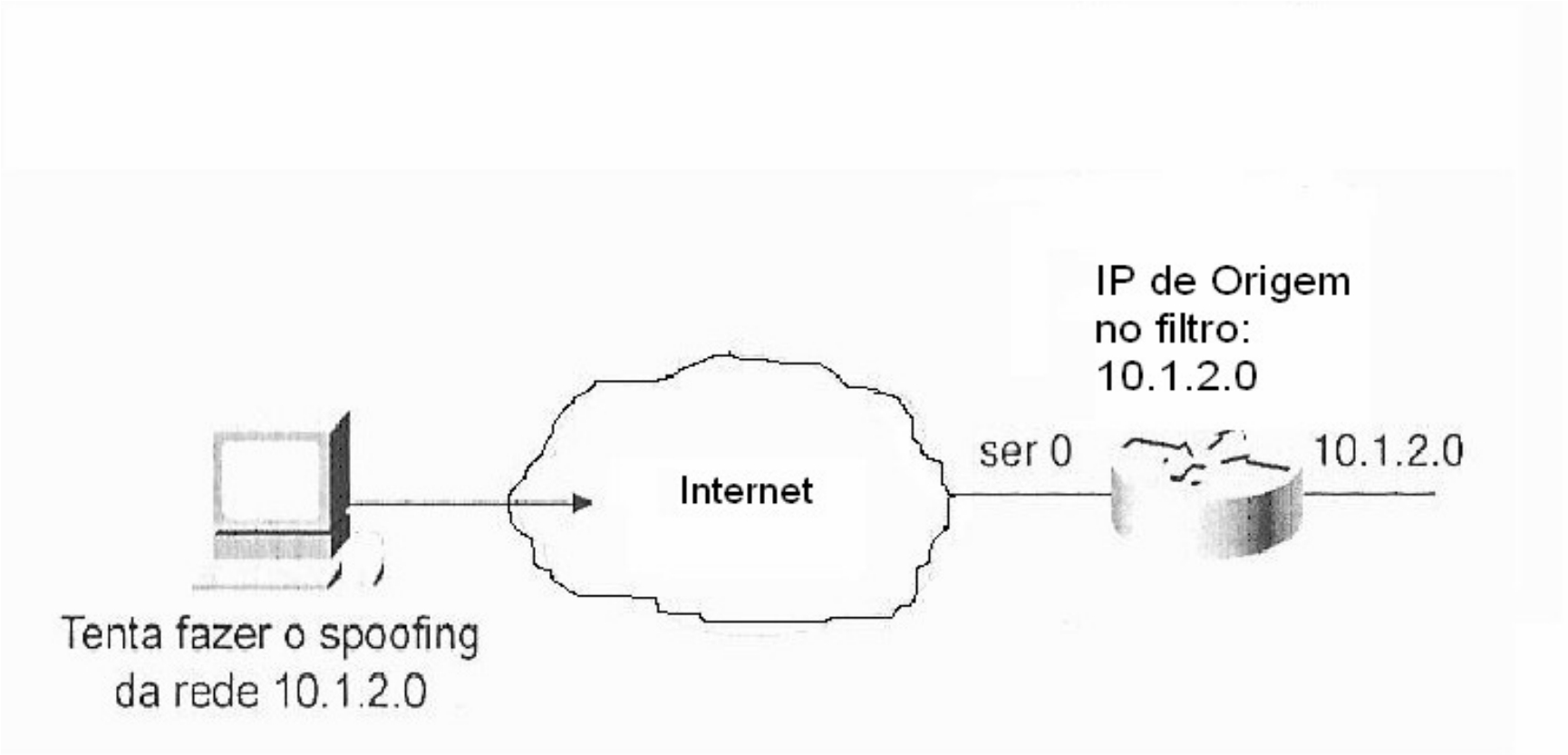
Controlando o tráfego com o uso de filtros

- Filtrando redes em atualizações de roteamento.
- Suprimindo o anúncio de rotas em atualizações de roteamento.

Listas de Acesso filtrando Atualizações de Roteamento



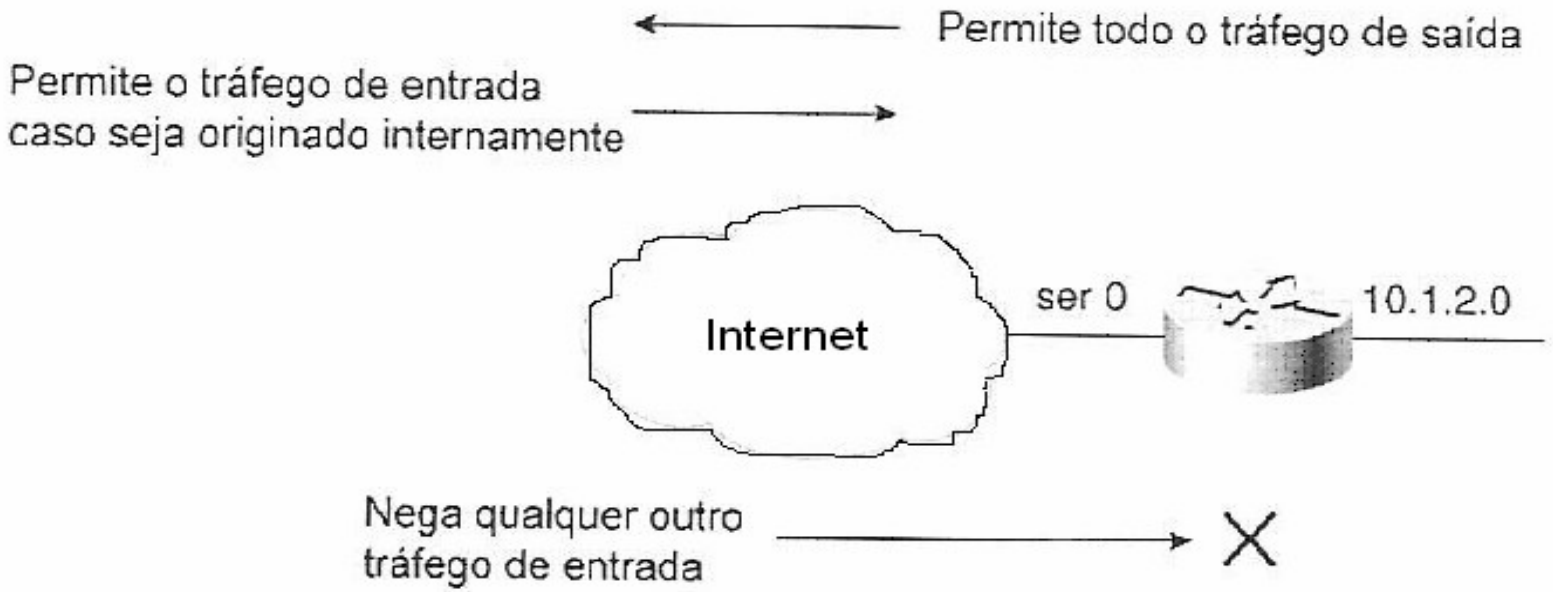
Filtros de rede de entrada



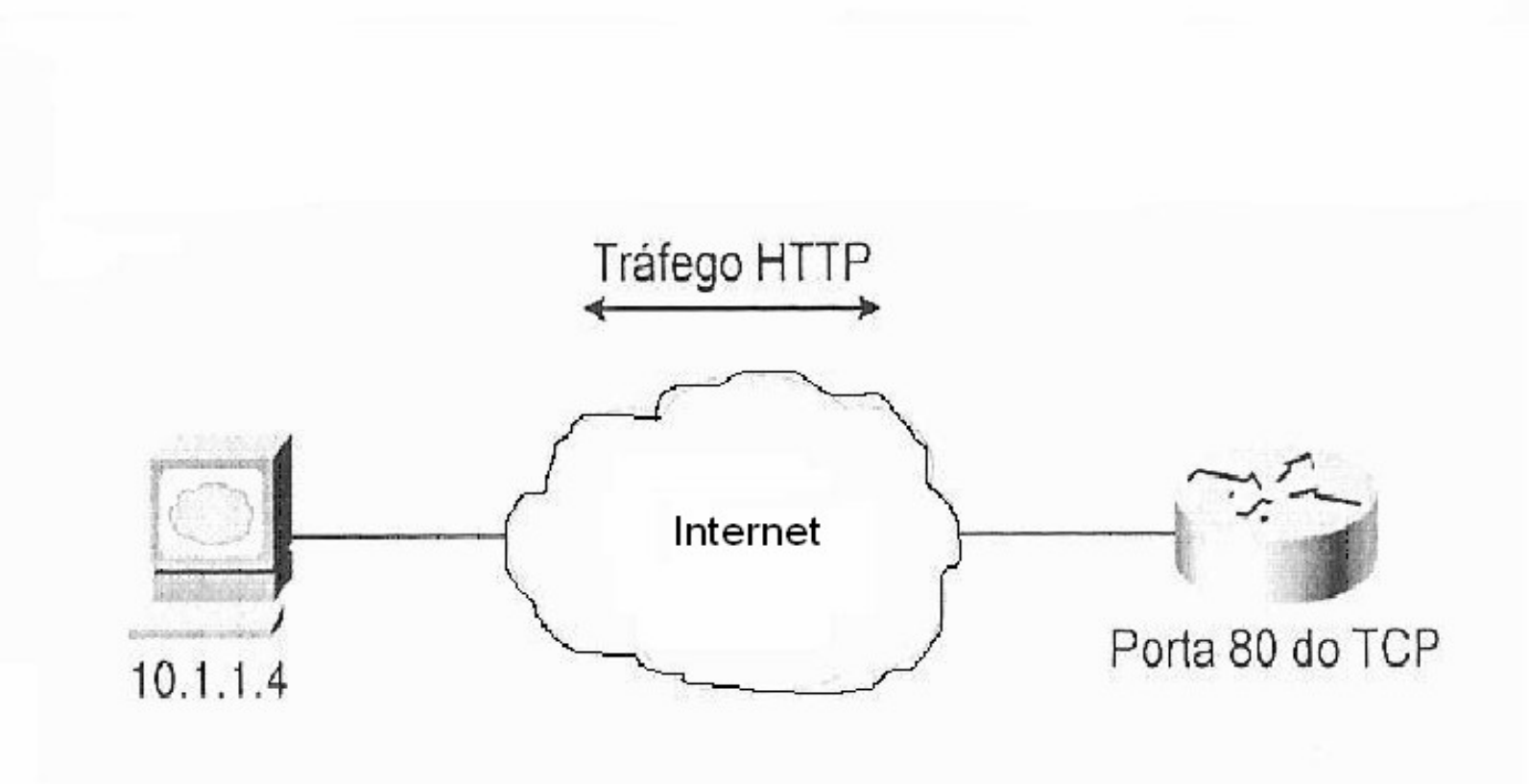
Filtros de rede de entrada

- Configurar uma lista de acesso para negar pacotes com spoofing da rede interna.
- Configurar uma lista de acesso para permitir tráfego de saída estabelecido.

Usando listas de acesso para controle de fluxo de tráfego



Controlando o acesso HTTP do roteador usando listas de acesso



Protegendo Switches Ethernet

- Controlando o acesso ao gerenciamento de switches
- Segurança de porta do switch
- Segurança de acesso dos switches

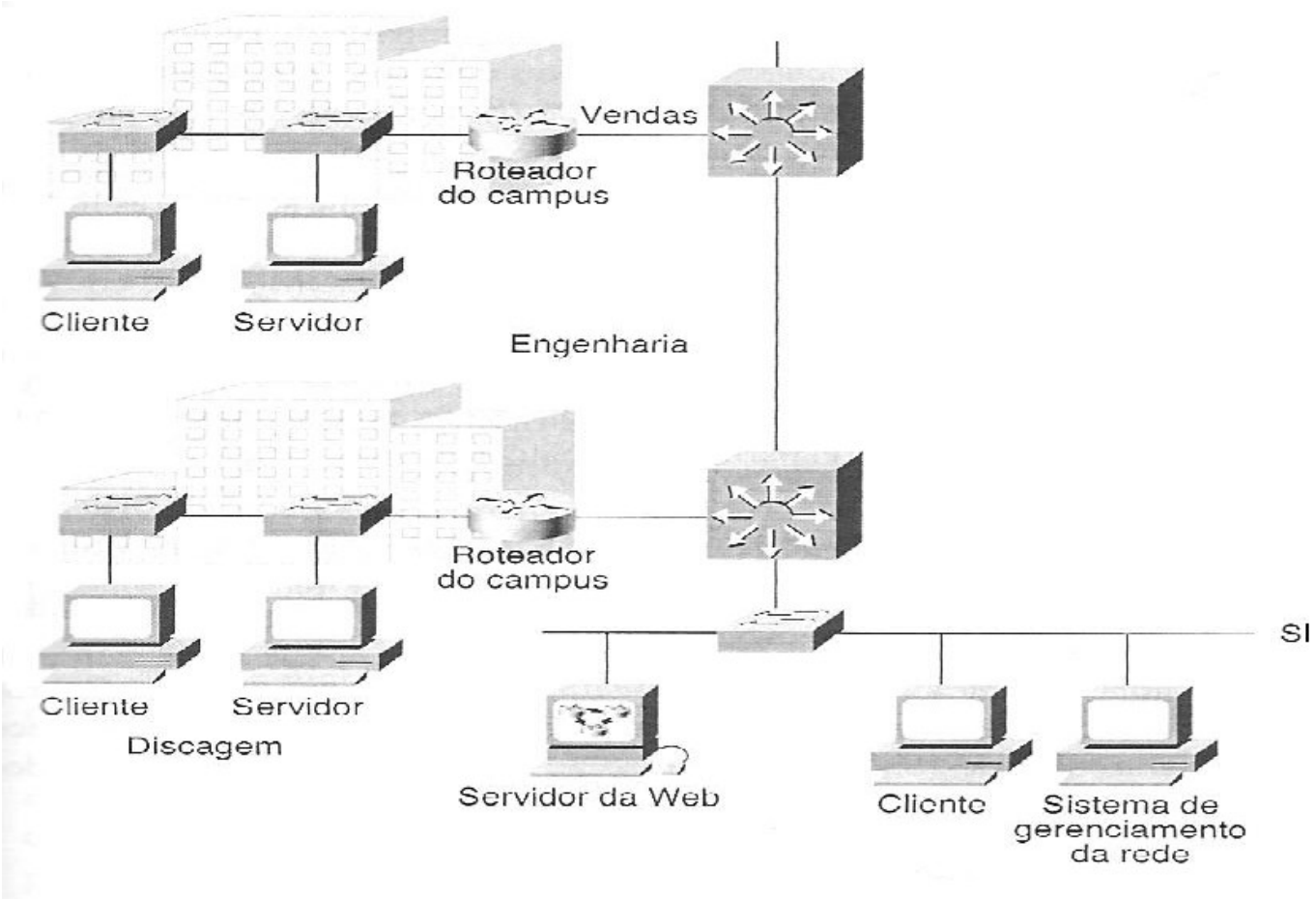
Estudo de Caso – Empresa XYZ
Configurando a segurança básica da rede

- Implementar os fatos e conceitos ensinados neste capítulo.
- Cenário
- Topologia
- Política de Segurança
- Configuração de roteadores

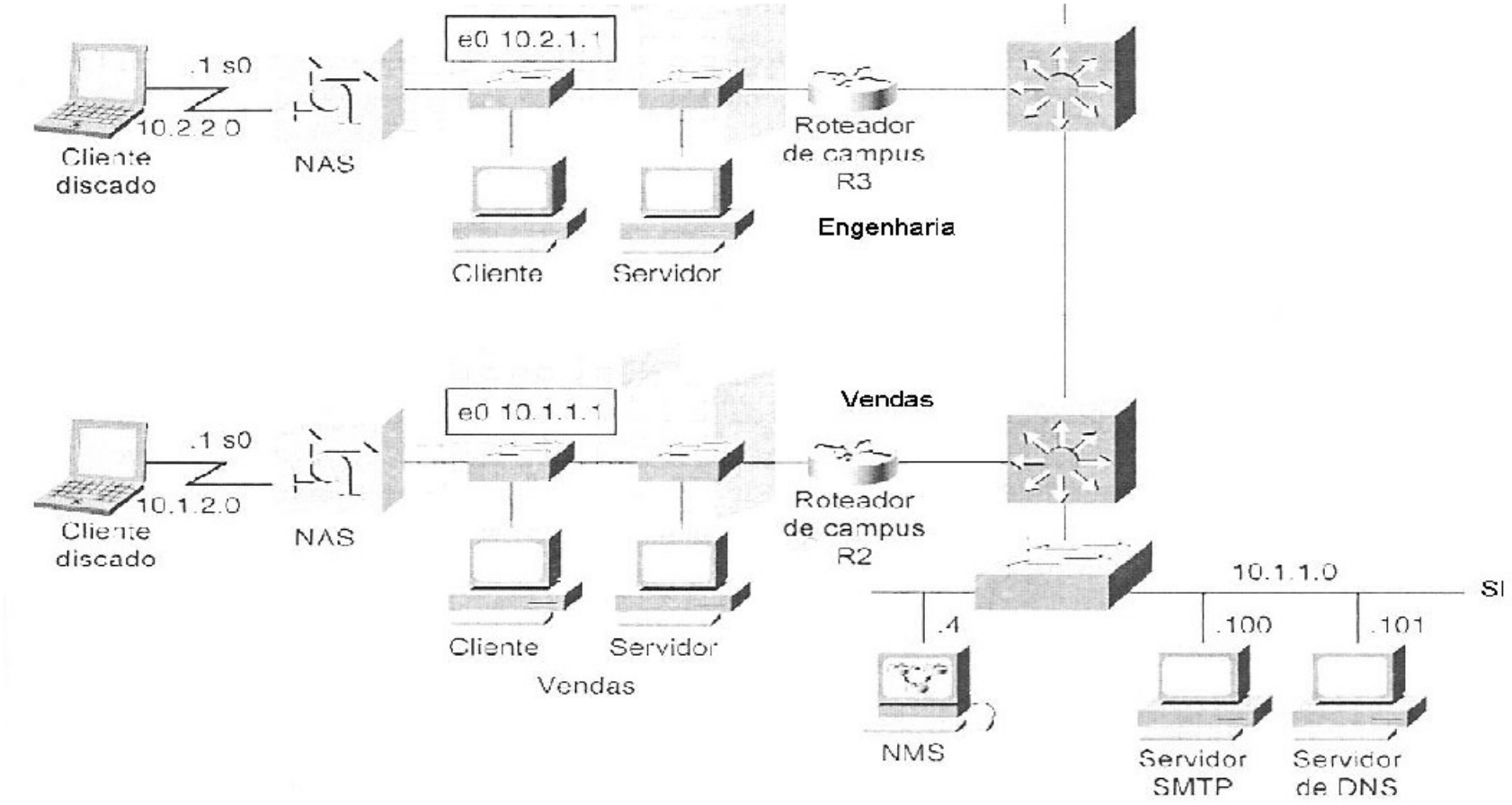
Cenário

- Empresa XYZ deseja proteger a infra-estrutura de sua rede configurando de forma segura seus roteadores de campus contra ameaças internas.

Infra-estrutura de campus da Empresa XYZ
Três segmentos de rede que precisam de segurança.



Topologia


.1 s0
10.2.2.0
Cliente discado
NAS
e0 10.2.1.1
Cliente
Servidor
Roteador de campus R3
Engenharia
Vendas
.1 s0
10.1.2.0
Cliente discado
NAS
e0 10.1.1.1
Cliente
Servidor
Vendas
Roteador de campus R2
10.1.1.0
.4
.100
.101
NMS
Servidor SMTP
Servidor de DNS

Política de Segurança

- Acesso seguro ao console e ao Telnet;
- Controle do trafego entre roteadores;
- Comunicações seguras entre roteadores;
- Controle do acesso SNMP;

Configurando roteadores

- Exemplo que implementa as instruções da política de segurança da rede relacionadas à segurança da rede do campus.
- Exemplo: roteador R2
- Roteador R3 é similar.