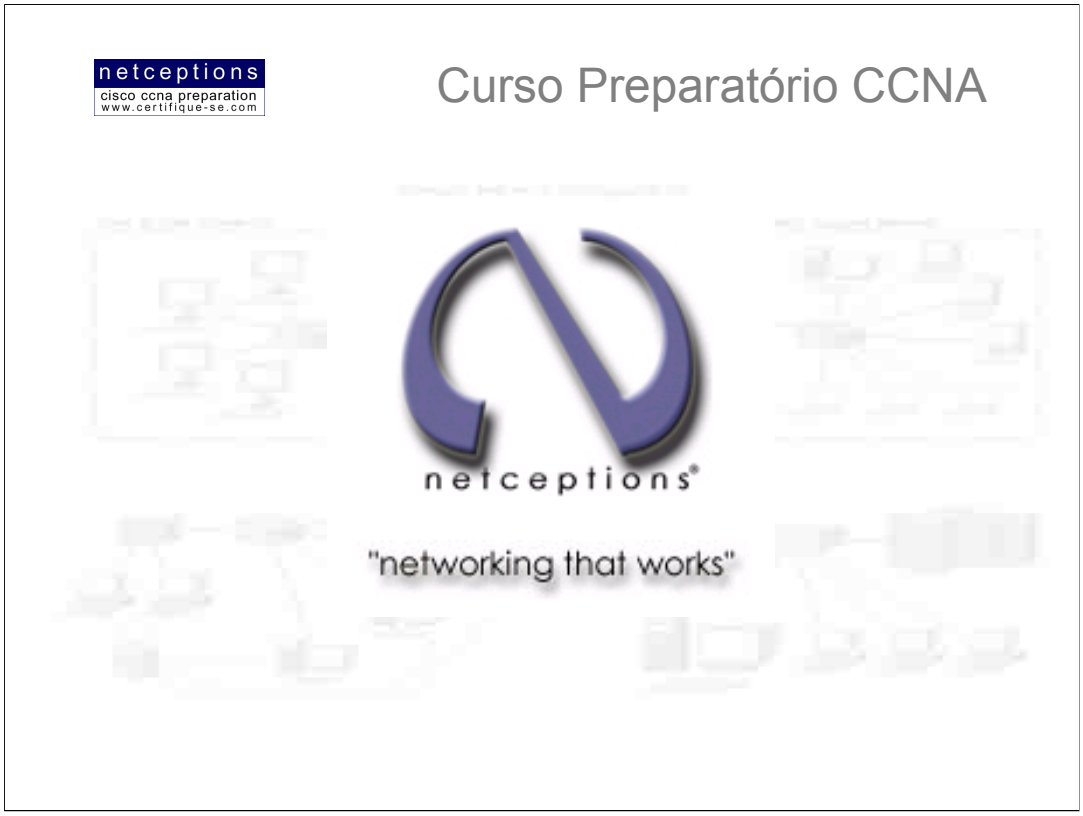
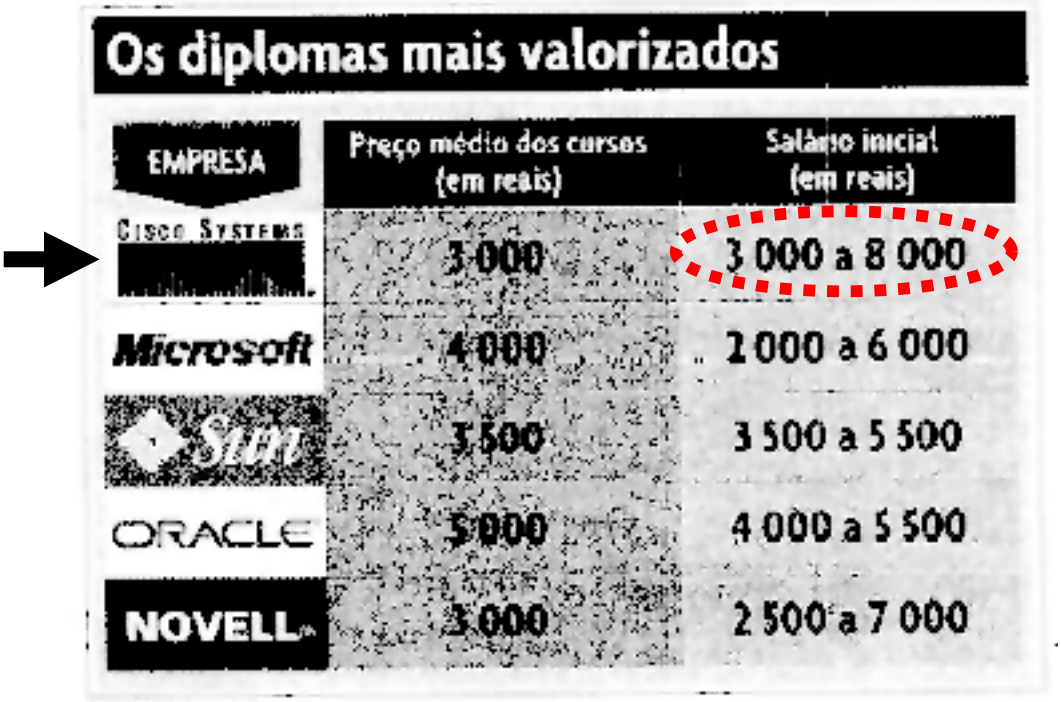


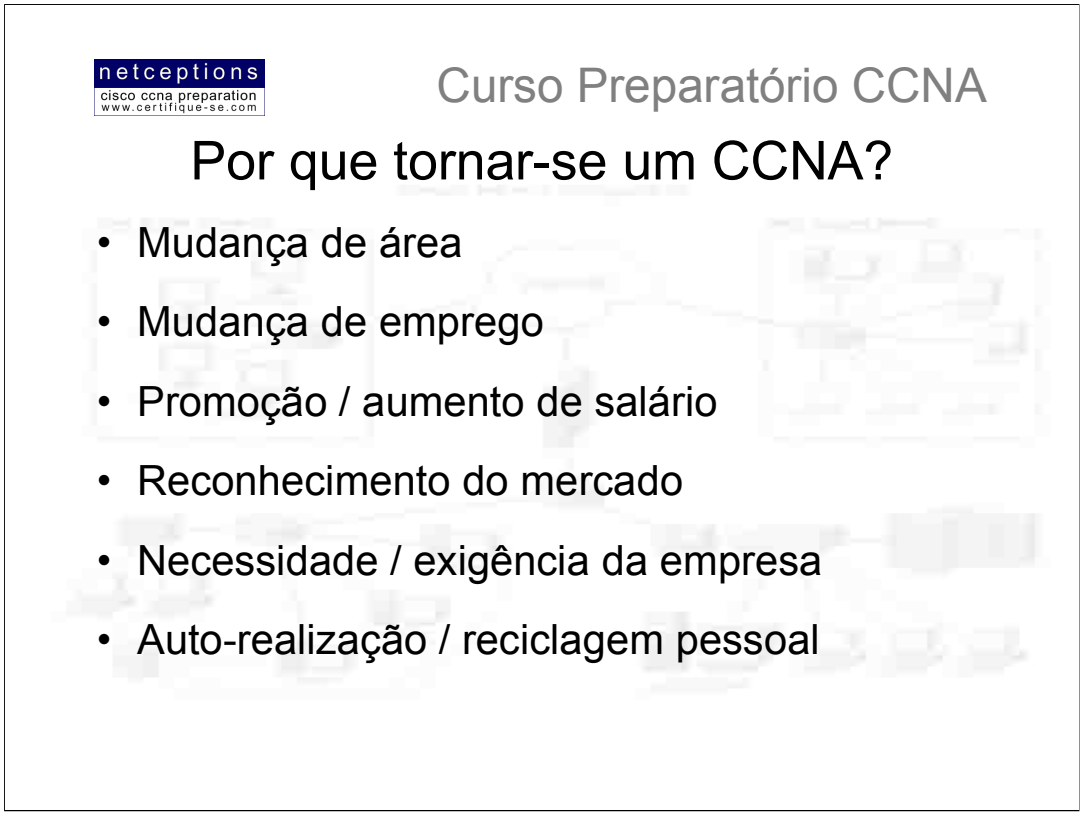
Apostila Aula 1

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA



Fonte: Revista Veja, página 78 - 25 Abril 2001



A certificação CCNA também melhorará seu entendimento geral na área de “internetworking”, indo além da mera interação com os produtos Cisco.

A linha de certificação Cisco se diferencia de outras certificações populares, como Microsoft MSCE/MCP ou Novell/CompTIA CNA, englobando uma gama de assuntos muito maior e de forma mais profunda. São, portanto, mais difíceis de se obter.

Ao optar pela linha de certificações Cisco, você está decidindo por ser o melhor - o melhor em roteamento e comutação de pacotes de dados.

Qual a vantagem de ser certificado? Num mercado competitivo como o atual, uma certificação de peso como o CCNA faz muita diferença na obtenção de um bom emprego, ou na procura de uma promoção e um melhor salário. O mercado para profissionais com a certificação CCNA é imenso, e bastante atrativo. CCNAs atuam configurando e operando LANs e WANs roteadas, e LANs comutadas, entendem à fundo e são capazes de configurar IP, IPX, IGRP, portas seriais, AppleTalk, Frame Relay, IP RIP, IPX RIP, Ethernet e listas de acesso, são requisitados para efetuar otimização de performance de redes e são capazes de configurar acesso remoto LAN-to-LAN, requerido por novas áreas e aplicações como e-commerce, B2B, VoIP, redes convergentes, etc.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Cisco - História

- **1984** - Cisco é fundada pelo casal Len e Sandy Bosack, em Palo Alto, California
- A origem do nome
- Primeiros produtos
- Foco da empresa
- Origem da linha de certificação Cisco

No começo dos anos 80, o casal Len e Sandy Bosack, que trabalhavam em diferentes departamentos de computação na Universidade de Stanford, estavam tendo problemas em fazer seus diferentes sistemas se comunicarem. Para solucionar esse problema, eles criaram, em sua própria casa, um gateway server que permitia à 2 máquinas utilizando sistemas e arquiteturas diferentes se comunicarem utilizando o protocolo IP. Em 1984 era fundada a Cisco Systems.

Acredita-se que o nome Cisco (inicialmente grafado com “c” minúsculo) foi originado de um erro de despachante na incorporação da empresa. O nome deveria ser “San Francisco Systems”, porém, parte da documentação da incorporação teria sido extraviada, deixando legível apenas “cisco Systems”.

A Cisco iniciou suas atividades comercializando um pequeno servidor gateway comercial - o que mudaria o conceito de redes para sempre. O primeiro produto foi chamado de Advanced Gateway Server (AGS). Depois vieram o Mid-range Gateway Server (MGS) e o Compact Gateway Server (CGS). Em 1993 surgiu o impressionante router 4000, e logo em seguida as linhas 7000, 2000 e 3000. Estas linhas ainda são utilizadas.

A Cisco rapidamente tornou-se líder mundial em infra-estrutura para internet e em soluções para conectividade ponta-a-ponta. Para manter-se líder, era preciso a criação de um programa de treinamento para formação de técnicos aptos à gerenciarem a infra-estrutura instalada. Surge, então, o programa Cisco Career Certifications, onde a primeira delas foi o Cisco Certified Internetwork Expert. O CCIE deu base para todas as outras certificações oferecidas pela empresa - CCNA, CCDA, CCNP e CCDP.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

As questões da Cisco para o exame CCNA caem em uma das três categorias:

1) Terminologia / definições

2) Conceitos (ex. RIP, EIGRP, etc.)

3) Implementação dos conceitos via Cisco IOS

Portanto, não há razão para se intimidar apenas porque você não possui conhecimentos profundos/experiência em Cisco IOS. Uma vez que você domine as primeiras 2 categorias de questões, questões específicas sobre Cisco IOS não serão um problema. Experiência prática ajuda muito, mas não é essencial para ser bem sucedido na prova CCNA. O grau de conhecimento exigido pode ser atingido através do uso de simuladores e 1 PC. Essa é a metodologia que estaremos utilizando, e é isso o que torna este curso mais barato e muito mais objetivo.

Estatísticas aproximadas sobre o exame:

• Aproximadamente 65 questões (esse número é variável) - 822 pontos para ser aprovado, em uma escala que varia de 300 a 1000.

• 75 minutos - tempo mais do que suficiente

• Não há questões “case study”

• 3/4 das questões de sub-redes IP tratam de redes classe C

• 15% das questões tratam do modelo OSI

• 15% de questões sobre comandos Cisco IOS

• 1 questão que exige a digitação de um comando IOS (simples, porém)

• Aproximadamente 3 questões VERDADEIRO / FALSO

• 1 questão sobre Frame Tagging

• 1 questão sobre PPP

• 1 questão sobre modo de comutação Cut-Through

• 1 questão sobre o comando “sh spantree”

• 3 questões sobre RIP

• 1 questão sobre modo de comutação Store-and-Forward

• 1 questão sobre endereçamento MAC (hardware)

• 1 questão sobre protocolos orientados à conexão X não-orientados à conexão

• 3 questões sobre segmentação através de switches

• 2 questões sobre segmentação através de redes

• 1 questão sobre segmentação através de roteadores

• 1 questão sobre passos de encapsulamento de dados

• 1 questão sobre o protocolo ICMP

• 4-5 questões sobre IPX

• 1 questão sobre OSPF

• 3-4 questões sobre ISDN

• 2 questões sobre Frame Relay

• 3 questões sobre listas de acesso

Dicas rápidas:

• Quando deparar com questões que envolvam comandos Cisco IOS, preste muita atenção à qual modo os comandos são executados (ex. EXEC, PRIVILEGED, GLOBAL CONFIG, CONFIG-IT, etc.)

• Espere deparar-se com informações sobre sub-redes no formato 128.252.144.0/24

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Estrutura do Curso

- **Aula 01:** Introdução, modelo OSI e encapsulamento de dados
- **Aula 02:** Comutação de pacotes (switching), visão geral da linha de produtos Cisco, e Virtual LANs (VLANs)
- **Aula 03:** Protocolo IP
- **Aula 04:** O sistema Cisco IOS em detalhes
- **Aula 05:** Roteamento IP

Aula I:

Introdução
- Visão geral da certificação Cisco CCNA
- Objetivos do Curso
- Estatísticas
- Dicas para um exame bem-sucedido
- Descrição de cada módulo

Internetworking
- O modelo OSI
- Encapsulamento de dados

Aula II:

Comutação de pacotes (switching technologies)
- Layer II switching
- O processo de *adress learning*
- Problemas de network looping e STP (Spanning Tree Protocol)
- Tipos de LAN switching

Visão geral da linha de produtos Cisco

VLANS
- Entendimento do conceito
- Frame tagging
- Inter Switch Routing
- Virtual Trunk Protocol (VTP)

Aula III:

O protocolo IP (Internet Protocol)
- O modelo DoD x o modelo OSI
- Portas lógicas
- Classes de endereços IP
- Técnicas de subnetting (segmentação de redes)
- Configuração de endereçamento IP no router
- Verificação da configuração no IOS

Aula IV:

O sistema Cisco IOS em detalhes
- Utilização do set up feature
- Efetuando log in no router
- Configurando senhas e banners
- Configurando interfaces
- Copiando a configuração para a NVRAM

Aula V:

Roteamento IP
- Compreendendo o processo de roteamento IP
- Criando e verificando rotas estáticas
- Criando e verificando rotas dinâmicas
- Solucionando problemas de network loops em distance-vector routing protocols
- Configurando e verificando RIP routing
- Configurando e verificando IGRP routing

Aula VI:

Gerenciando uma rede Cisco
- Back up do Cisco IOS para um servidor TFTP
- Upgrade ou recuperação do Cisco IOS de um servidor TFTP
- Back up e recuperação da configuração de um router usando o servidor TFTP
- Usando o Cisco Discovery Protocol (CDP)
- Resolvendo host names para endereços IP
- Verificando a tabela host IP
- Usando o modelo OSI para testar IP

Configurando Novell IPX
- Identificando a parte de rede e do nó em um endereço IPX
- Configurando IPX em um router Cisco
- Configurando múltiplos tipos de encapsulamento utilizando sub-interfaces e interfaces secundárias
- Monitorando e verificando operações IPX em um router

Aula VII:

Gerenciando o tráfego com listas de acesso
- Configurando listas IP/IPX básicas e extendidas
- Configurando filtros IPX SAP
- Monitorando e verificando listas de acesso

Protocolos WAN
- Identificando operações PPP para encapsulamento de dados
- Configurando autenticação PPP
- Compreendendo Frame Relay em uma extensa rede WAN
- Configurando Frame Relay LMIs, mapas e sub-interfaces
- Monitorando Frame Relay
- Compreendendo protocolos ISDN, suas funções e pontos de referência
- A implementação ISDN-BRI segundo a Cisco

Aula VIII:

Configurando o switch Catalyst 1900

Revisão Geral
- Simulados
- Perguntas e respostas

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Estrutura do Curso

- **Aula 06:** Gerenciando uma rede Cisco e configurando Novell IPX
- **Aula 07:** Gerenciando o tráfego de dados com o uso de listas de acesso e protocolos WAN (Frame Relay, PPP, ISDN)
- **Aula 08:** Configurando um switch Cisco Catalyst 1900 e revisão geral

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Aula 1: Internetworking - modelo OSI

- Benefícios de um **modelo em camadas**
- Benefício principal do modelo de referência **OSI**
- Entendendo cada camada
- Entendendo a **interatividade das camadas** e como essa interatividade é utilizada em uma internetwork
- A camada de **transporte** e o mecanismo de controle de fluxo de dados
- A camada de **rede** e uma visão geral de roteamento de pacotes
- Os cinco passos do **encapsulamento de dados**

Bem-vindo ao mundo da interconectividade. Essa aula ajudará você a entender o conceito básico por trás de internetworking. Discutiremos o modelo de camadas OSI em detalhes. O modelo OSI (Open Systems Interconnect) possui 7 camadas hierárquicas, desenvolvidas para facilitar a comunicação entre os diversos (e diferentes) sistemas existentes.

É importante entender o modelo OSI como a Cisco o enxerga, e é com esse foco que apresentaremos o modelo OSI à você.

Discutiremos nessa aula também o modelo de 3 camadas da Cisco. A Cisco criou um modelo hierárquico de 3 camadas para auxiliar no desenho, Implementação e gerenciamento de redes diversas. Entendendo este modelo, você será capaz de eficientemente construir, manter e identificar problemas em redes de praticamente qualquer tamanho.

Diferentes tipos de equipamentos são definidos nas diferentes camadas do modelo OSI. É muito importante o entendimento dos diferentes tipos de cabos e conectores utilizados para interconectar estes equipamentos à rede. Nesta aula, o cabeamento de equipamentos Cisco será discutido em conjunto com ethernet LANs, tecnologias WAN e até conexões de routers ou um switches via console. Falaremos também de como os dados são encapsulados camada à camada, através do modelo OSI.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

O Modelo de Camadas OSI

- Criado em 1970 pela ISO visando possibilitar a interoperabilidade entre sistemas e equipamentos heterogêneos
- Modelo arquitetural primário de redes
- Define, em detalhes, como dados e informações da rede devem ser transmitidas de uma aplicação em uma máquina, através do meio físico (ex. cabos), até uma aplicação em outra máquina

Quando as primeiras redes de dados surgiram, computadores podiam tipicamente comunicar-se com computadores de um mesmo fabricante. Por exemplo, empresas empregavam ou uma solução IBM ou uma solução DEC (Digital Equipment Corp., hoje Compaq) - nunca ambas.

O modelo de camadas OSI foi criado com o intuito de se quebrar essa barreira na comunicação de dados, de permitir a interoperabilidade, independentemente da marca (fabricante) ou sistema utilizado.

O modelo OSI é um modelo de referência, ou seja, ele especifica todos os processos requeridos para que a comunicação de dados ocorra e divide esses processos em grupos lógicos, chamados “layers” (camadas). Quando um sistema de comunicação é desenhado com base nesse modelo, seu desenho é tido como arquitetura em camadas.

Vantagens em se adotar um modelo de camadas:

• Divisão de complexas operações de rede em camadas gerenciáveis

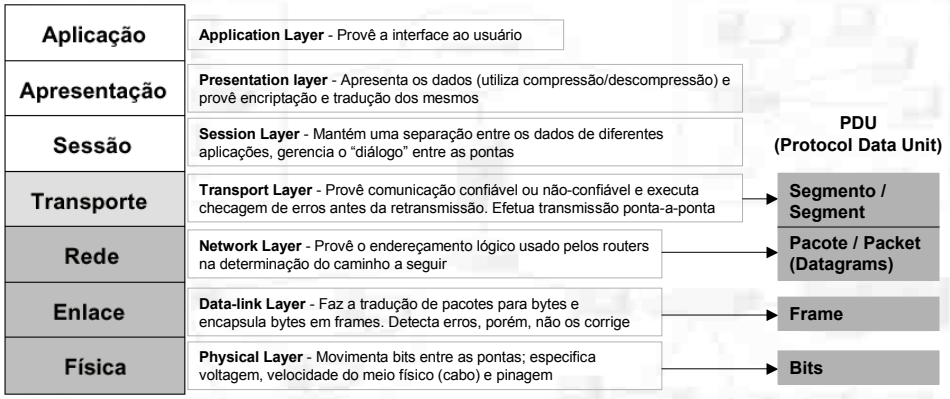
• Possibilidade de se alterar uma camada sem ter de alterar as outras

• Definição de um padrão de interface possibilitando a interoperabilidade (“plug-and-play”) entre diversos fabricantes

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

O Modelo de Camadas OSI



"Amanhã **A**o **S**air do **T**rabalho **R**esolverei **E**ntrar na **F**aculdade (*port.*)"

"Amanhã **P**rovavelmente **S**erei **T**ransportado **N**uma **D**eterminada **P**erua (*inglês*)" *(Application | Presentation | Session | Transport | Network | Data-Link | Physical)*

A camada de Aplicação

Camada onde ocorre a interação micro - usuário. A camada de aplicação é responsável por identificar e estabelecer a disponibilidade da aplicação na máquina destinatária e disponibilizar os recursos para que tal comunicação aconteça. Exemplos de aplicações e serviços nesta camada são: Web browser (Netscape e Explorer), e-mail gateways, Electronic Data Interchange (EDI), Bulletin Board Systems (BBS), Gopher, WAIS, financial transaction services, entre outros.

A camada de Apresentação

Camada responsável pela apresentação dos dados para a camada de aplicação. O modelo OSI adota padrões que definem como os dados devem ser formatados. Tarefas como compressão, descompressão, encriptação, decriptação, dentre outras estão associadas à esta camada. Alguns padrões da camada de apresentação estão envolvidos em processos multimídia (ex. TIFF, PICT, MIDI, QuickTime, MPEG, JPEG, MP3, etc.).

A camada de Sessão

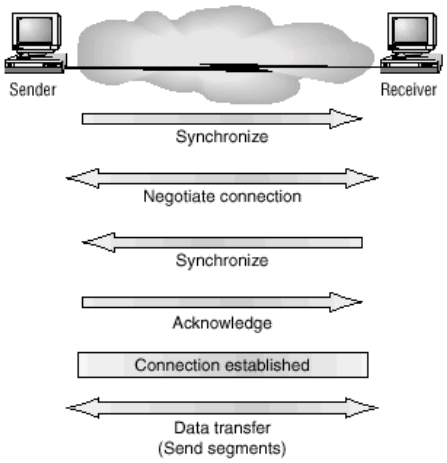
A camada de sessão é responsável pelo estabelecimento, gerenciamento e finalização de sessões entre entidades da camada de apresentação. Essa camada basicamente mantém os dados de diferentes aplicações separados uns dos outros. Alguns exemplos de protocolos desta camada são: Network File System (NFS), Structured Query Language (SQL), Remote Procedure Call (RPC), X Window, AppleTalk Session Protocol (ASP), etc.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

A Camada de Transporte

Comunicação orientada à conexão



Os serviços localizados na camada de transporte segmentam e reconstróem dados de aplicações de camadas superiores, unificando-os na mesma sequência de dados. Eles provêem comunicação ponto-a-ponto e podem estabelecer uma conexão lógica entre o computador remetente e o computador destinatário em uma internetwork.

Dois dos mais comuns protocolos encontrados nessa camada são o **TCP** (Transmission Control Protocol) e o **UDP** (User Datagram Protocol), uma das diferenças entre eles sendo que o TCP provê comunicação confiável, e o UDP, não.

A camada de transporte é responsável pela disponibilização de mecanismos para multiplexar aplicações de camadas superiores, estabelecimento de sessões, e a finalização (quebra) dos circuitos virtuais (lógicos). Esta camada também mascara detalhes de qualquer informação relacionada à rede das camadas superiores, promovendo uma transmissão de dados de modo transparente.

Controle de fluxo: A integridade dos dados é mantida pela camada de transporte mantendo-se o controle do fluxo de dados e permitindo aos usuários a requisição de transporte de dados confiável entre as pontas. O controle de fluxo previne o computador remetente de “inundar” os buffers do computador destinatário, o que resultaria em perda de dados. Para que essa comunicação seja confiável, é preciso que uma **comunicação orientada à conexão** seja estabelecida, e os protocolos envolvidos asseguram-se do seguinte:

• Os segmentos transmitidos são confirmados ao serem recebidos

• Qualquer segmento não confirmado é retransmitido

• Segmentos são reconstituídos em sua sequência original, uma vez recebidos pelo computador destinatário

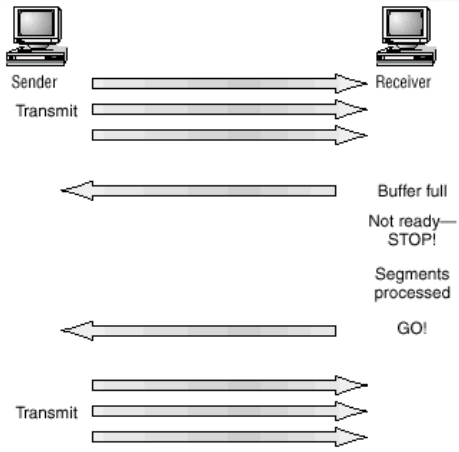
• Um fluxo de dados gerenciável é mantido a fim de evitar congestionamento, sobrecarga e perda de dados.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

A Camada de Transporte

Comunicação orientada à conexão



Enquanto dados estão sendo transmitidos entre os dispositivos, ambos checam, periodicamente, a conexão estabelecida para assegurar-se que os dados estão sendo enviados e recebidos apropriadamente.

Durante uma transmissão, congestionamento de dados pode ocorrer devido à computadores de alta velocidade gerando dados mais rapidamente do que a infra-estrutura de rede pode transmití-los, ou porque muitos computadores passam a transmitir simultaneamente datagramas através de um único gateway ou destino. No último caso, o gateway ou destino podem vir a ficar congestionado, mesmo que nenhuma das fontes, por ela só, seja a causadora do problema. Uma analogia com um estreitamento em uma estrada. Normalmente, o problema não é um único carro, mas a quantidade de carros naquela estrada.

Quando uma máquina recebe um fluxo de datagramas maior do que ela pode processar, ela os armazena em uma memória chamada buffer. Esse processo de “bufferização” resolve o problema apenas se os datagramas fizerem parte de uma pequena “rajada”. Entretanto, se o fluxo for contínuo, a memória buffer eventualmente se esgotará, a capacidade de recebimento da máquina se excederá e, como consequência, a máquina começará a descartar qualquer datagrama adicional.

Graças à função de transporte, congestionamentos de rede originados por uma “inundação” de dados pode ser bem gerenciada. Ao invés de descartar datagramas, permitindo a perda de dados, a camada de transporte pode enviar ao transmissor um sinal “not ready”, fazendo com que o mesmo aguarde antes de enviar mais dados. Após o receptor ter processado os datagramas armazenados em sua memória buffer, ele envia um sinal de transporte (“ready”) indicando que esta pronto para receber mais dados. A máquina transmissora, ao receber este sinal, retoma a transmissão de onde havia parado.

Em uma comunicação confiável, orientada à comunicação, datagramas devem ser entregues ao seu destino na exata ordem em que são transmitidos. Caso contrário, ocorre um erro de comunicação. Se qualquer segmento for perdido, duplicado ou corrompido durante o trajeto, um erro de comunicação também ocorrerá.

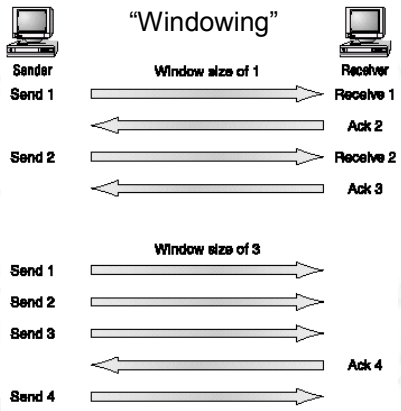
A resposta à esse problema é ter a máquina receptora confirmando o recebimento de cada datagrama.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

A Camada de Transporte

Comunicação orientada à conexão



A taxa de transmissão de dados seria extremamente baixa se a máquina transmissora tivesse de esperar uma confirmação antes de transmitir cada segmento. Uma vez que exista tempo, o transmissor irá enviar segmentos antes de finalizar o processamento de cada confirmação.

A quantidade de dados que a máquina transmissora é capaz de enviar sem antes receber a confirmação do(s) segmento(s) enviado(s) anteriormente é chamada de janela (window).

O processo de windowing controla a quantidade de informação transferida entre as máquinas participantes. Enquanto alguns protocolos quantificam a informação observando o número de pacotes, TCP/IP realiza essa quantificação contando o número de bytes. Na figura acima existe uma janela de tamanho 1 e uma janela de tamanho 3. Quando uma janela de tamanho 1 é configurada, a máquina transmissora aguarda o recebimento de uma confirmação para cada segmento transmitido antes de transmitir o próximo. Já em uma janela configurada com tamanho 3, a máquina transmissora é capaz de enviar 3 segmentos antes de receber uma confirmação.

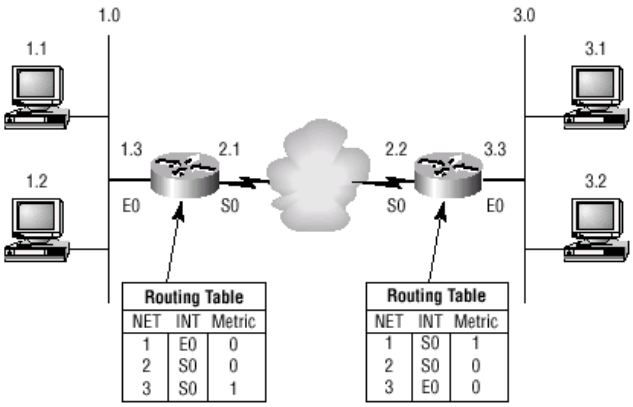
Confirmação ("acknowledgement")

Uma transmissão confiável garante a integridade dos dados transmitidos entre 2 pontas, através de um link funcional. Existe a garantia de que esses dados não serão duplicados ou perdidos. O método que torna isso possível é conhecido como "confirmação positiva com retransmissão", ou, em inglês, "*positive acknowledgement with retransmition*". Esta técnica exige que a máquina destinatária transmita uma mensagem de confirmação de volta para a máquina transmissora, quando o recebimento dos dados é efetuado com sucesso. *Podemos fazer uma analogia ao serviço de correio registrado. Assim que o destinatário recebe a carta registrada, ele assina um "cartão postal", que é enviado de volta ao remetente, garantindo a entrega da correspondência.*

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

A Camada de Rede



A camada de rede é responsável pelo roteamento dos dados através da internetwork, e também pelo endereçamento lógico dos pacotes de dados. Isso significa que a camada de rede é responsável pelo transporte de tráfego entre máquinas não conectadas localmente. **Routers** - também chamados de "layer 3 devices" - são definidos nesta camada, e provêem os serviços de roteamento em uma internetwork.

Quando um pacote é recebido em uma interface de um router, o endereço IP de destino é checado. Se o pacote não for destinado ao router em questão, este irá verificar se o endereço de destino se encontra na tabela de roteamento (routing table) - ilustrada na figura acima.

Existem **2 tipos de pacotes** utilizados na camada de rede: **Pacotes de Dados (data packets) e Pacotes de Atualização (router update packets)**. No primeiro tipo, os pacotes são usados para transporte de dados pela internetwork, e os protocolos usados para suportar tal tráfego são conhecidos como routed protocols. Exemplos de routed protocols são o IP e IPX. Já o segundo tipo é utilizado para transporte de atualizações sobre routers vizinhos. Protocolos usados para gerenciar tal transporte são chamados de routing protocols. Exemplos de routing protocols são RIP, EIGRP, OSPF, entre outros. Os pacotes de atualização são utilizados na formação e manutenção das tabelas de roteamento de cada router. As tabelas de roteamento usadas pelos routers incluem informações como: endereços de rede (network addresses), interface de saída (E0, E1, S0, etc), metric (distância relativa para uma rede remota).

Routers quebram domínios de broadcast (broadcast domains), ou seja, broadcasts não são repassados por um router. Routers também quebram domínios de colisão (collision domains), mas isso também é conseguido por switches definidos na camada de enlace. Cada interface de um router é uma rede isolada, e necessita de um número de identificação exclusivo. Cada host conectado à essa interface deve utilizar esse mesmo endereço de rede.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

A Camada de Rede

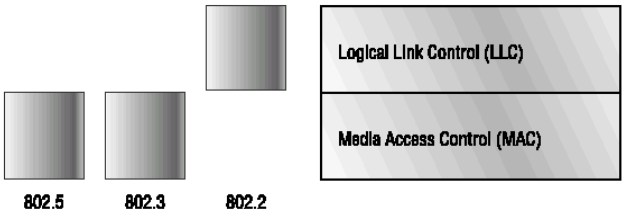
Alguns pontos importantes sobre routers:

- Não propagam mensagens de broadcast ou de multicast;
- Utilizam o endereço lógico no cabeçalho de camada de rede para determinar o router vizinho para qual o pacote deve ser enviado;
- Podem utilizar listas de acesso, criadas por um administrador, para gerenciar a segurança dos pacotes entrantes ou saintes;
- Podem prover funções de camada de enlace (bridging) se necessário e, simultaneamente, efetuar roteamento de pacotes na mesma interface;
- Equipamentos de camada de rede (routers) possibilitam a comunicação entre Virtual LANs (VLANs)
- Podem prover Qualidade de Serviço (Quality of Service - QoS) para tipos específicos de tráfego de dados

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

A Camada de Enlace



A camada de enlace assegura que os dados são transmitidos ao equipamento apropriado, e converte os dados vindos da camada superior (rede) em bits, tornando assim possível a transmissão através do meio físico, como cabos, definidos na camada física. A camada de rede formata a mensagem em frames e adiciona um cabeçalho customizado contendo o endereço de hardware (MAC address) das máquinas transmissora e destinatária. Essa informação adicionada forma uma espécie de capsula envolvendo a mensagem original, de modo análogo aos módulos lunares do projeto Apollo, onde módulos úteis apenas a alguns estágios da viagem passam a ser descartados a medida em que esses estágios são completados.

A figura mostra a camada de enlace com as especificações Ethernet e IEEE. Note que o padrão 802.2 é utilizado em conjunto com outros padrões IEEE, adicionando funcionalidade ao padrão existente.

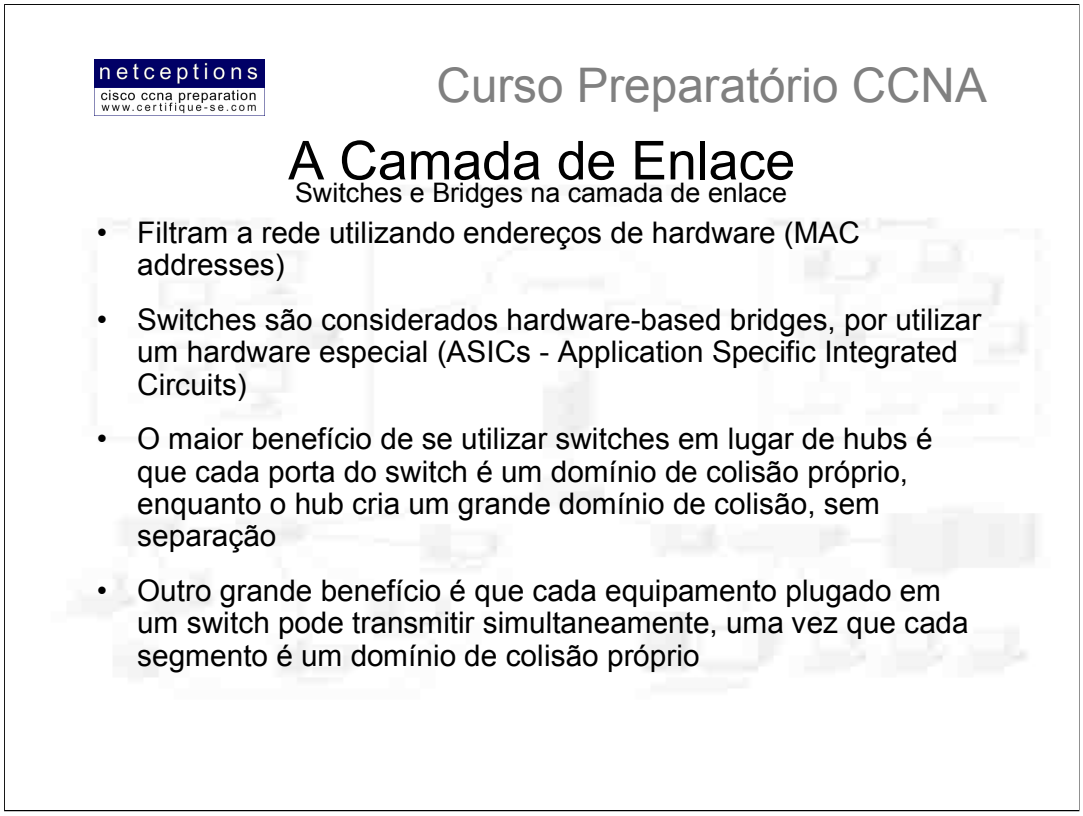
É importante entender que routers não se incomodam com a localização física das máquinas, apenas com a localização lógica das redes. A camada de enlace é a responsável pela identificação de cada máquina em uma rede local.

Para um host enviar dados à outro host e através de um router, a camada de enlace se utiliza do endereço de hardware, ou MAC address.

A camada de enlace IEEE Ethernet possui **2 sub-camadas**

• **Media Access Control (MAC) 802.3** - Define como os pacotes são alocados e transmitidos na mídia. Endereçamento físico é definido nessa sub-camada, assim como a topologia lógica. Disciplina da linha, notificação de erros (não a correção), entrega de frames ordenada, e controle de fluxo opcional também podem ser utilizados nessa sub-camada.

• **Logical Link Control (LLC) 802.2** - Responsável pela identificação de protocolos da camada de rede e seu encapsulamento. Um cabeçalho LLC diz à camada de enlace o que fazer com um pacote uma vez que o frame é recebido. Por exemplo, assim que um host recebe um frame ele analisa o cabeçalho LLC para entender para qual protocolo da camada de rede (IP, IPX, etc.) ele é destinado. LLC também pode prover controle de fluxo e sequenciamento de bits.



Switches e bridges analisam cada frame assim que cruzam a rede. O dispositivo de camada de enlace (seja um switch ou bridge) então, coloca o endereço do hardware transmissor em uma tabela-filtro e mantém um registro de qual porta do dispositivo recebeu este frame. Isto diz ao switch ou bridge onde o dispositivo está localizado.

Depois da formação da tabela-filtro, o dispositivo apenas enviará frames para o segmento onde o endereço de hardware está localizado. Isso é chamado de *transparent bridging.* Quando a interface de um switch recebe um frame e o endereço de destino é desconhecido, o switch transmite esse frame para todos os dispositivos conectados à ele. Se o dispositivo desconhecido responder à essa transmissão, o switch atualiza sua tabela com a localização (porta) e endereço de hardware daquele dispositivo.

Todos os dispositivos que recebem essa transmissão (broadcast) são tidos como estando em um mesmo **domínio de broadcast**. Dispositivos de camada de enlace propagam transmissões de broadcast, ou seja, **não há quebra de domínios de broadcast**. Apenas dispositivos de camada de rede são capazes de realizar essa quebra.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

A Camada Física

- Responsável pela transmissão e recepção de bits
- Comunica-se diretamente com diferentes tipos de mídia
- Protocolos específicos são necessários para tipos de mídia específicos
- Define procedimentos de acesso elétrico e mecânico à mídia (conectores, pinagem, voltagem, etc.), assim como requerimentos funcionais para ativação, manutenção e desativação de um link físico entre as pontas
- Ao exame CCNA importa apenas o padrão Ethernet

Na camada física, a interface entre Data Terminal Equipment (DTE) e Data Circuit-Terminating Equipment (DCE) é identificada. Os DCEs são, normalmente, localizados nos provedores de serviço, enquanto que DTEs são dispositivos conectados aos DCEs, e podem encontrar-se nas premissas do cliente. Routers podem ser tanto DCEs quanto DTEs, dependendo do contexto. Os serviços disponíveis para um DTE são, normalmente, acessados via modem ou um CSU/DSU (Channel Service Unit / Data Service Unit).

Hubs são definidos na camada física

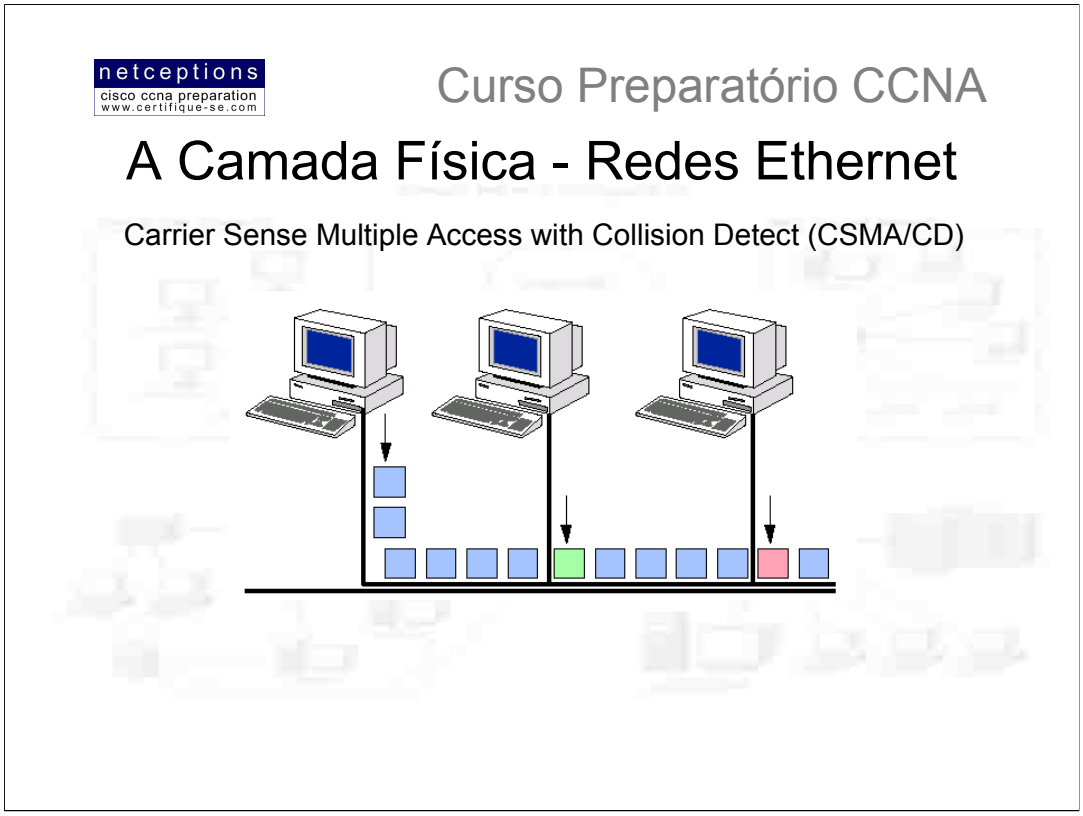
Hubs são, na verdade, repetidores com múltiplas portas. Ele apenas recebe um sinal, o amplifica e o repassa para todas as portas ativas, sem examinação dos dados no processo. Isso significa que todos os dispositivos conectados ao um hub estão dentro de um mesmo domínio de colisão, e também dentro do mesmo domínio de broadcast.

Hubs criam uma topologia física em forma estrela, onde o mesmo é o dispositivo central. Todos os dispositivos são bombardeados com dados toda vez que algum dispositivo isolado realiza uma transmissão.

Redes Ethernet

Ethernet é um método de acesso á mídia por contenção (contention media access method) que permite que todos os dispositivos (hosts) em uma rede ethernet compartilhem a mesma largura de banda de um link. Ethernet é popular devida à sua descomplicada implementação, consolidação no mercado, escalabilidade, baixo custo e facilidade de atualização quanto à novas tecnologias (como Gigabit e 10 Gigabit ethernet). Ethernet utiliza especificações das camadas de enlace e físicas.

Redes ethernet utilizam o que é chamado de Carrier Sense Multiple Access with Collision Detect (CSMA/CD), o que ajuda à dispositivos dividirem a largura de banda igualmente, sem ter dois dispositivos transmitindo simultaneamente no mesmo meio de transmissão. CSMA/CD foi a solução encontrada para o problema de colisões que ocorriam quando pacotes eram simultaneamente transmitidos de diferentes dispositivos em um mesmo meio.



O funcionamento do mecanismo CSMA/CD é relativamente simples. Observe a figura acima: No intervalo de tempo entre o término da transmissão de um pacote e a geração de outro pacotes, outros hosts podem utilizar o meio de comunicação para enviar seus próprios pacotes.Quando um host deseja transmitir através da rede, ele primeiramente verifica se há presença de sinal digital no meio (cabo). Caso não haja (nenhum outro host esteja transmitindo), o host iniciará, então, sua transmissão. O host monitora constantemente o meio. Se for detectado outro sinal no mesmo, é enviado um sinal de congestionamento, o que ocasiona uma pausa na transmissão de dados pelos outros hosts. Os hosts respondem ao sinal de congestionamento enviado esperando um determinado tempo antes de tentarem enviar dados novamente. Após 15 tentativas sem-sucesso (15 colisões), um “time-out” ocorre.

Half-duplex e full-duplex Ethernet

Half-duplex ethernet é definido no padrão original Ethernet 802.3 e utiliza apenas 1 par de cabos, com sinal fluindo em ambas as direções do mesmo. Half-duplex ethernet, tipicamente 10Base-T, atinge apenas 50% à 60% de eficiência, do modo como a Cisco enxerga. Entretanto, você tipicamente obterá apenas 3 à 4 Mbps, no máximo, em uma grande rede 10Base-T.

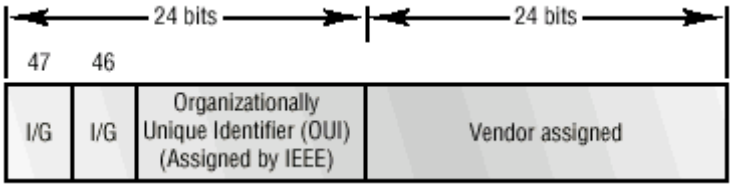
Full-duplex ethernet utiliza 2 pares de cabos. Não há colisões, uma vez que agora existe 1 caminho para transmitir e outro, independente, para receber dados. Supostamente, é possível obter uma taxa de transferência da ordem de 100Mbps em ambas as direções, o que nos dá uma **taxa agregada** de 200Mbps - supondo-se 100% de eficiência.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Ethernet na Camada de Enlace

Endereçamento Ethernet



Ethernet na camada de enlace é responsável pelo endereçamento Ethernet, tipicamente chamado de endereço de hardware, ou MAC addressing. Ethernet também é responsável pelo encapsulamento de pacotes recebidos da camada de rede, e pela preparação dos mesmos para transmissão pela da rede local, através do método do acesso à mídia por contenção.

Endereçamento Ethernet

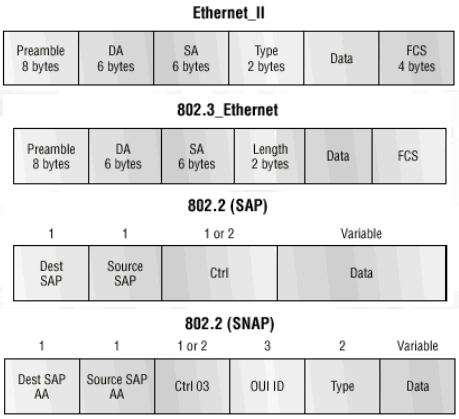
O esquema de endereçamento ethernet se utiliza do endereço MAC (Media Access Control), gravado em cada dispositivo de rede (ex. placas de rede - NIC). O endereço MAC é uma sequência de 48 bits (6 bytes), escritos em formato canônico, assegurando que todos os endereços MAC são escritos no mesmo formato, mesmo em se tratando de dispositivos de diferentes fabricantes ou plataformas. A figura acima nos mostra como é feita a divisão dos 48 bits para endereçamento.

O identificador organizacional único é imposto pelo IEEE, à uma determinada organização (ou fabricante). O fabricante, por sua vez, designa um endereço administrativo global de 24 bits, que é exclusivo aos produtos daquele fabricante. O bit 46 deve ser 0 caso seja um bit designado globalmente pelo fabricante, ou 1, caso seja localmente administrado pelo administrador de rede.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Ethernet na Camada de Enlace



• **Preamble -** Sequência alternada de 1 e 0 que provê um clocking de 5MHz no início de cada pacote, permitindo ao recipiente "travar" a cadeia de bits sendo recebida. O Preamble usa um campo de sincronização ou um SFD para indicar à estação receptora que a porção contendo dados da mensagem segue na sequência.

• **Start Frame Delimiter (SFD)** - Sequência alternada de 0 e 1, enquanto que o campo de sincronização é uma sequência de 1s. O preamble e o campo SFD/sinc possuem 64 bits (8 bytes).

• **Destination Address (DA)** - Transmite um campo de 48 bits utilizando o último bit significante (Last Significant Bit - LSB) primeiro. O campo DA é utilizado pelas estações receptoras para determinar se o pacote a caminho é destinado àquela estação específica. O endereço de destino (DA) pode ser um endereço específica, um endereço broadcast ou um endereço multicast.

• **Source Address (SA)** - Endereço de 48 bits fornecido pelo NIC da estação transmissora. Também utiliza o último bit significante primeiro.Endereços broadcast ou multicast são ilegais nesse campo.

• **Lenght ou Type of Field** - O frame 802.3 utiliza o campo "Lenght", enquanto que o frame Ethernet_II utiliza o campo "Type" para identificação do protocolo da camada de rede utilizado. O frame 802.3 não pode identificar o protocolo de camada de rede e, portanto, apenas pode ser usado em uma LAN proprietária, como IPX.

• **Data** - O campo Data contém, de fato, os dados transmitidos à camada de enlace pela camada de rede. O tamanho pode variar de 46 à 1500 bytes.

• **Frame Check Sequence (FCS)** - Campo no final do frame utilizado para o armazenamento do Cyclic Redundant Check (CRC) - checagem baseada em algoritmos matemáticos para verificação da integridade dos frames transmitidos. Identifica frames corrompidos, porém, não os corrige.

Lembre-se que o frame 802.3 não é capaz de identificar o protocolo da camada de rede. Para tal, ele necessita de "ajuda". O IEEE definiu a especificação 802.2 LLC (Logical Link Control) que incorpora essa e outras funções. Portanto, o protocolo 802.3 com LLC é conhecido como 802.2 (SAP).

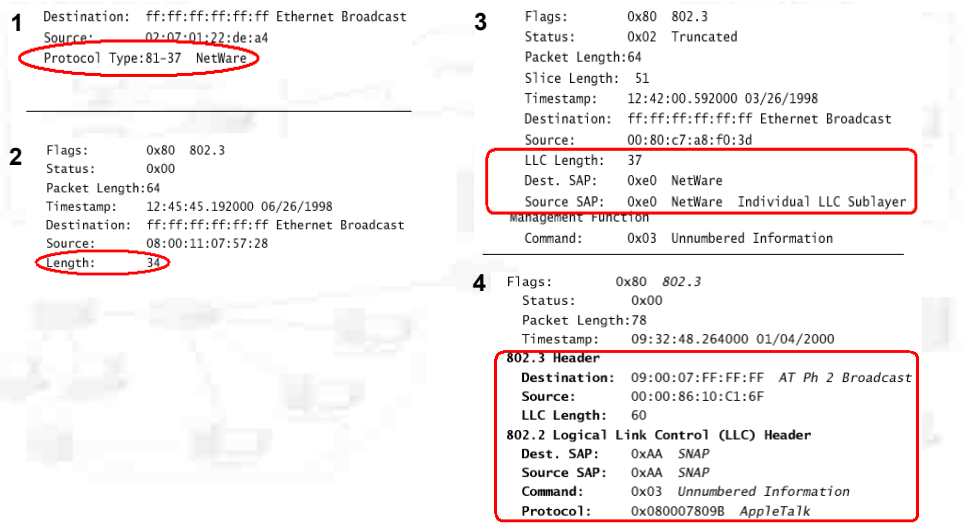
802.2 (SAP) frame - Incorpora os campos Destination SAP e Source SAP para identificação do protocolo de camada de rede. O frame 802.2 (SAP) é nada mais que um frame 802.3 com informações da sub-camada LLC.

SNAP frame - Possui seu próprio campo de protocolo para identificação do protocolo da camada de rede. É uma forma de se utilizar um frame Ethernet_II em um frame 802.3. Apesar de o campo ser chamado de "Protocol", este é, na verdade, o campo "Type" do frame Ethernet_II.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Ethernet na Camada de Enlace



Alguns frames capturados com a ferramenta *Etherpeek Network Analyser*.

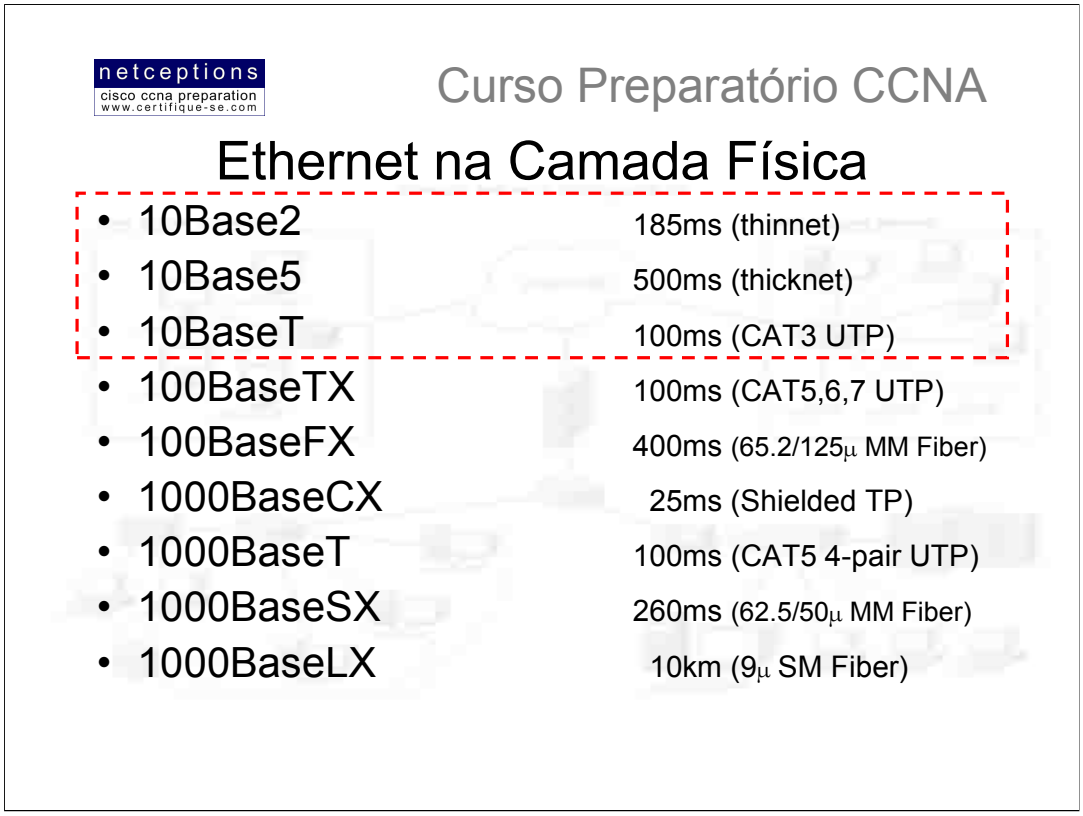
Podemos identificar os diferentes tipos de frames pelos campos apresentados (destacados).

1) Ethernet_II Frame

2) 802.3 Frame

3) 802.2 (802.3 LLC) Frame

4) SNAP Frame



Sintaxe: [taxa máxima de transmissão] [tipo de transmissão] [comprimento máximo do cabo]

Ex: 10Base2 = [10Mbps] [Baseband] [200 metros]

Os três primeiros padrões apresentados (em destaque) são os originais definidos pelo padrão IEEE (Institute of Electrical and Electronic Engineers) 802.3. Cada um dos padrões IEEE 802.3 apresentados (os 3 primeiros apenas) definem uma interface de conexão (Attachment Unit Interface - AUI), que permite a **transferência bit-a-bit** (*baseband*) da camada de enlace para a camada física. Isso permite que o MAC mantenha-se constante, ao mesmo tempo suportando novas tecnologias.

A interface AUI, entretanto, não suportava 100Mbps Ethernet devido às altas frequências envolvidas. 100BaseT Ethernet precisava de uma nova interface, e as especificações 802.3u vieram a definir um novo padrão de interface, chamado Media Independent Interface (MII), permitindo taxas de até 100Mbps a 4 bits por vez. Gigabit Ethernet utiliza outro padrão de interface, chamado de Gigabit Media Independent Interface (GMII), permitindo transferências à 1000Mbps, 8 bits por vez.

É importante entender e saber diferenciar as diferentes velocidades de acesso à mídia que o padrão Ethernet disponibiliza. Entretanto, é igualmente importante conhecer os requerimentos de cada tipo de conector para cada tipo de implementação, antes de se tomar uma decisão. EIA/TIA (Electronic Industry Association e Telecom Industry Association) são grupos que padronizam e definem as especificações físicas para o padrão Ethernet. EIA/TIA especifica que o padrão Ethernet utilize um conector registrado (Registered Jack - RJ-**45**), com uma sequência **4 5** em um cabo de par trançado não blindado (Unshielded Twisted Pair - UTP). Abaixo, listamos os tipos de conectores para cada caso:

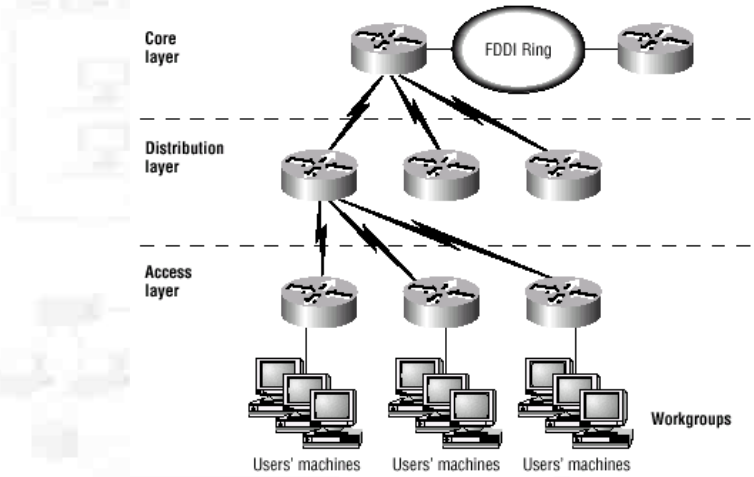
- **10Base2** - Utiliza barramento lógico e físico, com conector AUI
- **10Base5** - Utiliza barramento lógico e físico, com conector AUI
- **10BaseT** - Topologias estrela e barramento lógico, conector RJ-45
- **100BaseTX** - Topologias estrela e barramento lógico, conector RJ-45 MII
- **100BaseFX** - Topologia Ponto-a-Ponto, conector ST ou SC

Nota: 100VG-AnyLan - Foi o primeiro 100Mbps LAN. Utiliza par trançado e não é compatível com os padrões de sinalização Ethernet. Caiu em desuso.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

O Modelo de 3 Camadas Cisco



Sistemas hierárquicos nos ajudam a entender melhor onde cada coisa deve ser alocada, como cada coisa se encaixa e interage, e quais funcionalidades vão onde. Eles trazem ordem e compreensão para o que seriam, de outro modo, sistemas complexos.

Grandes redes podem vir a ser extremamente complexas, com múltiplos protocolos, configurações detalhadas, tecnologias diversas. Hierarquização nos ajuda a sumarizar uma complexa coleção de detalhes em um modelo compreensível.

O modelo de 3 camadas criados pela Cisco pode ajuda-lo a desenhar, implementar e manter uma rede hierárquica altamente escalável, confiável e custo-efetiva. Cisco define 3 camadas hierárquicas, como demonstradas na figura acima. É importante ter o conceito de “manter o tráfego local, localmente” ao se planejar uma rede hierárquica. Vamos estudar cada uma das camadas propostas pela Cisco.

• **Core Layer (Camada Principal)** - A camada principal é o coração da rede. Responsável pelo transporte de grandes volumes de dados, de forma simultaneamente rápida e confiável. Se ocorrer uma falha nesta camada, todos os usuários serão afetados. Portanto, tolerância à falha é um fator crítico nesta camada. O que **NÃO** se deve fazer nesta camada:

✓ Não faça nada que retarde o tráfego de dados, incluindo a implementação de listas de acesso, roteamento entre VLANs e filtragem de pacotes;

✓ Não suporte acesso à grupos de trabalho nesta camada;

✓ Evite a expansão do core adicionando mais routers. Se performance tornar-se um fator crítico no core, opte pelo upgrade à expansão.

• **Distribution Layer (Camada de Distribuição)** - Também referido como Camada de Grupos de Trabalho. A função principal desta camada é prover o roteamento, filtragem e acesso WAN, e determinar como os pacotes devem acessar o core, caso necessário. Nesta camada devem ser implementadas políticas de acesso à rede. Eis uma lista de itens que devem ser executados nesta camada:

✓ Implementação de ferramentas como listas de acesso, filtragem de pacotes e queuing;

✓ Implementação de políticas de segurança e acesso à rede, incluindo firewalls e address translation services;

✓ Redistribuição entre protocolos de roteamento, incluindo roteamento estático;

✓ Roteamento entre VLANs;

✓ Definição de domínios broadcast e multicast

• **Access Layer (Camada de Acesso)** - A camada de acesso controla o acesso de grupos e usuários aos recursos da rede. Grande parte dos recursos que os usuários precisarão estarão disponíveis localmente. Alguns itens que devem ser incluídos nesta camada:

✓ Implementação continuada de políticas de acesso à rede e segurança;

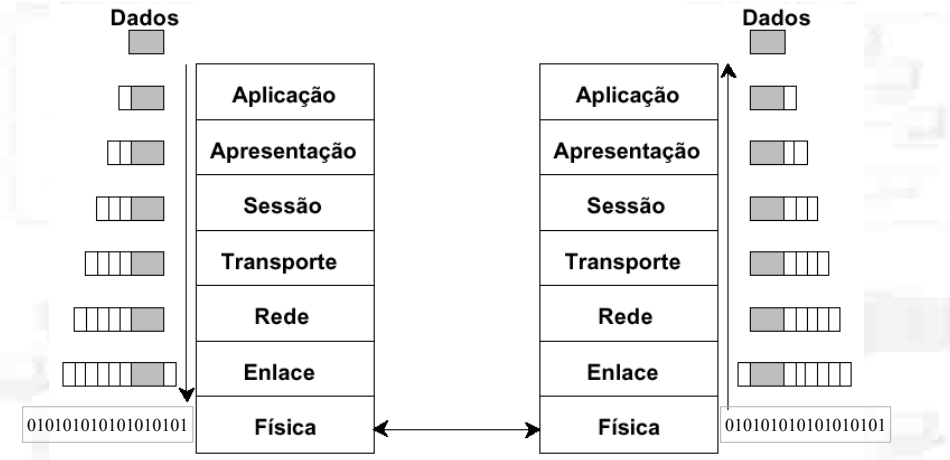
✓ Criação de diferentes domínios de colisão;

✓ Conectividade dos grupos de trabalho com a camada de distribuição

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Encapsulamento de Dados



Quando um dispositivo transmite dados através de uma rede para outro dispositivo, esses dados são encapsulados - “embrulhados” - com informações específicas em cada camada do modelo OSI.

Cada camada do dispositivo transmissor comunica-se apenas com sua camada “irmã” no dispositivo receptor. Para se comunicar e trocar informações, cada camada usa o que chamamos de **Protocol Data Units** (**PDUs**). Essas PDUs contém informações específicas de controle anexadas a medida em que os dados atravessam cada camada do modelo, tipicamente anexadas ao cabeçalho (**header**) do pacote de dados, podendo também ser anexada ao seu final (**trailer**).

Essas informações são anexadas aos dados através de um processo conhecido como encapsulamento, que ocorre em cada uma das camada do modelo. Cada PDU tem um nome específico, dependendo da informação que seu cabeçalho carrega. Essa informação apenas pode ser interpretada pela camada “irmã”, no dispositivo receptor, quando é retirada, e os dados são repassados para a camada imediatamente superior.

O processo se repete até que o pacote de dados atinja as camadas superiores do modelo (Sessão, Apresentação e Aplicação), quando podem ser interpretados e utilizados. A figura acima ilustra esse processo, camada à camada.

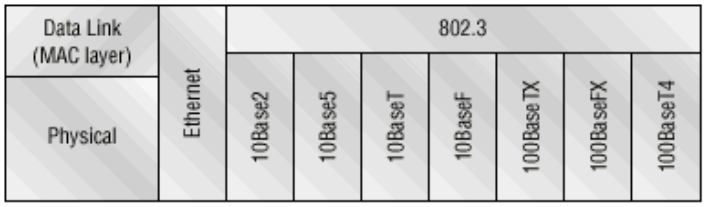
Observe que, na camada de enlace, além do cabeçalho, encontramos também um trailer. Este anexo contém o campo **FCS** (Frame Check Sequence), que detecta se os dados foram corrompidos durante o processo de transmissão pela camada física (bits).

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Cabeando uma Rede LAN Ethernet

Especificações Ethernet na Camada Física



O padrão Ethernet foi implementado pela primeira vez por um grupo conhecido como DIX (DEC, Intel e Xerox). Era uma rede 10Mbps, que utilizava cabos coaxiais, par-trançado e fibra óptica.

Quando planejar uma LAN, é importante ter-se em mente os diferentes tipos de mídia ethernet disponíveis. Seria, sem dúvida, maravilhoso implementar uma rede rodando gigabit ethernet em cada desktop e 10 gigabit ethernet entre switches e, embora isso venha a acontecer algum dia, seria muito difícil justificar o custo de uma rede com esse perfil nos dias de hoje.

Utilizando-se um “mix” das diferentes mídias ethernet disponíveis hoje, você pode criar uma rede eficiente e custo-efetiva. Eis uma lista com sugestões de onde utilizar cada tipo de mídia em uma rede hierárquica:

• Implemente switches 10Mbps na camada de acesso para promover uma boa performance à um custo baixo. Links de 100Mbps podem ser usados em clientes e servidores que demandem largura-de-banda mais elevada. Nenhum servidor deve rodar à 10Mbps, se possível;

• Implemente FastEthernet nos switches entre as camadas de acesso e distribuição. A utilização de 10Mbps criaria gargalos;

• Implemente FastEthernet (ou Gigabit Ethernet, se aplicável) nos switches entre a camada de distribuição e o core. Você também deve se preocupar em implementar as mais rápidas mídias disponíveis entre os switches do core. Links duplos nos switches presentes entre a camada de distribuição e o core são recomendáveis para redundância e balanceamento de carga.

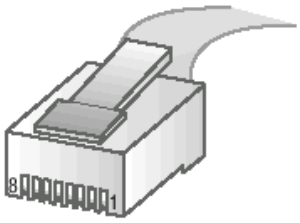
netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Cabeando uma Rede LAN Ethernet

Conexões UTP (RJ-45)

Pin	Wire Pair (T Is Tip; R Is Ring)
1	Pair 2 T2
2	Pair 2 R2
3	Pair 3 T3
4	Pair 1 R1
5	Pair 1 T1
6	Pair 3 R3
7	Pair 4 T4
8	Pair 4 R4



RJ-45 connector

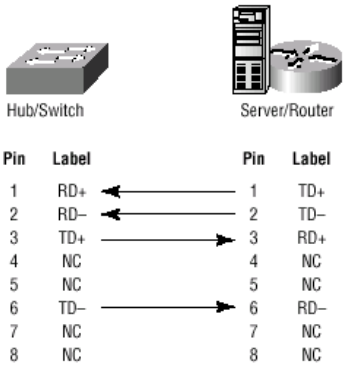
O conector UTP é transparente, e permite que você veja os 8 fios coloridos que se conectam aos pinos do conector. Esses fios são trançados em 4 pares. 4 fios (2 pares) carregam a voltagem e são chamados de *tip*. Os 2 pares restantes são aterrados e conhecidos como *ring*. O conector RJ-45 é crimpado na ponta do cabo, e a pinagem do conector é numerada de 8 a 1.

A figura acima ilustra um cabo UTP com um conector RJ-45 instalado. Os cabos UTP possuem pares trançados de fios em seu interior para eliminar o efeito cross talk. A proteção aos sinais digitais vem da torção dos fios. Quanto mais torções por polegada, mais distante, supostamente, o sinal pode viajar sem interferência.

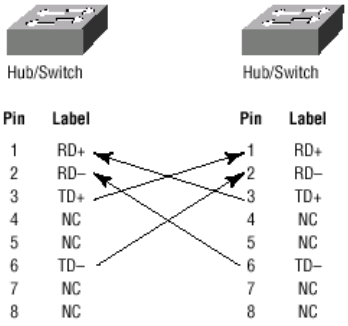
Cabos UTP categorias 5 e 6, por exemplo, têm muito mais torções por polegada que cabos categoria 3.

Diferentes tipos de cabos são necessários na implementação de uma rede. Você deve saber quando utilizar cabos **Straight-Through (a)** ou **Crossover (b)**.

a) Straight-Through



b) Crossover



• **Utilize cabos Straight-Through para conectar**: um router à um hub ou switch, um servidor à um hub ou switch, uma workstation à um hub ou switch.

• **Utilize cabos Crossover para conectar**: uplinks entre switches, hubs à switches, hub à outro hub, interface de um router à outra interface de router, 2 computadores sem um hub ou switch.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Conexões e Conectores WAN

- Transmissão serial
- DTE / DCE (Data Terminal Equipment / Data Communication Equipment)
- Interfaces modulares e fixas
- Conexões ISDN
- Conexões via console

As conexões seriais disponibilizadas pelos produtos Cisco suportam praticamente qualquer tipo de serviço WAN. As conexões típicas encontradas são linhas privativas / dedicadas (LPs) utilizando HDLC (High Level DataLink Control), PPP (Point-to-Point Protocol), ISDN (Integrated Services Digital Network) e Frame Relay. As velocidades mais comuns variam de 2400bps à 1.544Mbps (T1).

• **Transmissão serial** - Conectores seriais WAN utilizam transmissão serial, que é feita bit-a-bit, sobre um único canal. Transmissões paralelas podem ser feitas até 8 bits por vez. **Todas as WANs utilizam transmissão serial.**

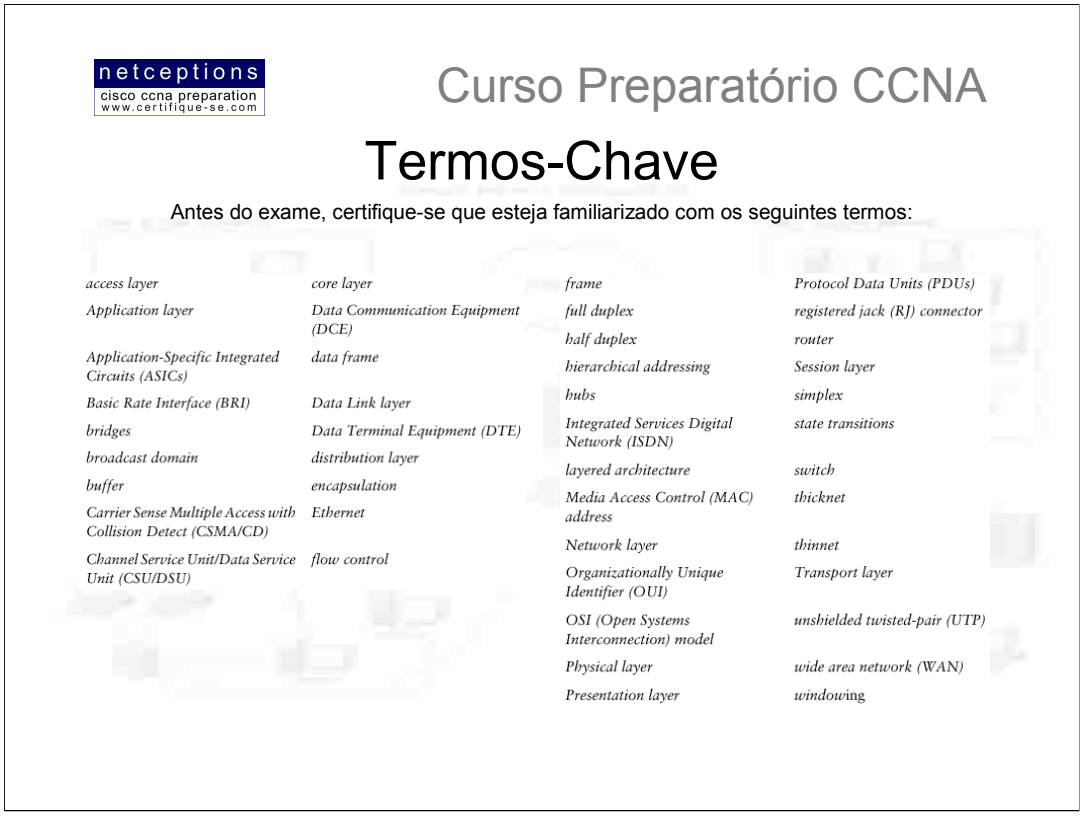
Roteadores Cisco utilizam um conector serial de 60 pinos, proprietário da Cisco (exclusivo). O tipo de conector que você encontrará na outra ponta vai depender do provedor de serviço ou dos requerimentos do dispositivo de ponta. As diferentes terminações disponíveis são EIA/TIA-232, EIA/TIA-449, V.35 (usados na conexão de CSU/DSU), X.21 (usados em redes X.25/Frame Relay), e EIA-530. Conexões seriais são descritas em frequência, ou ciclos-por-segundo (hertz). A quantidade de dados que podem ser transportados nessas frequências é chamada de largura-de-banda (bandwidth), ou seja, **bandwidth é a quantidade de dados, em bits-por-segundo, que uma conexão serial pode transportar**.

• **DTE / DCE** - Routers são, por definição, dispositivos DTE, e se conectam à um dispositivo DCE - por exemplo, um CSU/DSU (Channel Service Unit / Data Service Unit). Os CSU/DSU então, são conectados a um demarc (demarcation location - normalmente, simplesmente uma tomada RJ-45 fêmea na parede), sendo a última responsabilidade do provedor. Tudo o que se encontra nas premissas do contratante de serviço, até o demarc, é chamado de Customer Premise Equipment (CPE).

• **Interfaces modulares e fixas** - Alguns router Cisco têm interfaces fixas, outros, modulares. Os routers de interface fixa, como a série 2500, não podem ter suas interfaces mudadas ou atualizadas. Se você necessitar de uma nova interface, por exemplo, terá de comprar um novo router. Entretanto, routers como os da séries 1600, 1700, 2600 e 3600 possuem interfaces modulares, permitindo a adição, mudança ou atualização das interfaces disponíveis. São, portanto, mais customizáveis, e preservam o investimento. Routers da série 2600, por exemplo, provêem várias portas seriais, FastEthernet e, até a capacidade de se adicionar um módulo de voz.

• **ISDN** - ISDN-BRI (Basic Rate Interface) é composto de 2 canais B (Bearer) de 64Kbps e 1 canal D (Data) de 16Kbps para sinalização e sincronização. Routers que suportam ISDN-BRI vêm com uma interface U ou uma interface S/T. A diferença entre os 2 é que a interface U já é uma interface de 2 fios padrão ISDN, enquanto que a interface S/T possui 4 fios e precisa ser conectada à um terminal tipo 1 (NT 1) para converte-la em 2 fios, seguindo as especificações do padrão ISDN.

• **Conexões via Console** - Todos os produtos Cisco são comercializados com cabos e conectores de console, permitindo que você se conecte ao produto e o configure, o verifique e o monitore. O cabo utilizado na conexão entre um produto Cisco e um PC é um cabo rollover com conectores RJ-45. A pinagem dos cabos segue: 1-8;2-7;3-6;4-5;5-4;6-3;7-2;8-1. Como você pode perceber, basta se pegar um cabo Straight-Through, cortar uma das pontas, inverte-lo e crimpá-lo ao novo conector. Tipicamente, você utilizará um conector DB9 para conectar um produto Cisco ao seu PC e uma porta de comunicação para comunicação via HyperTerminal. A maioria dos produtos Cisco suportam conexões console via conectores RJ-45, entretanto, algumas séries ainda utilizam conectores DB25. A maioria dos routers têm uma porta AUX, que é uma porta auxiliar usada para conexão à um modem. As portas console e AUX são consideradas gerenciamento “out-of-band”, uma vez que você estará configurando o router fora da rede. Telnet é considerado gerenciamento “in-band”.



Resumo da aula 1:

Nesta aula começamos com a apresentação do modelo de referência OSI, que é um modelo de 7 camadas usado para ajudar desenvolvedores no desenho de aplicações que podem ser utilizadas em qualquer tipo de sistema ou rede.

Discutimos cada camada em detalhe, e apresentamos como a Cisco enxerga as especificações deste modelo.

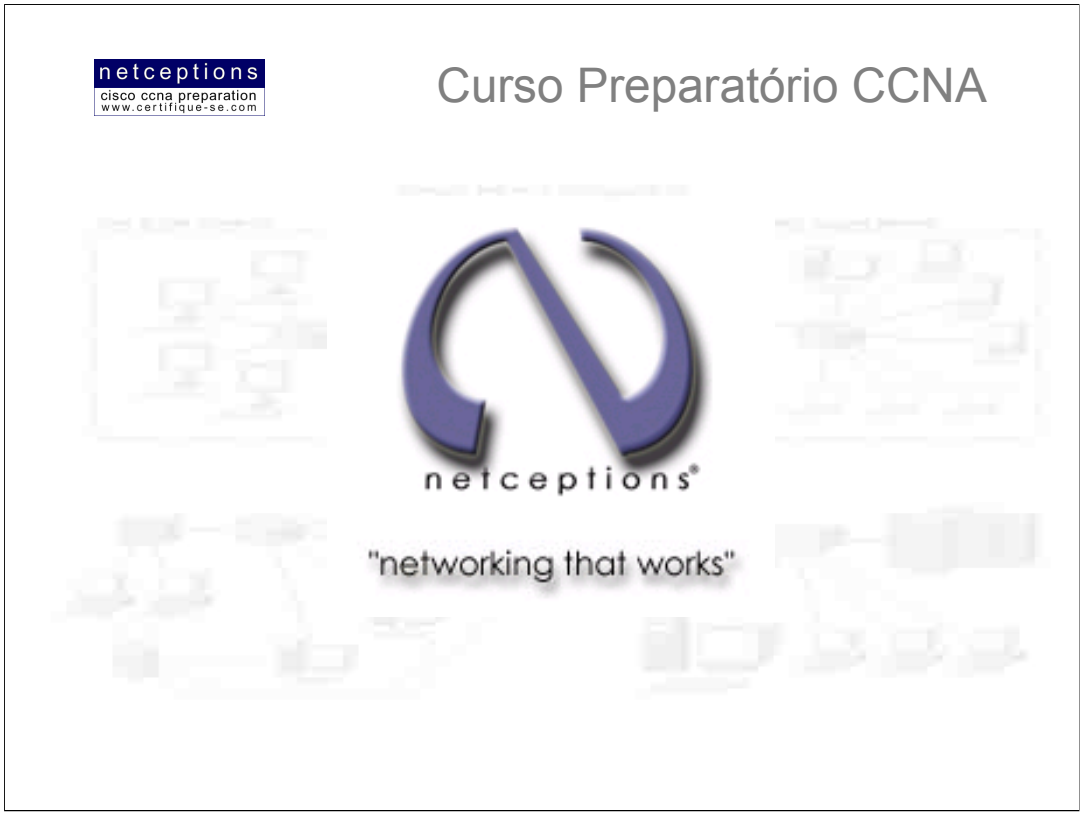
Diferentes tipos de dispositivos são especificados em cada camada do modelo OSI. Discutimos, nesta aula, os diferentes tipos de dispositivos, cabos, e conectores utilizados em cada uma das camadas.

Foi lhes apresentado o modelo hierárquico de 3 camadas desenvolvido pela Cisco, criado para ajudar administradores de rede a planejar e entender redes hierárquicas. Utilizando o modelo de 3 camadas Cisco, pode-se planejar, implementar e gerenciar efetivamente uma rede de qualquer tamanho.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

FIM AULA 01



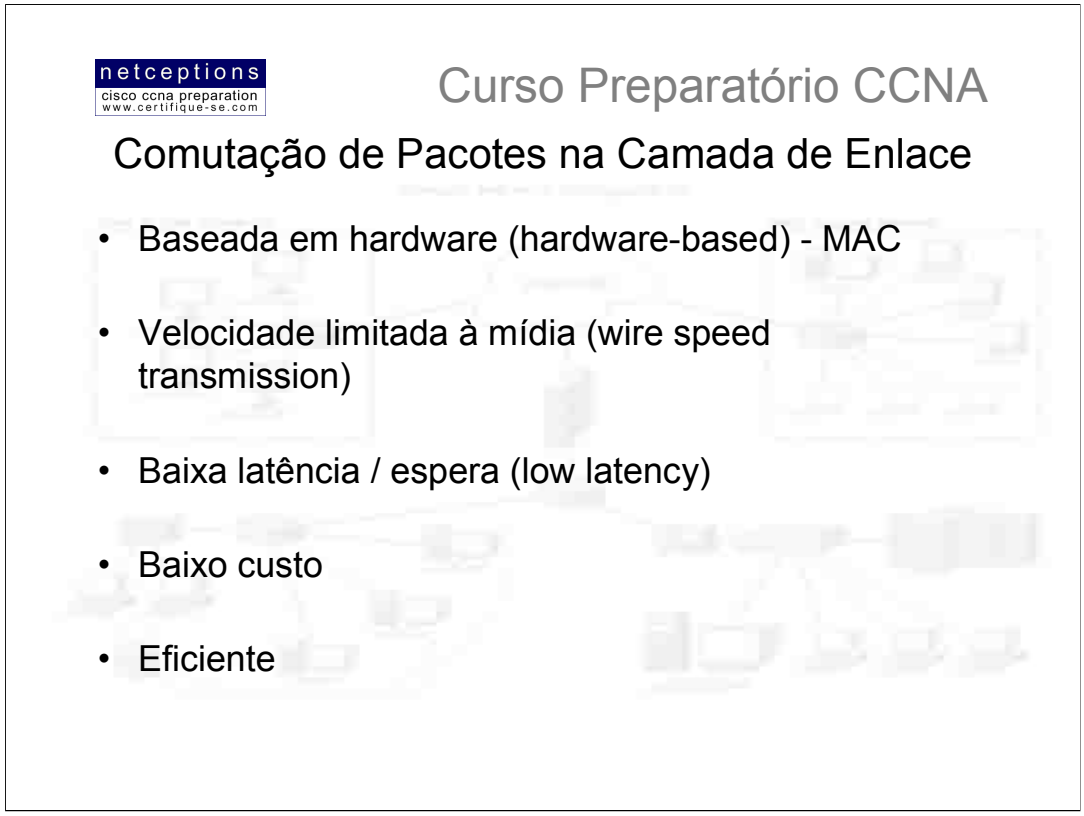
Apostila Aula 2

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Aula 2 / Módulo 1: Comutação de Pacotes

- Comutação na Camada de Enlace (Layer-2 Switching)
- O processo de “aprendizagem” de endereços (address learning process)
- Decisões de Encaminhamento / Filtragem
- Esquemas de Inibição de Loops (Loop Avoidance Schemes)
- Protocolo Spanning-Tree (STP)
- Tipos de Comutação LAN



Comutação na camada de enlace é baseada em hardware, o que significa que é utilizado o endereço MAC da placa de rede do dispositivo para filtrar a rede. Switches utilizam chips especiais (ASICs) para formar e manter tabelas de filtragem.

Switches são rápidos porque não analisam informações da camada de rede, analisando, em seu lugar, os endereços de hardware dos frames antes de decidir pelo encaminhamento ou abandono dos mesmos. O que torna a comutação na camada de enlace tão eficiente é a não modificação no pacote de dados, apenas no frame que o encapsula. Como nenhuma modificação no pacote é feita, o processo de comutação é mais rápido e menos suscetível à erros do que o processo de roteamento.

Comutação na C.E. pode ser utilizada para conectividade entre grupos de trabalho, e para a segmentação da rede (quebra dos domínios de colisão). Comutação na C.E. aumenta a largura-de-banda disponível para cada usuário, uma vez que cada conexão (interface) disponibilizada pelo switch é o seu próprio domínio de colisão. Devido à esse fator, pode-se conectar múltiplos dispositivos em cada interface.

A comutação na C.E., entretanto, tem algumas limitações. O modo correto de se criar redes comutadas eficientes é certificando-se que os usuários permanecerão ao menos 80% do seu tempo no segmento local. Redes comutadas quebram domínios de colisão, entretanto, a rede ainda é um grande domínio de broadcast, o que pode limitar o tamanho da rede, assim como causar problemas de performance. Broadcasts e multicasts, juntamente com a vagarosa convergência do Spanning Tree podem vir a ser problemas sérios à medida em que a rede cresce. Devido à esses (e outros) fatores, comutação na C.E. não pode substituir completamente os routers (dispositivos de camada 3 - rede) em uma internetwork.

Diferenças básicas entre um switch e uma bridge: **1)** bridges são baseadas em software, enquanto que switches são baseados em hardware (ASICs); **2)** bridges podem ter apenas uma ocorrência de spanning tree por bridge, enquanto que switches podem ter várias; **3)** bridges podem ter até 16 portas, enquanto que switches podem ter centenas.

3 funções básicas de um switch na camada de enlace:

• **Aprendizagem de endereços** - switches e bridges registram o endereço do hardware transmissor de cada frame recebido em determinada porta (interface), e adiciona essa informação à tabela MAC.

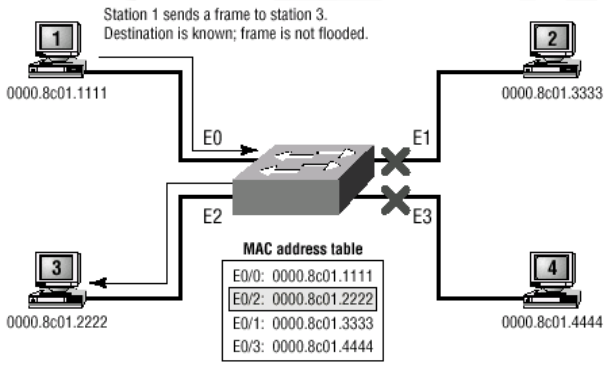
• **Decisões de filtragem / encaminhamento** - Assim que um frame é recebido em uma porta do switch, este verifica o endereço do hardware de destino e identifica a interface de saída através de checagem na tabela MAC.

• **Esquema de inibição de loops** - Se múltiplas conexões forem criadas entre switches visando redundância, loops de rede podem vir à ocorrer. O protocolo Spanning Tree (STP) é usado para evitar que loops de rede ocorram e permitir a redundância entre links.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Aprendizagem de Endereços



Assim que um switch é ligado, sua tabela de endereços MAC encontra-se vazia. Quando um dispositivo transmite e uma porta (interface) do switch recebe um frame, o switch armazena o endereço de hardware do dispositivo transmissor em sua tabela MAC, registrando a interface na qual este dispositivo está conectado. O switch não tem outra opção, a não ser “inundar” a rede com este frame, uma vez que ele não tem registro da localização do dispositivo destinatário. Se um dispositivo responder à essa “inundação” enviando o frame de volta, o switch irá, então, captar o endereço de hardware desse dispositivo e registrá-lo na tabela MAC, associando este endereço com a interface (porta) que recebeu o frame.

Como o switch tem agora 2 endereços em sua tabela MAC, os dispositivos podem realizar uma conexão ponto-a-ponto, e os frames serão encaminhados apenas aos 2 dispositivos participantes. É essa a grande diferença entre switches e hubs. Em uma rede composta por hubs, frames são encaminhados à todas as portas, o tempo todo.

Se os dois dispositivos não se comunicarem com o switch novamente por um determinado período de tempo, o switch irá deletar seus endereços de sua tabela MAC, com o intuito de mantê-la o mais atualizada possível.

A figura acima ilustra como a tabela MAC é formada.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Decisões de Encaminhamento ou Filtragem

- Descrição do processo de filtragem e encaminhamento

- Definição de frames broadcast e multicast

	Binary	Decimal
Broadcast	11111111.11111111.11111111.11111111	255.255.255.255
Multicast	10101100.00010000.11111111.11111111	172.16.255.255

Assim que um frame chega à interface de um switch, o endereço do hardware de destino é comparado com a tabela de encaminhamento / filtragem (MAC). Se o endereço de destino for conhecido e estiver presente na tabela, o frame será encaminhado apenas para a porta de saída relacionada àquele endereço.

O switch não transmite o frame para todas as interfaces, apenas para a interface de destino. Esse processo preserva a largura-de-banda de outros segmentos da rede, e é conhecido como filtragem de frames (*frame filtering*).

Se o endereço do hardware de destino, entretanto, não estiver listado na tabela MAC do switch, o frame, então, é encaminhado à todas as interfaces ativas (broadcasting), com exceção da interface na qual ele foi recebido. Se um dispositivo responder à essa transmissão, a tabela MAC é atualizada com a localização desse dispositivo (interface).

Frames broadcast e multicast.

Esses são tipos especiais de frames, e não possuem o endereço do hardware de destino especificados. O endereço destinatário será sempre o endereço do hardware transmissor, e o endereço de destino será ou uma série de 1s, ou com o endereço de rede ou sub-rede definido e o endereço do dispositivo uma série de 1s (veja figura acima).

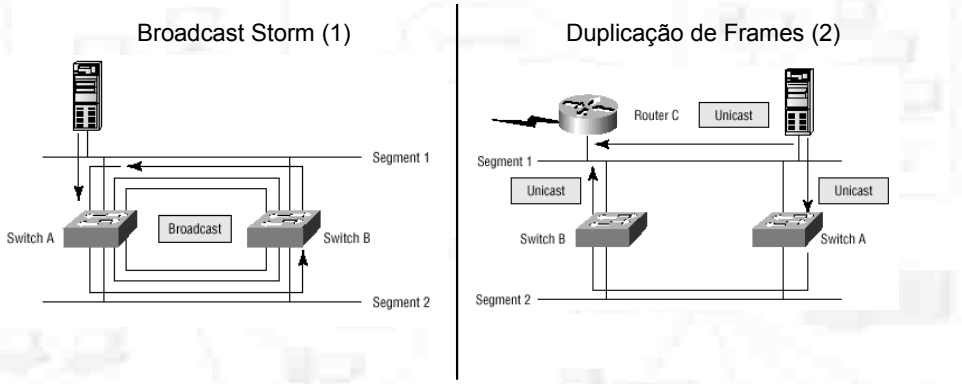
Note, na figura, que o endereço de broadcast é formado por uma série de 1s, enquanto que o de multicast, não. Ambos são tipos de broadcasts, com a diferença que frames multicast apenas são enviados à uma determinada rede ou sub-rede, enquanto que frames broadcasts são enviados à todas as redes e dispositivos conectados.

Quando um switch recebe esses tipos de frames, eles são rapidamente encaminhados à todas as portas ativas. Para conter encaminhamentos de frames broadcast e multicast a uma porção limitada de portas administrativamente designadas, pode-se criar LANs virtuais (VLANs), que são assunto de outra aula.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Esquemas de Inibição de Loops de Rede



Estabelecimento de conexões (links) redundantes são uma boa idéia entre switches. Eles são usados para se evitar a completa queda da rede no caso da falha de um link. Embora links redundantes sejam extremamente úteis, eles podem trazer mais problemas do que resolve-los. Uma vez que frames podem ser propagados através de todos os links redundantes simultaneamente, loops de rede podem ocorrer, entre outros problemas. Alguns dos mais sérios discutiremos à seguir.

• Se nenhum esquema de inibição de loops de rede for implantado, os switches poderão inundar continuamente a rede com frames broadcast. Esse fenômeno é conhecido como tempestade de broadcast (*broadcast storm*). A figura 1 ilustra como uma transmissão broadcast pode ser propagada pela rede.

• Um dispositivo pode vir a receber múltiplas cópias do mesmo frame, uma vez que este frame pode chegar de diferentes segmentos ao mesmo tempo. (figura 2)

• A tabela MAC ficará “confusa” sobre a localização (interface) de um determinado dispositivo, uma vez que o switch pode receber determinado frame de mais de um link. Pode ocorrer de o switch não encaminhar o frame, uma vez que estará constantemente atualizando sua tabela MAC com a localização do hardware transmissor. Esse fenômeno é conhecido como *trashing* da tabela MAC.

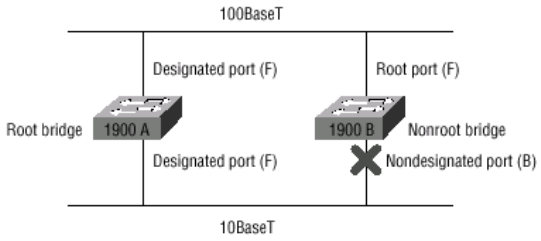
• Um dos maiores problemas é a geração de múltiplos loops através da internetwork. Isso significa que loops podem ocorrer dentro de outros loops. Se um broadcast storm então ocorrer, o switch ficará sem condições de desempenhar a comutação de pacotes, travando a rede.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Esquemas de Inibição de Loops de Rede

- O Protocolo Spanning Tree (STP)



O criador original do protocolo Spanning Tree foi a DEC (Digital Equipment Corporation), que foi comprada e hoje é conhecida como Compaq. O IEEE desenvolveu sua própria versão do protocolo, denominado 802.1d. Os switches Cisco utilizam a versão IEEE do protocolo Spanning Tree, que não é compatível com a versão da DEC.

O papel principal do STP é evitar que loops de rede ocorram em redes de camada de enlace. STP monitora constantemente a rede identificando todos os links e certificando-se que loops de rede não ocorram, através do desligamento de links redundantes. O modo como o protocolo STP faz isso é elegendo um **switch-raiz (root bridge),** que será responsável por toda a topologia da rede.

Em uma rede, apenas 1 switch-raiz pode existir. As interfaces - ou portas - dos switches raiz são denominadas **portas designadas (designated ports),** que possuem modo de operação chamados **modo de encaminhamento (forwarding-state).** Portas em modo forwarding-state podem enviar e receber dados.

Os outros switches presentes na rede são denominados **não-raiz (non-root bridges),** conforme ilustração acima. **A porta com menor custo (determinada pela largura-de-banda do link) ao switch-raiz é chamada de porta-raiz (root-port),** e também pode enviar e receber dados. Portas que tenham o menor custo de distância para o switch-raiz são chamadas de portas designadas. **As portas restantes são consideradas portas não-designadas e não podem enviar ou receber dados**, encontrando-se em modo de bloqueio **(blocking mode).**

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Esquemas de Inibição de Loops de Rede

- Determinando o switch-raiz
- Determinando a porta designada

Speed	New IEEE Cost	Original IEEE Cost
10Gbps	2	1
1Gbps	4	1
100Mbps	19	10
10Mbps	100	100

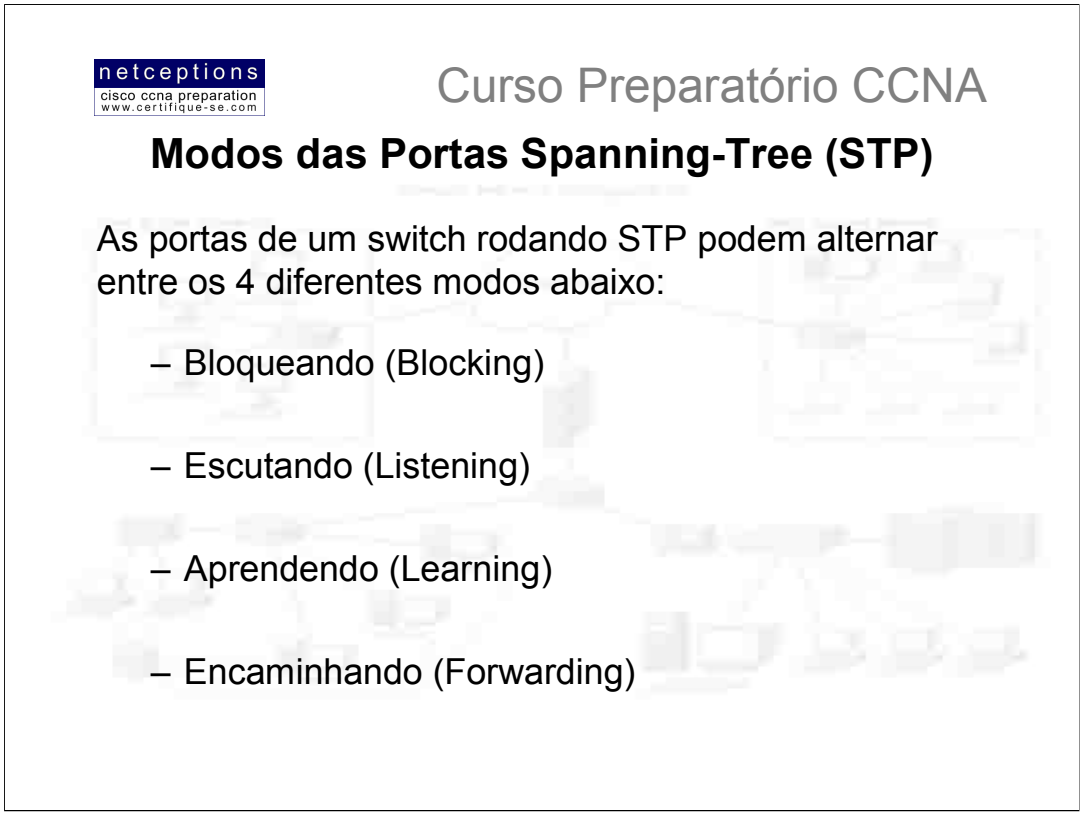
Custos típicos de diferentes tipos de rede Ethernet

Switches e bridges rodando STP trocam informações através do que chamamos de Bridge Protocol Data Units (BPDUs). BPDUs enviam mensagens de configuração via frames broadcast. O ID (identificador) de cada switch é enviado aos outros dispositivos através das BPDUs. O **ID** do switch é utilizado na determinação do switch-raiz na rede, e também da porta-raiz. Esse ID tem um comprimento de 8 bytes, e inclui o **valor de prioridade (priority value)** e o endereço de hardware (MAC address) do dispositivo. **O valor de prioridade default para todos os dispositivos rodando a versão IEEE do STP é 32.768.**

Para determinar o switch-raiz, os valores de prioridade e os endereços de hardware são combinados. **Se 2 switches têm o mesmo valor de prioridade, então o endereço de hardware será utilizado para a definição do switch-raiz, que será aquele com o ID mais baixo.** Por exemplo, vamos supor 2 switches - A e B. O switch A tem seu valor de prioridade default (32.768), e seu endereço de hardware 0000.0c00.1111.1111. O switch B, por sua vez, também tem seu valor de prioridade default (32.768), porém, seu endereço de hardware é 0000.0c00.2222.2222. Pelas regras acima descritas, o switch A seria, neste caso, definido como switch-raiz, pois seu ID (combinando-se prioridade e MAC) é menor do que o do switch B (...1111.1111 < ...2222.2222).

Determinação da porta designada

Para se determinar a porta - ou as portas - que será usada para comunicação com o switch-raiz, você precisa determinar, antes, o custo de distância. O protocolo STP determina esse custo baseando o custo de distância na largura-de-banda disponível à cada link. A figura acima ilustra os custos típicos associados às diferentes redes Ethernet.



As portas de um switch ou bridge rodando STP podem alternar entre os 4 modos seguintes:

• **Blocking** - Não encaminhará frames. Pode receber e analisar BPDUs (listen). Todas as portas de um switch encontram-se em blocking mode quando o mesmo é ligado.

• **Listening** - Recebe e analisa BPDUs para certificar-se que não ocorrerão loops na rede antes de começar o encaminhamento de frames.

• **Learning** - Registra os endereços dos hardwares conectados às interfaces e forma a tabela MAC. Não encaminha frames, ainda.

• **Forwarding** - Envia e recebe dados

Tipicamente, switches se encontram ou no modo blocking, ou no modo forwarding. Uma porta forward é tida como tendo o menor custo ao switch-raiz. Entretando, se a topologia da rede se alterar devido à uma falha em um link, ou à adição de outro switch pelo administrador de rede, as portas em um switch se encontrarão nos modos listening e learning.

O modo blocking é usado para deter loops de rede. Uma vez que o switch determina o melhor caminho (porta) ao switch-raiz, todas as outras portas entrarão em modo blocking. Portas em modo blocking podem receber BPDUs. Se um switch determinar que uma porta em modo blocking deve, então, tornar-se uma porta designada, esta porta entrará em modo listening. Ela analisará todas as BPDUs recebidas para certificar-se de que não criará um loop uma vez que a porta entre em modo forwarding.

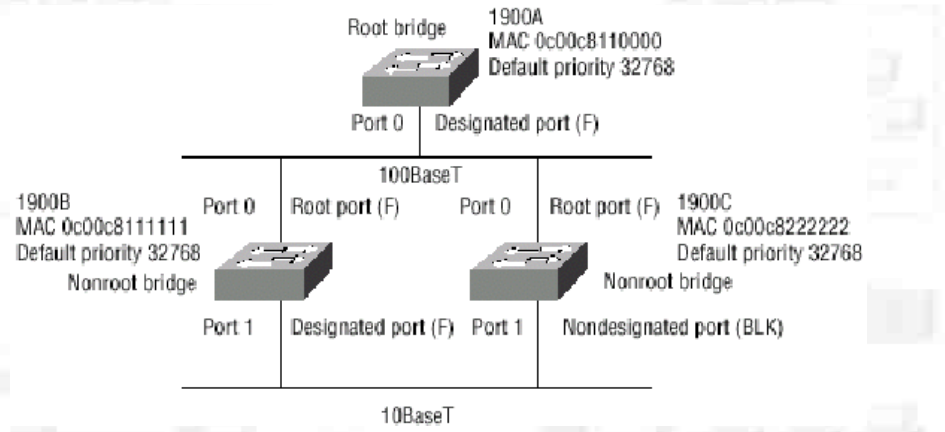
Convergência

Convergência ocorre quando switches acabam o processo de alternância do modo blocking até o modo forwarding. Não há transmissão de dados durante esse processo de convergência. O processo é importante para assegurar que todos os switches tenham o mesmo banco de dados (tabela MAC). Antes de dados serem encaminhados, as tabelas de todos os dispositivos devem ser atualizadas. O grande problema inerente ao processo de convergência é o tempo consumido - normalmente 50 segundos para ir do modo blocking para o modo forwarding. Esse timer default pode ser alterado se necessário, embora não seja recomendado.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Exemplo de Spanning-Tree



É importante entender claramente como o protocolo STP funciona em uma rede. A figura acima ilustra uma situação onde os 3 switches (1900A, 1900B e 1900C) têm a mesma prioridade (32.768). Entretanto, note os endereços de hardware (MAC address) de cada um. Analisando-os você será capaz de determinar o switch-raiz.

Como o switch 1900A possui o endereço de hardware mais baixo (...8110000), este será o switch-raiz. Para definição das portas-raiz nos switches 1900B e 1900C, você precisa analisar o custo dos links conectando cada switch. Uma vez que a conexão de ambos os switches ao switch-raiz ocorre através da porta 0 usando um link de 100Mbps, as portas-raiz para ambos os switches será a porta 0.

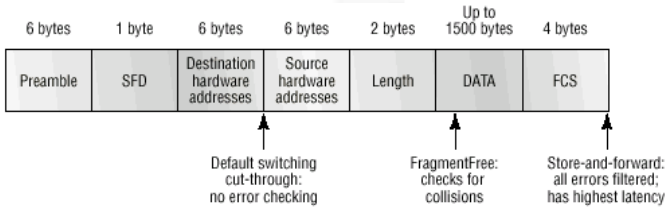
Agora, para determinar as portas designadas, o ID deve ser usado. **O switch-raiz SEMPRE tem todas as suas portas designadas**. Ambos os switches (1900B e 1900C) têm o mesmo custo para o switch-raiz, entretanto, a porta designada será a do switch 1900B, uma vez que este apresenta o menor ID. Como a porta designada pertence ao switch 1900B, o switch 1900C colocará a porta 1 em modo blocking, evitando assim que qualquer loop de rede venha a ocorrer.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Tipos de Comutação LAN

- Store and Forward (maior latência)
- Cut-through (tempo real)
- FragmentFree (cut-through modificado)

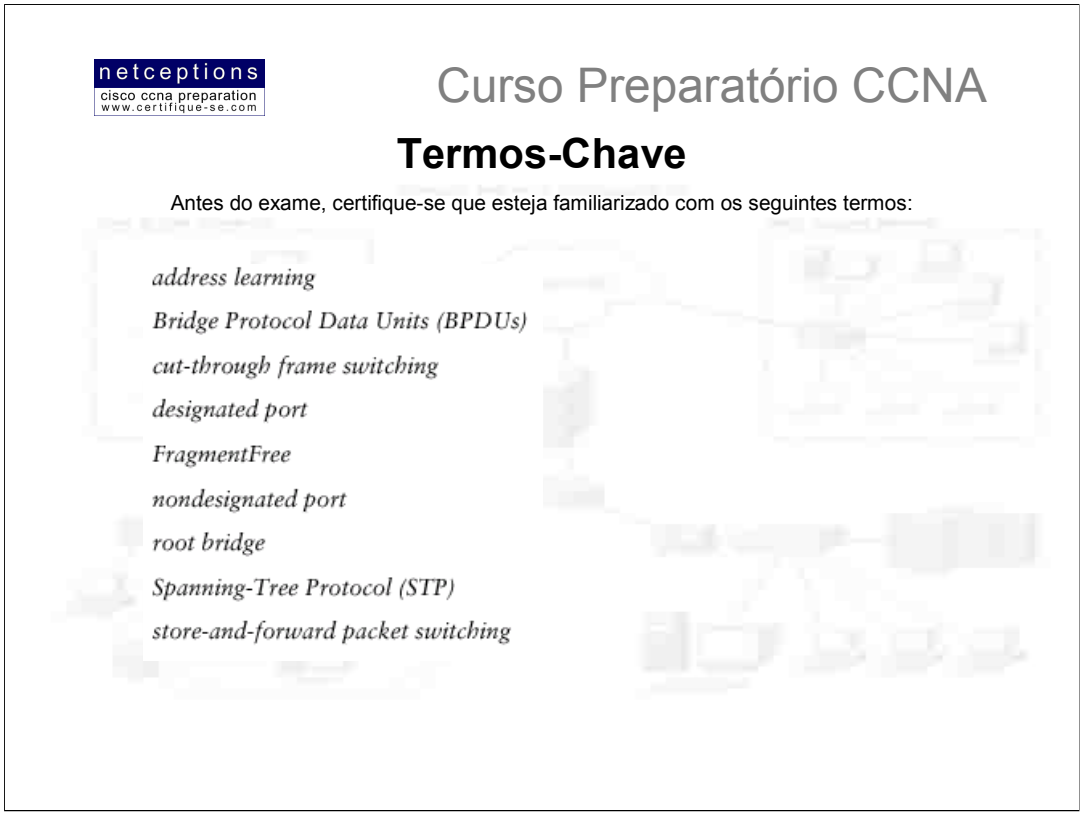


O tempo requerido para a comutação de um pacote em um switch depende do modo de comutação escolhido:

• **Store and forward** - Como o nome sugere - armazene e encaminhe -, este tipo de comutação faz com que o frame seja completamente recebido e armazenado no buffer do switch. Uma checagem de erros (CRC - Cyclic Redundant Check) é efetuada e, finalmente, o endereço de destino é localizado na tabela MAC. Como o frame é antes copiado para o buffer do switch para posteriormente ser encaminhado, a latência deste método é a maior dentre os 3. O frame é descartado caso um erro seja detectado na checagem, caso seja muito curto (menos de 64 bytes, incluindo o campo CRC), ou caso seja muito longo (maior que 1518 bytes, incluindo o campo CRC). Caso não sejam identificados erros, o endereço do hardware destino é localizado na tabela MAC e a porta de saída é identificada (caso o endereço exista na tabela). Somente então o frame é encaminhado ao seu destino. Os switches da linha Catalyst 5000 utilizam esse modo como default, não podendo ser alterado.

• **Cut-through (tempo real)** - Esse é o modo predominante em comutação LAN. Através deste método, o switch LAN copia apenas o endereço de destino (os primeiros 7 bytes seguindo o campo preamble - figura) para seu buffer. Logo após, o endereço do hardware de destino é localizado na tabela MAC, a interface de saída é determinada e o frame é encaminhado ao seu destino. Esse modo provê baixa latência pois o encaminhamento do frame começa assim que o endereço de destino é lido e a interface de saída determinada. Alguns modelos de switch podem ter o modo cut-through configurado porta-à-porta, até que um ponto inicial de erro definido pelo usuário seja atingido. Nesse ponto, o modo de comutação é automaticamente trocado para store and forward, eliminando, assim, o encaminhamento de erros

• **FragmentFree (cut-through modificado)** - Esse modo é uma modificação do modo cut-through, na medida em que aguarda a passagem da janela de colisão (collision window - 64 bytes) antes de encaminhar o pacote. Se o pacote possui algum erro, é muito provável que seja identificado nos 64 bytes iniciais. Portanto, o modo FragmentFree promove uma checagem de erros mais confiável, praticamente sem aumento de latência. Esse é o modo default de switches da linha Catalyst 1900.



Resumo:

O objetivo deste módulo foi prepará-lo com as informações sobre comutação na camada de enlace, necessárias para prosseguirmos com o curso.

Cobrimos, neste módulo, os seguintes tópicos:

• Comutação na camada de enlace e diferenças entre switches e bridges;

• O processo de aprendizado de endereços (address learning) e como a tabela MAC é formada;

• O processo de decisão de encaminhamento / filtragem que switches executam, e como eles o fazem;

• Esquemas de inibição de loops de rede e os problemas causados quando tais esquemas não são utilizados;

• O protocolo Spanning-Tree (STP) e como ele é utilizado na prevenção de loops;

• Os tipos de comutação LAN utilizados em switches Cisco e como diferenciá-los.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Módulo 2: Visão Geral da Linha de Produtos Cisco

Selecionando produtos Cisco

- Hubs 
- Switches 
- Routers 

Você pode se utilizar do modelo de 3 camadas desenvolvido pela Cisco para ajudá-lo a determinar qual tipo de produto Cisco é mais adequado à sua rede. Entendendo os serviços requeridos em cada camada, e a funcionalidade de cada dispositivo, você estará apto a selecionar produtos que satisfaçam as necessidades de sua internetwork.

Ao selecionar produtos Cisco para sua rede, comece por coletar informações sobre onde os dispositivos devem operar, na organização hierárquica da sua rede. Considere, então, características como facilidade de instalação, densidade de portas, entre outras.

Se você possui escritórios remotos, ou outras necessidades WAN, por exemplo, você precisa, antes de mais nada, avaliar quais tipos de serviços estão disponíveis. De nada adiantará planejar uma grande rede baseada em Frame Relay e descobrir, posteriormente, que o serviço é suportado apenas em metade das localidade envolvidas. Após alguma pesquisa entre os provedores de serviço disponíveis, você poderá se concentrar na escolha do melhor equipamento que satisfaça suas necessidades.

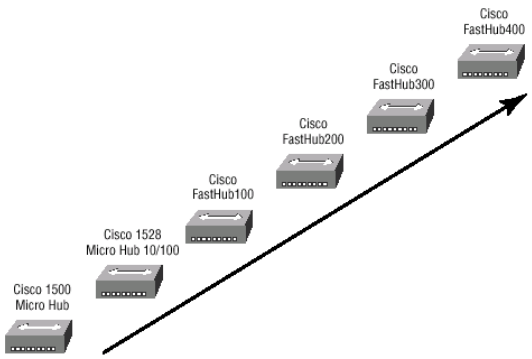
Você terá algumas opções, tipicamente: dial-up, conexões assíncronas, linhas arrendadas até 1.544Mbps, Frame Relay, e ISDN, que perfazem o conjunto de tecnologias WAN mais populares. Entretanto, a tecnologia xDSL vem ganhando terreno como uma tecnologia WAN confiável, rápida, prática e barata.

Você precisa considerar o uso, antes de adquirir e implementar a tecnologia. Por exemplo, se os usuários dos escritórios remotos ficam conectados à matriz mais de 4 horas por dia, você deveria considerar a implementação ou de Frame Relay, ou de uma linha arrendada. Se a frequência de conexão não é constante, então, talvez uma conexão dial-up ou ISDN seja uma boa - e barata - alternativa. Discutiremos, a seguir, diferentes tipos de Hubs, Switches e Routers Cisco, que podem ser utilizados na construção de sua rede hierárquica.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Hubs Cisco



A Cisco certamente não ficou famosa e fez fortuna apoiada em sua linha de hubs. Mas, na eventualidade de alguém cogitar a compra de um, a Cisco tem uma linha completa.

Antes de adquirir um hub, você precisa saber exatamente quais usuários podem dividir a largura-de-banda de uma rede 10Mbps, ou 100Mbps. A linha mais simples de hubs Cisco suporta apenas 10Mbps, enquanto que as linhas intermediárias suportam 10-100Mbps, com portas auto-sensing.

A linha top - e mais cara - oferecem portas de gerenciamento de rede e conexões via console, ou seja, são configuráveis. Se você planeja gastar o suficiente para comprar um hub top de linha, talvez valha mais a pena considerar a aquisição de um switch.

A figura acima ilustra a linha completa de hubs Cisco. Todos eles podem ser empilhados e conectados entre si, disponibilizando uma maior densidade de portas.

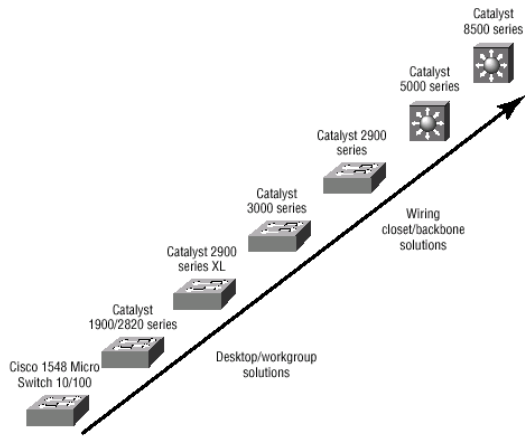
Eis alguns pontos à serem analisados:

- Requerimentos de rede para 10 ou 100Mbps
- Densidade de portas
- Gerenciamento
- Facilidade de operação

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Switches Cisco



O preço dos switches vem caindo diariamente. Há 4 anos atrás, um switch Cisco 10/100 de 12 portas chegava a custar US$15.000. Hoje, um switch com características semelhantes pode ser encontrado por US$7.000. Com a queda dos preços dos switches, começa a fazer mais sentido considerar seu emprego em substituição aos hubs.

A Cisco possui uma linha completa de Switches, que satisfazem absolutamente qualquer necessidade corporativa.

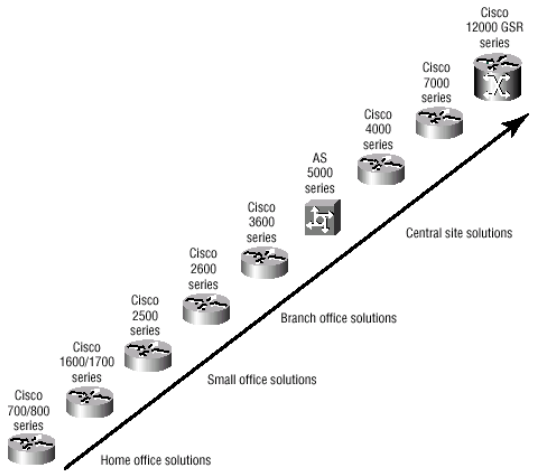
Itens à serem considerados na escolha de um switch:

- Requerimentos de rede para 10, 100 ou 1000Mbps
- Necessidade de interconexão de switches (trunking)
- Segmentação de grupos de trabalho (VLANs)
- Densidade de portas
- Diferentes tipos de interfaces com o usuário

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Routers Cisco



Quando se pensa em Cisco, se pensa em routers. A Cisco é líder na produção de routers, oferecendo produtos com características únicas, altíssima performance e uma série de recursos exclusivos.

A Cisco está sempre atualizando sua linha de routers, estando sempre em dia com a demanda do mercado por novas tecnologias. Por exemplo, você precisa de suporte à IP, Frame Relay e VPN? Cisco tem o produto que você procura.

Outras características à serem consideradas a compra de um router são densidade de portas e velocidade das interfaces. Quanto mais se sobe na escala dos routers, mais se encontra uma densidade maior de portas e uma maior velocidade das interfaces. Por exemplo, a linha 12000 é o primeiro gigabit switch da Cisco, e possui uma enorme capacidade e funcionalidade. Você também deve considerar suporte à WAN, ao comprar um router. A linha 800 praticamente substituiu a linha 700, uma vez que essa não suportava o sistema Cisco IOS.

Eis os itens principais à serem considerados ao se comprar um router:

- Escala dos serviços de roteamento requeridos
- Densidade de portas
- Capacidade e performance
- Interface com o usuário
- Escalabilidade - capacidade de expansão e atualização (sistemas modulares)

netceptions
cisco ccna preparation
www.certifique-se.com

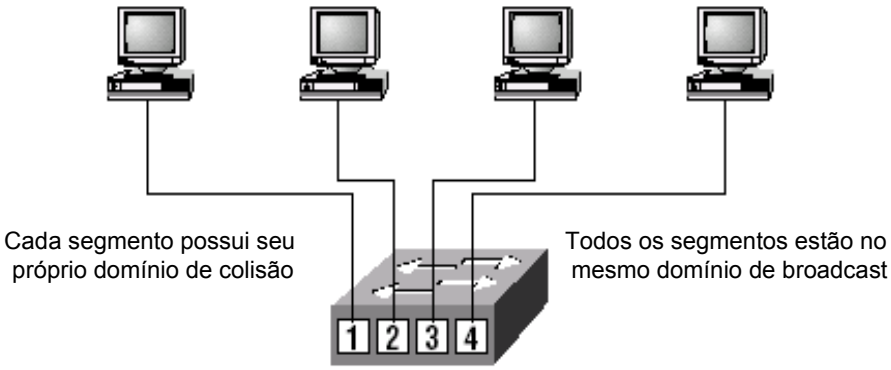
Curso Preparatório CCNA

Módulo 3: Virtual LANs (VLANs)

Vantagens da criação de VLANs:

- Criação de domínios de broadcast menores
- Agrupamento lógico de usuários e recursos conectados em portas administrativamente definidas no switch
- VLANs podem ser organizadas por localidade, função, departamento, etc., independentemente de onde os recursos estejam localizados
- Melhor gerenciabilidade e aumento de segurança da rede local (LAN)

Em uma rede comutada na camada 2 (layer-2 switching), a rede é plana (flat), conforme ilustração abaixo. Todos os pacotes broadcast transmitidos são “enxergados” por todos os dispositivos conectados à rede, mesmo que o dispositivo não precise receber tais dados.



Uma vez que comutação na camada 2 cria segmentos de domínio de colisão individuais para cada dispositivo conectado ao switch, as restrições de distância Ethernet são reduzidas, o que significa que redes geograficamente maiores podem ser construídas. Quanto maior o número de usuários e dispositivos, maior o volume de broadcasts e pacotes que cada dispositivo tem de dar conta. Outro problema de redes comutadas na camada 2 é a segurança, uma vez que todos os usuários “enxergam” todos os dispositivos.

Com a criação de VLANs, você pode resolver uma gama de problemas associados com comutação na camada 2.

Controle de Broadcast

Routers, por default, mantém mensagens de broadcasts dentro da rede que os originou. Switches, por outro lado, propagam broadcasts para todos os seus segmentos. Por esse motivo chamamos uma rede comutada de plana. Porque trata-se de um grande domínio de broadcast.

Como administrador de redes, você deve se certificar que a rede esteja devidamente segmentada para evitar que problemas em um determinado segmento se propaguem para a rede como um todo. A maneira mais eficaz de se fazer isso é através da comutação e do roteamento (switching e routing). Uma vez que o custo dos switches vem caindo, empresas vêm substituindo redes baseadas em hubs por redes baseadas em switches e VLANs. Todos os dispositivos em uma VLAN são membros do mesmo domínio de broadcast. Os broadcasts, por default, são barrados de todas as portas em um switch que não sejam membras da mesma VLAN.

Routers ou módulos de switch para routers (RSMs) devem ser usados em conjunto com os switches para estabelecimento de conexão entre VLANs, o que pode impedir que broadcasts sejam propagados através da rede como um todo.

Segurança

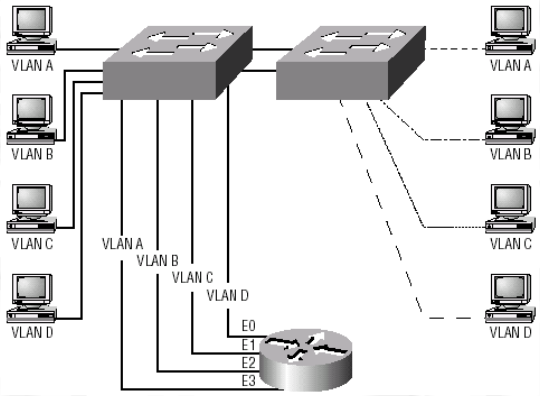
Um dos problemas com redes planas é que segurança é implementada através da conexão de hubs e switches com routers. A segurança é mantida pelo router, porém, qualquer um que se conecte à rede local tem acesso aos recursos de rede disponíveis naquela VLAN específica. Outro problema é que qualquer um pode plugar um analisador de rede em um hub e ter acesso à todo o tráfego da rede. Ainda um outro problema é que usuários podem se unir à um determinado workgroup simplesmente conectando suas workstations no hub existente.

Através da criação de VLANs, os administradores adquirem o controle sobre cada porta e cada usuário. O administrador controla cada porta e quais recursos a mesma poderá estar utilizando. Switches podem ser configurados para informar uma estação de gerenciamento de rede sobre qualquer tentativa de acesso à recursos não autorizados. Se comunicação inter-VLAN precisa acontecer, restrições em um router podem ser implementadas. Restrições também podem ser impostas à endereços de hardware (MAC), protocolos, e aplicações.

netceptions
cisco ccna preparation
www.certifique-se.com

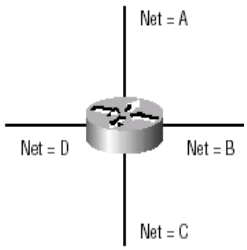
Curso Preparatório CCNA

Virtual LANs (VLANs)
Switches removem a barreira física



Switches apenas analisam frames para filtragem, eles não chegam à analisar os protocolos de camada de rede. Isso pode ocasionar que o switch propague broadcasts. Entretanto, ao se criar VLANs, você está, essencialmente, criando domínios de broadcast, ou seja, está segmentando sua rede local. Uma mensagem de broadcast enviada por um dispositivo em uma VLAN não será propagada para portas do switch onde outra VLAN esteja configurada. Ao se alocar portas em um switch ou grupo de switches conectados entre si (switch fabric) para determinadas VLANs, você tem a flexibilidade de adicionar apenas os usuários desejados ao domínio de broadcast, independentemente de sua localização física. Isso pode evitar fenômenos como "broadcast storms", causados por uma placa de rede defeituosa, ou uma aplicação de ser propagada por toda a rede.

Quando uma VLAN torna-se muito volumosa, você pode criar mais VLANs para evitar que mensagens de broadcast consumam excessiva largura-de-banda. Quanto menor o número de usuários em um grupo VLAN, menor o domínio de broadcast criado. A figura abaixo ilustra um "backbone colapsado", criado pela conexão de diversas LANs físicas à um router. Esta ilustração nos ajudará a compreender como uma VLAN é vista por um switch.



Cada rede é conectada ao router, possuindo sua própria identificação lógica de rede. Um dispositivo conectado à uma dessas LANs deve possuir o mesmo endereço de rede da rede em que se encontra para que seja possível a comunicação do mesmo com a rede como um todo. Vamos ver o que um switch consegue: A ilustração principal desta página demonstra como os switches removem a barreira física.

Switches criam uma flexibilidade e escalabilidade maior do que routers. Através da utilização de switches você pode agrupar usuários por grupos de interesse, que são conhecidos como organizações VLAN. Mesmo com todos esses recursos, switches não podem substituir routers. Na ilustração principal, repare que temos 4 VLANs. Os dispositivos em uma VLAN podem se comunicar entre eles sem problemas, porém, para se comunicarem com dispositivos de outra VLAN, um router deve ser utilizado. Quando configurados em uma VLAN, os dispositivos entendem que, de fato, fazem parte de um "backbone colapsado", como o apresentado anteriormente. Resumindo, comunicação entre VLANs, assim como uma comunicação entre diferentes LANs físicas, deve ser feita pelo intermédio de um router, ou outro dispositivo de camada 3.

VLANs são, tipicamente, criadas por um administrador de redes, que designa portas de um switch para uma determinada VLAN. Essas são chamadas VLAN estáticas. Caso o administrador se adiante e inclua todos os endereços de hardware dos dispositivos em um banco de dados específico, os switches podem, então, serem configurados para designar VLANs dinamicamente.

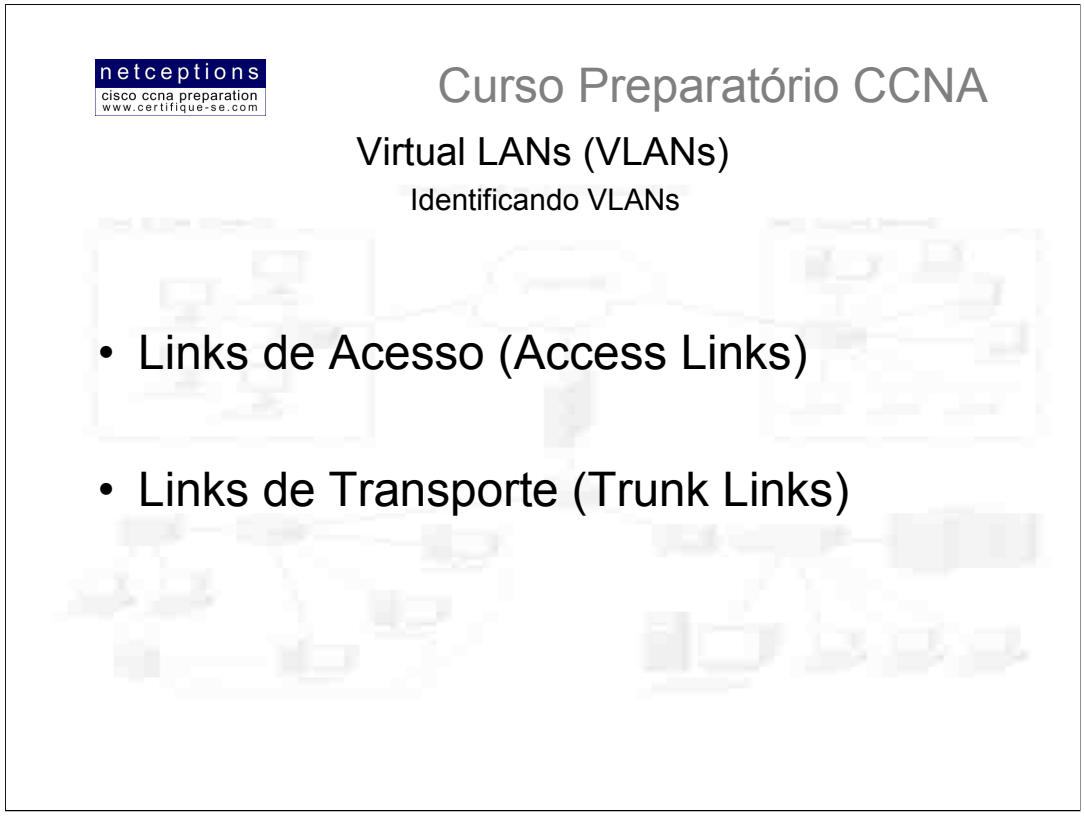
VLANs estáticas

O modo mais comum de se criar uma VLAN é estaticamente, sendo esse método o mais seguro. A porta do switch designada para manter a associação com uma determinada VLAN manterá essa associação até que um administrador mude a designação da porta. Esse método de criação de VLANs é fácil de se implementar e monitorar, funcionando muito bem em ambientes onde o movimento de usuários dentro de uma determinada rede é controlado. Softwares de gerenciamento de rede podem ser usados na configuração das portas de switches, facilitando a vida do administrador de redes.

VLANs dinâmicas

VLANs dinâmicas determinam a designação de uma VLAN para um dispositivo automaticamente. Através do uso de softwares de gerenciamento inteligentes, você pode habilitar endereços de hardware (MAC), protocolos, e até mesmo aplicações para criação de LANs dinâmicas. Por exemplo, suponha que os endereços de hardware tenham sido incluídos em uma aplicação que centraliza o gerenciamento de VLANs. Se um host é, então, conectado à uma porta não designada de um switch, o software gerenciador procurará pelos endereços de hardware armazenados e, então, designará e configurará a porta do switch para a VLAN correta. Se um usuário se move, o switch automaticamente designará a VLAN correta para o mesmo. Apesar de simplificar a vida do administrador uma vez que os dados estejam no banco, mais administração é necessária, inicialmente, para configuração do banco de dados.

Administradores de switches Cisco podem utilizar o serviço chamado VLAN Management Policy Server (**VMPS**) para estruturar o banco de dados com endereços MAC, que pode ser utilizado no endereçamento dinâmico de VLANs. Para simplificar, **VMPS** é um banco de dados que mapea endereços MAC para VLANs específicas.

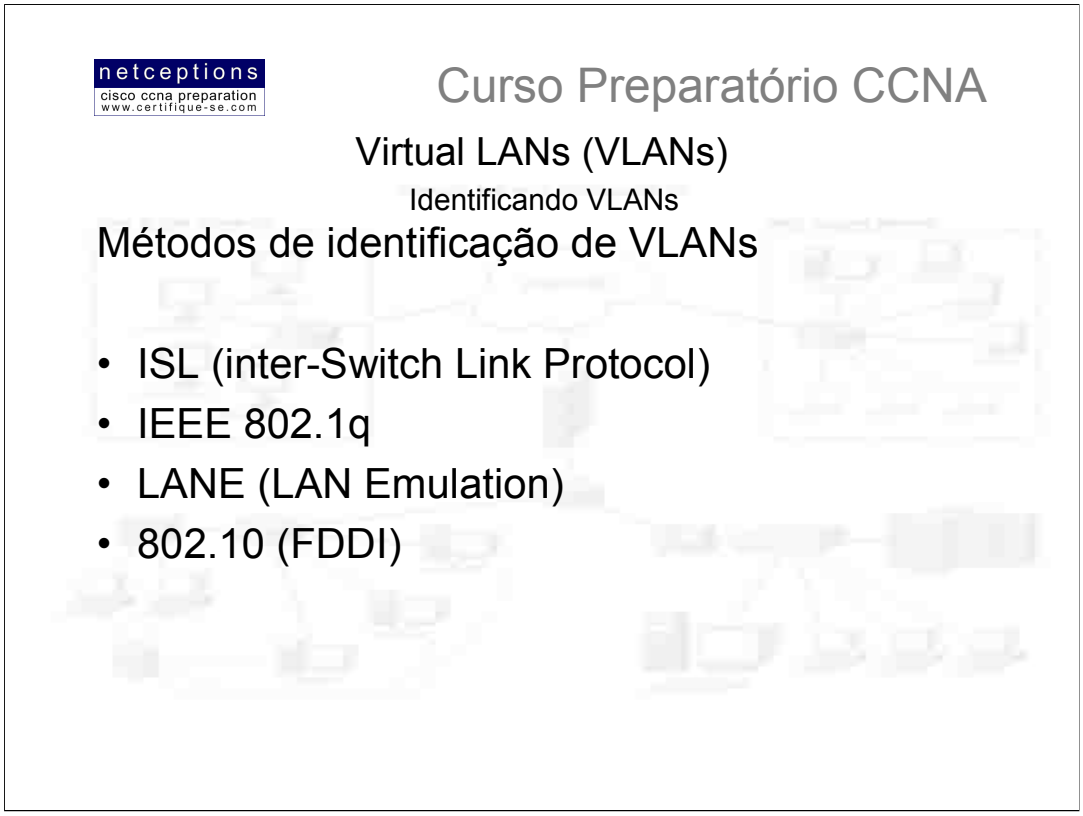


VLANs podem se espalhar por múltiplo switches conectados. Os switches desse aglomerado devem acompanhar os frames e as VLANs aos quais estes pertencem. Essa é a função do frame tagging (etiquetamento/identificação de frames). Switches podem, então, direcionar os frames para as portas apropriadas.

Existem 2 tipos diferentes de links em um ambiente comutado:

Links de acesso (access links) - Links que são apenas parte de uma VLAN e são tidos como a VLAN nativa da porta. Qualquer dispositivo conectado à uma porta de acesso não tem conhecimento sobre a qual VLAN pertence. Este dispositivo apenas assumirá que é parte de um domínio de broadcast, sem entender a real situação da rede física. Os switches removem qualquer informação referente à VLAN antes de enviá-lo à um link de acesso. Dispositivos conectados à links de acesso não podem se comunicar com dispositivos fora de sua VLAN, à não ser que o pacote seja roteado por um router.

Links de Transporte (trunk links) - Links de Transporte podem carregar múltiplas VLANs. Originalmente nomeados por causa dos trunks do sistema telefônico, que carregavam múltiplas conversas telefônicas, Links de Transporte são usados para conectar switches à outros switches, à routers, ou mesmo à servidores. Links de Transporte são suportados em Fast ou Gigabit Ethernet, somente. Para identificar a VLAN a qual um frame pertence com tecnologia Ethernet, os switches Cisco suportam 2 técnicas diferentes para identificação de frames: ISL (Inter-Switch Link Protocol) e 802.1q. Links de Transporte são utilizados para transportar VLANs entre dispositivos, e podem ser configurados para transportar todas as VLANs, ou somente algumas. Links de Transporte ainda possuem uma VLAN nativa (default) que é utilizada caso o trunk link venha a falhar.



Frame Tagging

Um switch em uma internetwork necessita fazer um acompanhamento dos usuários e frames que atravessam o aglomerado de switches e VLANs. Um aglomerado de switches (switch fabric) é um grupo de switches que compartilham as mesmas informações de VLAN. O processo de identificação de frames (frame tagging) designa, de forma única, uma identificação à cada frame. Isso também é conhecido como VLAN ID ou VLAN color.

Frame tagging foi criado pela Cisco para ser utilizado quando um frame Ethernet atravessasse um link truncado (trunked link). A identificação (tag) da VLAN é removida do frame antes que o mesmo deixe o link truncado. Cada switch alcançado pelo frame deve identificar o ID (tag) da VLAN, e então, determinar o que fazer com o frame baseado na tabela de filtragem (filter table). Caso o frame alcance um switch que possua outro link truncado, o frame será encaminhado através da porta onde este link se encontra. Uma vez que o frame alcance uma porta para um link de acesso, o switch remove a identificação da VLAN. O dispositivo final receberá os frames sem ter de entender à qual VLAN os mesmos pertencem.

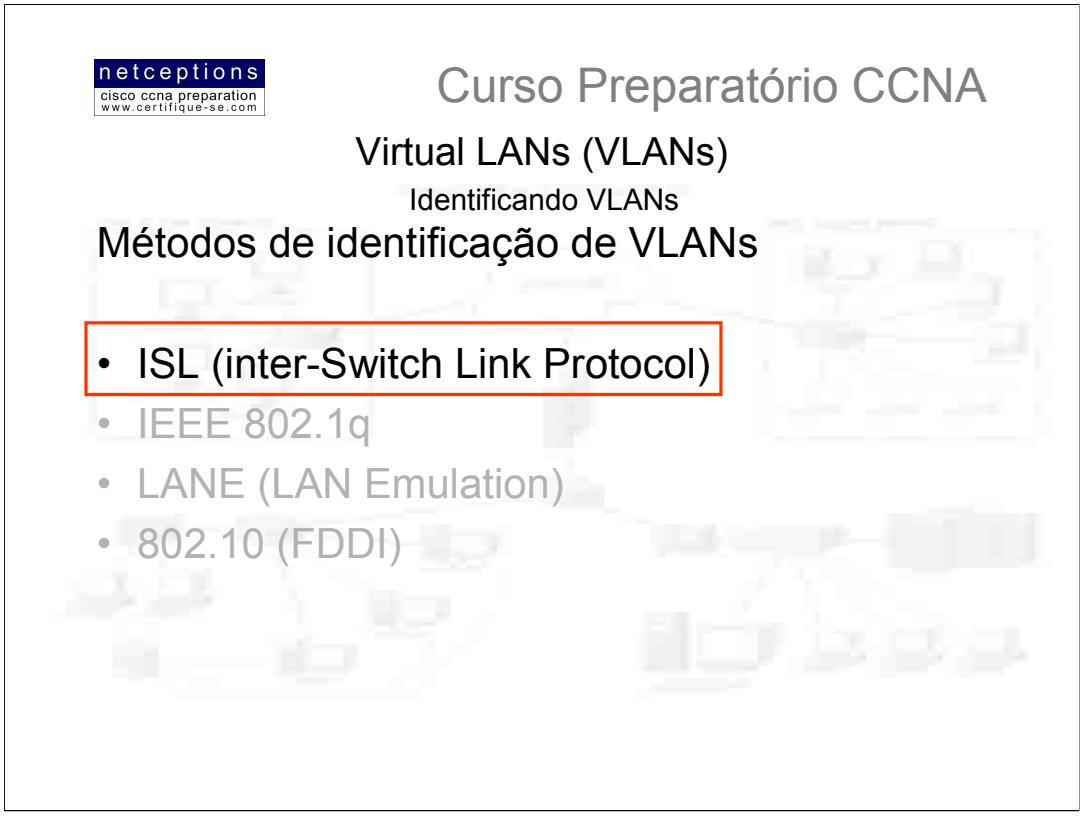
Métodos de identificação de VLANs:

ISL (Inter-Switch Link) - Exclusivo à switches Cisco, é utilizado em links Fast e Gigabit Ethernet, somente. Pode ser utilizado em um porta de switch, interfaces de routers, e interfaces em servidores para truncamento de servidores. O truncamento de servidores é muito útil se você estiver criando VLANs funcionais e não quiser quebrar a regra 80/20 (80% do tráfego deve ser mantido localmente). O servidor que é truncado é parte de todas as VLANs (domínios de broadcast), simultaneamente, o que significa que os usuários não precisam atravessar um dispositivo de camada 3 (router) para ter acesso à um servidor compartilhado na empresa, por exemplo.

IEEE 802.1q - Criado pelo IEEE (Instituto de Engenheiros Elétricos e Eletrônicos) como um método padrão para etiquetamento de frames. Esse método insere um campo dentro do frame que identifica a VLAN. Se você deseja estabelecer Links de Transporte entre switches Cisco e switches de outra marca, esse é o método que deve ser utilizado.

LANE (LAN Emulation) - Utilizado para comunicação entre múltiplas VLANs sobre ATM

802.10 (FDDI) - Utilizado para envio de informações de VLANs sobre FDDI. Insere um campo SAID no cabeçalho do frame para identificação de VLANs. É exclusivo à dispositivos Cisco.



ISL (Inter-Switch Link)

ISL é um modo de, explicitamente, adicionar informações sobre VLANs em um frame Ethernet. Essa informação adicionada permite que VLANs sejam multiplexadas através de um trunk link utilizando um método externo de encapsulamento. Através do uso do ISL, você pode interconectar múltiplos switches e ainda manter informações sobre VLANs conforme dados trafegam entre switches em Links de Transporte.

ISL provê baixa latência, velocidade limitada à mídia (wire speed) sobre FastEthernet, utilizando modos full ou half-duplex. ISL é um método de identificação externo, ou seja, o frame original não é alterado, sendo apenas encapsulado por um cabeçalho ISL de 26-bytes. Uma vez que o frame é encapsulado, apenas dispositivos que entendem frames ISL podem ler este frame. Outro detalhe é que o frame encapsulado pode ter um comprimento de até 1522 bytes. Dispositivos não-ISL que recebam um frame ISL podem entender este como um frame anormal, uma vez que ele ultrapassa o tamanho máximo de frame definido para Ethernet (1518 bytes).

Em portas truncadas (também chamadas de portas multi-VLAN), cada frame é etiquetado assim que entra no switch. Interfaces de rede que suportam ISL permitem que servidores enviem e recebam frames com identificação de múltiplas VLANs, assim, os frames podem atravessar múltiplas VLANs sem ter que atravessar um dispositivo de camada 3, como um router. Isso reduz a latência enormemente.

É importante o entendimento de que a informação ISL é adicionada ao frame apenas se o mesmo for encaminhado à uma porta truncada (trunk link). O encapsulamento ISL é removido do frame assim que esse é encaminhado à uma porta de acesso.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Virtual LANs (VLANs)

Trunking

Links de transporte

- Links de transporte são sempre links ponto-a-ponto de 100 ou 1000Mbps entre 2 switches, 1 switch e 1 router ou 1 switch e 1 servidor
- Links de transporte podem carregar informações de múltiplas VLANs (1 à 1005) simultaneamente

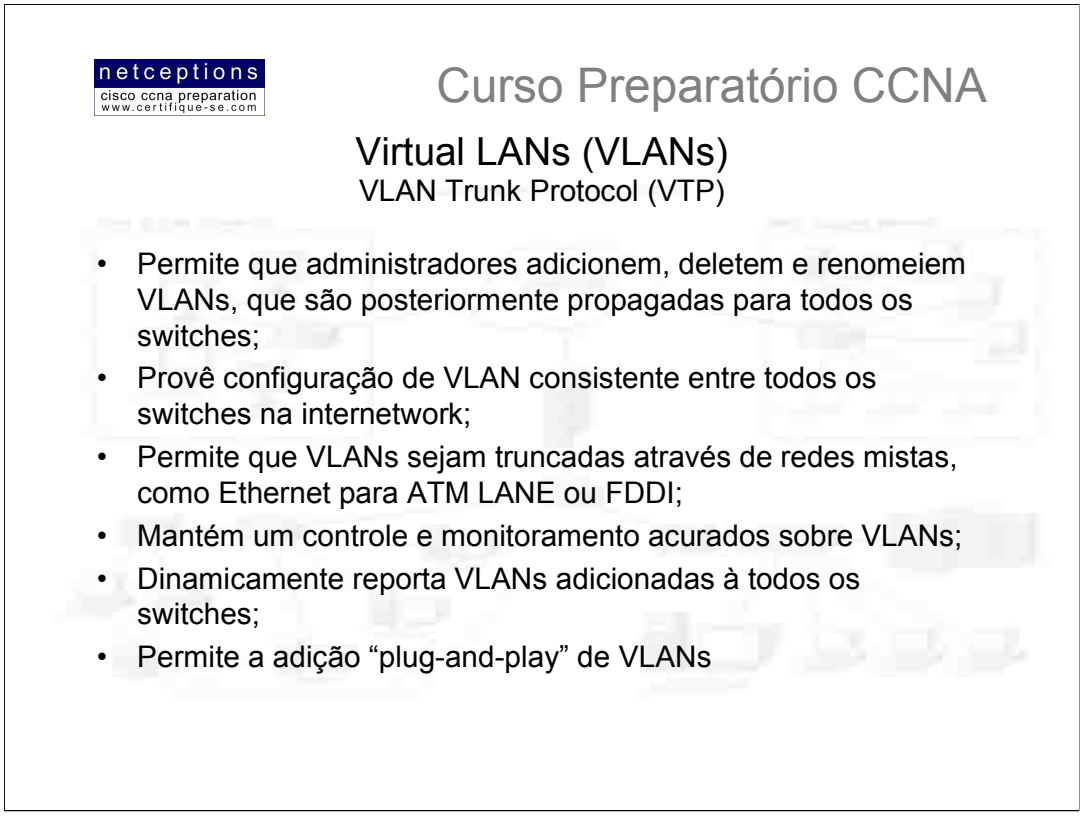
O processo de “truncagem” de links permite que você torne uma única porta em um switch parte de múltiplas VLANs simultaneamente. O benefício disso é que um servidor, por exemplo, pode se encontrar em 2 domínios de broadcast simultaneamente. Isso evitará que usuários tenham de atravessar um router para se conectar e ter acesso aos recursos do servidor. Também, ao se conectar switches uns nos outros, links de transporte podem carregar informações sobre algumas ou sobre todas as VLANs sobre o mesmo link. Caso links entre switches não sejam truncados, os switches apenas enviarão informações sobre a VLAN 1 (default) através do link. Todas as VLANs são configuradas em um link de transporte (default), a não ser que um administrador, manualmente, faça a deleção.

Switches Cisco utilizam o protocolo DTP (Dynamic Trunking Protocol) para gerenciamento de links de transporte na linha Catalyst de switches. DTP é um protocolo ponto-a-ponto que foi criado para enviar informação de transporte sobre trunks 802.1q.

Roteamento entre VLANs

Dispositivos dentro de uma VLAN encontram-se dentro do mesmo domínio de broadcast e podem se comunicar sem problemas. VLANs criam segmentação de rede e segregação de tráfego na camada 2 do modelo OSI. Para que dispositivos em diferentes VLANs comuniquem-se entre si, é necessário o uso de um router.

Um router com uma interface para cada VLAN pode ser usado, ou, simplesmente, um router que suporte roteamento ISL. O router mais barato que suporta roteamento ISL são os da série 2600. Se você tem apenas algumas VLANs (2 ou 3), um router com 2 ou 3 interfaces 10BaseT já é o suficiente. Entretanto, se você tem mais VLANs do que interfaces disponíveis no router, você pode utilizar roteamento ISL em uma interface FastEthernet, ou adquirir um módulo chamado Route Switch Module (RSM) para um switch da série 5000. O módulo RSM pode suportar até 1005 VLANs. Se você utiliza uma interface FastEthernet e utiliza roteamento ISL na mesma, chamamos isso de “router-on-a-stick”.



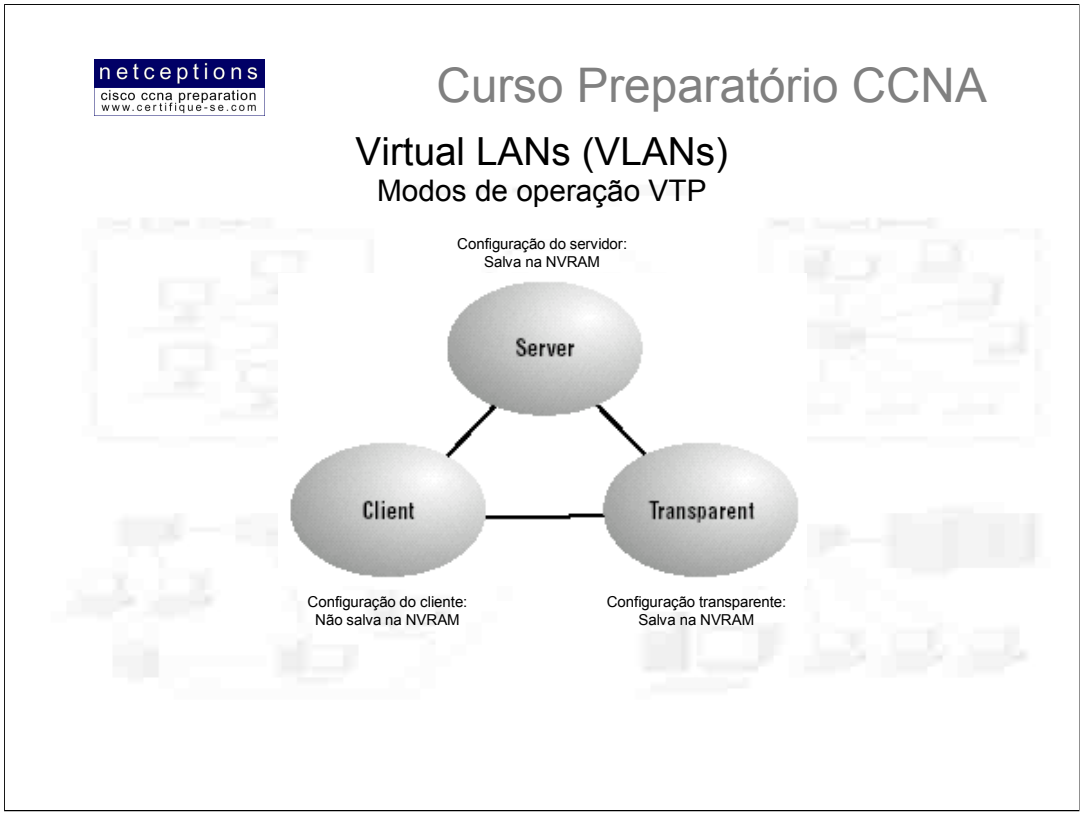
A Cisco criou o VLAN Trunk Protocol para gerenciar todas as VLANs configuradas em uma rede comutada, e para manter a consistência através da rede como um todo.

Para permitir que o protocolo VTP gerencie suas VLANs através da rede, é necessário que se crie, antes, um servidor VTP. Todos os servidores que necessitem compartilhar informações sobre VLANs devem utilizar a mesma identificação de domínio, e um switch pode se encontrar em apenas 1 domínio a cada vez. Isso significa que um switch pode compartilhar informações do domínio VTP apenas com switches configurados dentro do mesmo domínio VTP. Informações VTP são enviadas entre switches através de portas de transporte (trunk ports).

Switches propagam informações gerenciais do domínio VTP a qual pertencem, assim como o número de revisão da configuração (configuration revision number) e todas as VLANs conhecidas com parâmetros específicos. Switches podem ser configurados para encaminharem informações VTP, mas para não receberem informações sobre atualizações, assim como não permitir atualizações em seus banco-de-dados VTP. Isso é chamado de Modo VTP Transparente (VTP Transparent Mode).

Caso você venha a ter problemas com usuários adicionando switches ao seu domínio VTP, senhas podem ser criadas objetivando um maior controle. Lembre-se, no entanto, que todos os switches devem ser configurados com a mesma senha, o que pode vir a ser difícil.

Switches detectam VLANs adicionais dentro de uma atualização VTP e se preparam para receber em suas portas de transporte informações sobre as novas VLANs adicionadas. Atualizações são enviadas como números de revisão (revision numbers), a qualquer hora que um switch identifique um número de revisão mais alto ele sabe que a informação à ser recebida é mais atual e irá sobrescrever o banco de dados corrente.

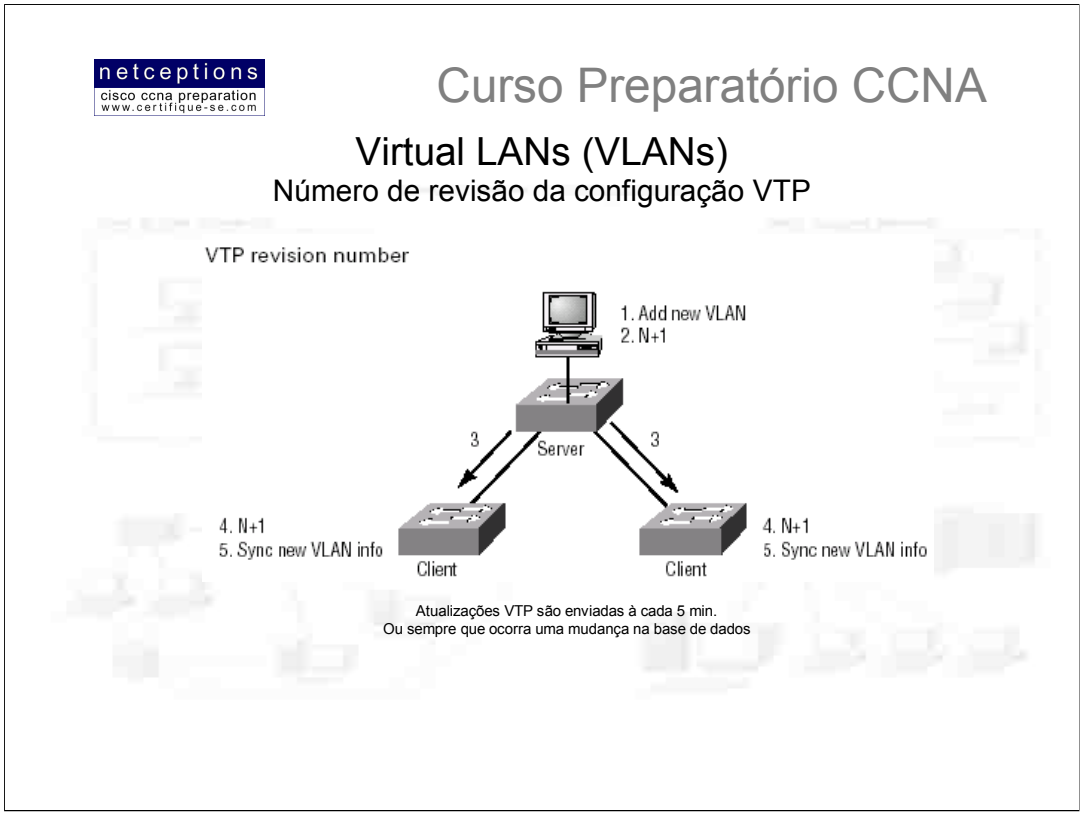


Modos de operação VTP:

Server (servidor): Default para todos os switches da linha Catalyst. Você necessita de pelo menos um servidor VTP em seu domínio VTP para propagação de informação sobre VLANs através do domínio. O switch deve se encontrar em modo servidor (server mode) para ser capaz de criar, adicionar ou deletar VLANs em um domínio VTP. A mudança de informações VTP também deve ser efetuada em modo servidor. Qualquer alteração sofrida por um switch em modo servidor é propagada para todo o domínio VTP.

Client (cliente): Recebe informação de servidores VTP e envia e recebe atualizações, mas não pode efetuar mudanças. Nenhuma porta em um switch cliente pode ser adicionada à uma nova VLAN antes do servidor VTP notificar o switch cliente dessa nova VLAN. Se você desejar que um switch seja ativado como servidor, antes de mais nada, configure-o como cliente. Dessa forma, ele receberá todas as informações corretas sobre VLANs. Uma vez atualizado, torne-o servidor.

Transparent (transparente): Não participa do domínio VTP, mas ainda assim encaminhará atualizações VTP através dos links configurados. Switches VTP transparentes podem adicionar ou deletar VLANs, uma vez que o switch mantém sua própria base de dados e não a compartilha com outros switches. Esse modo é considerado significante apenas localmente.



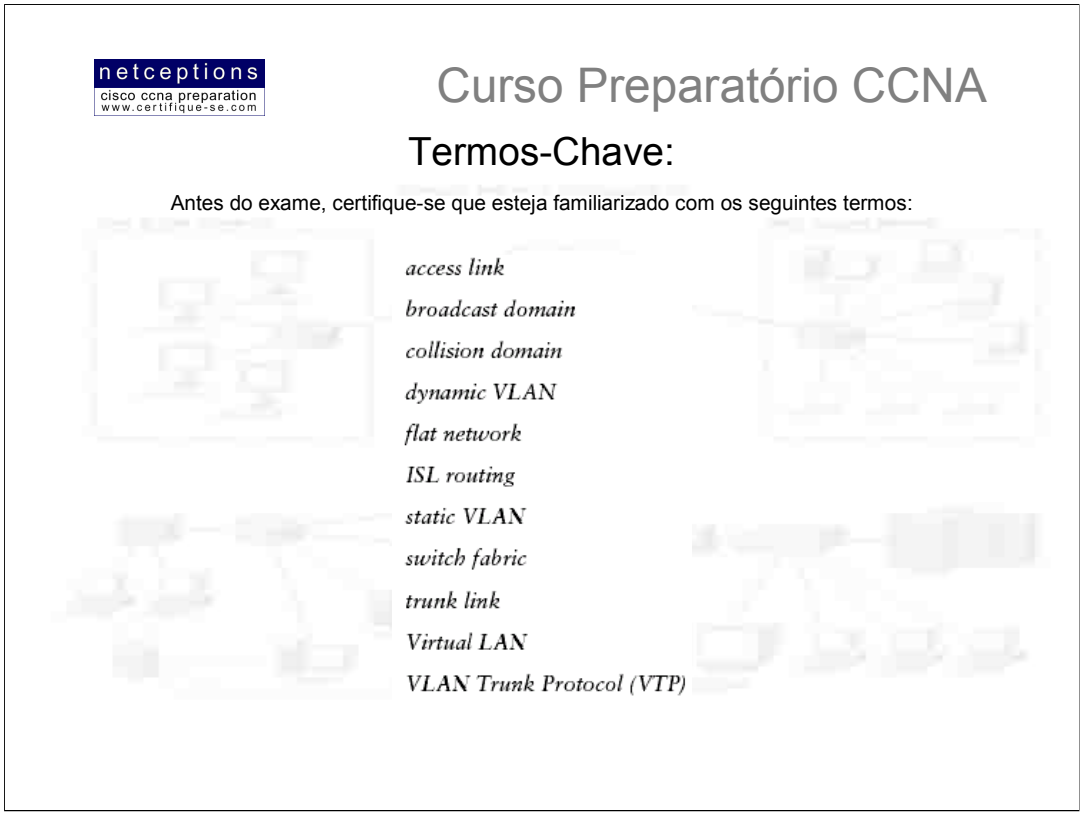
O número de revisão é o mais importante dado de um anúncio VTP. A figura acima ilustra um exemplo de como o número de revisão é usado em um anúncio (atualização):

A figura mostra o número de revisão da configuração como sendo “N”. Ao passo que o banco de dados sofre modificações, o servidor VTP incrementa esse número de revisão em 1. O servidor VTP, então, envia a atualização do banco de dados com o novo número de revisão. Quando um switch recebe a atualização com um número de revisão mais alto do que o atual, ele sobrescreve o banco de dados armazenado na NVRAM com o novo banco de dados sendo anunciado na atualização.

VTP Pruning

Você pode conservar largura-de-banda configurando VTP para reduzir o volume de broadcasts (anúncios de atualizações), o que ajuda na preservação de banda. Isso é chamado de pruning. VTP pruning apenas envia broadcasts para links de transporte que, de fato, necessitem tal informação. Qualquer link de transporte que não necessite da informação não a receberá. Por exemplo, se um switch não tiver nenhuma porta configurada para a VLAN 5, e uma mensagem de broadcast é enviada através da VLAN 5, a mensagem de broadcast não atravessará o link de transporte até esse switch. VTP pruning encontra-se desabilitado por default em todos os switches.

Quando você habilita VTP pruning em um servidor VTP, você o habilita para todo o domínio. Por default, VLANs 2 à 1005 são consideráveis para implementação de pruning. Pruning nunca pode ser implementado na VLAN 1 por esta ser considerada a VLAN administrativa.



Resumo do módulo 3 - aula 2:

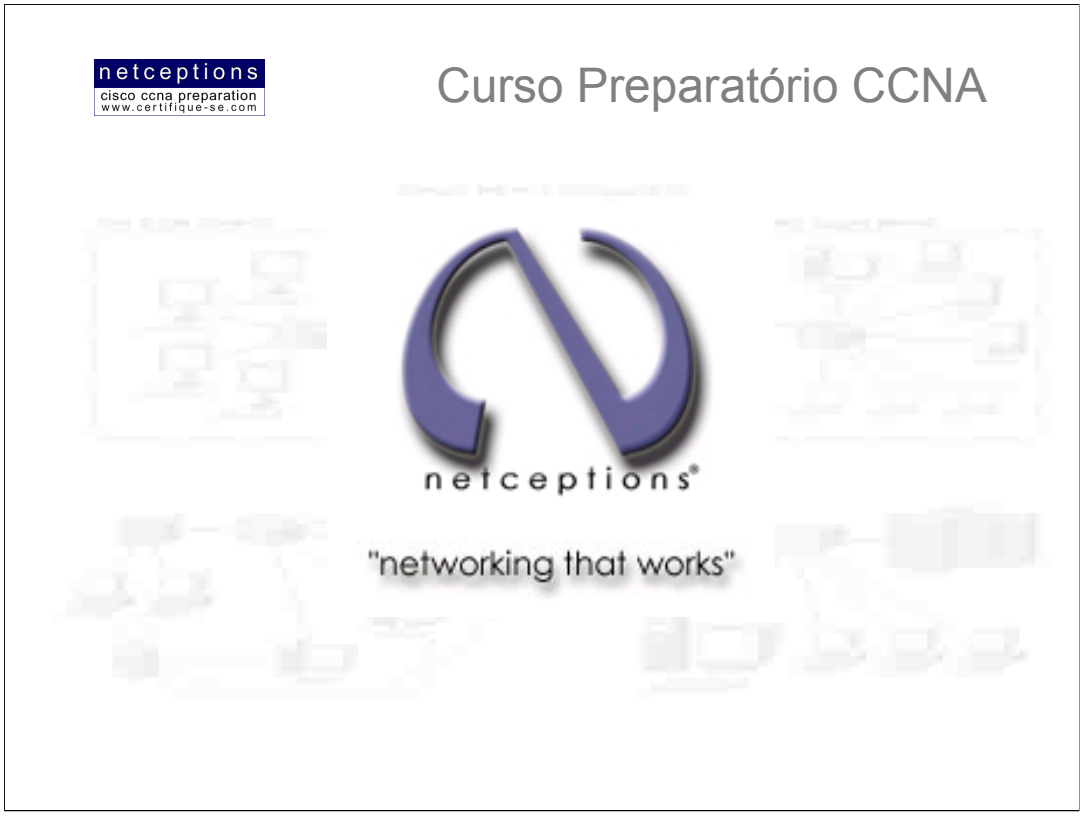
Nesta aula falamos de Virtual LANs e descrevemos como switches Cisco podem utiliza-las. VLANs segmentam domínios de broadcast em uma rede comutada. Isso é importante, pois switches segmentam apenas domínios de colisão e, por default, todos os switches formam um grande domínio de broadcast.

Falamos também de VLANs truncadas através de um link FastEthernet. Trunking é importante em uma rede com múltiplos switches operando múltiplas VLANs. Também vimos o protocolo VTP (VLAN Trunking Protocol), que **na verdade, nada tem a ver com trunking**. O que ele faz é enviar informações sobre VLANs através de links de transporte (trunk links), porém, a configuração destes links não é parte das operações do VTP.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

FIM AULA 02



Apostila Aula 3

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Aula 3: O Protocolo IP

- O modelo DoD (Department of Defense Model)
- Definição de portas lógicas
- Classes de endereços IP
- Técnicas de subnetting (máscaras de rede)
- Configuração de endereços IP em routers
- Verificação da configuração via IOS

O padrão TCP/IP foi criado pelo departamento de defesa americano (DoD) para garantir a preservação da integridade dos dados, assim como manter a comunicação entre dispositivos no advento de uma guerra catastrófica.

Se bem planejada e corretamente implementada, uma rede baseada na combinação de protocolos (suite) TCP/IP pode ser independente, confiável e muito eficiente.

O processo de endereçamento IP não é uma tarefa complexa, mas trabalhosa - para mentes destreinadas. Existe uma série de fatores que devem ser entendidos, e estaremos discutindo os mesmos nas páginas à seguir. O entendimento e domínio das técnicas para criação e identificação de máscaras de rede (subnetting masks) só é atingido com muita prática.

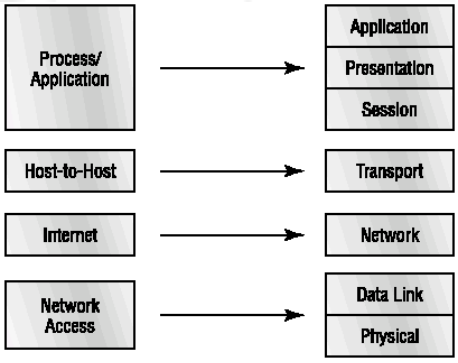
O domínio deste capítulo é vital para um bom resultado na prova CCNA. Caso um entendimento profundo do que for apresentado não seja atingido, recomenda-se extender os estudos com relação à esse capítulo em suas horas vagas. Pratique até que as tarefas de se designar e se determinar endereços IP seja completamente dominada.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

O Modelo TCP/IP (DoD)

- O modelo TCP/IP (também conhecido como DoD - Department of Defense - model) é composto de 4 - ao invés de 7 - camadas, que podem ser mapeadas ao modelo OSI:



Uma vasta gama de protocolos atuam na camada de Processo/Aplicação do modelo DoD (TCP/IP), com funções espelhando àquelas das 3 camadas OSI equivalentes (Aplicação, Apresentação e Sessão). **A camada de Processo/Aplicação** é responsável pela definição dos protocolos necessários à comunicação ponto-a-ponto pelas aplicações, bem como pelo controle das especificações de interface com o usuário.

A camada host-to-host espelha as funções da camada de transporte no modelo OSI, definindo protocolos que estabelecem o nível do serviço de transmissão para as aplicações. Esta camada se encarrega de tarefas como a criação de uma conexão ponto-a-ponto confiável e a entrega de dados, zelando pela integridade dos mesmos. Essa camada é também responsável pelo sequenciamento de pacotes de dados.

A camada Internet corresponde à camada de rede no modelo OSI, designando protocolos responsáveis pela transmissão lógica de pacotes através da rede. Essa camada é responsável pelo endereçamento lógico dos dispositivos, designando endereços IP aos mesmos. A camada Internet também é responsável pelo roteamento de pacotes através da rede e pelo controle do fluxo de dados entre 2 dispositivos.

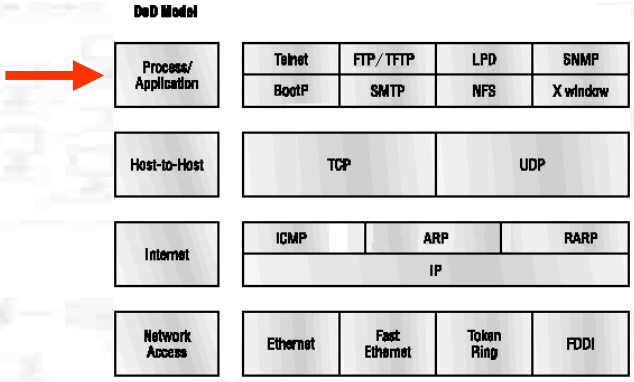
A camada de Acesso à Rede, equivalente às camadas de enlace e física no modelo OSI, é responsável pelo monitoramento do tráfego de dados entre os dispositivos e a rede. Nessa camada também são definidos os protocolos para a transmissão através dos meios físicos, assim como o análise e utilização dos endereços de hardware.

Embora os modelos DoD e OSI possuam semelhanças em desenho e conceito, o modo de operação de cada modelo é diferente.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

O Modelo TCP/IP (DoD)



Camada de aplicação

Descreveremos, à seguir, algumas dos protocolos e aplicações tipicamente utilizados em redes IP.

• **Telnet** - Telnet é conhecido como o "camaleão" dos protocolos. Sua especialidade é a emulação de terminais. Ele permite que um usuário em uma máquina remota - chamado cliente - conecte-se aos recursos de outra máquina - o servidor Telnet. O nome Telnet vem de "Telephone Network".

• **FTP/TFTP (File Transfer Protocol/TrivialFTP)** - Protocolo utilizado para transferência de arquivos entre 2 máquinas. FTP não é apenas um protocolo, mas também um programa, em si. Operando como um protocolo, FTP é utilizado por outras aplicações. Como um programa, é utilizado para executar transferência de arquivos. TFTP (T=Trivial) é uma versão mais simplista do protocolo FTP, usado quando você sabe exatamente o que quer e onde buscar. TFTP não possui as facilidades do FTP como pesquisa entre diretórios. Ele não faz nada além de enviar e receber arquivos. TFTP é o protocolo utilizado para instalar uma atualização do sistema Cisco IOS (ou o sistema em si) em um router Cisco.

• **NFS (Network File System)** - Protocolo especializado em compartilhamento de arquivos, permitindo a inter-operação entre 2 tipos de sistemas de arquivos heterogêneos.

• **SMTP (Simple Mail Transfer Protocol)** - SMTP é utilizado no gerenciamento e distribuição de e-mails.

• **LPD (Line Printer Daemon)** - Protocolo utilizado para compartilhamento de impressoras

• **X Window** - X Window define um padrão para o desenvolvimento de interfaces gráficas em sistemas cliente-servidor.

• **SNMP (Simple Network Management Protocol)** - Coleta e manipula informações de rede. Esse protocolo pode também agir como um "cão-de-guarda" de toda a rede, transmitindo avisos para os administradores sempre que algum evento inesperado ocorrer.

• **DNS (Domain Name Service)** - Responsável pelo mapeamento de nomes na internet (ex. www.netceptions.com.br) para os respectivos endereços IP.

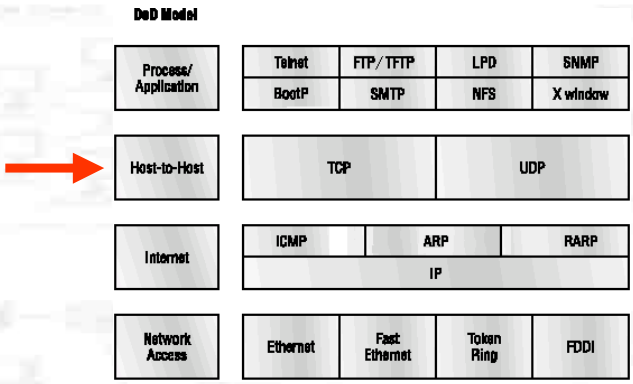
• **BootP (Boot Strap Protocol)** - Quando uma estação sem disco é ligada, ela emite uma requisição de BootP pela rede. Um servidor BootP recebe esta requisição e analisa o endereço de hardware do transmissor no arquivo BootP enviado. Se o servidor encontrar esse endereço, ele envia à máquina o seu endereço IP e a localização do arquivo (normalmente via TFTP) de onde esta deve efetuar o "boot". O protocolo BootP é utilizado por estações sem disco para: receber seu endereço IP, receber o endereço IP do servidor e receber a localização do arquivo a partir do qual ela deve efetuar o boot.

• **DHCP (Dynamic Host Configuration Protocol)** - Uma versão mais moderna do protocolo BootP. Realiza as mesmas tarefas, exceto que não disponibiliza um endereço para o boot da máquina, ou seja, a máquina utilizando o protocolo DHCP deve possuir um disco interno, através do qual deve efetuar o boot. DHCP incorpora algumas outras funções, como: provisão de informações sobre máscaras de rede, DNS, WINS, Default gateways, domain name, entre outras.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

O Modelo TCP/IP (DoD)



Camada host-to-host

A função principal da camada host-to-host é mascarar das aplicações de camada superior as complexidades da rede. 2 protocolos se encontram nessa camada: TCP e UDP.

TCP (Transmission Control Protocol) - TCP recebe um fluxo de dados de uma aplicação e os "quebra" em segmentos. Esses segmentos são numerados e sequenciados, permitindo a remontagem dos blocos assim que os segmentos atinjam seu destino. Após o envio desses segmentos, o protocolo TCP aguarda uma confirmação da máquina receptora, retransmitindo os segmentos que não forem confirmados. Antes que a transmissão se inicie, o protocolo TCP da máquina transmissora contata o protocolo TCP da máquina destinatária para que uma conexão seja estabelecida. Essa conexão é chamada de circuito virtual (virtual circuit). Esse tipo de comunicação é chamada de orientada à conexão (connection-oriented). Durante esse "aperto-de-mão" (hand-shake) inicial, o protocolo TCP das pontas envolvidas também determinam o volume de dados à ser transmitido antes de ocorrer a confirmação por parte do destinatário. Com tudo acertado com antecedência, o caminho para uma comunicação confiável está pavimentado.

TCP é um protocolo full-duplex, orientado à conexão, acurado e confiável. TCP é bastante complexo e, não surpreendentemente, custoso em termos de cabeçalho (overhead). Como as redes de hoje são muito mais confiáveis do que as redes existentes quando o protocolo TCP foi criado, grande parte das características que garantem essa confiabilidade na transmissão se faz desnecessária atualmente.

UDP (User Datagram Protocol) - Desenvolvedores podem se utilizar do protocolo UDP em lugar ao TCP. UDP é considerado um modelo de escala econômico e um protocolo "magro". Por esse fato, o protocolo UDP utiliza muito menos largura-de-banda do que o TCP. O protocolo UDP não oferece todo o requinte do TCP, mas realiza eficientemente o trabalho de transporte de dados que não requeiram confiabilidade na entrega dos mesmos. Existem uma gama de situações onde o protocolo UDP poderia ser sabiamente empregado em lugar ao TCP. Como exemplo, os sinais de rede constantemente transmitidos pelo protocolo SNMP (os "cães-de-guarda") congestionariam a rede caso fossem enviados via TCP. UDP, nesse caso, realiza o transporte desses sinais, uma vez que confiabilidade de entrega não é um fator crítico. Outra utilização para UDP em lugar ao TCP seria quando a confiabilidade de transmissão é plenamente alcançada na camada de processos e aplicações. O protocolo NFS, por exemplo, lida com questões de segurança à sua própria maneira, tornando desnecessário a utilização do TCP para transporte nesse caso.

UDP recebe blocos de dados das camadas superiores, ao invés de fluxos de dados como ocorre com TCP, e os quebra em segmentos. Como ocorre com TCP, cada segmento UDP é numerado para que a reconstrução do bloco ocorra na máquina de destino. UDP, no entanto, não sequencia os segmentos como TCP, e não se importa com a ordem na qual tais segmentos chegam ao seu destino. Após a numeração dos segmentos, UDP efetua o transporte dos mesmos e, simplesmente, os esquece. Não existe a confirmação de recebimento pela máquina destinatária, como ocorre com TCP. O que ocorre, de fato, é o completo abandono do segmento na rede. Por esse motivo, UDP é considerado um protocolo não-confiável. Além disso, UDP não estabelece um circuito virtual antes do início da transmissão, como ocorre com TCP. Por esse motivo, UDP também é considerado um protocolo não-orientado à conexão.

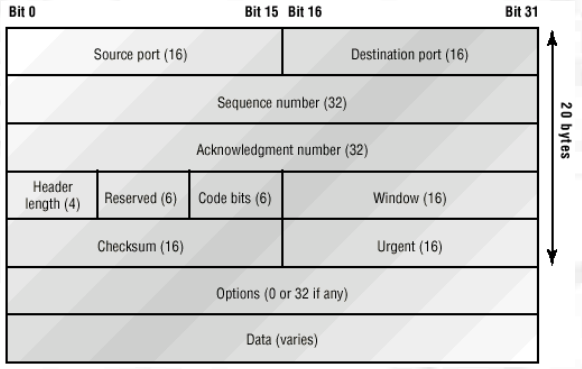
Isso deixa o desenvolvedor com alternativas no uso de protocolos para transporte de dados: TCP para um transporte de dados confiável ou UDP para um transporte rápido.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

O Modelo TCP/IP (DoD)

Formato do segmento TCP



As camadas superiores enviam um fluxo de dados para os protocolos da camada de transporte. A camada de rede encarrega-se de rotear os segmentos como pacotes através da internertwork. Esses pacotes são entregues ao protocolo da camada de transporte do dispositivo destinatário, que se encarrega de reconstruir o fluxo de dados e passa-lo às aplicações ou protocolos das camadas superiores. A figura acima ilustra o formato de um segmento TCP, e os diferentes campos presentes em seu cabeçalho. A partir dessa figura podemos entender como o protocolo TCP segmenta o fluxo de dados recebido e os prepara para a camada de rede (Internet).

O cabeçalho TCP possui o tamanho de 20 bytes, contendo os seguintes campos:

• Source Port (Porta Origem) - Número da porta lógica onde a aplicação transmissora está localizada

• Destination port (Porta Destino) - Número da porta lógica onde a aplicação ou protocolo requisitado esta localizado na máquina destinatária

• Sequence Number (Número Sequencial) - Número utilizado na recolocação dos segmentos na ordem correta

• Acknowledgement Number (Número de Confirmação) - Define qual octeto TCP deve ser aguardado na sequência

• HLEN (Header Lenght - Comprimento do Cabeçalho) - Define o comprimento do cabeçalho TCP

• Reserved - Sempre 0

• Code Bits - Funções de controle utilizadas para iniciar e encerrar uma sessão

• Window - Tamanho da janela dados que o remetente tem capacidade de receber, medida em octetos

• CheckSum - Checagem de redundância (CRC), uma vez que o TCP não confia nas camadas mais baixas e realiza a checagem de tudo

• Urgent Pointer - Indica o fim de dados críticos (urgentes)

• Option - Define o tamanho máximo do segmento TCP

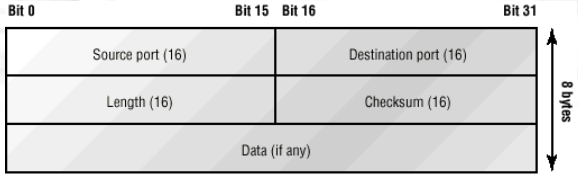
• Data - Dados passados para a camada de transporte, que inclui os cabeçalhos das camadas superiores (encapsulamento)

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

O Modelo TCP/IP (DoD)

Formato do segmento UDP



O segmento UDP contém os seguintes campos:

• Source Port (Porta Origem) - Número da porta lógica onde a aplicação transmissora está localizada

• Destination port (Porta Destino) - Número da porta lógica onde a aplicação ou protocolo requisitado esta localizado na máquina destinatária

• Lenght (Comprimento) - Define o tamanho do segmento UDP, incluindo o cabeçalho e dados

• CheckSum - Checagem de redundância (CRC) de campos do cabeçalho e dados

• Data - Dados passados para a camada de transporte, que inclui os cabeçalhos das camadas superiores (encapsulamento)

* Note a diferença de tamanho do cabeçalho UDP, em relação ao TCP.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

O Modelo TCP/IP (DoD)

Análise comparativa dos segmentos TCP e UDP

```
TCP - Transport Control Protocol
  Source Port:        5973
  Destination Port:   23
  Sequence Number:    1456389907
  Ack Number:         1242056456
  Offset:             5
  Reserved:           %000000
  Code:               %011000
            Ack is valid
            Push Request
  Window:             61320
  Checksum:           0x61a6
  Urgent Pointer:     0
  No TCP Options
  TCP Data Area:
  vL.5.+.5.+.5.+.5   76 4c 19 35 11 2b 19 35 11 2b 19 35
11 2b 19 35 +. 11 2b 19
Frame Check Sequence:  0x0d00000f
```

```
UDP - User Datagram Protocol
  Source Port:        1085
  Destination Port:   5136
  Length:             41
  Checksum:           0x7a3c
  UDP Data Area:
  ..Z.............   00 01 5a 96 00 01 00 00 00 00 00 11
00 00 00
...C..2...._C._C   2e 03 00 43 02 1e 32 0a 00 0a 00 80 43
00 80
Frame Check Sequence:  0x00000000
```

Note que todos os campos mencionados nas páginas anteriores estão presentes nos segmentos capturados. Como pode ser percebido, o protocolo TCP possui muito mais "overhead" do que o protocolo UDP.

Pontos importantes à serem lembrados com relação aos 2 protocolos:

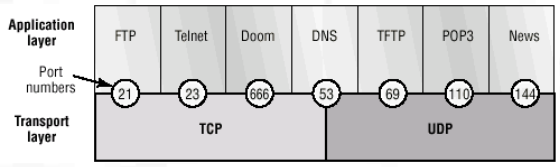
TCP	**UDP**
Sequenced (sequencial)	Unsequenced (não-sequencial)
Reliable (confiável)	Unreliable (não-confiável)
Connection-oriented (orientado à conexão)	Connectionless (não-orientado)
Virtual Circuit (estabelece circuito virtual)	Low overhead (cabeçalho pequeno)

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

O Modelo TCP/IP (DoD)

Portas lógicas de comunicação (TCP e UDP)



Os protocolos TCP e UDP se utilizam de portas lógicas para comunicação com as camadas superiores. Portas lógicas mantém uma trilha das diferentes comunicações que cruzam a rede simultaneamente. Números de portas lógicas de aplicações transmissoras (source) são designadas dinamicamente pela máquina fonte, e deve ser um número iniciando em 1024. Os números 1023 e abaixo são conhecidos como números de portas conhecidas (well-known port numbers). Circuitos virtuais que não utilizem uma aplicação com um número de porta conhecido designado à mesma têm seus números de porta gerados randomicamente, escolhidos dentro de um intervalo específico. Esses números de porta identificam o protocolo ou aplicação transmissor e destinatário em um segmento TCP.

Os diferentes números de porta que podem ser utilizados são:

• Números abaixo de 1024 - Conhecidos como well-known port numbers, definidos pelo RFC 1700 (Request For Comment)

• Números 1024 e acima - Usados pelas camadas superiores para estabelecer sessões com outros dispositivos e pelo protocolo TCP para utilização como endereços de transmissão e destino em um segmento TCP.

```
TCP - Transport Control Protocol
  Source Port:      1144
  Destination Port: 80  World Wide Web HTTP
  Sequence Number:  9356570
  Ack Number:       0
  Offset:           7
  Reserved:         %000000
  Code:             %000010
          Synch Sequence
  Window:           8192
  Checksum:         0x57E7
  Urgent Pointer:   0
  TCP Options:
    Option Type:    2  Maximum Segment Size
        Length:     4
        MSS:        536
    Option Type:    1  No Operation
    Option Type:    1  No Operation
    Option Type:    4
        Length:     2
        Opt Value:
    No More HTTP Data
Frame Check Sequence:  0x43697363
```

```
TCP - Transport Control Protocol
  Source Port:      80  World Wide Web HTTP
  Destination Port: 1144
  Sequence Number:  2873580788
  Ack Number:       9356571
  Offset:           6
  Reserved:         %000000
  Code:             %010010
            Ack is valid
            Synch Sequence
  Window:           8576
  Checksum:         0x5F85
  Urgent Pointer:   0
  TCP Options:
    Option Type:    2  Maximum Segment Size
        Length:     4
        MSS:        1460
    No More HTTP Data
Frame Check Sequence:  0x6E203132
```

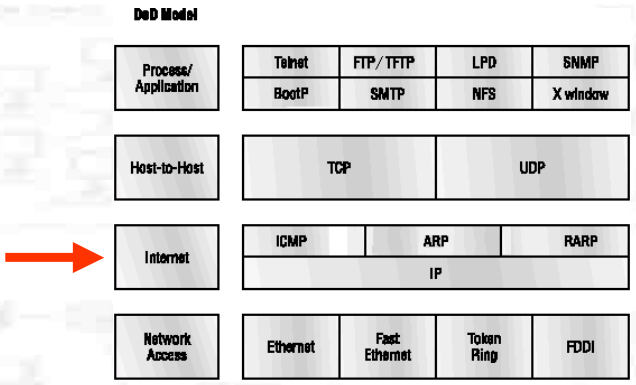
Note no primeiro “trace” TCP acima que a máquina transmissora gera aleatoriamente o número da porta de saída (source port - 1144). Por que esse número é gerado? O motivo é diferenciar entre diferentes sessões, estabelecidas com diferentes destinatários. De que outro modo um servidor saberia de onde estão chegando determinadas informações se não houvesse um número diferente para cada sessão TCP? **TCP e camadas superiores não “entendem” endereços físicos (MAC) ou lógicos (ex. IP) para identificação de dispositivos na rede, como as camadas de enlace e de rede fazem**. Em seu lugar, essa identificação é feita através da associação entre números de porta lógicas. Note, ainda no primeiro “trace” TCP, que o número da porta destino (destination port) é abaixo de 1024, ou seja, é um número de porta conhecido (HTTP, no caso).

Observe agora o segundo “trace”, logo ao lado. Ambos fazem parte de uma mesma sessão TCP. Observe os números das portas. O número da porta de destino em um é o número da porta transmissora no outro, e vice-versa.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

O Modelo TCP/IP (DoD)



Existem 2 razões principais para a existência da camada Internet: roteamento e provisão de uma interface de rede unificada para as camadas superiores. Nenhuma das camadas superiores ou inferiores tem funções relativas ao roteamento de pacotes. Essa complexa e importante tarefa é responsabilidade exclusiva da camada Internet. A segunda tarefa, de prover uma interface de rede unificada às camadas superiores, garante a compatibilidade entre os diferentes tipos de protocolos de acesso à rede. Se essa função não fosse desempenhada pela camada Internet, programadores teriam de desenvolver diferentes versões de aplicações para cada tipo de acesso existente; uma versão para Ethernet, outra para Token-Ring, e assim por diante. Para prevenir isso, o protocolo IP promove uma interface de rede unificada para os protocolos das camadas superiores. Todos os caminhos não levam à Roma. Levam ao IP! E todos os outros protocolos presentes nesta camada o utilizam. Não se esqueça disso. Todos os caminhos através do modelo DoD passam pelo protocolo IP.

Existem 4 protocolos que coexistem na camada Internet:

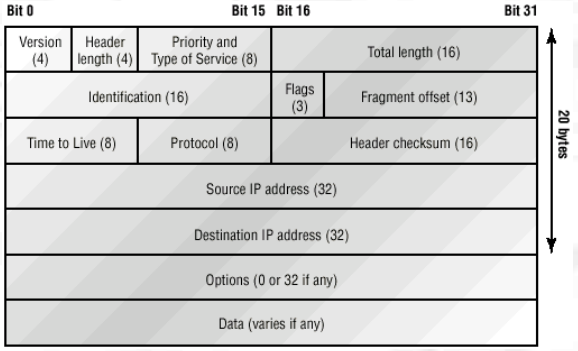
- Protocolo Internet (IP)
- Internet Control Message Protocol (ICMP)
- Address Resolution Protocol (ARP)
- Reverse Address Resolution Protocol (RARP)

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

O Modelo TCP/IP (DoD)

Formato do cabeçalho IP



O protocolo IP **é** essencialmente a camada Internet. Os outros protocolos existentes nesta camada existem por apenas uma razão: suportá-lo. IP poderia ser visto como o protocolo onipotente, no sentido de que esta ciente de todas as redes interconectadas. Isso é possível pois todos os dispositivos de rede possuem um endereço lógico chamado endereço IP. IP analisa o endereço de cada pacote de dados. Em seguida, utilizando uma tabela de roteamento (routing table), decide para onde o pacote deve ser enviado, selecionando a melhor rota. A identificação de dispositivos na rede requer que 2 perguntas sejam respondidas: Em qual rede esse dispositivo se encontra? E qual seu endereço nesta rede? A primeira resposta é o endereço lógico (análogo à rua). A segunda, o endereço físico (a caixa de correio). IP recebe segmentos da camada host-to-host e os fragmenta em datagramas, ou pacotes. No lado destinatário, IP então remonta esses datagramas de volta em segmentos. Cada datagrama recebe o endereço IP do transmissor e do destinatário. Routers (dispositivos de camada 3) que recebem os datagramas decidem sobre rotas à serem tomadas baseados no endereço IP de destino dos pacotes.

A figura acima ilustra o formato do cabeçalho IP. Com base nesta figura, podemos analisar pelo que o protocolo IP tem de passar cada vez que dados são enviados das camadas superiores tendo como destino uma rede remota.

Eis os campos que compõem o cabeçalho IP:

• Version - Número da versão do protocolo (atualmente 4)

• HLEN - Comprimento do cabeçalho

• Priority ou ToS (Type of Service) - Indica como o datagrama deve ser manipulado. Os primeiros 3 bits definem a prioridade

• Total Lenght - Comprimento total do pacote, incluindo o cabeçalho

• Identification - Valor único de IP-Pacote

• Flags - Especifica se fragmentação deve ou não ocorrer

• Frag offset - Provê fragmentação e remontagem se um pacote de dados for muito extenso para se colocar em um frame. Também permite diferentes unidades máximas de transmissão (Maximum Transmission Units - MTUs) na Internet

• TTL (Time To Live - tempo de vida) - O valor TTL é estabelecido quando um pacote é originalmente gerado. Ele estabelece o tempo de vida do pacote através de diferentes métricas (número de nós, tempo, etc.). Se o pacote não atingir seu destino antes do timer TTL expirar, o pacote é descartado. Isso impede pacotes IP de circular continuamente pela Internet.

• **Protocol** - Número da porta lógica do protocolo de camada superior (host-to-host). A porta TCP é 6 e a UDP é 17, em hexadecimal.

• Header CheckSum - Checagem de redundância efetuada no cabeçalho, apenas

• Source IP address - Endereço IP de 32-bits da estação transmissora

• Destination IP address - Endereço IP de 32-bits da estação para a qual o pacote é destinado

• IP option - Utilizado para testes de rede, debugging, segurança, entre outros.

• Data - Dados da camada superior

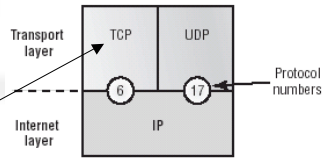
netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

O Modelo TCP/IP (DoD)

O campo “Protocol” do cabeçalho IP

```
IP Header - Internet Protocol Datagram
  Version:              4
  Header Length:        5
  Precedence:           0
  Type of Service:      %000
  Unused:               %00
  Total Length:         187
  Identifier:           22486
  Fragmentation Flags:  %010  Do Not Fragment
  Fragment Offset:      0
  Time To Live:         60
  IP Type:              0x06  TCP
  Header Checksum:      0xd031
  Source IP Address:    10.7.1.30
  Dest. IP Address:     10.7.1.10
  No Internet Datagram Options
```



Note, neste pacote capturado por um analisador de rede, que todos os campos discutidos na página anterior estão presentes. O campo “IP Type” é, na verdade, o campo “Protocol” - este analisador, por algum motivo, o enxerga como “Type”.

Se o cabeçalho IP não carregasse a informação do protocolo da próxima camada, o protocolo IP não saberia o que fazer com os dados contidos no pacote.

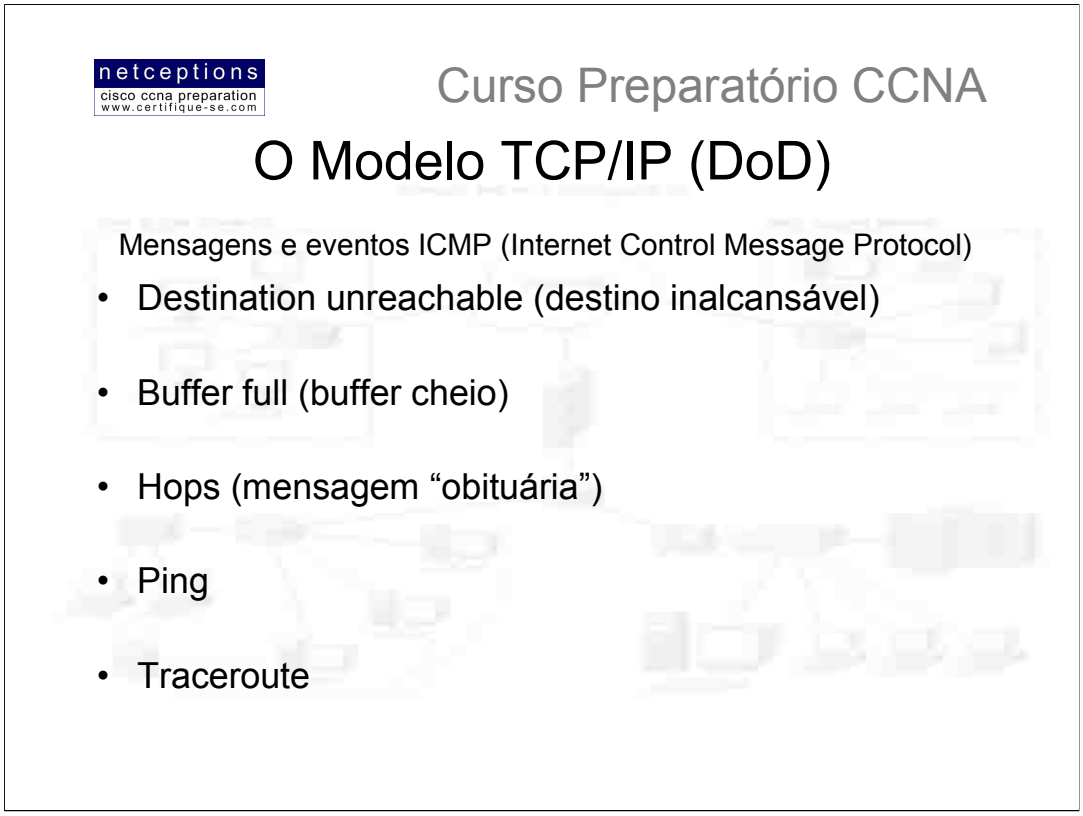
Note também a presença de endereços lógicos, ou endereços IP.

A figura à direita ilustra como a camada de rede interpreta os protocolos na camada de transporte quando o pacote precisa ser passado aos protocolos desta camada.

Neste exemplo, o campo “Protocol” diz ao protocolo IP para enviar os dados pela porta UDP (17) ou pela porta TCP(6) – ambos em formato hexadecimal. Os pacotes poderiam também ser destinados à protocolos da camada de rede, como ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol), ou algum outro.

Abaixo apresentamos uma lista com os protocolos mais comuns de serem encontrados no campo “Protocol” do cabeçalho IP:

Protocol	Protocol Number
ICMP	1
IGRP	9
IPv6	41
GRE	47
IPX in IP	111
Layer-2 tunnel	115



O protocolo ICMP (Internet Control Message Protocol) é definido na camada de rede e é usado pelo protocolo IP por muitos serviços distintos. O ICMP é um protocolo gerenciador, e age também como um “mensageiro” para o protocolo IP. Suas mensagens são transportadas como datagramas IP.

ICMP também é usado na descoberta de rotas para gateways. Periodicamente, anúncios (advertisements) de routers são transmitidos pela rede, contendo os endereços IP das interfaces dos mesmos. Dispositivos (hosts) analisam estes “anúncios” para capturar informações sobre rotas.

Uma “solicitação” de um router é uma requisição de anúncios imediatos e podem ser enviados por dispositivos conectados na rede assim que os mesmos se iniciem. O quadro acima ilustra eventos e mensagens comuns relacionados ao protocolo ICMP.

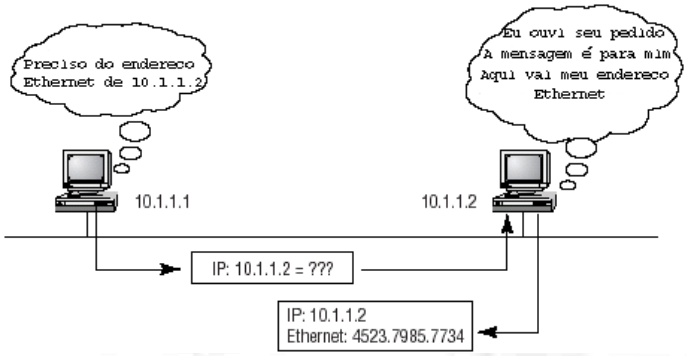
Note que, embora o protocolo ICMP esteja definido na camada de rede, ele ainda se utiliza do protocolo IP para uma requisição de serviço (ex. ping).

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

O Modelo TCP/IP (DoD)

ARP – Address Resolution Protocol



O protocolo ARP (Protocolo de Resolução de Endereço) é responsável por localizar o endereço de hardware de um dispositivo à partir de seu endereço IP conhecido. Eis como funciona: quando o protocolo IP tem um datagrama para transmitir, ele precisa informar ao protocolo de acesso à rede (network access protocol) - como Ethernet ou Token Ring – o endereço de hardware (MAC address) do dispositivo destinatário na rede local. Se o protocolo IP não encontrar o endereço do hardware destinatário no ARP cache, ele utilizará o protocolo ARP para conseguir esta informação (veja figura acima).

ARP funcionado como um “detetive” para o protocolo IP. Ele irá “interrogar” todas as máquinas presentes na rede local (através de uma mensagem de “broadcast”), enviando o endereço IP da máquina que deve responder à este chamado. Resumindo, o protocolo ARP resolve o endereço lógico (IP) para o endereço físico (MAC).

```
Flags:          0x00
  Status:       0x00
  Packet Length:64
  Timestamp:    09:17:29.574000 01/04/2000
Ethernet Header
  Destination:  FF:FF:FF:FF:FF:FF  Ethernet Broadcast
  Source:       00:A0:24:48:60:A5
  Protocol Type:0x0806  IP ARP
ARP - Address Resolution Protocol
  Hardware:                 1  Ethernet (10Mb)
  Protocol:                 0x0800  IP
  Hardware Address Length:  6
  Protocol Address Length:  4
  Operation:                1  ARP Request
  Sender Hardware Address:  00:A0:24:48:60:A5
  Sender Internet Address:  172.16.10.3
  Target Hardware Address:  00:00:00:00:00:00  (ignored)
  Target Internet Address:  172.16.10.10
Extra bytes (Padding):
  ..............  0A 0A 0A 0A 0A 0A 0A 0A 0A 0A 0A 0A 0A 0A
0A 0A 0A 0A 0A
Frame Check Sequence:  0x00000000
```

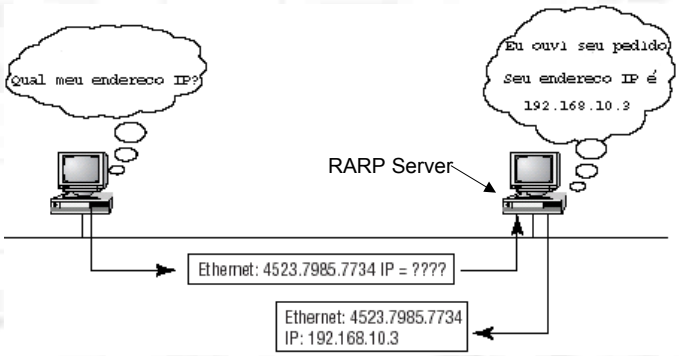
Eis um “trace” que ilustra uma mensagem de broadcast ARP. Note que o endereço do hardware de destino é desconhecido sendo uma série de “F’s (em HEX), equivalente à 1s em binário, o que denota um MAC broadcast.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

O Modelo TCP/IP (DoD)

RARP – Reverse Address Resolution Protocol



Quando uma máquina IP acontece de ser uma máquina sem disco, ela não tem como saber, inicialmente, seu endereço IP. Mas ela sabe seu endereço de hardware (MAC).

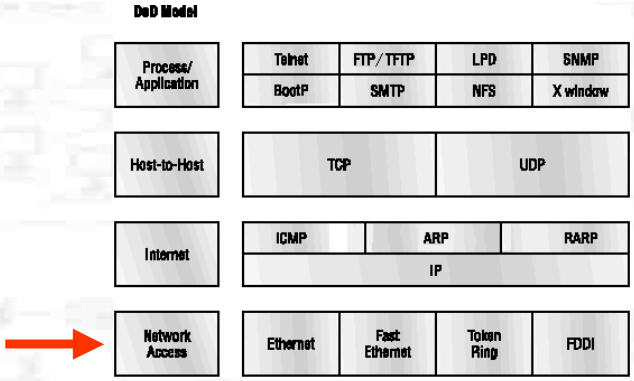
O protocolo RARP (Protocolo Reverso de Resolução de Endereço) se encarrega de descobrir o endereço IP de uma máquina sem disco (diskless station) enviando mensagens de broadcast que contém seu endereço MAC e uma requisição de endereço IP designado para aquele endereço MAC específico.

Uma máquina especialmente designada, chamada RARP server, responde à esse chamado enviando uma resposta contendo o endereço IP da máquina em questão, encerrando assim a “crise de identidade”. Resumindo, o protocolo RARP resolve endereços físicos (MAC) para endereços lógicos (IP), exatamente o oposto do protocolo ARP. Daí o nome Protocolo Reverso de Resolução de Endereço (RARP).

netceptions
cisco ccna preparation
www.certifique-se.com

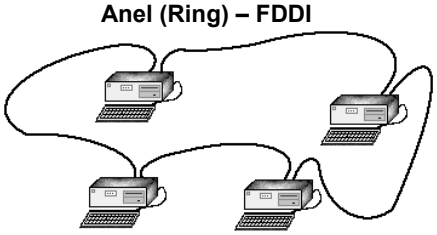
Curso Preparatório CCNA

O Modelo TCP/IP (DoD)

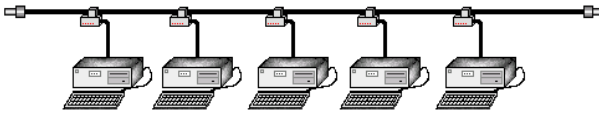


Na camada de acesso (Network Access) são definidos os principais métodos de acesso à mídia, assim como as topologias de rede possíveis:

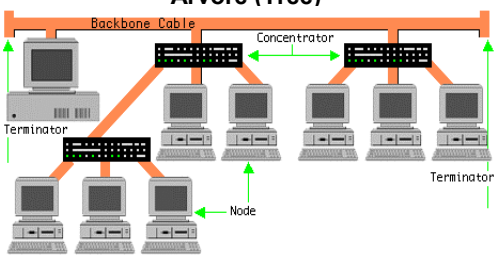
Anel (Ring) – FDDI



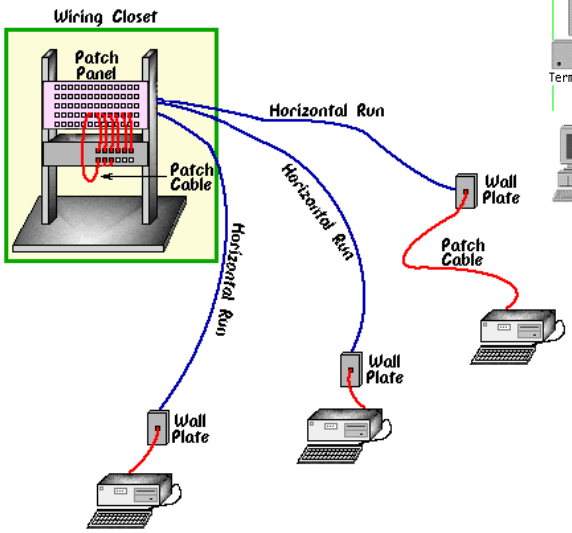
Barramento (Bus) – Ethernet e LocalTalk



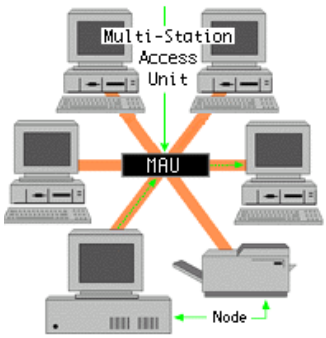
Árvore (Tree)



Estrela (Star) – Ethernet, Fast Ethernet e LocalTa



Anel cabeado em estrela – Token Ring



netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

O Modelo TCP/IP (DoD)

Vantagens e desvantagens dos tipos de topologia

- Barramento (Bus)
- Estrela (Star)
- Anel (Ring)
- Árvore (Tree)

1) Barramento:

Vantagens:
- Fácil conexão de periféricos ou outras máquinas nesse tipo de topologia
- Necessita de menor comprimento de cabo do que a topologia estrela

Desvantagens:
- A rede inteira colapsa caso o cabo principal venha a ter problemas
- Terminadores requeridos em ambos os lados do cabo principal
- Difícil identificação do problema se a rede vier a colapsar
- Não foi planejado para ser usado como solução única em um implantação

2) Estrela:

Vantagens:
- Fácil instalar e cabear
- Não há alteração na rede quando se instala ou se retira algum dispositivo
- Fácil detecção de falhas e remoção de dispositivos falhos

Desvantagens:
- Precisa de maior comprimento de cabo do que a topologia de Barramento
- Se o concentrador (Hub) falhar, todos os dispositivos conectados à ele são afetados
- Mais caro que a topologia de rede devido ao custo dos concentradores (Hubs)

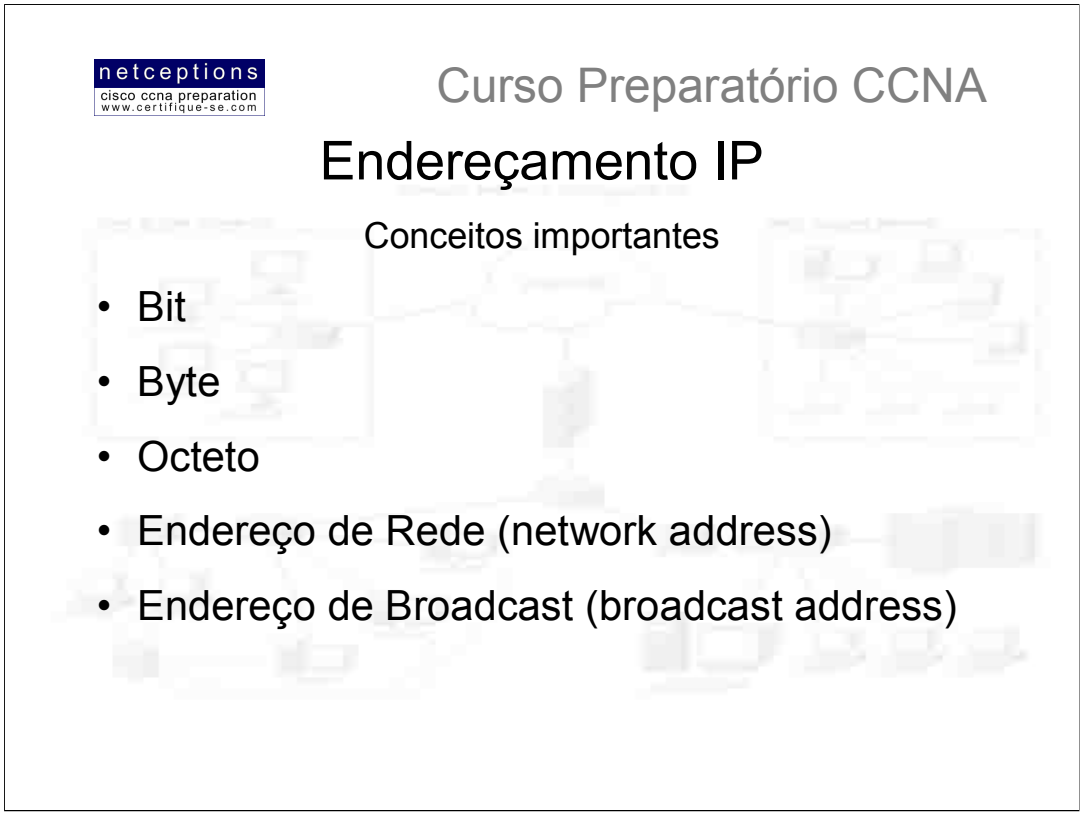
3) Anel cabeado em estrela (Token Ring):

Vantagens / Desvantagens:
- Ver estrela (apesar de ser conhecido como anel, a topologia se assemelha à estrela, uma vez que o anel se encontra, de fato, dentro do concentrador, chamado MAU (multistation access unit).

4) Árvore

Vantagens:
- Cabeamento ponto-a-ponto para segmentos individuais
- Suportado por uma grande gama de revendedores de hardware e software

Desvantagens:
- Comprimento total de cada segmento é limitado pelo tipo de cabo utilizado
- Se o segmento principal tiver problemas, a rede inteira irá colapsar
- Mais difícil de se cabear e se configurar que outras topologias



Um dos mais importantes tópicos na discussão TCP/IP trata dos esquemas de endereçamento IP. O endereço IP é um identificador numérico designado à cada dispositivo conectado à uma rede IP. Ele designa um local para o dispositivo na rede.

O endereço IP é um endereço lógico (software), e não físico (hardware). O esquema de endereçamento IP foi criado para permitir que um dispositivo em uma rede possa se comunicar com um dispositivo em outra, indiferentemente aos tipos de LANs envolvidos no processo (Ethernet, Token-Ring, etc.).

Para entender e dominar os esquemas de endereçamento IP e de suas sub-redes (subnetting), é muito importante que se domine técnicas de conversão binária para decimal assim como potências de base 2. Nessa aula praticaremos essas técnicas.

Terminologia IP:

• **Bit**: Um dígito - 1 ou 0.

• **Byte**: Uma sequência de 7 ou 8 bits, dependendo da paridade utilizada. O normal é uma sequência de 8 bits.

• **Octeto** (octet): Sempre 8 bits.

• **Endereço de rede (network address):** Definição utilizada por roteadores para envio de pacotes à uma rede remota (ex. 10.0.1.32, 192.168.10.0 ou 232.21.2.98).

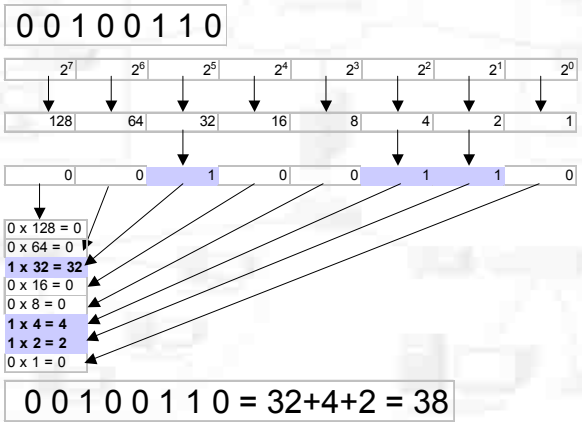
• **Endereço de broadcast (broadcast address):** Endereço usado por aplicações e dispositivos para o envio de mensagens à todos os dispositivos de uma rede, simultaneamente (ex. 255.255.255.255, 172.16.255.255 ou 10.255.255.255).

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Endereçamento IP

Conversão binário – decimal



Antes de entrarmos em mais detalhes sobre endereçamento IP, é imprescindível que você conheça à fundo técnicas de Conversão binário-decimal. Para se dominar esta técnica, prática se faz necessária. Eis como funciona:

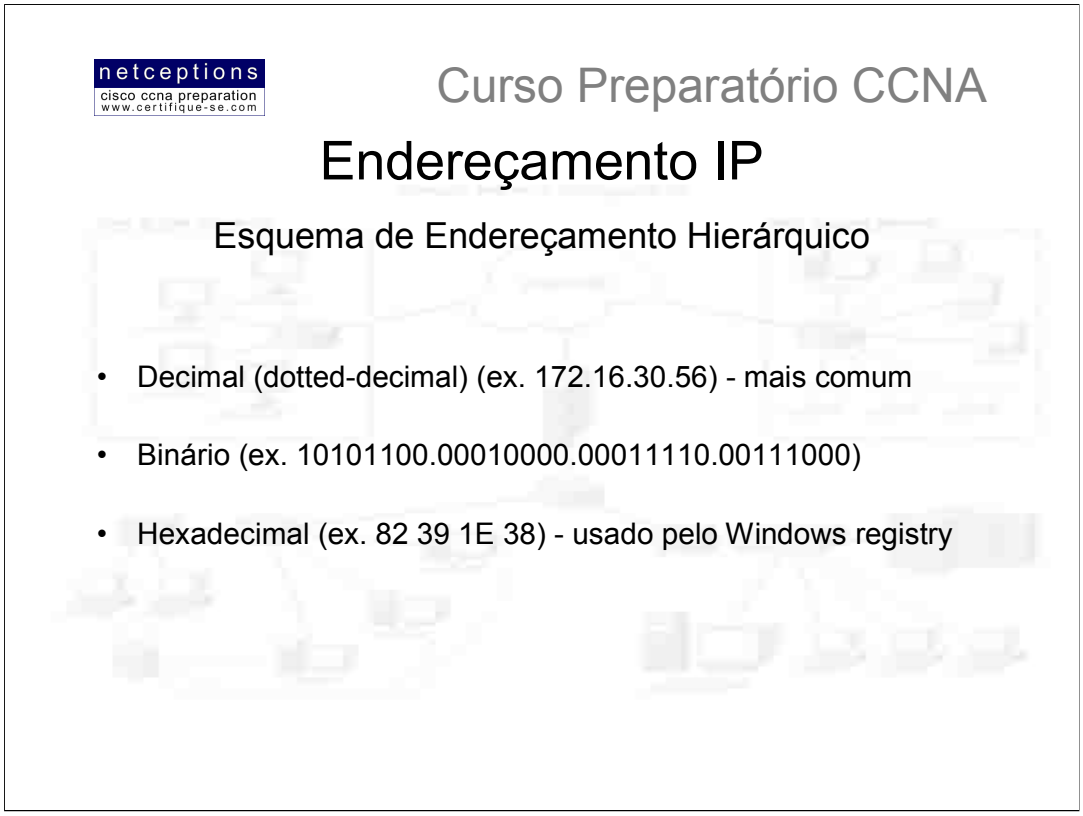
Números binários utilizam 8 bits para definir um número decimal. Esses bits têm seus valores considerados da direita para a esquerda através de um fator que dobra seu valor. Isso ocorre pois são determinados através de potências de base 2. Eis o porque do nome do sistema ser binário.

Por exemplo, o número binário 00100110 nada mais é do que a representação de $0x2^7+ 0x2^6+ 1x2^5+ 0x2^4+ 0x2^3+ 1x2^2+ 1x2^1+ 0x2^0 = 0+0+32+0+0+4+2+0 = 38$.

Técnicas de memorização e muita prática são muito úteis no domínio do processo de conversão binário-decimal. Memorize a seguinte tabela:

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

Acredite, a memorização da mesma lhe será muito útil para a prova CCNA. A seguir descreveremos as classes de endereços IP (A,B e C) e suas peculiaridades, assim como a criação e determinação de sub-redes das mesmas (subnetting).

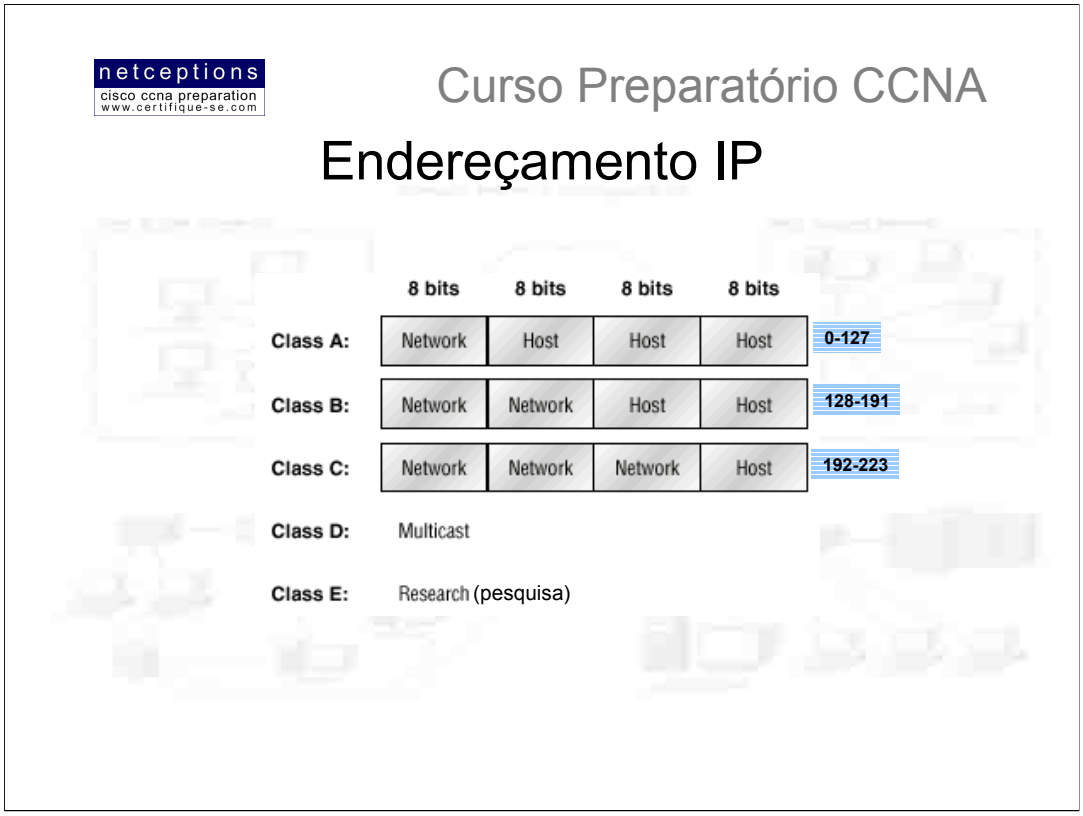


Um endereço IP consiste de 32 bits de informação. Esses bits são divididos em 4 sessões, chamadas de octetos ou bytes, cada uma contendo 1 byte (8 bits).

Todos os exemplos ilustrados acima representam o mesmo endereço IP, notados de formas diferentes (decimal, binário e hexadecimal).

O endereço de 32-bit é estruturado de forma hierárquica, em oposição à uma forma plana, não-hierárquica. Embora ambos os esquemas pudessem vir a ser utilizados, o esquema hierárquico foi escolhido por uma excelente razão: agilidade no roteamento. Embora o esquema “plano” possa nos fornecer um intervalo enorme de endereços (4,3 bilhões - 2^{32}), se cada endereço fosse único, todos os roteadores na Internet teriam que armazenar o endereço de cada um dos dispositivos conectado à mesma. Isso tornaria o processo de roteamento eficaz impossível, mesmo que apenas uma fração dos endereços viesse à ser, efetivamente, utilizada.

A solução para esse dilema foi a utilização de um esquema de endereçamento de 3 níveis, divididos em: network, <subnet> e host. Esse esquema de endereçamento é análogo ao esquema de endereçamento telefônico tradicional. A primeira parte identifica uma grande área. A segunda parte já é mais específica e define a área de chamada. Finalmente, a última parte - o sufixo - identifica a conexão direta com o cliente.

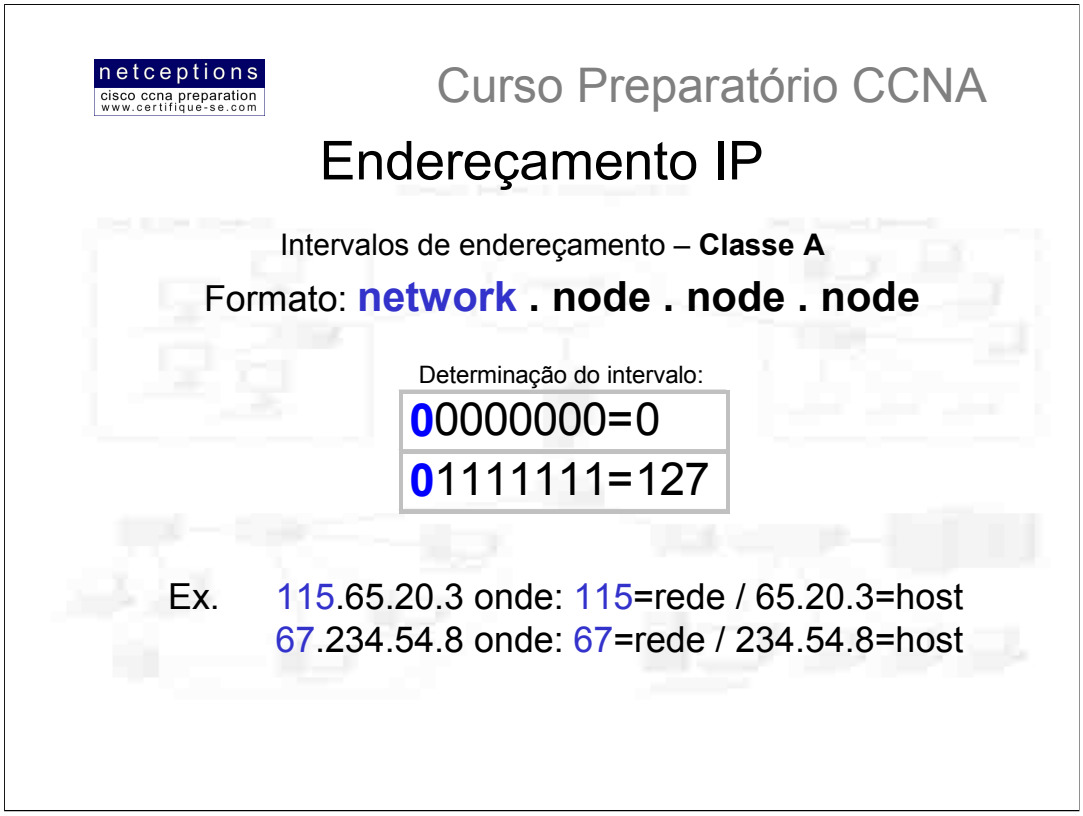


O endereço de rede (network address) identifica cada rede distintamente. Toda e qualquer máquina em uma mesma rede divide o mesmo endereço de rede como parte de seu endereço IP. No endereço IP 172.16.30.56, por exemplo, a parte 172.16 identifica a rede, sendo portanto o endereço da mesma. O endereço do nó (node address) identifica individualmente cada dispositivo conectado na rede, em oposição ao endereço de rede, que identifica em grupo. No exemplo anterior, .30.56 seria o endereço do dispositivo na rede.

Os projetistas da Internet decidiram por criar classes de redes baseadas no tamanho das mesmas. Para um pequeno número de redes possuindo um grande número de dispositivos conectados foi criada a classe A de redes (class A networks). No outro extremo, temos a classe C de redes, que possui um grande número de redes e um pequeno número de dispositivos conectados à cada uma. A classe B seria um meio termo entre a classe A e a C.

A subdivisão de um endereço IP nas porções de rede e nó é determinada pela classe em que se encontra alocado tal endereço. A figura acima sumariza as 3 classes de rede existentes. Comentaremos o funcionamento do processo de alocação de endereços mais adiante.

Para assegurar a eficiência no processo de roteamento, os projetistas da “Grande Rede” definiram uma regra para a seção de bits iniciais de cada endereço para cada classe existente. Por exemplo, como um roteador “sabe” que um endereço pertencente à classe A **sempre** tem seu primeiro bit 0, o roteador pode ser capaz iniciar o encaminhamento do pacote depois de ler apenas esse bit. É aí que está a grande diferença entre as classes de endereços A, B e C.



Em um endereço pertencente à classe A de endereços, o primeiro byte sempre define o endereço de rede, enquanto que os 3 bytes restantes definem o endereço do dispositivo nessa rede (host).

Os projetistas do esquema de endereçamento definiram que o primeiro bit do primeiro byte de um endereço pertencente à classe A de endereços deve estar "desligado", ou seja, tem valor 0. Isso significa que um endereço pertencente à classe A deve estar compreendido entre 0 e 127, pois o endereço máximo seria 01111111 = 127. Eis como esses endereços são definidos:

0xxxxxxx: Se "desligarmos", e depois, "ligarmos" todos os 7 bits seguintes ao 0, ou seja, se todos assumirem o valor 1 descobriremos o intervalo de endereços IP pertencentes à classe A de endereçamento:

00000000 = 0

01111111 = 127

Portanto, um endereço pertencente à classe A seria definido entre 0 e 127, não podendo ser nem mais, nem menos (discutiremos endereços "ilegais" mais adiante).

Endereços de classe A tem o tamanho de 1 byte, com o primeiro bit deste byte reservado e os 7 bits restantes disponíveis para manipulação. Como resultado, o número máximo de redes que pode ser obtido com um endereço de classe A é de 128. 126, na verdade, uma vez que os 7 bits restantes não podem ser todos 0 (00000000), assim como o número 127 também está restrito por tratar-se de um endereço reservado. Cada endereço de classe A possui 24 bits (3 bytes) disponíveis para endereçamento de dispositivos na rede (node address). Portanto, poderia-se obter 2^{24} (16.777.216) endereço únicos para cada endereço de rede pertencente à classe A. Entretanto, uma vez que não é permitido endereços com todos os bits iguais à 1, ou à 0 (por serem reservados), o número real de endereços disponíveis para endereçamento de dispositivos em uma rede classe A seria de:

2^{24}-2=16.777.214 de endereços possíveis.

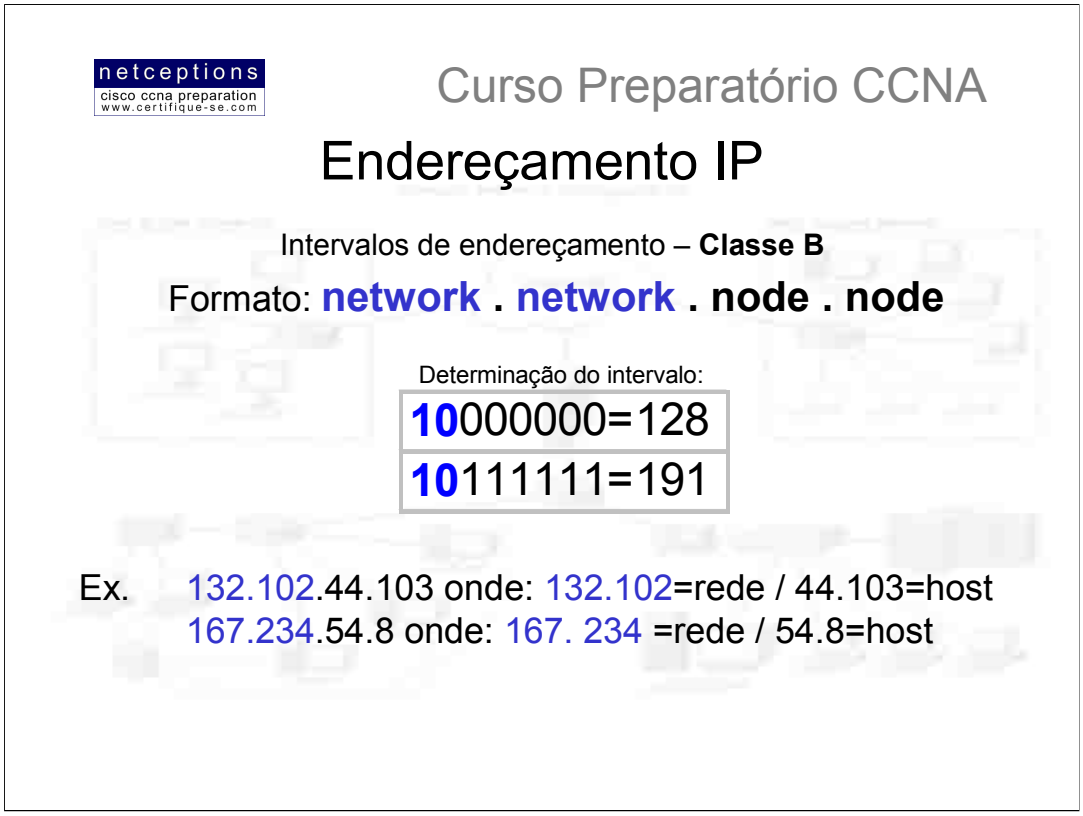
Classe A – Endereços válidos:

Eis um exemplo de como se descobrir os endereços de dispositivos válidos de uma rede classe A:

10.**0.0.0** – Todos os bits desligados (0) = endereço de rede

10.**255.255.255** – Todos os bits ligados (1) = endereço de broadcast

Os endereços válidos para dispositivos estão compreendidos entre o endereço de rede e o endereço de broadcast (10.0.0.1 a 10.255.255.254). Note que 0s e 255s são endereços válidos. Tudo o que você deve lembrar ao determinar endereços válidos é que nem todos os bits podem estar ligados ou desligados simultaneamente.



Em um endereço de classe B, os primeiros 2 bytes designam a porção de rede, enquanto que os 2 bytes restantes designam a porção do host. O formato de um endereço de classe B, então, seria:

rede . rede . host . host

Por exemplo, no endereço IP 172.16.30.56, 172.16 determina o endereço da rede, enquanto que 30.56 determina o endereço do dispositivo nessa rede.

Com o endereço de rede sendo formado por 2 bytes (com 8 bits cada), teríamos então 2^{16} possíveis combinações de endereços. Porém, os projetistas da Internet definiram que os 2 primeiros bits do primeiro byte de um endereço classe B sejam fixados em 1 e 0, respectivamente, o que nos deixa apenas 14 bits para manipulação (2^{14} = 16.384 endereços possíveis).

Endereços de classe B disponibilizam 2 bytes para endereçamento de dispositivos na rede, menos os dois padrões reservados (tudo 0 e tudo 1), o que nos deixa um número de 2^{16} - 2 = 65.534 endereços possíveis para dispositivos para cada endereço de rede classe B.

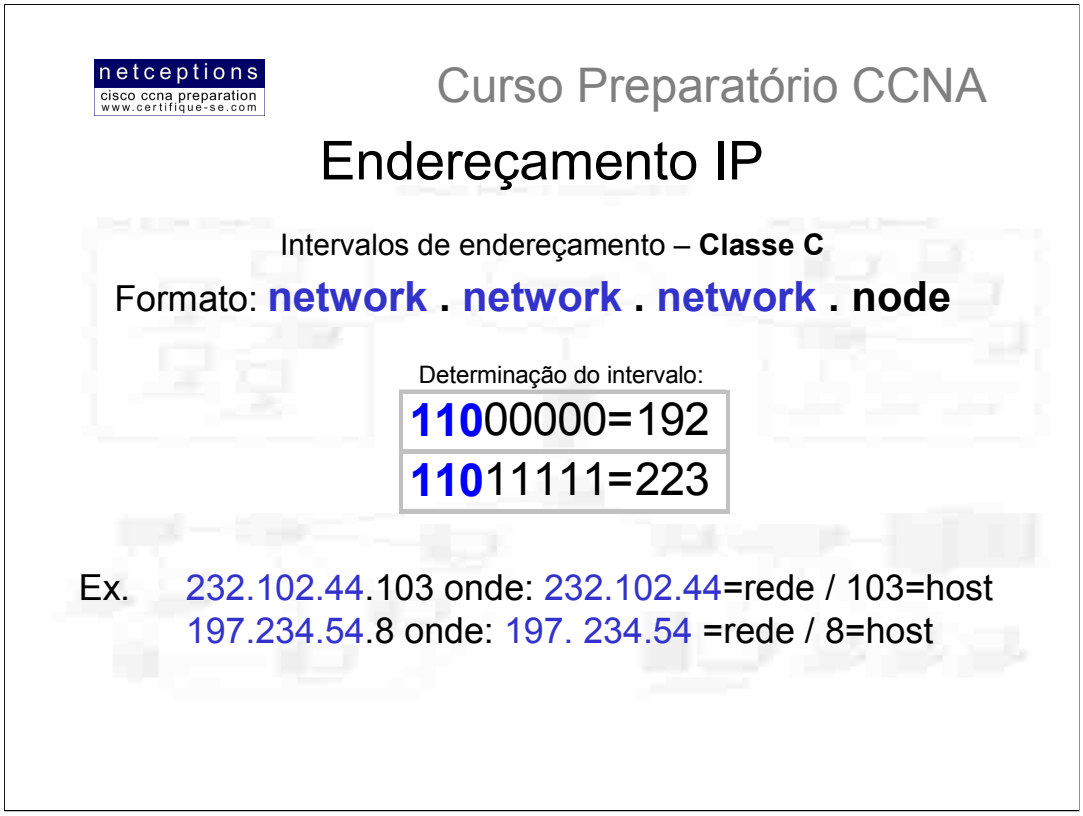
Classe B – Endereços válidos:

Eis um exemplo de como se descobrir os endereços de dispositivos válidos de uma rede classe B:

172.16.**0.0** – Todos os bits desligados (0) = endereço de rede

172.16.**255.255** – Todos os bits ligados (1) = endereço de broadcast

Os endereços válidos para dispositivos estão compreendidos entre o endereço de rede e o endereço de broadcast (172.16.0.1 a 172.16.255.254). Note que 0s e 255s são endereços válidos. Mais uma vez, ao se determinar o intervalo de endereços válidos para dispositivos, você deve se lembrar que nem todos os bits podem estar ligados ou desligados simultaneamente.



Em um endereço de classe C, os primeiros 3 bytes designam a porção de rede, enquanto que o byte restante designa a porção do host. O formato de um endereço de classe C, então, seria:

rede . rede . rede . host

Por exemplo, no endereço IP 192.16.30.56, 192.16.30 determina o endereço da rede, enquanto que 56 determina o endereço do dispositivo nessa rede.

Com o endereço de rede sendo formado por 3 bytes (com 8 bits cada), teríamos então 2^{24} possíveis combinações de endereços. Porém, os projetistas da Internet definiram que os 3 primeiros bits do primeiro byte de um endereço classe C sejam fixados em 1, 1 e 0, respectivamente, o que nos deixa apenas 21 bits para manipulação (2^{21} = 2.097.152 endereços de rede possíveis).

Endereços de classe C disponibilizam apenas 1 byte para endereçamento de dispositivos na rede, menos os dois padrões reservados (tudo 0 e tudo 1), o que nos deixa um número de 2^8 - 2 = 254 endereços possíveis para dispositivos para cada endereço de rede pertencente à classe C.

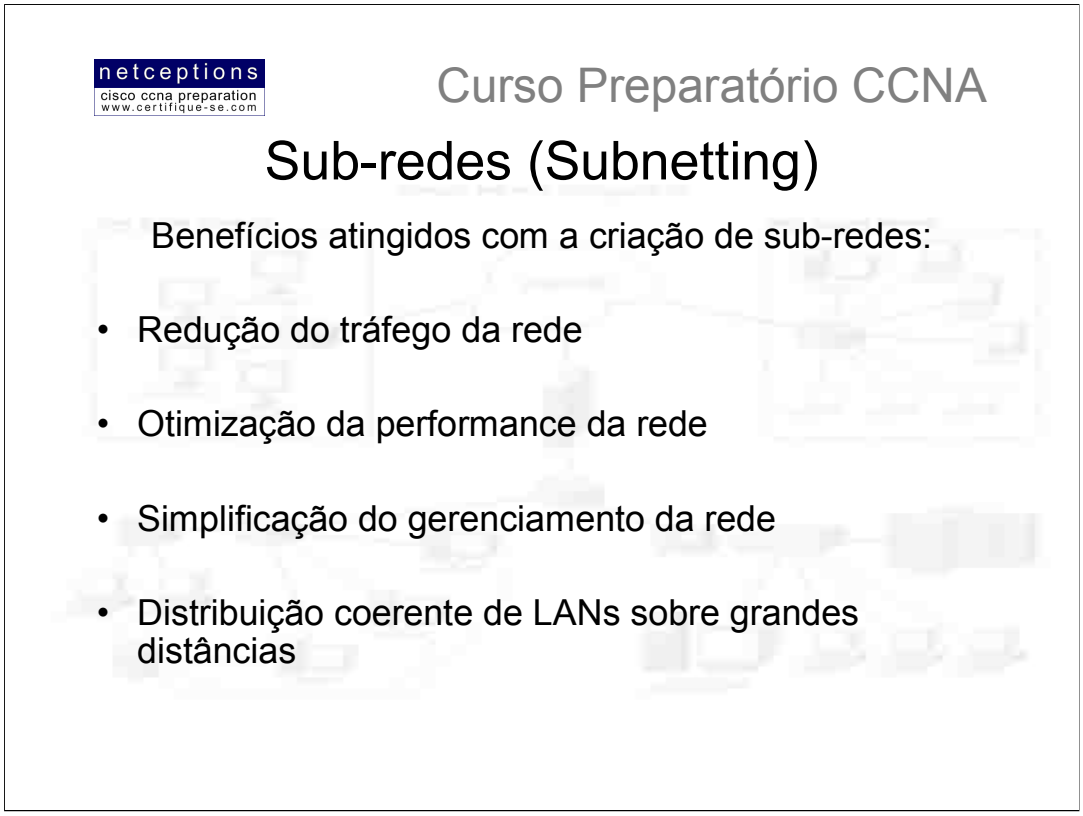
Classe C – Endereços válidos:

Eis um exemplo de como se descobrir os endereços de dispositivos válidos de uma rede classe C:

192.16.10.**0** – Todos os bits desligados (0) = endereço de rede

172.16.10.**255** – Todos os bits ligados (1) = endereço de broadcast

Os endereços válidos para dispositivos estão compreendidos entre o endereço de rede e o endereço de broadcast (172.16.10.1 a 172.16.10.254). Mais uma vez, ao se determinar o intervalo de endereços válidos para dispositivos, você deve se lembrar que nem todos os bits podem estar ligados ou desligados simultaneamente.



Discutimos, anteriormente, como definir e identificar intervalos válidos para endereçamento de dispositivos sobre redes pertencentes às classes A, B e C através do "ligamento" e do "desligamento" dos bits reservados para o endereçamento dos mesmos. Entretanto, estávamos definindo apenas uma rede. E se desejássemos pegar um endereço de rede e criar 6 sub-redes à partir do mesmo? Teríamos de efetuar uma operação conhecida como "subnetting", que permite que peguemos uma grande rede e a "desmembremos" em redes menores. Existem muitas razões para se efetuar tal operação. Alguns dos benefícios incluem:

• **Redução do tráfego na rede** - Tráfego reduzido significa melhor performance e mais segurança. Com o uso de roteadores, a maior parte do tráfego permanece na rede local, e apenas pacotes destinados à outras redes atravessam os mesmos. Recordemos que roteadores criam domínios de broadcast. Quanto menor o domínio de broadcast criado, menor o tráfego naquele segmento de rede.

• **Gerenciamento simplificado** - É mais fácil a identificação e isolamento de problemas em grupos de redes menores, interconectadas, do que em uma única, grande rede.

• **Distribuição coerente de LANs sobre grandes distâncias** - Uma vez que links WAN (wide area network) são consideravelmente mais lentos que links LAN, uma única e volumosa rede que atinge grandes distâncias está mais sujeita à gerar problemas em cada um dos pontos listados acima. A conexão de múltiplas redes menores faz o sistema funcionar mais eficientemente.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Sub-redes (Subnetting)

Passos para a criação de sub-redes:

- Determine o número de endereços de rede necessário
  - Um para cada sub-rede
  - Um para cada conexão WAN
- Determine o número de hosts por sub-rede necessário
  - Um para cada dispositivo TCP/IP conectado à sub-rede
  - Um para cada interface do roteador
- Baseado nos requerimentos acima, defina o seguinte:
  - Uma máscara de sub-rede (subnet mask) para toda a rede
  - Um endereço de sub-rede único para cada segmento físico
  - Um intervalo de endereços de dispositivos para cada sub-rede

Para se criar sub-redes, separe bits da porção de um endereço IP destinada ao endereçamento de hosts e reserve-os para a definição de uma sub-rede. Isso significa menos bits para o endereçamento de hosts. Portanto, quanto mais sub-redes definidas, menor o número de bits destinados ao endereçamento de dispositivos.

Antes de se definir sub-redes, é importante se determinar os requisitos necessários e planejar para condições futuras (vide passos acima).

Máscaras de rede - ou de sub-rede (subnet masks)

Para que o esquema de endereçamento de sub-redes funcione à contento, todos os dispositivos conectados necessitam saber qual a parte do endereço de host que será destinada ao endereço da sub-rede. Isso é conseguido através da designação de uma máscara de rede à cada dispositivo. Essa máscara é um valor de 32-bits que permite ao recipiente dos pacotes IP destinguir entre as porções de rede e de host de um endereço IP.

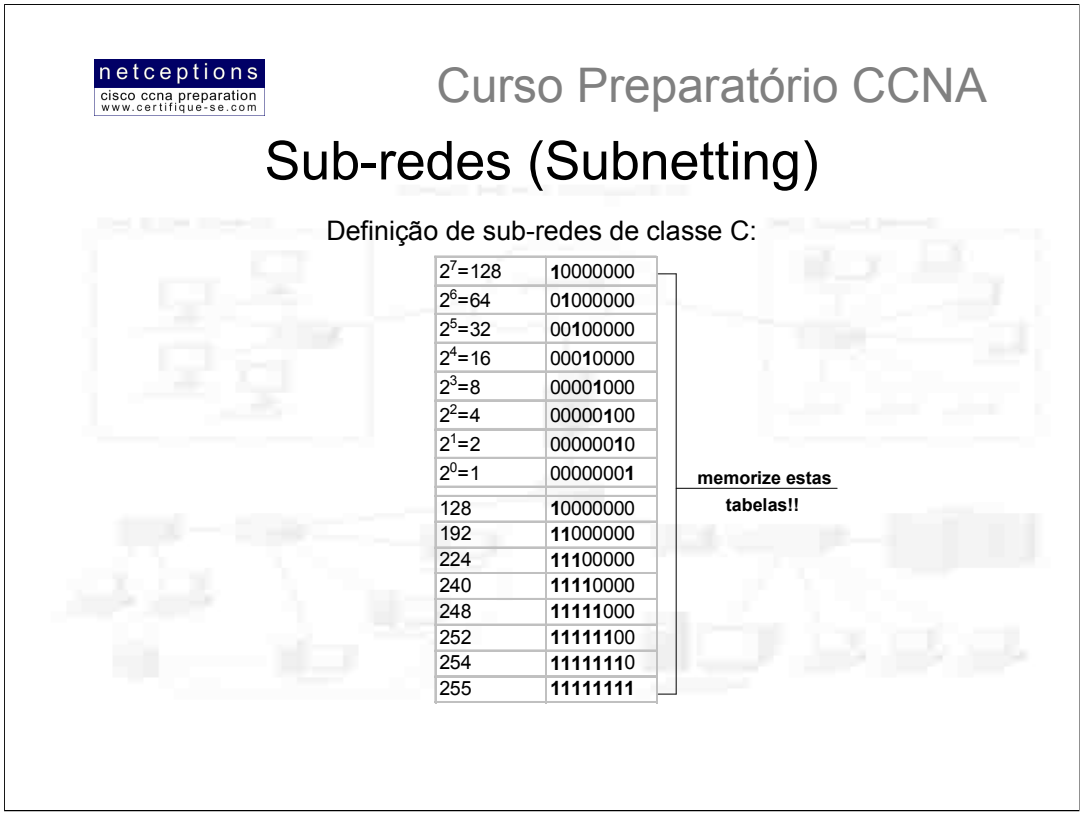
A máscara de rede de 32-bits é composta de 0s e 1s. A ocorrência de 1s na máscara de rede representa as posições que se referem ao endereço de rede, ou de sub-rede.

Nem todos os endereços de rede necessitam que uma sub-rede seja criada. Nesses casos, uma máscara de rede padrão (default subnet mask) é utilizada. Isso é, basicamente, o mesmo que se dizer que essa rede não possui um endereço de sub-rede. As máscaras de rede padrão utilizadas para classes de endereço A, B e C são ilustradas abaixo:

Classe	Formato	Máscara de Rede Padrão
A	rede.host.host.host	255.0.0.0
B	rede.rede.host.host	255.255.0.0
C	rede.rede.rede.host	255.255.255.0

Essas máscaras são imutáveis. Em outras palavras, não é possível se definir uma máscara de sub-rede de classe B como 255.0.0.0.

Para uma máscara de sub-rede de classe A, o primeiro byte não pode ser alterado. Ele deve ter o formato mínimo de 255.0.0.0. Do mesmo modo, não se é permitido designar uma máscara no formato 255.255.255.255, uma vez que isso seria o equivalente a todos os bits 1, ou um endereço de broadcast. Uma máscara de classe B deve começar como 255.255.0.0 e para classe C, 255.255.255.0.



Existem diversos modos de se criar sub-redes. O modo certo é o modo que funciona para você. Primeiro, discutiremos o modo binário de criação. Mais adiante, veremos um modo mais simples de se fazer a mesma coisa. Por que já não ir para o modo mais simples, você deve estar se perguntando… Porque é necessário entender como sub-redes são definidas em detalhes, uma vez que isso é uma importante parte da prova CCNA.

Em um endereço de classe C, apenas 1 byte (8 bits) estão disponíveis para endereçamento de dispositivos na rede. Lembre-se que os bits reservados para sub-redes devem começar da esquerda para a direita, consecutivamente. Isso significa que as máscaras de rede de classe A podem ser as ilustradas na figura acima (128, 192, 224, 240, 248, 252 e 254).

As RFCs (Request For Comments - são “standards” definidos que regem, entre outras coisas, os esquemas de endereçamento IP) determinam que não se pode haver apenas 1 bit para definição de sub-redes, uma vez que esse bit teria de estar sempre “ligado” ou “desligado”, o que seria “ilegal”. Portanto, a primeira máscara de rede que se é permitida seria 192 (11000000), e a última, 252 (11111100), uma vez que são necessários pelo menos 2 bits para definição de hosts.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Sub-redes (Subnetting)

Definição de sub-redes de classe C:

Sub-rede 64		
Sub-rede	**Host**	**Significado**
01	000000=64	Endereço da rede
01	000001=65	Primeiro host válido
01	111110=126	Último host válido
01	111111=127	Endereço de broadcast

Sub-rede 128		
Sub-rede	**Host**	**Significado**
10	000000=128	Endereço da rede
10	000001=129	Primeiro host válido
10	111110=190	Último host válido
10	111111=191	Endereço de broadcast

Faça isso primeiro!

A prova CCNA não vai lhe pedir simplesmente para determinar máscaras de sub-redes de diferentes classes. Ela também poderá lhe passar uma máscara de rede pronta e perguntar:

Quantas sub-redes tal máscara produz?

Quantos endereços de host válidos são obtidos por sub-rede?

Quais são as sub-redes válidas?

Quais os hosts válidos em cada sub-rede?

Qual o endereço de broadcast de cada sub-rede?

O método binário

Nesta seção você aprenderá a determinar sub-redes de classe C e a responder as perguntas acima utilizando o método binário. Pegaremos a primeira máscara de rede disponível à classe C, que utiliza 2 bits para sub-rede. No exemplo mencionado, falamos da máscara 255.255.255.192 (**11111111.11111111.11111111.11**000000)

Como vimos, 192 é o mesmo que 11000000 em binário (lembre-se da dica de decorar o esquema apresentado na página anterior…), ou seja, 2 bits para sub-redes e 6 bits para definição de hosts. Quais são as sub-redes? Uma vez que os bits reservados para sub-redes não podem estar todos ligados ou desligados simultaneamente, as 2 sub-redes válidas são:

01000000 = 64 e **10**000000 = 128 (**00**000000 = ilegal e **11**000000 = ilegal)

Os hosts válidos serão definidos como números compreendidos entre os intervalos das sub-redes, menos todos os bits ligados e todos os bits desligados. Para identificar os hosts válidos, primeiramente identifique a sub-rede, desligando todos os bits de host (veja quadro acima). Em seguida, ligue todos os bits de host para identificar o endereço de broadcast da sub-rede identificada. Os endereços válidos para hosts deverão estar compreendidos entre esses 2 números (sub-rede e endereço de broadcast). O quadro acima ilustra o processo para as duas sub-redes possíveis para este caso (64 e 128).

O método apresentado até que é bastante simples. No entanto, o que aconteceria se, ao invés de apenas 2 bits para sub-redes, tivéssemos 9? Ou 10? Ou mesmo 20? Esse método seria praticamente inviável. Ele apenas é útil para efeito de aprendizagem. Para uso na prova, utilizaremos um método mais prático e dinâmico.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Sub-redes (Subnetting)

O método alternativo: sub-redes de classe C:
Procure responder às seguintes perguntas:

- Quantas sub-redes a máscara de rede produz?
- Quantos endereços de hosts válidos podem ser obtidos por sub-rede?
- Quais são as sub-redes válidas obtidas?
- Qual é o endereço de broadcast para cada sub-rede?
- Quais são os hosts em cada sub-rede?

Quando você se depara com uma máscara de rede e precisa determinar o número de sub-redes, hosts válidos e endereços de broadcast que a máscara define, tudo o que você tem a fazer é responder as 5 perguntas ilustradas acima.

É importante, nessa altura dos acontecimentos, que você domine potências de base 2 (veja modelo na página 27). Eis como determinar a resposta para cada uma das 5 questões:

1) Quantas sub-redes? 2^x - 2 = quantidade de sub-redes, onde X representa o número de bits "mascarados", ou o número de 1s. Por exemplo: **11**000000 seria 2^2 - 2 = **2**. Nesse caso, haveriam **2** sub-redes possíveis com tal máscara.

2) Quantos hosts válidos por sub-rede? 2^y - 2 = quantidade de hosts válidos, onde Y representa o número de bits disponíveis para manipulação dos endereços de host, ou o número de 0s. Por exemplo: 11**000000** seria 2^6 - 2 = **62**. Nesse caso, existem **62** endereços válidos para hosts por sub-rede.

3) Quais são as sub-redes válidas? 256 - máscara de rede = valor da sub-rede base. À esse resultado, soma-se o valor obtido até que se atinja o número da máscara (que seria inválido). Seguindo nosso exemplo: 256 - 192 = **64** (número base e primeira sub-rede válida). 64 + 64 = **128** (segunda sub-rede válida). 128 + 64 = 192 (valor da máscara = sub-rede inválida). Portanto, as sub-redes válidas seriam **64** e **128**.

4) Qual o endereço de broadcast para cada sub-rede? O endereço de broadcast seria o valor imediatamente anterior ao valor da próxima sub-rede (ou da máscara, se estivermos falando da última sub-rede na sequência…). Em nosso exemplo, temos as sub-redes 64 e 128. O endereço de broadcast da primeira seria 128 - 1 = **127**. Já o da segunda: 192 (valor da máscara) - 1 = **191**.

5) Quais os hosts válidos? Os valores válidos seriam os compreendidos entre as sub-redes, menos todos os bits ligados e desligados. A melhor maneira de se identificar esses valores é se descobrindo as sub-redes válidas e os endereços de broadcast de cada uma. Em nosso exemplo, os hosts válidos estariam compreendidos nos intervalos entre **65-126** para a primeira sub-rede e **129-190** para a segunda.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Sub-redes (Subnetting)

O método alternativo: sub-redes de classe C:

Criando sub-redes de cabeça

Exemplo:

Dados o endereço e máscara de rede abaixo, determine à que sub-rede o mesmo pertence, qual o intervalo válido de hosts e qual o endereço de broadcast.

- **192.168.10.33 = Endereço de rede**
- **255.255.255.224 = Máscara de rede**

Apesar de tudo o que vimos até agora, é possível criar sub-redes mentalmente, assim como determinar as respostas de perguntas como as ilustradas na página anterior. Como fazê-lo? Simples. Apenas siga os passos descritos. Vamos utilizar como exemplo o endereço ilustrado acima:

192.168.10.**33** = Endereço de rede

255.255.255.**224** = Máscara de rede

Primeiramente, determine a sub-rede e endereço de broadcast do endereço de rede acima (192.169.10.33) - **ATENÇÃO**: essa é uma típica questão da prova CCNA.

Isso pode ser feito respondendo-se à questão 3 das 5 questões colocadas na página anterior:

256 - **224** = **32**.

32 + 32 = **64**.

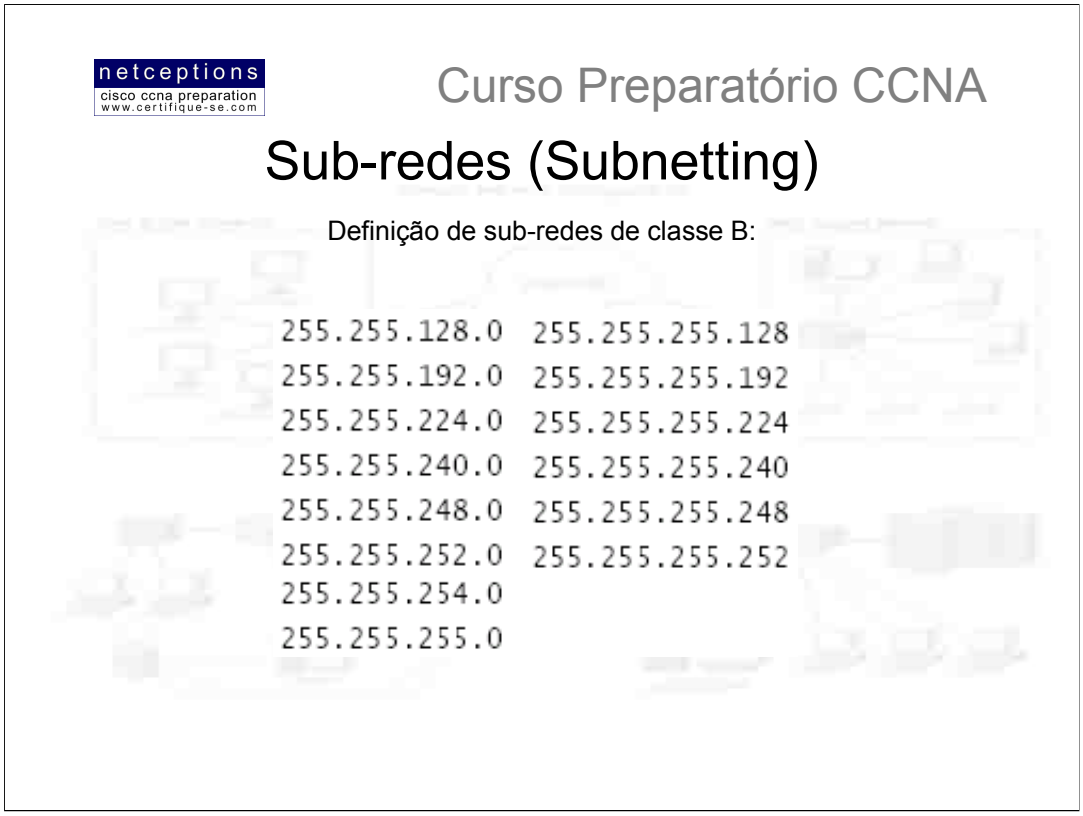
O endereço encontra-se entre as 2 sub-redes e, portanto, deve ser parte da sub-rede **32**.

A próxima sub-rede é a **64**, portanto, o endereço de broadcast dessa sub-rede é o **63**.

O intervalo válido de hosts é **33-62.**

Pronto! Mental e rapidamente o problema foi resolvido. Esse método pode ser aplicado não apenas à classe C de endereços, mas também às classes A e B, como veremos à seguir.

Vale ressaltar mais uma vez que esse é o formato de questão comum à prova CCNA quando se trata de sub-redes. Um endereço e uma máscara de rede são dados. A prova pede que se determine os itens exemplificados acima. Pratique bastante. 4 à 5 questões da prova tratam de sub-redes IP. Acertá-las pode ser a diferença entre passar ou ser reprovado na prova.



A definição sub-redes em endereços de classe B não foge às regras utilizadas para a classe A. A única diferença é que, agora, teremos menos bits disponíveis para manipulação de sub-redes, e, consequentemente, mais bits disponíveis para manipulação de hosts.

Ilustramos acima todas as sub-redes possíveis de serem definidas em um endereço de classe B. Note que temos um maior número de possibilidades que no caso de endereços classe A.

Endereços de classe B nos disponibiliza 16 bits para endereçamento de hosts. Isso significa que podemos, de fato, utilizar 14 bits para definição de hosts, uma vez que devemos deixar ao menos 2 bits para endereçamento de hosts, obrigatoriamente.

Você nota um padrão nos valores de sub-redes acima? Por esse motivo sugeri que se memorizasse a tabela de conversão binário-decimal apresentada na página 27. Uma vez que os bits de sub-rede têm seu início da esquerda para a direita, os números obtidos são sempre os mesmos. É importante que se memorize esse padrão.

Para a definição de sub-redes de classe B, o processo é o mesmo utilizado para casos de classe C. Utilize os mesmos valores de sub-rede utilizados para classe C, porém, adicione um 0 à porção de rede e um 255 à seção de broadcast, no quarto octeto.

Exemplo: Máscara de rede **255.255.255**.0 (ao contrário do que se possa pensar, neste caso essa é uma máscara de rede classe B, e não uma máscara padrão de classe C)

Endereços de classe B utilizam a máscara padrão 255.255.0.0, o que deixa 14 bits para definição de sub-redes, uma vez que deve-se deixar ao menos 2 bits para definição de hosts. A máscara 255.255.255.0 aplicada a um endereço de classe B utiliza 8 bits para definição de sub-redes. Portanto:

1) Número de sub-redes: $2^8 - 2 = 254$

2) Número de hosts: $2^8 - 2 = 254$

3) Sub-redes válidas: 256 - 255 = 1, 2, 3, 4, etc. (todas definidas no terceiro octeto!), ou seja, as sub-redes seriam: 172.16.1.0, 172.16.2.0, 172.16.3.0, 172.16.4.0, ..., 172.16.254.0.

4) Endereço de broadcast para cada sub-rede: 172.16.1.255, 172.16.2.255, etc.

5) Intervalo válido de hosts para cada sub-rede: 172.16.1.1 - 172.16.1.254 (lembre-se: tratam-se dos valores compreendidos entre o valor da sub-rede [ex. 172.16.1.0] e o valor do endereço de broadcast [172.16 .1.255])

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Sub-redes (Subnetting)

O método alternativo: sub-redes de classe B:

Criando sub-redes de cabeça

Exemplo:

Dados o endereço e máscara de rede abaixo, determine à que sub-rede o mesmo pertence, qual o intervalo válido de hosts e qual o endereço de broadcast.

- **172.16.10.33 = Endereço de rede**
- **255.255.255.224 = Máscara de rede**

172.16.**10.33** = Endereço de rede

255.255.**255.224** = Máscara de rede

Primeiramente, determine a sub-rede e endereço de broadcast do endereço de rede acima (172.16.10.33). Isso pode ser feito respondendo-se à questão 3 das 5 questões colocadas na página 29:

256 - **224** = **32**.

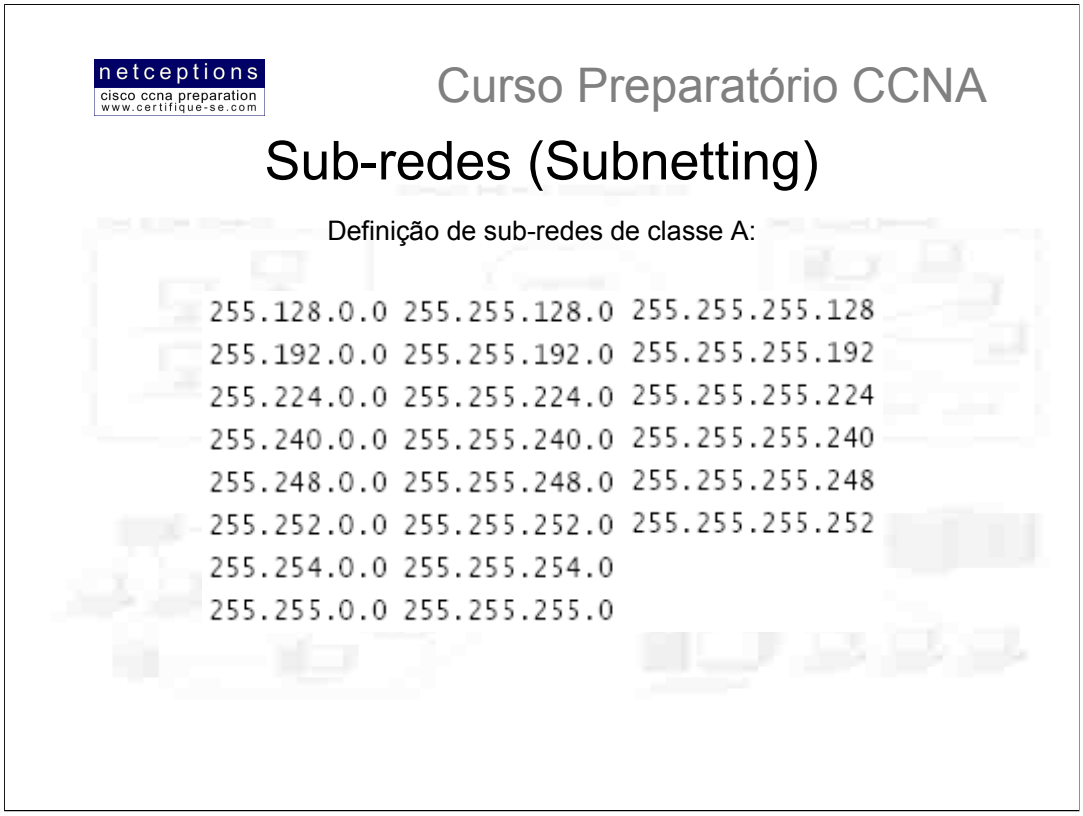
32 + 32 = **64**.

O endereço encontra-se entre as 2 sub-redes e, portanto, deve ser parte da sub-rede **32**. Entretanto, recorde-se que o terceiro octeto é tido como parte da sub-rede, portanto, a resposta seria a sub-rede **10.32**.

A próxima sub-rede seria a **10.64**, portanto, o endereço de broadcast dessa sub-rede é o **10.63**.

O intervalo válido de hosts seria, para este caso, **10.33-10.62.**

Mais uma vez o problema foi resolvido mental e rapidamente.



O método para se definir sub-redes de classe A em nada difere do utilizado na definição de sub-redes de classes C e B, porém, temos agora 24 bits para manipulação de endereços de sub-redes, e apenas 8 bits para manipulação de hosts. Na tabela acima encontram-se listadas todas as sub-redes de classe A possíveis.

Recorde-se de deixar ao menos 2 bits para definição de hosts. Isso é mandatório.

Exemplo: Máscara de rede **255.255**.0.0

Endereços de classe A utilizam a máscara padrão 255.0.0.0, o que deixa 22 bits para definição de sub-redes, uma vez que deve-se deixar ao menos 2 bits para definição de hosts. A máscara 255.255.0.0 aplicada a um endereço de classe A utiliza 8 bits para definição de sub-redes. Portanto:

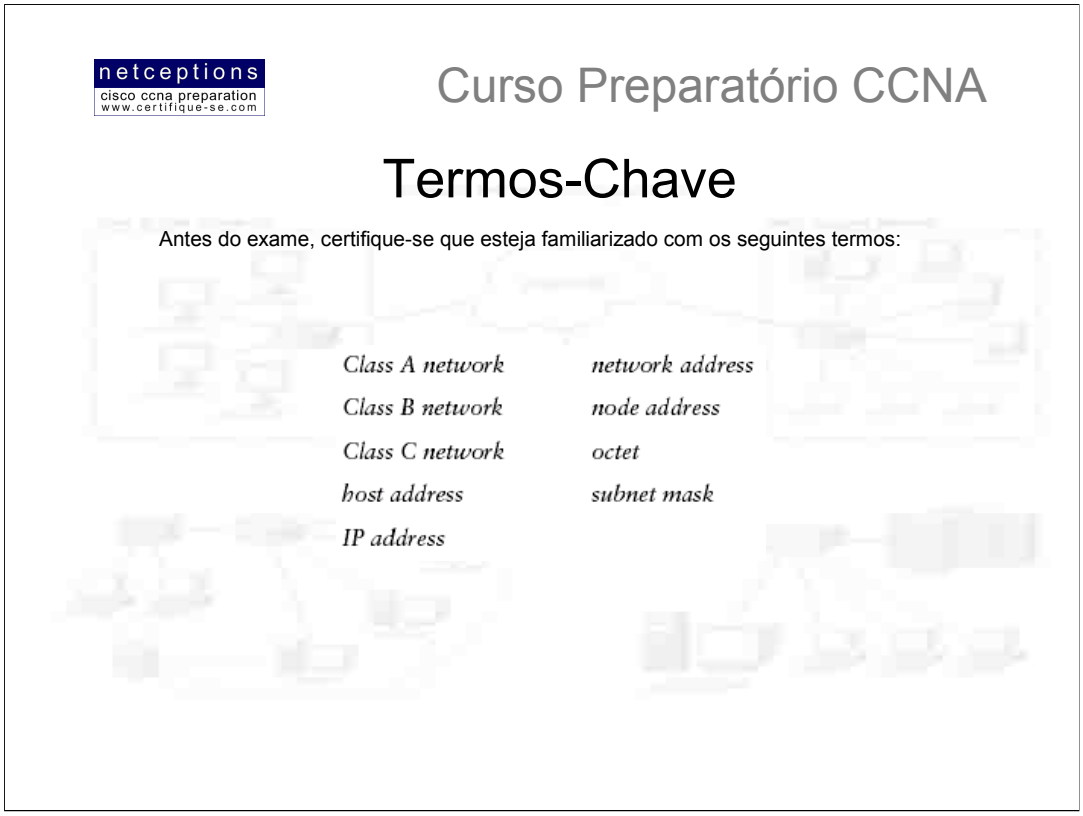
1) Número de sub-redes: $2^8 - 2 = 254$

2) Número de hosts: $2^{16} - 2 = 65.534$

3) Sub-redes válidas: 256 - 255 = 1, 2, 3, 4, etc. (todas definidas no segundo octeto!), ou seja, as sub-redes seriam: 10.1.0.0, 10.2.0.0, 10.3.0.0, 10.4.0.0, ..., 10.254.0.0.

4) Endereço de broadcast para cada sub-rede: 10.1.255.255, 10.2.255.255, etc.

5) Intervalo válido de hosts para cada sub-rede: 10.1.0.1 - 10.1.255.254 (lembre-se: tratam-se dos valores compreendidos entre o valor da sub-rede [ex. 10.1.0.0] e o valor do endereço de broadcast [10.1.255.255])



Resumo

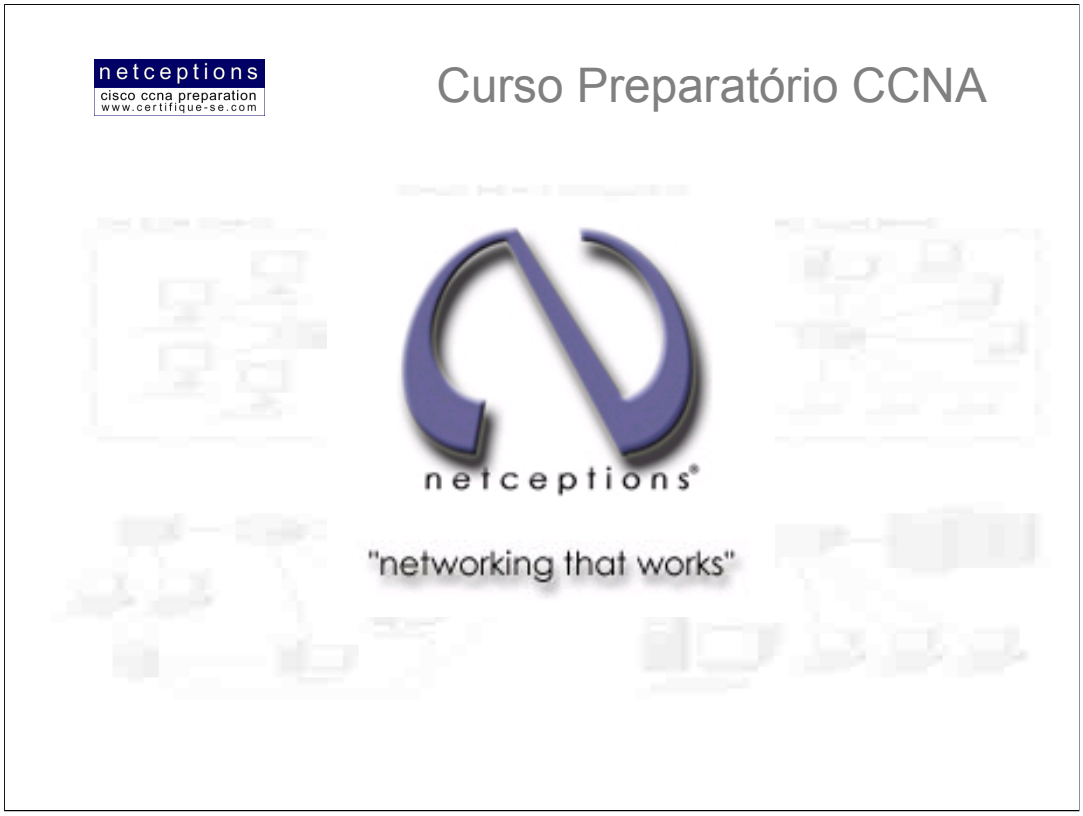
Esse é um dos módulos de maior importância dentro de nosso curso, e deve ser compreendido profundamente. Pratique a criação e determinação de sub-redes o máximo que puder. Isso é importante não apenas para a prova, em si, mas também para seu futuro como um bom profissional de redes.

Nesse módulo discutimos à fundo o protocolo IP, assim como técnicas de subnetting para as classes A, B e C.

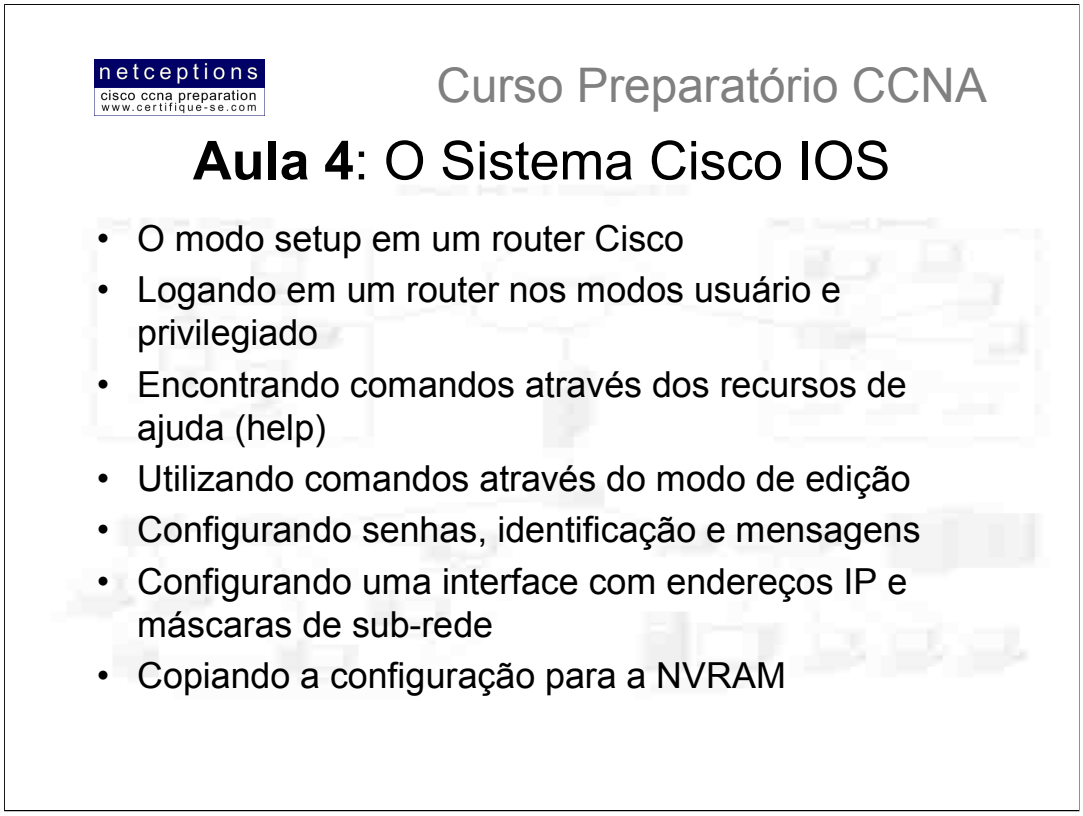
netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

FIM AULA 03



Apostila Aula 4



Nesta aula introduziremos o Cisco Internetwork Operating System (Cisco IOS). O IOS é o sistema que gerencia os roteadores Cisco (e também alguns switches, como os da linha Catalyst), estabelecendo uma interface baseada em linhas de comando (CLI - Command Line Interface) que permite a configuração dos mesmos. Os detalhes cobertos nessa aula incluem os seguintes:

- Entendimento e configuração do sistema Cisco IOS
- Conexão à um router
- Inicialização de um router
- O processo de login
- Entendimento dos prompts de router
- Entendimento dos prompts do CLI (interface de comando)
- Entendimento de funções de edição e ajuda
- Estabelecimento de senhas para o roteador
- Criação de “banners”
- Configuração de interfaces
- Estabelecimento de hostname para o roteador

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

O Sistema Cisco IOS

Funções:

- Transportar funções e protocolos de rede;
- Estabelecer tráfego de alta velocidade entre dispositivos;
- Disponibilizar ferramentas de segurança para controle de acesso e bloqueio de usuários não autorizados;
- Prover escalabilidade para facilitar o crescimento da rede e redundância;
- Prover confiabilidade para conexão à recursos da rede

O Cisco IOS é o núcleo dos roteadores e grande parte dos switches da Cisco.Quase que a totalidade dos roteadores Cisco rodam o IOS (apenas alguns modelos mais antigos não o fazem), entretanto, apenas metade dos switches o rodam.

O IOS foi criado para transportar serviços de rede e disponibilizar aplicações voltadas à rede. O sistema IOS é utilizado para implementar as seguintes funções em um hardware Cisco:

• Transportar funções e protocolos de rede;

• Estabelecer tráfego de alta velocidade entre dispositivos;

• Disponibilizar ferramentas de segurança para controle de acesso e bloqueio de usuários não autorizados;

• Prover escalabilidade para facilitar o crescimento da rede e redundância;

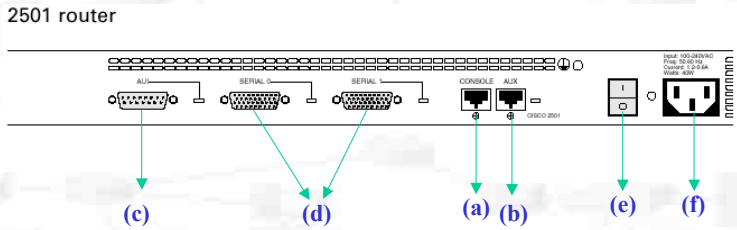
• Prover confiabilidade para conexão à recursos da rede

O sistema IOS pode ser acessado através da porta de console de um roteador, através de um modem, ou mesmo via Telnet. O acesso ao sistema IOS via linhas de comando é conhecido como uma sessão EXEC (EXEC session).

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

O Sistema Cisco IOS



Você pode se conectar a um router Cisco para configura-lo, verificar sua configuração, e checar estatísticas. Existem diferentes maneiras de se conectar a um router Cisco, sendo a mais comum através da porta Console **(a)**.

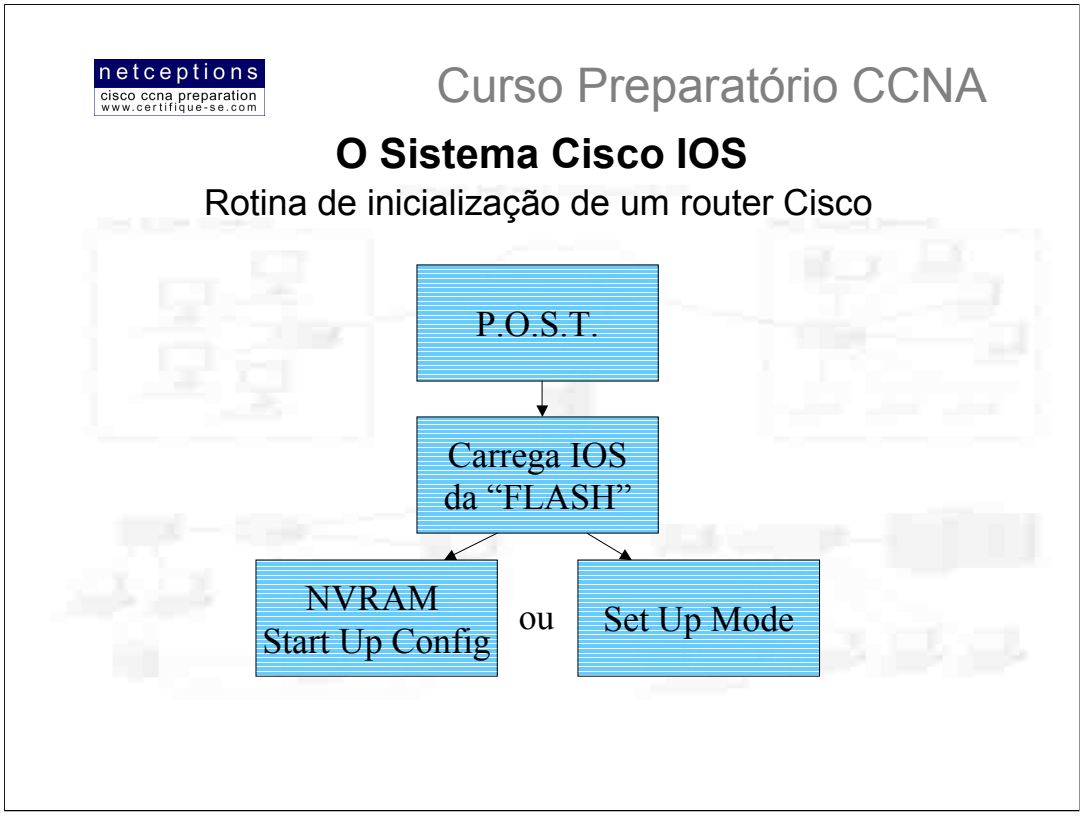
A porta Console usualmente é uma conexão RJ-45 na parte traseira do router (figura). Não há senha pré-estabelecida para esta porta, como default.

Outro modo de se conectar a um router Cisco é através de uma porta Auxiliar (Auxiliary port) **(b)**. Esta porta funciona como uma porta Console, e pode ser utilizada como tal. Entretanto, esta porta permite que sejam configurados comandos de modem, para que um acesso discado (via modem) possa ser realizado. Isso significa que você pode discar para o modem conectado à porta Auxiliar do router e configura-lo remotamente, muito útil em casos onde portas locais do router estão “down”.

O terceiro modo de se conectar a um router é através de um programa Telnet. Telnet é um programa emulador que emula um “terminal-burro”. Você pode utilizar Telnet para se conectar à qualquer porta ativa de um router, seja ela serial, Ethernet, ou qualquer outra porta de comunicação ativa.

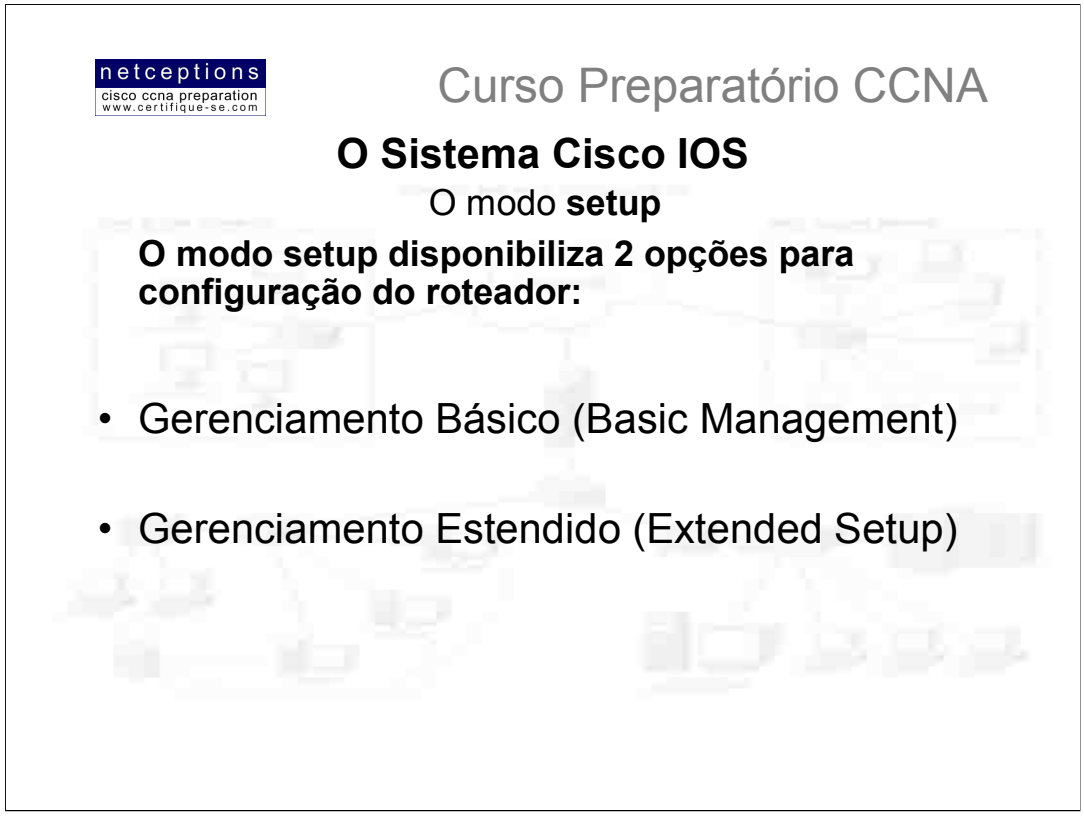
Na figura, ilustramos um router da série 2500 (um 2501). Note que esse router possui 2 portas seriais **(d)** - serial 0 e serial 1. Note também a existência de uma porta AIU (Attachment Unit Interface) **(c)**, que oferece uma conexão Ethernet a 10 Mbps.

Vemos também o interruptor de força **(e)** e a conexão do cabo de força **(f)**.



Quando você liga um router Cisco pela primeira vez, ele executa uma checagem geral do hardware chamada POST (Power On Self Test) e, se passar ele irá procurar e carregar o sistema IOS da memória FLASH, se o arquivo estiver presente. A memória FLASH é um tipo de memória eletronicamente deletável, programável e acessível apenas para leitura (Erasable Programmable Read-Only Memory = EEPROM). O IOS será carregado e então ele procurará por um arquivo de configuração chamado startup-config, que fica armazenado por default na memória RAM não volátil (NVRAM).

Caso não exista nenhum arquivo de configuração na NVRAM (ex. router novo ou o arquivo foi deletado), o router irá trazer então o que chamamos de *setup mode* (vide ilustração). Este seria um modo que permite a configuração do router passo-a-passo. Você pode optar pela configuração via linha de comando a qualquer momento digitando o comando **setup** no modo de configuração global (global configuration mode). O modo setup cobre apenas alguns comandos genéricos, mas é bastante útil quando você não sabe como configurar determinados protocolos, como bridging ou DCnet, por exemplo.



Você tem a sua disposição 2 escolhas quando utiliza o modo setup: Gerenciamento Básico - bastante limitado, e setup estendido. O modo básico permite apenas configurações para conectividade básica do router. Já o modo estendido permite que se configure parâmetros globais, assim como parâmetros de interface, oferecendo um maior controle sobre o hardware (router).

Na próxima página veremos um exemplo da interface do modo setup.

Nota: Repare na configuração à seguir que o modo setup configura 2 senhas (passwords). Falaremos de senhas mais adiante, porém, é necessário que se entenda que, na verdade, apenas uma senha é importante: **enable secret password**

A outra senha (**enable password**) era utilizada em routers com sistema IOS pré-10.3. Entretanto, o modo setup exige que ambas sejam configuradas. E elas precisam ser distintas. A **enable password** NUNCA será usada se a **enable secret password** estiver configurada no router.

A próxima senha é utilizada para sessões Telnet com o router. A razão pela qual o modo setup configura uma senha Telnet (VTY) é porque se uma senha para as linhas VTY (Telnet) não for configurada, você não pode, por default, conectar-se ao um router via Telnet.

Mais uma vez: falaremos em detalhes sobre senhas mais adiante.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

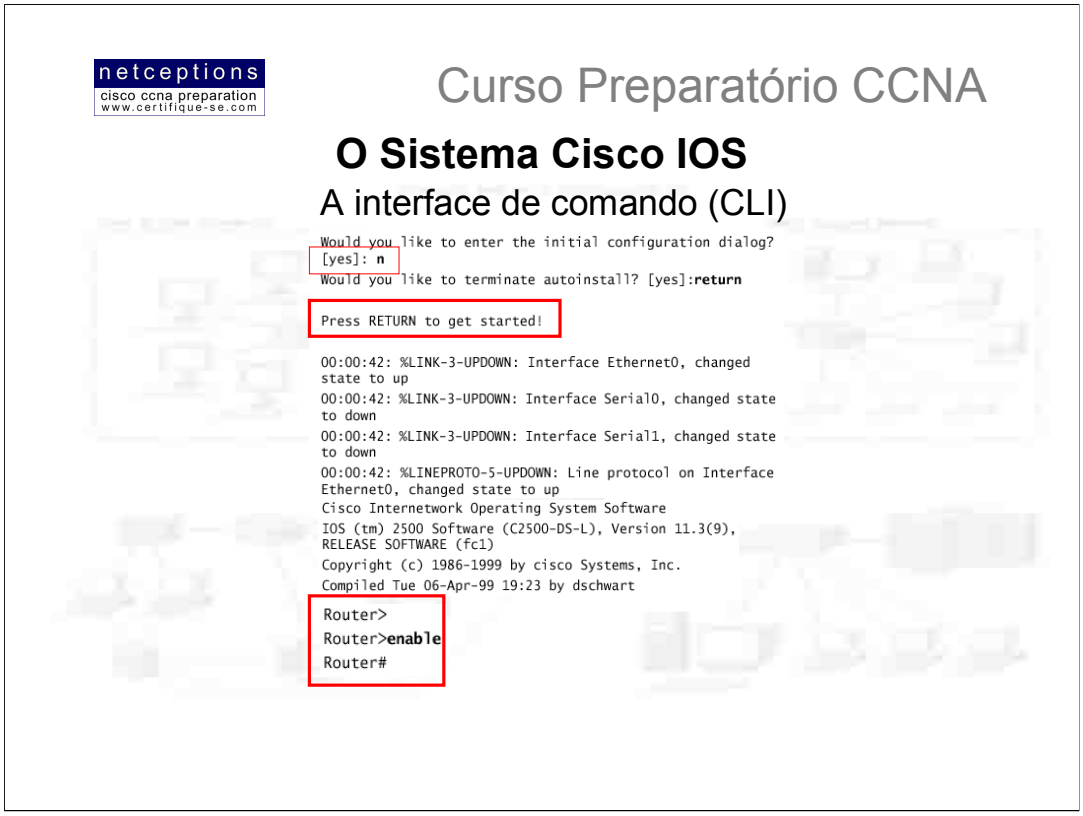
```
---System Configuration Dialog ---
Would you like to enter the initial configuration dialog?
[yes/no ]:y
At any point you may enter a question mark '?'for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
Would you like to enter basic management setup?
[yes/no ]:n
First,would you like to see the current interface summary?
[yes ]:return
Any interface listed with OK?value "NO"does not have a
valid configuration
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 unassigned NO unset up up
FastEthernet0/1 unassigned NO unset up up
Configuring global parameters:
Enter host name [Router ]:Todd
The enable secret is a password used to protect access to
privileged EXEC and configuration modes.This password,
after entered,becomes encrypted in the configuration.
Enter enable secret:todd
The enable password is used when you do not specify an
enable secret password,with some older software
versions,and some boot images.
Enter enable password:todd
%Please choose a password that is different from the
enable secret
Enter enable password:todd1
The virtual terminal password is used to protect
access to the router over a network interface.
Enter virtual terminal password:todd
Configure SNMP Network Management?[yes ]:enter or no
Community string [public ]:enter
Configure DECnet?[no ]:enter
Configure AppleTalk?[no ]:enter
Configure IP?[yes ]:enter
Configure IGRP routing?[yes ]:n
Configure RIP routing?[no ]:enter
Configure bridging?[no ]:enter
Configure IPX?[no ]:enter
Async lines accept incoming modems calls.If you will have
users dialing in via modems,configure these lines.
Configure Async lines?[yes ]:n

BRI interface needs isdn switch-type to be configured
Valid switch types are:
[0 ] none.....Only if you don't want to configure
BRI.
[1 ] basic--1tr6....1TR6 switch type for Germany
[2 ] basic--5ess....AT&T 5ESS switch type for the US/Canada
[3 ] basic--dms100..Northern DMS-100 switch type for US/
Canada
[4 ] basic--net3....NET3 switch type for UK and Europe
[5 ] basic--ni......National ISDN switch type
[6 ] basic--ts013...TS013 switch type for Australia
[7 ] ntt.............NTT switch type for Japan
[8 ] vn3.............VN3 and VN4 switch types for France
Choose ISDN BRI Switch Type [2 ]:2
Configuring interface parameters:
Do you want to configure FastEthernet0/0 interface?
[yes ]:return
Use the 100 Base-TX (RJ-45)connector?[yes ]:return
Operate in full-duplex mode?[no ]:y and return
Configure IP on this interface?[yes ]:return
IP address for this interface:1.1.1.1
Subnet mask for this interface [255.0.0.0 ] ::
255.255.0.0
Class A network is 1.0.0.0,16 subnet bits;mask is /
16
Do you want to configure FastEthernet0/1 interface?
[yes ]:return
Use the 100 Base-TX (RJ-45)connector?[yes ]:return
Operate in full-duplex mode?[no ]:y and return
Configure IP on this interface?[yes ]:return
IP address for this interface:2.2.2.2
Subnet mask for this interface [255.0.0.0 ] ::
255.255.0.0
Class A network is 2.0.0.0,16 subnet bits;mask is /
16
```

A configuração ilustrada acima é deveras simplista, mas já é o suficiente para inicializar e configurar um router de modo muito rápido.

Note que a máscara de rede é apresentada no formato /16, o que significa que 16 de 32 bits estão sendo usados para definição de sub-redes. No próximo passo, o gerenciamento estendido produziria a configuração (running-config) criada, ilustrada à direita: Uma parte interessante do gerenciamento estendido é a opção que você recebe no final. Você pode ir para o modo CLI (linha de comando) e descartar o running-config [0], pode voltar ao setup e repetir o processo [1], ou pode salvar a configuração criada na NVRAM, que é conhecida como startup-config. Esse arquivo será então carregado toda vez que o router for inicializado. No nosso caso, a opção [0] (descartar configuração e entrar no modo CLI) foi escolhida.

```
Hostname Todd
enable secret 5 $1$B0wu$5F0m/EDdtRkQ4vy4a8qwC/
enable password todd1
line vty 0 4
password todd
snmp-server community public
!
no decnet routing
no appletalk routing
ip routing
no bridge 1
no ipx routing
!
interface FastEthernet0/0
media-type 100BaseX
full-duplex
ip address 1.1.1.1 255.255.0.0
no mop enabled
!
interface FastEthernet0/1
media-type 100BaseX
half-duplex
ip address 2.2.2.2 255.255.0.0
no mop enabled
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
end
[0 ] Go to the IOS command prompt without saving
this
config.
[1 ] Return back to the setup without saving this
config..
[2 ] Save this configuration to nvram and exit..
Enter your selection [2 ]:0
```



A interface de linha de comando (CLI = Command Line Interface) é sem dúvida o melhor modo de se configurar um router, uma vez que lhe oferece uma gama de opções muito mais variada e um maior poder de customização. Para entrar na interface de comando, simplesmente escolha NO para entrada de diálogo inicial (vide ilustração). Após esse passo, o router irá lhe mostrar mensagens com informações sobre todas as interfaces disponíveis no mesmo.

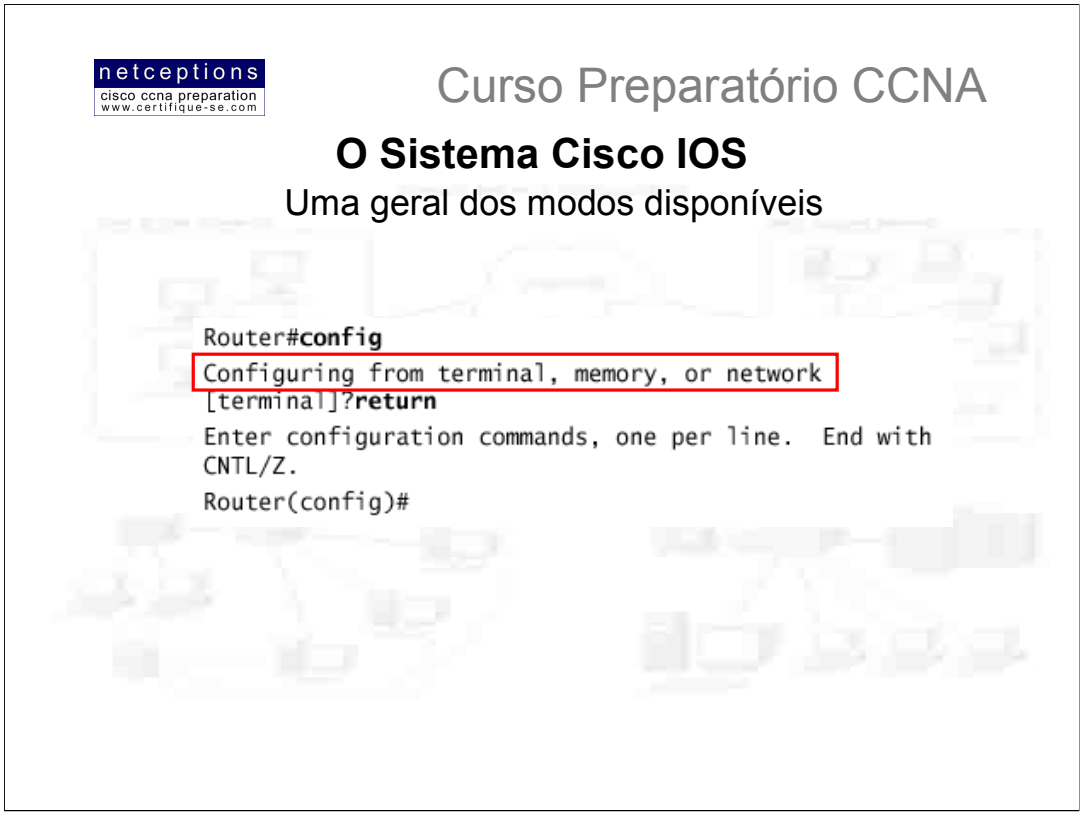
Conectando-se (logging into) à um router

Após a apresentação do status das interfaces e você ter pressionado <ENTER>, um prompt aparecerá (similar à um prompt do DOS - veja ilustração acima). Você encontra-se no que chamamos de modo usuário (user mode). Você apenas pode alterar ou criar configurações em um router se estiver logado em **modo privilegiado (privileged mode).** Para entrar em modo privilegiado, digite **`enable`** no prompt do modo usuário (**`router>enable`**). Ao entrar com esse comando e teclar <ENTER>, o prompt se altera para um sinal **#** (**`router#`**). Você deve lembrar-se disso:

Prompt	Modo
>	Usuário
#	Privilegiado

É importante saber diferenciar em que modo você está entrando os comandos em um router. E o exame CCNA sabe disso, e irá testar seus conhecimentos neste ponto. Uma vez em modo privilegiado, você pode digitar **`router#disable`** para retornar ao modo usuário. Uma vez no modo usuário, digitando-se **`router>logout`** ou **`router>exit`** você encerra a sessão.

Para tornar a vida dos administradores de rede mais fácil, o IOS aceita abreviações para alguns comandos, por exemplo, **enable** pode ser digitado apenas **`en.`**



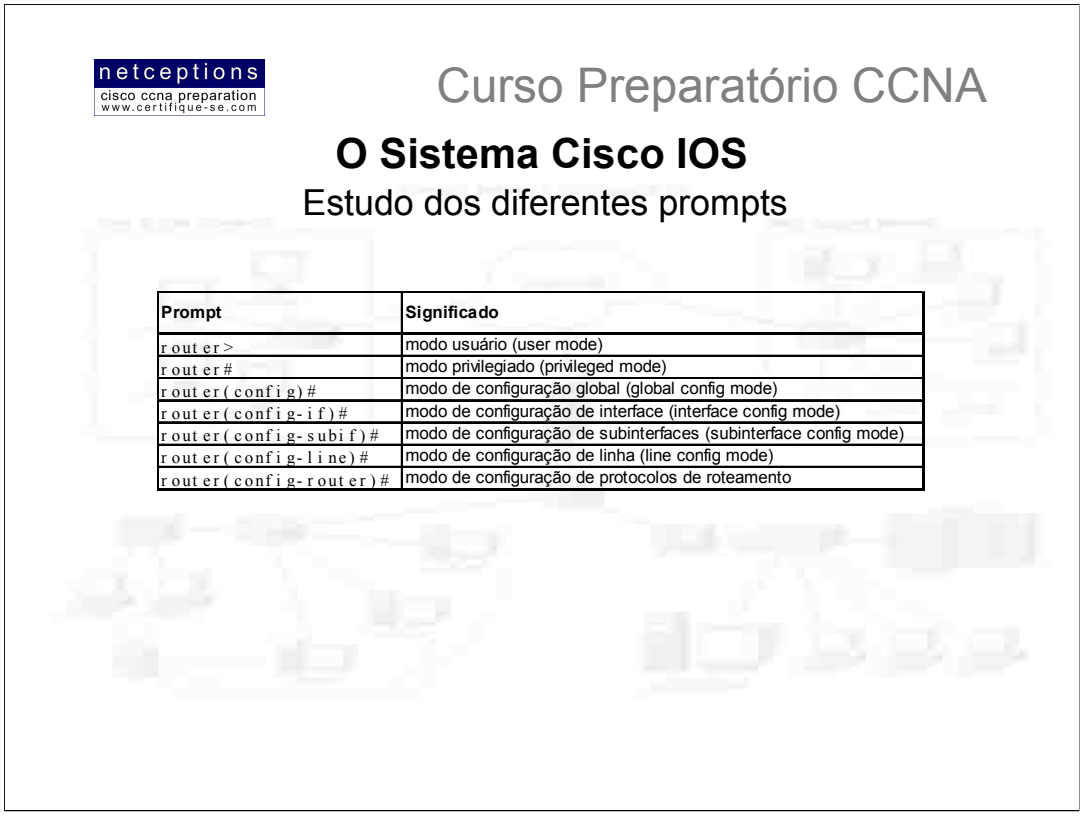
No modo de configuração CLI, você pode efetuar configurações globais no router digitando **`#config terminal (#config t)`**, o que o colocará em modo de configuração global (global configuration mode), e possibilitará mudanças ao que chamamos de running-config (configuração armazenada na DRAM). À partir deste ponto, todas as configurações afetarão o router como um todo. Na ilustração acima, notamos que, digitando apenas **`#config`** o router nos mostra algumas opções, sendo terminal a default.

Para alterar configurações armazenadas na DRAM (running-config), utilizamos a opção **`terminal`**. Para efetuar alterações nas configurações armazenadas na NVRAM (startup-config), utilizamos a opção **`memory (ou mem)`**. Finalmente, se você desejar alterar um arquivo de configuração armazenado em um servidor TFTP, você optaria pela opção **`network (ou net).`** Portanto, se você digitar **`#config-mem`** ou **`#config-net`** você estará, de fato, substituindo sua running-config atual por uma armazenada na NVRAM (mem) ou em um servidor TFTP (net). **É importantíssimo lembrar-se disso!**

Diferentes prompts do CLI

Como foi anteriormente mencionado, é de extrema importância que se entenda os diferentes tipos de prompts que existem no sistema IOS, assim você pode saber exatamente onde esta quando estiver configurando um router. SEMPRE CHEQUE OS PROMPTS ANTES DE EFETUAR UMA CONFIGURAÇÃO!

Descreveremos brevemente todos os prompts com os quais você se deparará ao decorrer dos próximos tópicos.



Prompt	Significado
router>	modo usuário (user mode)
router#	modo privilegiado (privileged mode)
router(config)#	modo de configuração global (global config mode)
router(config-if)#	modo de configuração de interface (interface config mode)
router(config-subif)#	modo de configuração de subinterfaces (subinterface config mode)
router(config-line)#	modo de configuração de linha (line config mode)
router(config-router)#	modo de configuração de protocolos de roteamento

Prompt de interfaces

Note, na figura acima (destaque), que logo após digitarmos o comando **`#interface`**, digitamos um ponto de interrogação (?). Isso é parte do sistema de ajuda do IOS. Observe que o IOS trás todas as interfaces disponíveis no router em questão, facilitando o próximo passo do comando. Basta identificar a interface desejada e adicioná-la ao comando (ex. **`#interface FastEthernet0/0`** ou, simplesmente, **`#int f0/0`**). Note que o prompt mudará para **`(config-if)#,`** indicando que você se encontra agora no modo de configuração de interface.

O sistema IOS NÃO indica em qual interface você está trabalhando, o que pode tornar sua vida mais complicada se você não souber onde exatamente você está. Um modo simples de contornar essa situação e tomando-se nota de cada ação que você tomar. Isso pode evitar um retrabalho posterior, ou mesmo a configuração errônea de uma interface.

Prompt de subinterfaces

O recurso de subinterfaces permite que você crie uma enorme gama de interfaces virtuais em um router. O prompt mudaria então para **`(config-subif)#`** nesse modo. Falaremos mais a fundo sobre subinterfaces mais adiante. Por hora, concentre-se no prompt, apenas.

```
Router(config)#int f0/0.?
  <0-4294967295>  FastEthernet interface number
Router(config)#int f0/0.1
Router(config-subif)#
```

Prompt de comandos de linha (line commands)

Para configuração de senhas de modo usuário, utilize o comando line no modo de configuração global. No exemplo abaixo, o comando **`(config)#line console 0`** é tido como um comando maioral, ou global, e qualquer comando digitado à partir do prompt **`(config-line)#`** é tido como um sub-comando.

```
Router#config t
Enter configuration commands, one per line.  End with
CNTL/Z.
Router(config)#line ?
  <0-70>   First Line number
  aux      Auxiliary line
  console  Primary terminal line
  tty      Terminal controller
  vty      Virtual terminal

Router(config)#line console 0
Router(config-line)#
```

E, finalmente, para configuração de protocolos de roteamento como RIP ou IGRP, o prompt seria **`(config-router)#`**

Recursos de ajuda

Você pode se utilizar dos recursos de ajuda para auxiliá-lo na configuração de um router. Utilizando um ponto de interrogação (?) em qualquer prompt (e em qualquer modo) você obtém uma lista dos comandos disponíveis para aquele prompt.

Para localizar comandos que começam com uma determinada letra, utilize a letra seguida de um ponto de interrogação (?), como no exemplo abaixo:

```
Router#c?
clear  clock  configure  connect  copy
```

Para determinar o próximo comando em uma string, digite primeiro o comando e, em seguida um espaço e um ponto de interrogação (?), como no exemplo abaixo:

```
Router#clock ?
  set  Set the time and date

Router#clock set ?
  hh:mm:ss  Current Time
```

Se acontecer de você receber um erro "`% Incomplete command`", você saberá que a linha de comando digitada não está completa. Algo esta faltando. Utilize o recurso acima para determinação do comando faltante. Outras mensagens de erro comuns são:

```
Router(config)#access-list 110 permit host 1.1.1.1
                                           ^
% Invalid input detected at '^' marker.
```

```
Router#sh te
% Ambiguous command:  "sh te"
```

O primeiro dos erros acima aponta que após a marca "^" um comando inválido ou inexistente foi digitado. À partir deste ponto, utilize o recurso de ajuda para auxiliá-lo na identificação do comando apropriado. No segundo caso, utilize o ponto de interrogação imediatamente após o comando digitado para que lhe seja apresentada uma lista com as opções de comando válidas.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

O Sistema Cisco IOS

Comandos de edição avançados

Comando	Função
Ctrl+A	Move o cursor para o início da linha
Ctrl+E	Move o cursor para o final da linha
Esc+B	Move o cursor uma palavra para trás
Ctrl+F	Move o cursor um caracter para frente
Esc+F	Move o cursor uma palavra para frente
Ctrl+D	Deleta um único caracter
Backspace	Deleta um único caracter
Ctrl+R	Reapresenta uma linha
Ctrl+U	Deleta uma linha
Ctrl+W	Deleta uma palavra
Ctrl+Z	Finaliza o modo de configuração e retorna ao modo EXEC
Tab	Completa a digitação de um comando
Ctrl+P	Apresenta o último comando digitado
Ctrl+N ou seta p/ baixo	Apresenta o comando previamente digitado
Show history	Apresenta os últimos 10 comandos digitados (default)
Show terminal	Apresenta configurações do terminal e tamanho do buffer do history
Terminal history size	Altera o tamanho do buffer (máximo = 256)

A tabela acima ilustra os comandos de edição avançada que o IOS utiliza.

Outro recurso de edição que deve ser mencionado é o rolamento automático de linhas longas. No exemplo abaixo, o comando digitado atingiu a margem direita e foi, automaticamente, movido 10 espaços para a esquerda. O sinal $ indica que a linha foi rolada para a esquerda.

```
Router#config t
Enter configuration commands, one per line.  End with
CNTL/Z.
Router(config)#$ l10 permit host 171.10.10.10 0.0.0.0 host
```

Você pode rever o histórico de comandos digitados no router através do comando **`show history`**, ilustrado na tabela acima.

É de extrema importância o entendimento, prática e memorização da tabela acima. Por mais desnecessária que a mesma possa parecer, o exame CCNA irá testar seus conhecimentos nos comandos apresentados.

Abaixo, um exemplo de saída do comando **`show history`** :

```
Router#sh history
  en
  sh history
  show terminal
  sh cdp neig
  sh ver
  sh flash
  sh int e0
  sh history
  sh int s0
  sh int s1
```

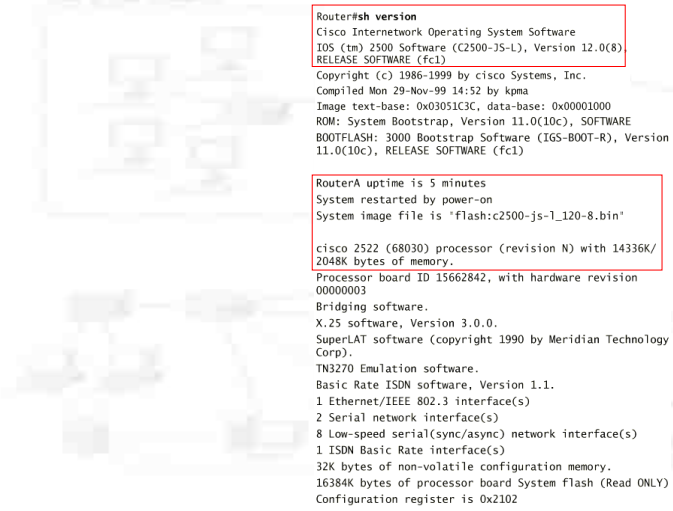
O comando **`show terminal`** é utilizado para verificação do tamanho do histórico do terminal. O default é o tamanho de 10, ou seja, os 10 últimos comandos são apresentados ao se digitar o comando **`show history`**. Esse valor pode ser alterado através do comando **`terminal history size xxx`** – digitado no modo privilegiado, onde "**`xxx`**" pode ser um número compreendido entre 0 à 256.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

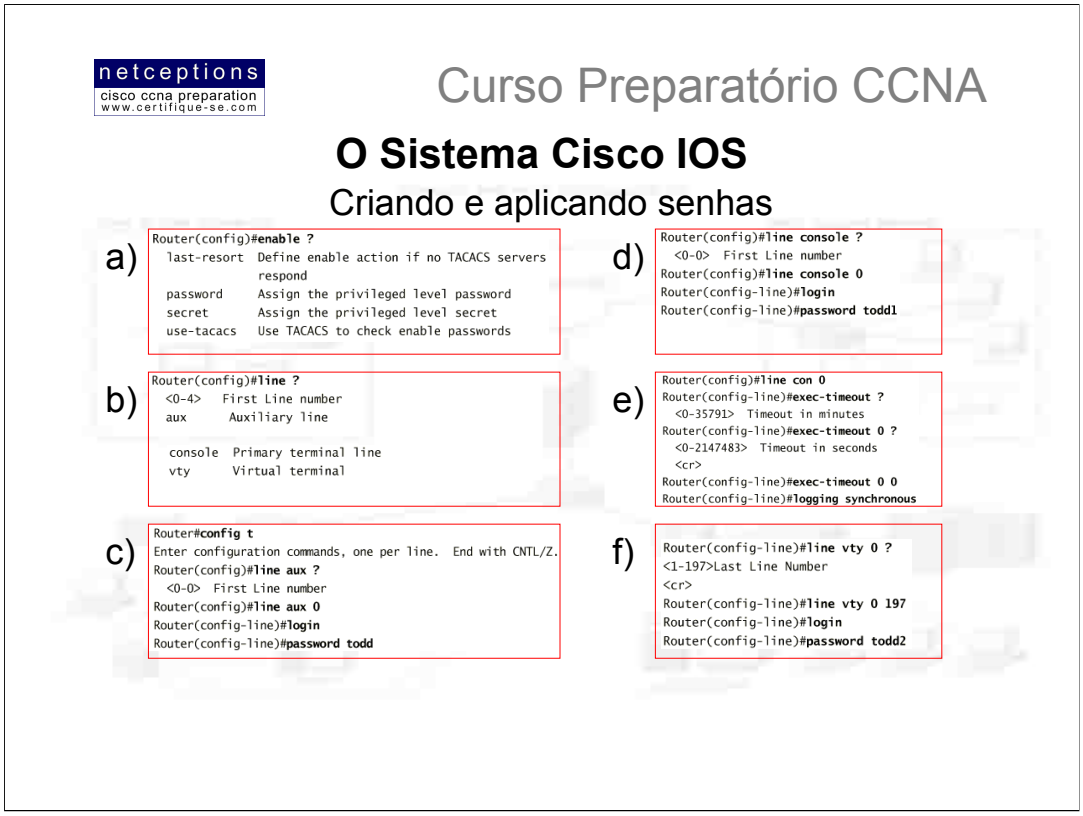
O Sistema Cisco IOS

Reunindo informações básicas sobre o router



O comando **`sh version`** é de extrema utilidade, sendo utilizado para se obter as seguintes informações, dentre outras (a figura acima ilustra uma saída real deste comando):

- Versão do sistema IOS em uso;
- Tempo em que o router esta ligado;
- Nome da imagem flash em uso;
- Modelo e configuração física do router em uso;
- Listagem das interfaces disponíveis;
- Tamanho da NVRAM;
- Tamanho da FLASH;
- Configuração do registro (register). Default = 0x2102;



Existem 5 tipos de senhas que podem ser criadas e aplicadas para segurança de routers Cisco. As 2 primeiras são utilizadas para restringir acesso ao modo privilegiado (enable). Assim sendo, uma vez aplicadas, uma senha será pedida toda vez que o comando **`enable`** for digitado no modo usuário.As outras 3 são utilizadas para restringir acessos ao router através das portas de console, auxiliar ou Telnet.

a) Senhas em modo privilegiado (enable passwords)

Devem ser configuradas em modo privilegiado. As seguintes opções são disponibilizadas:

Last-resort – Deve ser utilizada se a autenticação é feita através de um servidor TACACS. Apenas é utilizada se o servidor TACACS estiver com problemas. Caso esteja OK, não é utilizada.

Password – Utilizada para configuração de senhas de modo privilegiado em routers rodando o sistema IOS versão anterior à 10.3. Não é utilizada caso a senha **`enable secret`** estiver configurada no router.

Secret – Senha criptografada, definida em modo privilegiado para restrição de acesso ao router

Use-tacacs – Direciona o router à efetuar o processo de autenticação através de um servidor TACACS. Muito conveniente se você dispõe de dezenas, ou mesmo centenas de routers. Imagine-se alterando a senha de 200 routers… Os servidores TACACS permitem que você altere a senha de vários routers de uma só vez.

Se você tentar configurar a senha enable e a senha enable secret como sendo a mesma, o router lhe apresentará uma mensagem um aviso. Caso você tente novamente inserir a mesma senha, o router aceitará, porém, nenhuma das senhas estará funcionando. Portanto, não se preocupe em configurar a senha enable, a não ser que você esteja utilizando um router antigo.

b) Senhas de modo usuário (line passwords)

Devem ser configuradas em modo privilegiado. As opções são ilustradas acima.

c) Senha auxiliar (auxiliary passwords)

Para configurar a senha auxiliar, você deve estar no modo de configuração global (global configuration mode) e, então, digitar o comando **`line aux ?`**. Note que você recebe apenas a alternativa 0-0, uma vez que há apenas uma porta auxiliar.

d) Senhas de console (console passwords)

Para configurar a senha de console, você também deve estar no modo de configuração global. Digite o comando **`line console ?`**. Note que você recebe apenas a alternativa 0-0, uma vez que há apenas uma porta auxiliar.

e) Outros comandos de console

Existem outros comandos importantes de se saber com relação às portas de console. O comando **`exec-timeout 0 0`** define o timeout para o modo EXEC do console para 0, ou seja, para não ocorrer o timeout. Se você quiser definir um timeout de 1 segundo, por exemplo, utilize o comando **`exec-timeout 0 1`**. Outro comando interessante é o **`logging synchronous`**. Deveria ser definido por default, mas não o é. O que ele faz é impedir que mensagens de console fiquem constantemente aparecendo em sua tela, interrompendo a entrada que você está tentando digitar. Isso faz com que a leitura de suas entradas sejam muito mais claras. Acima ilustramos esses comandos.

f) Senhas de Telnet (Telnet passwords)

Para configurar senhas para usuários terem acesso ao seu router via Telnet, utilize o comando line vty. Routers que não estejam rodando a versão Enterprise do Cisco IOS estão limitados à 5 portas Telnet <0-4>. Em nosso exemplo, o router dispõe de 198 portas Telnet <0-197>. A melhor maneira de se determinar a quantidade de portas Telnet disponíveis é utilizando o recurso de ajuda (?).

Se você tentar se logar à um router que não esteja com uma senha Telnet (VTY) configurada, você receberá uma mensagem de erro dizendo que que a conexão foi recusada pois a senha não foi definida ("connection refused because VTY password is not set"). Você pode configurar um router para que o mesmo aceite conexões Telnet mesmo que uma senha não se encontre definida através do comando **`no login`** (veja abaixo). Após os routers terem sido devidamente configurados com endereços IP, você pode se logar remotamente à um router através do aplicativo Telnet (basta ir ao prompt do DOS e digitar telnet e o IP do router-alvo, por exemplo).

```
Router(config-line)#line vty 0 197
Router(config-line)#no login
```

O processo de encriptação de senhas

Por default, apenas o comando **`enable secret`** encripta a senha. A encriptação de senhas de modo usuário deve ser efetuada manualmente. Note que você pode identificar todas as senhas menos a enable secret quando você digita o comando **`show running-config`** em um router:

```
Router#sh run
[output cut]
!
enable secret 5 $1$rFbM$8.aXocHg6yHrM/zzeNkAI.
enable password todd1
!
[output cut]
line con 0
 password todd1
 login
line aux 0
 password todd
 login
line vty 0 4
 password todd2
 login
line vty 5 197
 password todd2
 login
!
end
```

Para manualmente encriptar as senhas não criptografadas por default (user-passwords), utilize o comando **`service password-encryption.`** Abaixo ilustramos um exemplo de como proceder:

```
Router#config t
Enter configuration commands, one per line.  End with
CNTL/Z.
Router(config)#service password-encryption
Router(config)#enable password todd
Router(config)#line vty 0 197
Router(config-line)#login
Router(config-line)#password todd2
Router(config-line)#line con 0
Router(config-line)#login
Router(config-line)#password todd1
Router(config-line)#line aux 0
Router(config-line)#login
Router(config-line)#password todd
Router(config-line)#exit
Router(config)#no service password-encryption
Router(config)#^Z
```

Agora, ao digitar-se o comando **`show running-config`** você notará que as senhas enable e as senhas de linha (enable / line passwords) aparecem todas criptografadas.

Configurando “banners” em um router

Você pode configurar banners em um router para que, assim que um usuário se conecte neste determinado router, ou um administrador estabeleça uma sessão Telnet à esse router, por exemplo, um banner apresentará a informação que você deseja que eles vejam. Uma razão para configuração de banners em um router é a apresentação de avisos de segurança à usuários que se conectam à sua rede através desse router. Existem 4 diferentes tipos de banners disponíveis:

`exec, incoming, login` e **`motd`**

O banner motd (**m**essage **o**f **t**he **d**ay - “mensagem do dia”) é o mais utilizado e apresenta uma mensagem à todos que se conectem ao router, não importando o caminho. O modo para configurá-lo é exemplificado abaixo:

```
Router(config)#banner motd ?
  LINE  c banner-text c, where 'c' is a delimiting
character
Router(config)#banner motd #
Enter TEXT message.  End with the character '#'.
$ized to be in Acme.com network, then you must disconnect
immediately.
#
Router(config)#^Z
Router#
00:25:12: %SYS-5-CONFIG_I: Configured from console by
console
Router#exit
```

O resultado, para quem se conectar à esse router, seria o seguinte:

```
Router con0 is now available

Press RETURN to get started.

If you are not authorized to be in Acme.com network, then
you must disconnect immediately.

Router>
```

Note, em destaque, o caracter delimitador utilizado (#). Você pode utilizar qualquer caracter que deseje, desde que o mesmo não apareça na mensagem em si.

Os outros banners existentes (exec, incoming e login) possuem as seguintes funções:

`exec` - configuração de banner para ser apresentado quando um processo EXEC (como uma ativação de linha ou uma conexão entrante via Telnet) é criado.

`Incoming` - configuração de banners que são apresentados à usuários de Telnet reverso (reverse Telnet)

`login` - configuração de banner para ser apresentado à todos os terminais conectados. Esse banner é apresentado após o banner motd, mas antes dos prompts de login. Para desabilitar globalmente o banner login, você deve deletá-lo através do comando **`no banner login.`**

Configurando as interfaces de um router

A configuração de interfaces é uma das mais importantes configurações realizadas em um router. Sem interfaces devidamente configuradas, um router é inútil. Algumas das configurações utilizadas em uma interface tratam de endereços de rede, largura-de-banda, tipo de mídia de acesso, entre outros. Diferentes routers utilizam diferentes métodos para escolha das interfaces utilizadas, uma vez que suas configurações físicas variam de modelo para modelo, e de acordo com quais placas de expansão os mesmos possuem instaladas. Para determinar quais as interfaces disponíveis em seu router, utilize o ponto de interrogação (?): **`(config)#int ?`**

Uma vez descoberto quais as interfaces disponíveis, descubra quantas portas podem ser configuradas através do comando: **`(config)#int serial ?`** (exemplo interface serial).

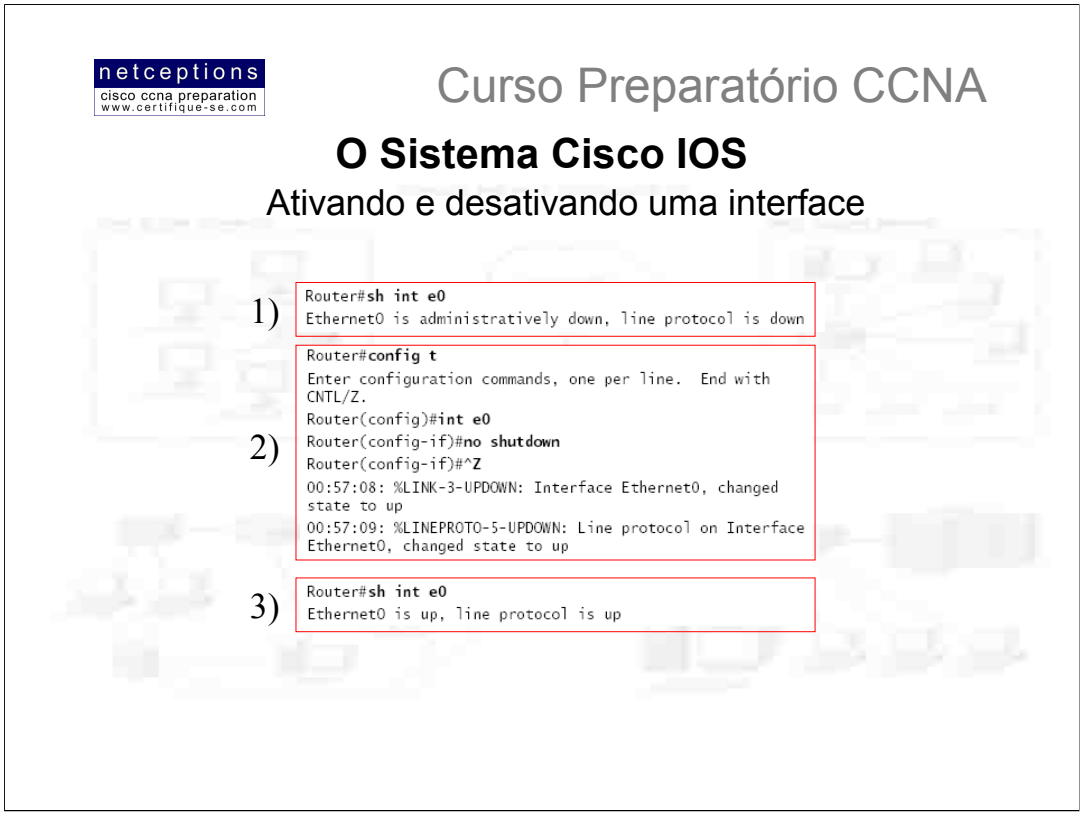
Dependendo do router que você irá configurar você irá se deparar com diferentes configurações de hardware. Por exemplo, O router modelo 2522 possui uma interface 10BaseT. A linha 2500 é uma linha fixa, ou seja, não permite que módulos sejam acoplados, expandindo sua funcionalidade. Já linhas mais high-end, como a 2600, são modulares, oferecendo uma maior flexibilidade. Séries modulares utilizam um slot físico no router e um número de porta no módulo plugado à esse slot. Por exemplo, em um router da linha 2600, a configuração de uma porta Fast Ethernet seria **`interface slot/porta:`**

```
Router(config)#int fastethernet ?
  <0-1>  FastEthernet interface number
Router(config)#int fastethernet 0
% Incomplete command.
Router(config)#int fastethernet 0?
/
Router(config)#int fastethernet 0/?
  <0-1>  FastEthernet interface number
```

Note que você NÃO PODE digitar **`int fastethernet 0`**. Você deve digitar o comando inteiro, incluindo os respectivos slot e porta. Você poderia digitar **`int fa 0/0`**, para abreviar.

Para definir o tipo de conector utilizado, utilize o comando **`(config-if)#media-type ? :`**

```
Router(config)#int fa 0/0
Router(config-if)#media-type ?
  100BaseX  Use RJ45 for -TX; SC FO for -FX
  MII       Use MII connector
```



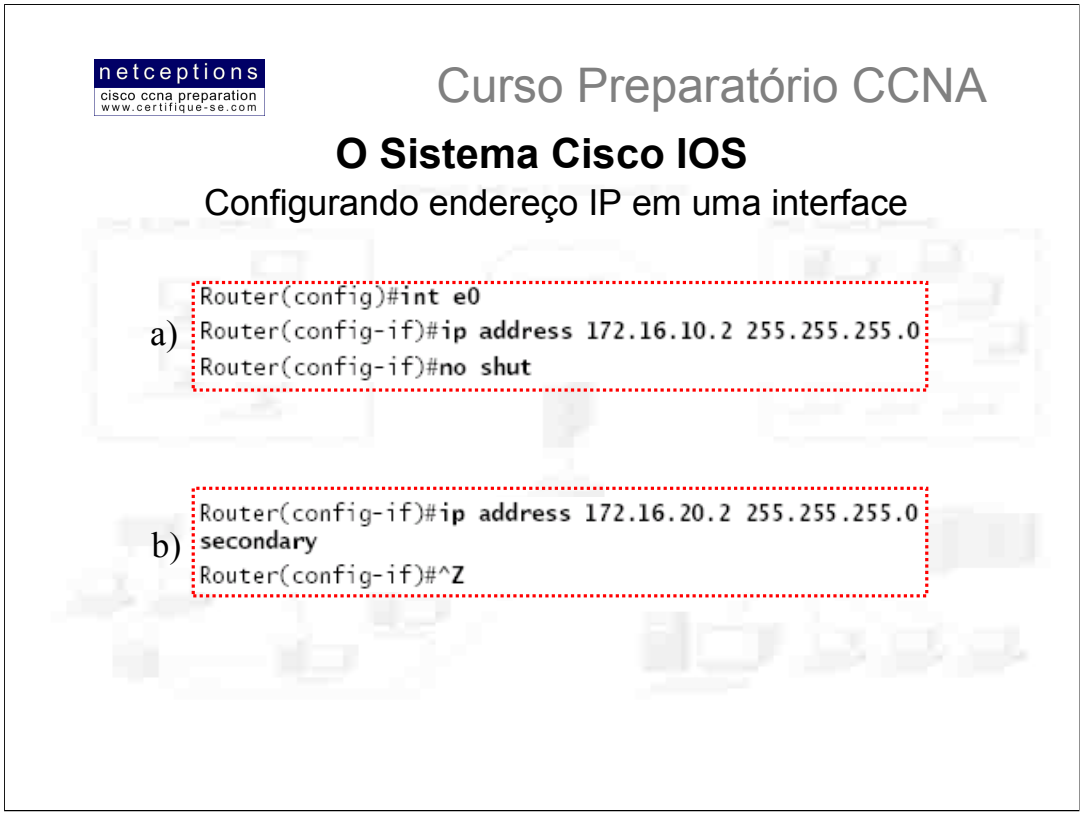
Ativando uma interface

Por default, todas as interfaces em um router encontram-se desativadas (shut down). Para se ativar uma interface, utilize o comando **`no shutdown`**. Para desativa la, simplesmente, **`shutdown`**.

Se uma interface estiver desativada, quando você digitar o comando **`show interface`** a mensagem **administratively down** será apresentada, indicando que a interface está desativada por opção do administrador, e não por problemas de hardware **(1).**

Utilizando o comando **`no shutdown`** **(2),** ativamos a interface em questão.

Finalmente, digitando o comando **`show interface`**, novamente, a mensagem apresentada será de que a interface e o protocolo de linha (line protocol) estão “up” (ativos) **(3)**, indicando que a interface em questão está funcional.

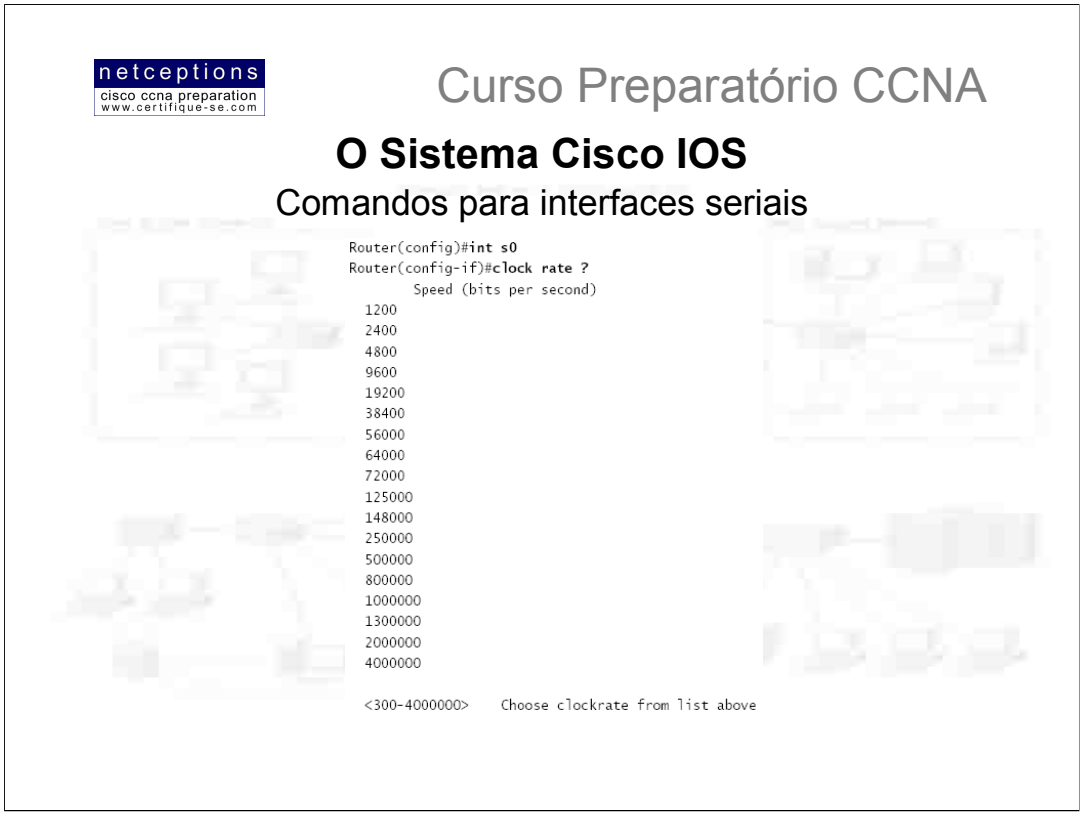


Você não é obrigado a utilizar endereços IP em seus routers, entretanto, IP é tipicamente utilizado em todos os routers. Para configurar endereços IP nas interfaces de um router, utilize o comando **`ip address`**, no modo de configuração de interface. Não se esqueça de digitar o comando **`no shut`**, para ativar a interface configurada **(a)**. Para verificar o status da interface, utilize os comandos **`show int`** ou **`show running-config`**. Ambos servem à esse propósito.

Se você desejar adicionar um segundo endereço IP (da mesma sub-rede) à uma mesma interface, então você deverá utilizar o comando **`secondary`**. Se você simplesmente digitar outro endereço IP e teclar <ENTER>, este irá substituir o endereço IP existente e sua máscara de rede. Para adicionar um endereço IP secundário, utilize, então , o comando **`secondary`** **(b)**.

Para verificar os endereços configurados na interface, utilize o comando **`show running-config`** (ou **`sh run`**, abreviando…):

```
Router#sh run
Building configuration...
Current configuration:
[output cut]
!
interface Ethernet0
 ip address 172.16.20.2 255.255.255.0 secondary
 ip address 172.16.10.2 255.255.255.0
!
```



Cartões VIP (VIP cards)

Se você se deparar com um router das séries 7000 ou 7500 com cartões VIP (Versatile Interface processor) instalados, você deve definir uma interface através da seguinte sintaxe de comando: **`interface slot/porta do adaptador/número da porta`**

Por exemplo: **`7000(config)#interface ethernet 2/0/0`**

Comandos de interface serial

Para se configurar uma interface serial, existem algumas especificações que devem ser discutidas. Tipicamente, a interface estará conectada à um dispositivo CSU/DSU (Channel Service Unit/Data Service Unit), que proverá o clocking (sincronização) para a linha. Entretanto, se você dispuser de uma topologia "back-to-back", como as utilizadas em laboratório, uma das pontas precisa prover o clocking. Esse seria o dispositivo que se encontrasse na ponta DCE (Data Communication Equipment) do cabo. Por default, todos os routers Cisco são dispositivos DTE (Data Terminal Equipment), portanto, você deve configurar determinada interface para prover o clocking se essa é para agir como um dispositivo DCE. Você deve configurar uma interface serial DCE através do comando **`clock rate`** :

```
Router(config-if)#clock rate 64000
%Error: This command applies only to DCE interfaces
Router(config-if)#int s1
Router(config-if)#clock rate 64000
```

Não há mal algum em se tentar configurar o clocking em uma interface serial. No entanto, se a interface em questão não se tratar de uma interface DCE (como no exemplo acima, onde tentamos aplicar o comando à interface DTE S0), a configuração será rejeitada. Note que o comando **`clock rate`** é dado em bits por segundo.

O próximo comando que deve ser compreendido com relação à interfaces seriais é o comando bandwidth. Todo router Cisco vêm de fábrica com a largura-de-banda (bandwidth) default para links seriais de uma T1 (1.544Kbps). Entretanto, é importante compreender que isto nada tem a ver com o modo como os dados são transmitidos através do link serial. A largura-de-banda (bandwidth) de um link serial é utilizada por protocolos roteadores, como IGRP, EIGRP e OSPF para o cálculo do melhor custo para uma rede remota. Se você está utilizando roteamento RIP, então a configuração de bandwidth será irrelevante (uma vez que esse protocolo utiliza o número de "hops" [nós] até o destino como medida):

```
Router(config-if)#bandwidth ?
  <1-10000000>  Bandwidth in kilobits
Router(config-if)#bandwidth 64
```

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

O Sistema Cisco IOS

Configurando hostnames, descrições e salvando configurações

- Designando um nome para o router (hostname)
- Configurando descrições em interfaces (description)
- Salvando configurações

Para configurar um nome para determinado router, utilize o comando **hostname**. Este comando é relevante apenas localmente, o que significa que não há interferência em como o router executa a procura de nomes pela rede:

```
Router#config t
Enter configuration commands, one per line.  End with
CNTL/Z.
Router(config)#hostname todd
todd(config)#hostname Atlanta
Atlanta(config)#
```

Descrições

Configurar descrições em interfaces de um router pode ser muito útil para o administrador. Como o comando **hostname**, o comando **description** é apenas localmente relevante. Esse é um comando útil, pois pode ser usado para se manter números de circuitos organizados, como no exemplo:

```
Atlanta(config)#int e0
Atlanta(config-if)#description Sales Lan
Atlanta(config-if)#int s0
Atlanta(config-if)#desc Wan to Miami circuit:6fdda4321
```

Você pode verificar a descrição das interfaces tanto com o comando **show run**, quanto com o comando **show int**

Salvando configurações

Quando você executa configurações em um router, você está alterando a configuração chamada running-config, ou seja, a configuração que está armazenada na memória volátil do router (DRAM). Se você não a salvar, se o router for desligado ela é perdida (como no conteúdo da memória RAM de um computador). Uma vez finalizada a configuração, portanto, essa deve ser salva na memória não volátil (NVRAM) - e passará a se chamar startup-config, assim, na próxima vez que o router for ligado, essa configuração predominará. Você pode efetuar esse processo manualmente através do comando **copy running-config startup-config**, ou, simplesmente, **copy run start.**

Para verificar o conteudo das configurações, utilize os comandos: **sh run** (running-config) ou **sh start** (startup-config). Você ainda pode deletar a startup-config através do comando: **erase start**

Obviamente, o comando **`show running-config`** seria a melhor maneira de se verificar a configuração de um router, assim como o comando **`show startup-config`** seria a melhor maneira de se verificar a configuração a ser carregada na próxima vez que o router for ligado.

Entretanto, uma vez que você verifica a running-config e constata que tudo parece em ordem, você pode verificar essa configuração com utilidades, como o comando **`ping`** e o comando **`telnet`**.

Você pode "pingar" utilizando-se de diferentes protocolos, e você pode verificar isso digitando **`ping ?`** No modo usuário ou privilegiado.

Você pode utilizar o comando **`trace`** para determinar o caminho que um pacote utiliza quando atravessa a rede. O comando trace também pode ser utilizado com diferentes protocolos.

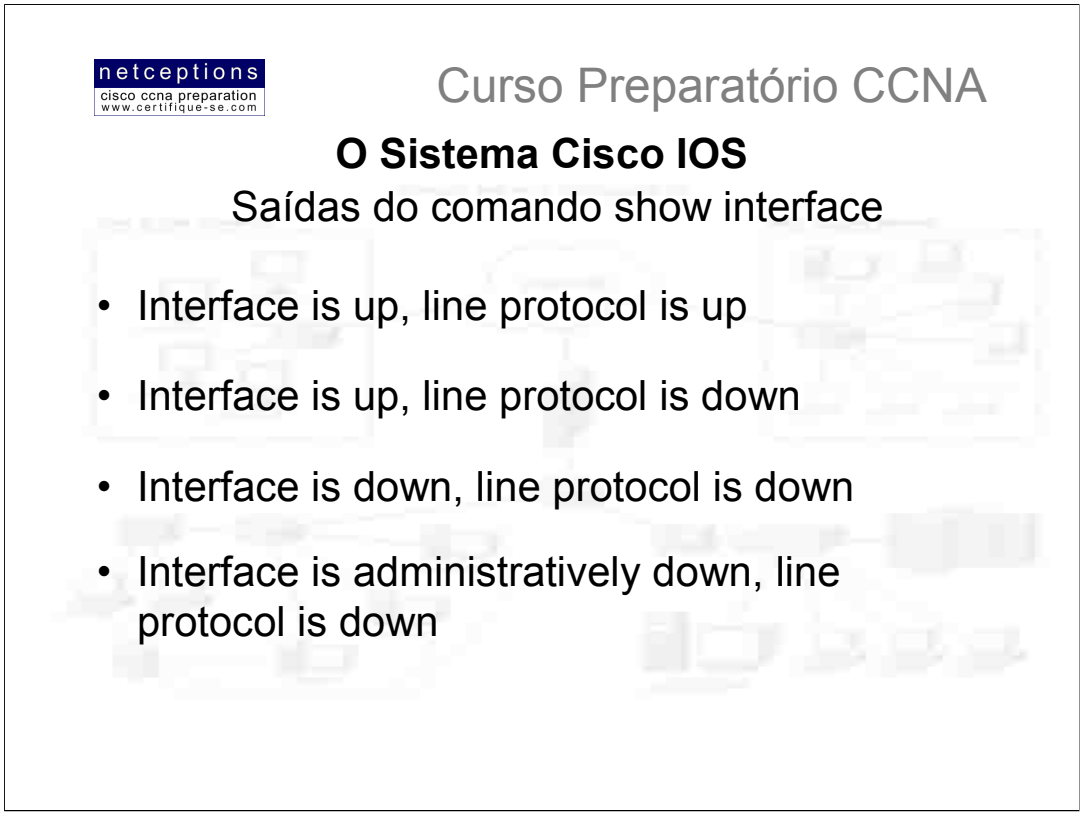
Ambos os comandos apresentados são muito úteis para diagnóstico e teste de redes. O comando **`telnet,`** no entanto, é a melhor utilidade, uma vez que utiliza o protocolo IP na camada de rede e o TCP na camada de transporte para estabelecer uma sessão com um dispositivo remoto. Resumindo, se você consegue estabelecer uma sessão telnet com outro host, sua conectividade IP tem de estar boa.

Verificando a configuração com o comando `show interface`

Outro modo de se verificar a configuração é através do comando **`show interface`** (**`sh int`**). O primeiro comando, por instinto, seria **`sh int ?`**. Este apresenta uma lista das interfaces disponíveis, como já mencionamos antes. Escolha a interface desejada e verifique-a digitando, por exemplo, show int e0

Neste caso, obteríamos a seguinte saída:

```
Router#sh int e0
Ethernet0 is up, line protocol is up
  Hardware is Lance, address is 0010.7b7f.c26c (bia
0010.7b7f.c26c)
Internet address is 172.16.10.1/24
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10
sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:08:23, output 00:08:20, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     25 packets input, 2459 bytes, 0 no buffer
     Received 25 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored,
0 abort
     0 input packets with dribble condition detected
     33 packets output, 7056 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```



A mais importante informação obtida pelo comando show interface é o estado dos links e dos protocolos. Se, no caso anterior, `Ethernet 0 is up, line protocol is up`, então o link está ativo e sem problemas.

O primeiro parâmetro refere-se à camada física (cabos), e encontra-se ativada quando recebe entrada de dados. O segundo parâmetro refere-se à cada de enlace e monitora "keepalives" da outra ponta conectada.

No primeiro caso (Int up, line up), o link está ativo e funcional.

Já no segundo caso (Int up, line down), deve existir um problema de clocking (sincronização) ou de framing. Cheque os keepalives de ambas as pontas e certifique-se que são equivalentes, verifique se o clocking esta configurado e se o tipo de encapsulamento é o mesmo para ambas as pontas.

No terceiro caso (Int down, line down) o problema deve ser no cabo ou na interface. Verifique se o cabo encontra-se devidamente conectado, e se as interfaces envolvidas encontram-se operacionais.

No último caso (Int administratively down, line down), verifique se as interfaces encontram-se ativas e, caso negativo, ative-as utilizando o comando **`no shut`**.

Uma outra saída de configuração que é importante ser notada refere-se ao keepalive, que é o intervalo sob o qual os routers se comunicam. O tempo default é de 10 segundos. Se ambos os routers não tiverem seu keepalive configurados com o mesmo parâmetro, a comunicação falhará (caso 2). Você pode resetar os contadores em uma interface através do comando **`clear counters [interface]`**

```
Router#sh int s0
Serial0 is up, line protocol is up
  Hardware is HD64570
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10
sec)
```

Outra informação importante que notamos nessa interface serial é o campo MTU (Maximum Transmission Units), que é default em 1500 bytes. Notamos também o bandwidth default (1544Kbps).

O comando `show controllers`

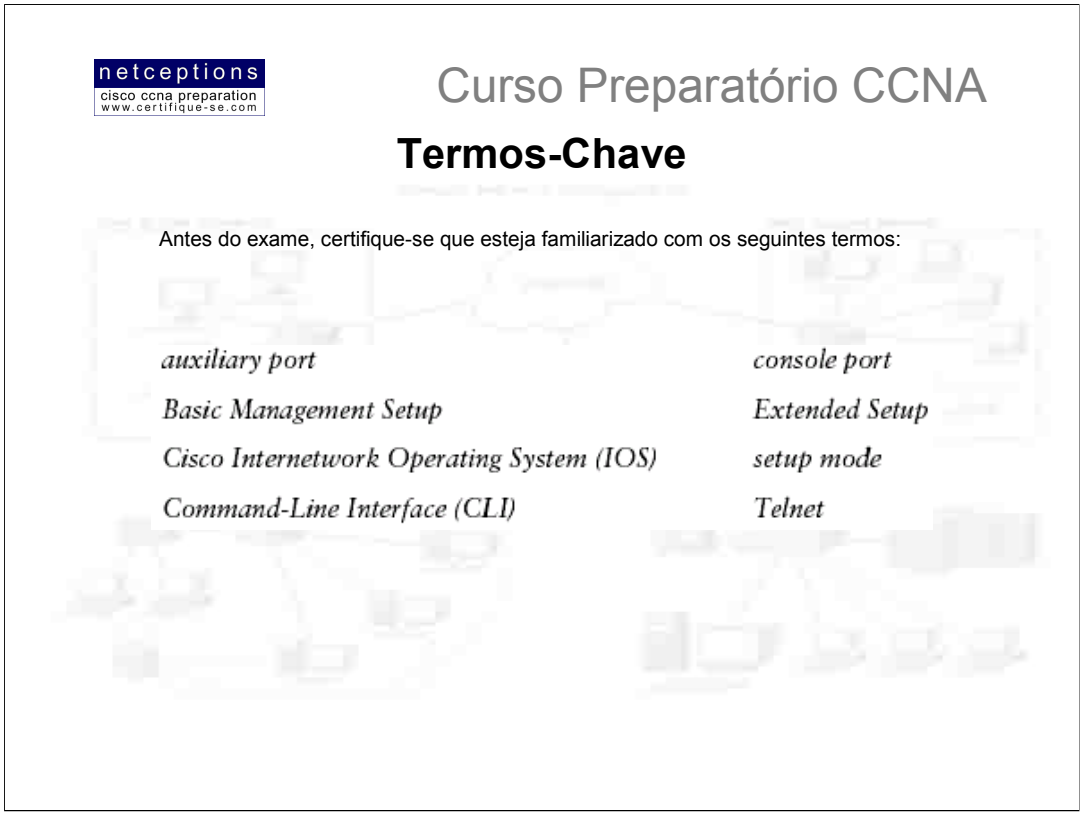
O comando show controllers apresenta informações sobre a interface física per se. Ele também nos informará sobre o tipo de cabo serial conectado à uma porta serial. Tipicamente será um cabo DTE, que então se conectará á um tipo de DSU. A sintaxe deste comando é: **`sh controllers s [x]`**, onde [x] é o número da interface serial. Note o espaço entre a letra **`s`** e o número da interface. Isso é importante!

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Relação dos comandos analisados:

Comando	Descrição
?	apresenta ajuda sobre determinado comando
Bandwidth	define a largura-de-banda em uma determinada interface
Banner	Cria um banner que é apresentado sempre que alguém se conecta ao router
clear counters	Limpa as estatísticas de uma interface
Clock rate	Prove sincronização (clocking) em uma interface serial DCE
Config memory	Copia a configuração NVRAM (startup) para FLASH (running)
Config network	Copia a configuração armazenada em um servidor TFTP para a FLASH
Config terminal	O coloca no modo de configuração global
Copy run start	Copia a configuração da FLASH para a NVRAM
Description	Define uma descrição para uma interface
Disable	Encerra a sessão em modo privilegiado e o leva para o modo usuário
Enable	Inicia sessão em modo privilegiado
Enable password	Define a senha não criptografada enable
Enable secret	Define a senha criptografada enable secret. Esta substitui a senha enable
Erase startup	Deleta a configuração armazenada na NVRAM
Exec-timeout	Define o timeout para uma sessão de console em minutos e segundos
Hostname	Define o nome de um router
Interface	O leva para o modo de configuração de interface
Interface fastethernet 0/0	Modo de configuração de interface para uma interface FastEthernet
Interface fastethernet 0/0.1	Cria uma sub-interface
Interface serial 5	Modo de configuração de interface para a interface serial 5
Ip address	Configura endereçamento IP em uma interface
Line	Permite a configuração de senhas de modo usuário
Line aux	Modo de configuração de interface auxiliar
Line console 0	Modo de configuração de console
Line vty	Modo de configuração de terminal VTY (Telnet)
Logging synchronous	Barra mensagens de console
Logout	Encerra uma sessão de console
Media-type	Define o tipo de mídia em uma interface
No shutdown	Ativa uma interface
Ping	Testa conectividade IP
Router rip	Modo de configuração router RIP
Service password-encryption	Usado para criptografar senahs de modo usuário e a senha enable
Show controllers s 0	Apresenta o status de uma interface DTE ou DCE
Show history	Apresenta os 10 últimos comandos digitados, por default
Show interface s0	Apresenta as estatísticas da interface Serial 0
Show run	Apresenta a configuração ativa no router
Show start	Apresenta a configuração backup (NVRAM) do router
Show terminal	Apresenta o tamanho do histórico definido
Show version	Apresenta estatísticas do router
Shutdown	Desativa uma interface, levando-a ao modo administrativamente desativada
Tab	Acaba de digitar um comando para você
Telnet	Usado para testar conectividade e configurar um router
Terminal history size	Altera o tamanho do histórico (10-256)
Trace	Testa conectividade IP



Resumo aula 4:

Nesta aula, apresentamos o sistema Cisco IOS. É de extrema importância que você tenha um profundo entendimento dos tópicos estudados nesta aula, pois serão de extrema importância nas aulas que se seguem.

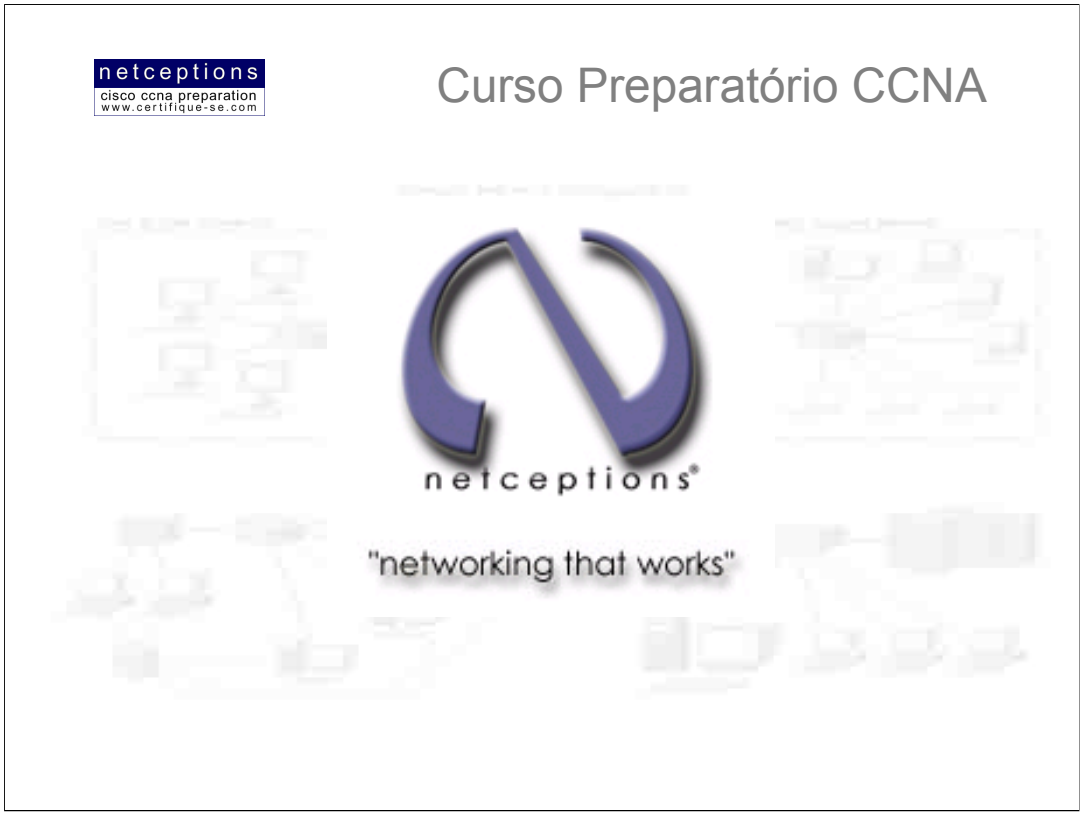
Nesta aula, cobrimos:

- Entendimento do Sistema IOS
- Conectando-se à um router via console e LAN
- Ativando um router e entrando no modo setup
- Conectando-se à um router e as diferenças entre modo usuário e privilegiado
- Entendendo os diferentes prompts
- Entendendo os mecanismos de edição e de ajuda
- Reunindo informações básicas utilizando o comando **`show`**
- Configurando senhas para modo usuário e privilegiado
- Configurando banners
- Configuração básica de interfaces
- Configurando nomes em routers
- Configurando descrições em interfaces
- Verificando e salvando configurações

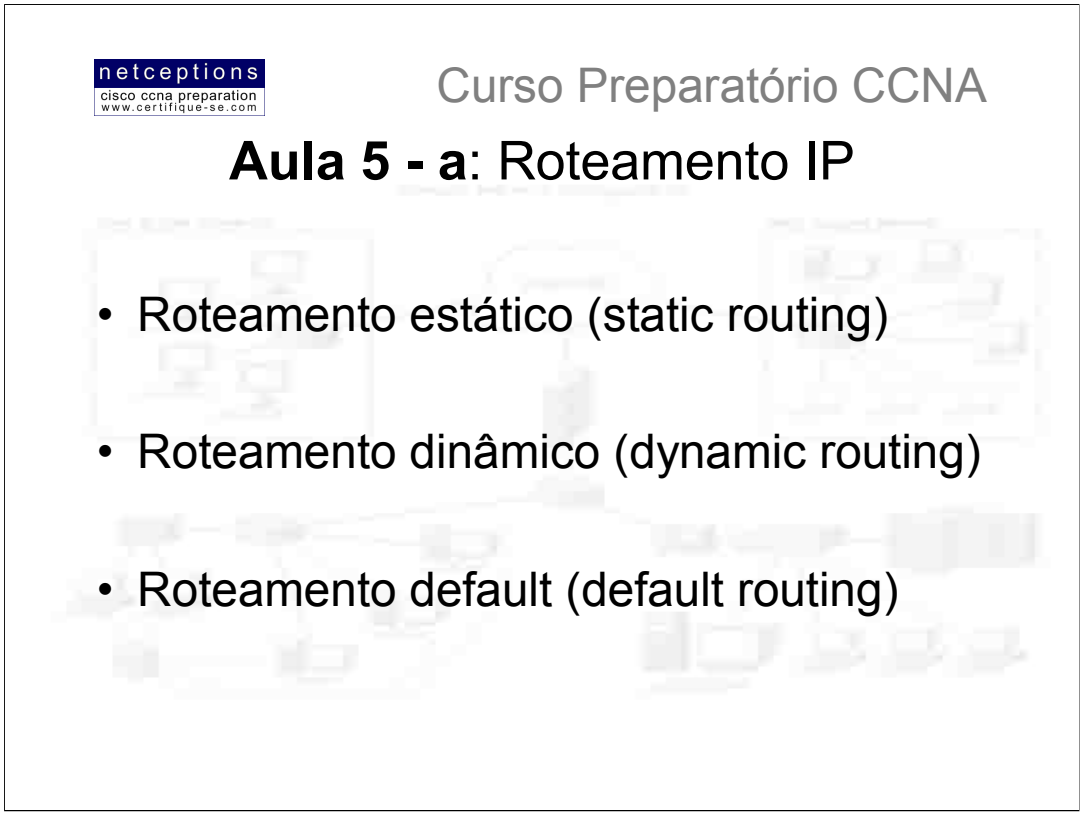
netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

FIM AULA 04

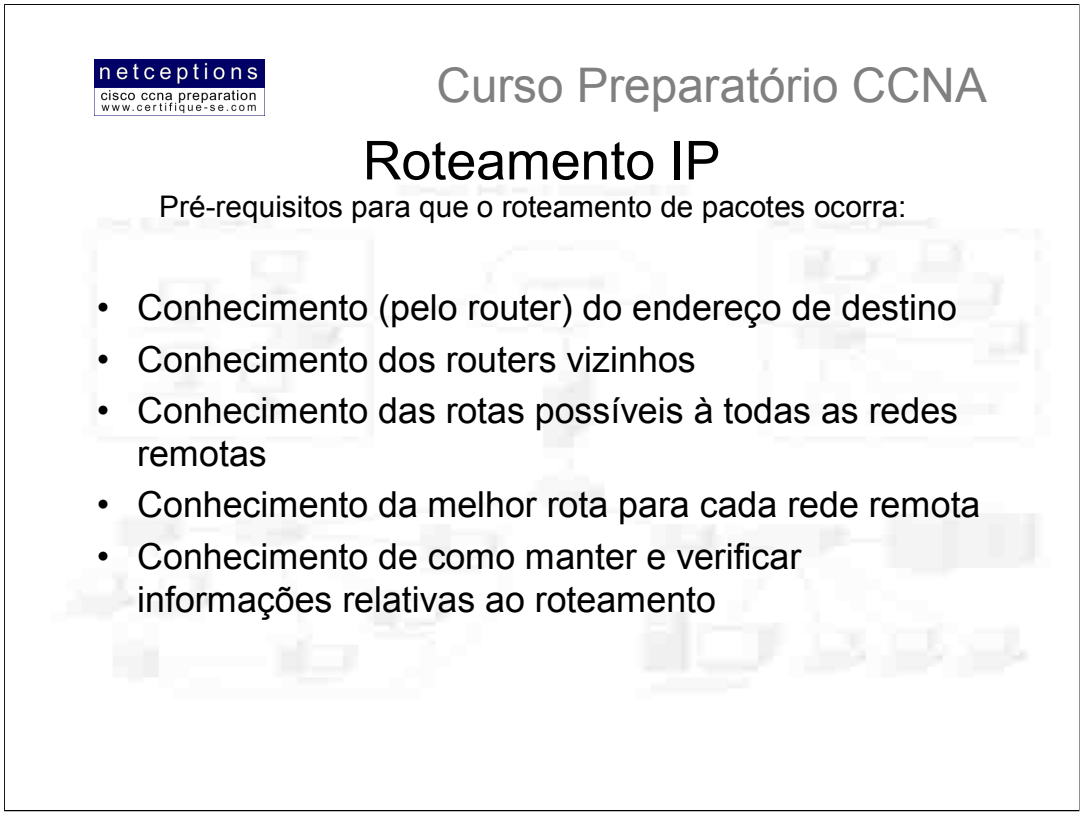


Apostila Aula 5



Neste módulo discutiremos o processo de roteamento IP. Este é um tópico muito importante de ser entendido, uma vez que é pertinente à todos os routers e configurações que utilizam o protocolo IP. Os três tipos básicos de roteamento encontram-se listados acima, e será sobre esses tipos que estaremos discutindo.

É importante ter habilidade de configurar routers Cisco e, depois, configurar e verificar esquemas de roteamento IP. É isso o que estaremos discutindo.

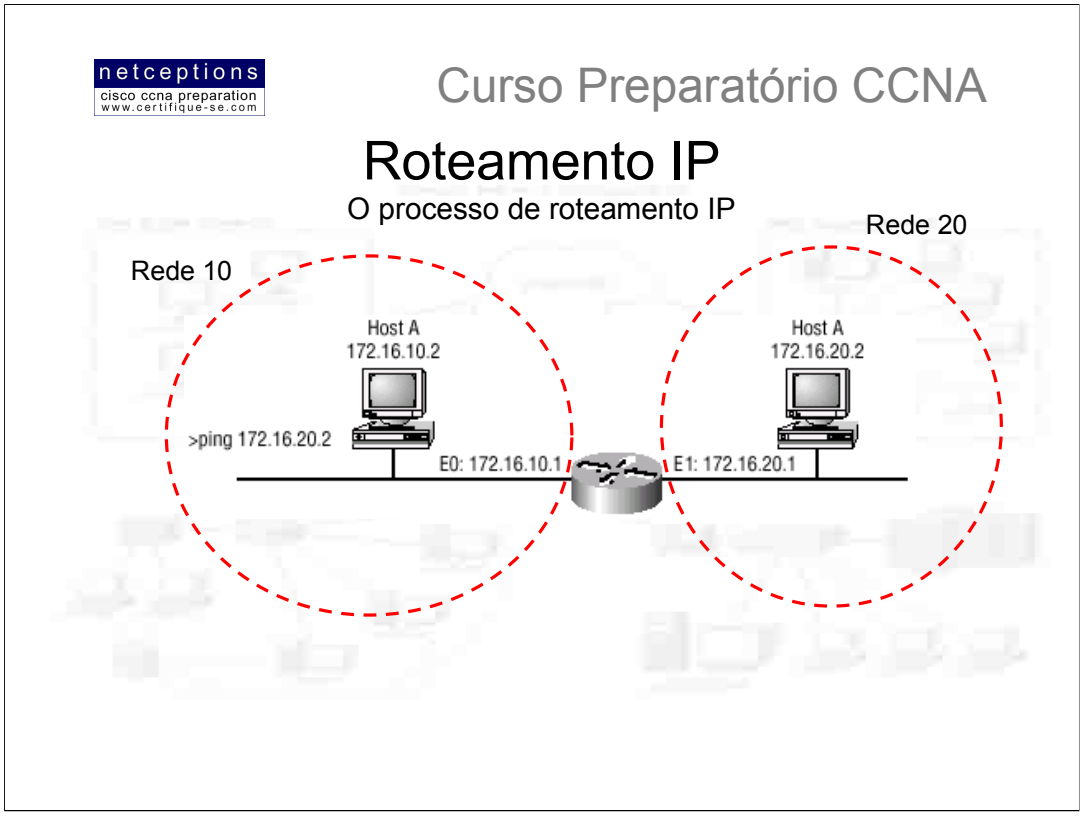


Roteamento

O processo de roteamento é efetuado para se transmitir um pacote de dados de um dispositivo em uma rede para um dispositivo em outra. Se sua rede não possui routers, então você não está roteando. O papel dos routers é direcionar o tráfego para todas as redes em sua internetwork. Para ser capaz de efetuar o roteamento de pacotes, o router deve conhecer, no mínimo, o seguinte:

• endereço de destino
• routers vizinhos
• rotas possíveis à todas as redes remotas
• melhor rota para cada rede remota
• como manter e verificar informações relativas ao roteamento

O router “aprende” sobre redes remotas através da comunicação com routers vizinhos, ou através do administrador. O router, então, cria uma tabela de roteamento que descreve como encontrar tais redes remotas. Se a rede estiver diretamente conectada, então o router já sabe como encontra-la. Caso a rede não se encontre diretamente conectada, o router deve descobrir o caminho para alcança-la, seja via roteamento dinâmico, estático ou default. Roteamento estático é o processo de criação de tabelas de rotas (routing tables) pelo administrador, manualmente. Já roteamento dinâmico utiliza protocolos de roteamento (routing protocols) para se comunicar com routers vizinhos e, automaticamente, gerar tal tabela. Os routers, então, atualizam suas tabelas entre si após um determinado intervalo constante de tempo. Se uma mudança ocorrer na rede, os protocolos dinâmicos informam automaticamente todos os routers conectados sobre a mudança. Caso roteamento estático esteja sendo utilizado, o administrador deve então, neste caso, atualizar manualmente as tabelas de rotas de todos os routers da rede.



O processo de roteamento IP é bastante simples, e não se altera - independente do tamanho ou complexidade da rede. Utilizemos a ilustração acima para explicar passo-a-passo o que acontece quando o Host A tenta se comunicar com o Host B (executando um comando “ping”), em uma rede diferente:

1) Da interface de comando (CLI), um usuário na rede **10** digita o comando **`ping 172.16.20.2`**. Um pacote é gerado no Host A utilizando os protocolos de rede IP e ICMP.

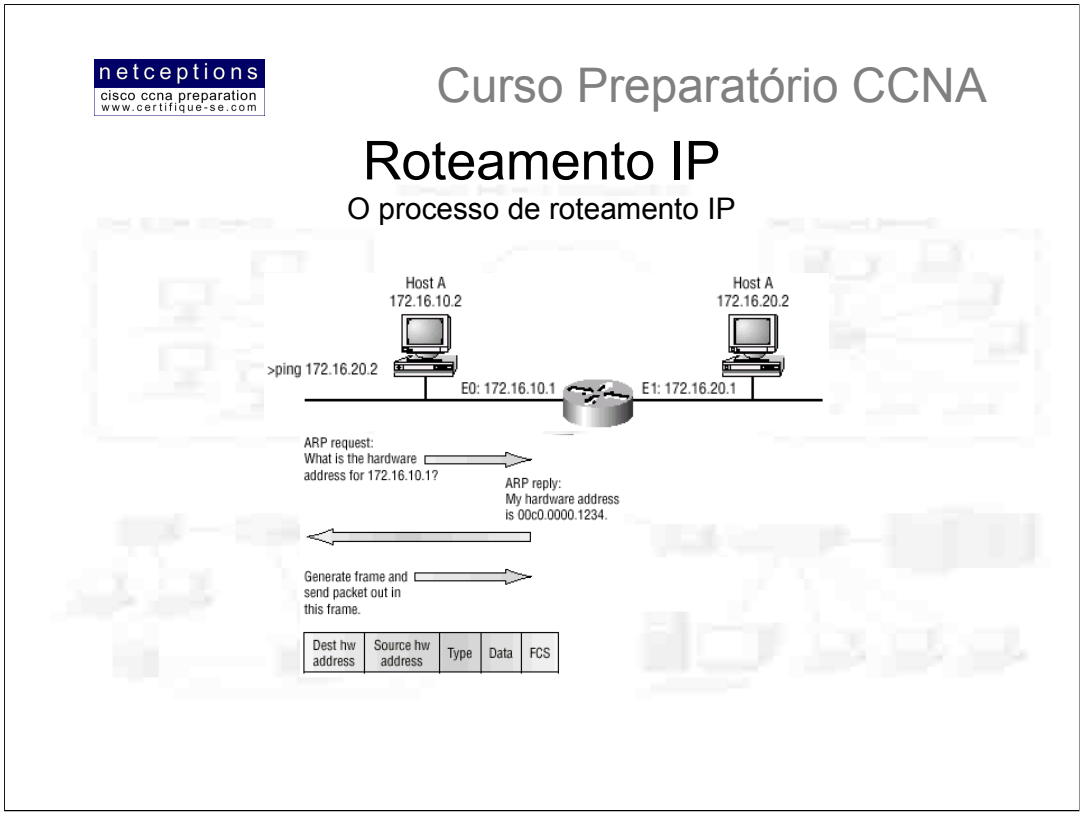
2) O protocolo IP trabalha em conjunto com o protocolo ARP (Address Resolution Protocol) para determinar para qual rede o pacote é destinado. Uma vez que se determina que o pacote é destinado para uma rede remota, e não para a local, ele é enviado para o router para que, então, ele possa ser roteado para a rede remota

3) Para o host A enviar um pacote para o router, ele deve saber o endereço de hardware (MAC) da interface conectada à rede local. Para obter este endereço, o host realiza uma pesquisa no ARP cache.

4) Caso o endereço IP não seja resolvido para um endereço de hardware e não esteja no ARP cache, o host emite uma mensagem de broadcast ARP, procurando identificar o endereço de hardware que corresponde ao endereço IP 172.16.10.1. É por esse motivo que, normalmente, o primeiro PING expira (time-out) e os outros 4 são bem-sucedidos. Uma vez que o endereço seja armazenado no ARP cache, não ocorrem mais time-outs.

5) O router responde com o endereço de hardware da interface conectada à rede local. O host, agora, tem tudo o que é necessário para transmitir o pacote para o router. A camada de rede passa o pacote gerado através da requisição ICMP (ICMP echo request = PING) para a camada de enlace, juntamente com o endereço de hardware para onde o host deseja enviar o pacote. O pacote inclui o endereço IP do remetente (source address), assim como o ICMP especificado no campo “protocolo” da camada de rede.

6) A camada de enlace gera um frame (quadro) que encapsula o pacote com informações de controle necessárias à transmissão do mesmo pela rede local. Essas informações incluem os endereços de hardware do remetente (source) e do destinatário (destination) e o campo “type”, especificando o protocolo de camada de rede (é um campo “type”, uma vez que o protocolo IP utiliza o formato de frame Ethernet_II como default).



A figura acima ilustra todas as informações necessárias para que o processo de comunicação ocorra.

7) A camada de enlace do host A passa o frame gerado para a camada física, que codifica os dados em 0s e 1s e os transmite através da interface local.

8) O sinal é captado pela interface Ethernet 0 do router, que realiza um processo de sincronização com o preâmbulo (preamble = sequência alternada de 0s e 1s para sincronização) e efetua a extração do frame. A interface, após a extração do frame, roda uma checagem (CRC) e compara esse resultado com o campo FCS, localizado no final do frame, assegurando-se que a integridade do frame foi mantida.

9) O endereço de hardware de destino é checado. O campo “type” no frame, então, se encarrega de informar o que o router deve fazer com o pacote de dados. Uma vez que protocolo IP aparece no campo “type”, o router passa o pacote de dados para este protocolo. O frame é então descartado, e o pacote original, gerado pelo host A, é armazenado no buffer do router.

10) O protocolo IP checa o endereço IP de destino do pacote para certificar-se que o pacote é, de fato, destinado ao router. Como o endereço de destino é 172.16.20.2, o router determina, através da tabela de roteamento (routing table) que o endereço 172.16.20.2 é uma rede diretamente conectada à interface Ethernet 1 (rede 172.16.20.x)

11) O router armazena o pacote no buffer da interface Ethernet 1. O router agora precisa gerar um frame para transmitir o pacote ao seu destino final, o host B. Primeiramente, o router checa sua tabela ARP (ARP cache) para determinar se o endereço de hardware de destino já foi resolvido para o endereço IP em uma comunicação anterior. Caso negativo, o router emite uma mensagem de broadcast ARP pela interface E1, para que se encontre o endereço 172.16.20.2

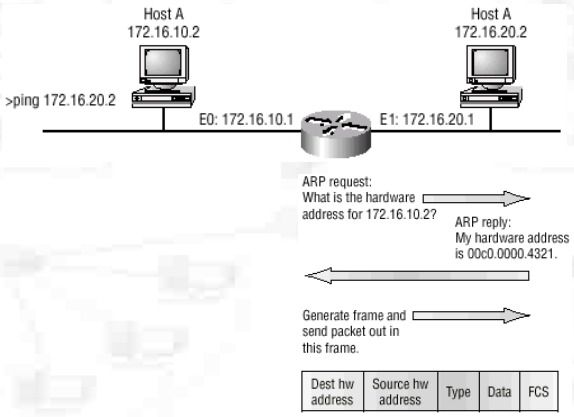
12) O host B responde à essa mensagem com o endereço de hardware de sua interface de rede. O router, agora, possui tudo o que necessita para transmitir o pacote ao seu destino final.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Roteamento IP

O processo de roteamento IP



O frame gerado pela interface E1 do router possui o endereço de hardware de origem (interface E1) e o endereço de hardware de destino (interface de rede instalada no host B). O ponto mais importante aqui é notar que, mesmo que os endereços de hardware (de origem e de destino) do frame mudem a cada interface pelo qual passa, os endereços IP de origem e de destino **nunca** são alterados, ou seja, o pacote de dados nunca é alterado. Apenas sua moldura (o frame) sofre alterações.

13) O host B recebe o frame e executa um procedimento de checagem (CRC) sobre o mesmo. Caso não existam problemas, o frame é descartado e o pacote é passado para o protocolo IP. O protocolo IP, então, checa o endereço IP de destino. Uma vez que o endereço IP checado coincida com o endereço IP da interface instalada no host B, o protocolo IP, então, analisa o campo “protocolo” do pacote para determinar qual o seu propósito.

14) Uma vez determinado que o pacote é uma requisição ICMP, o host B gera um novo pacote ICMP com o endereço de destino sendo o endereço IP do host A.

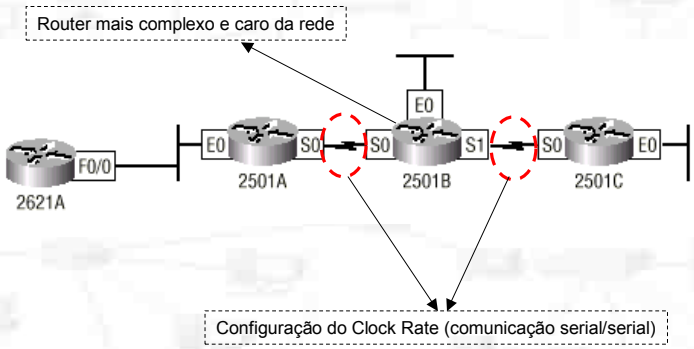
15) O processo, então, se reinicia.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Roteamento IP

O processo de roteamento IP em uma grande rede

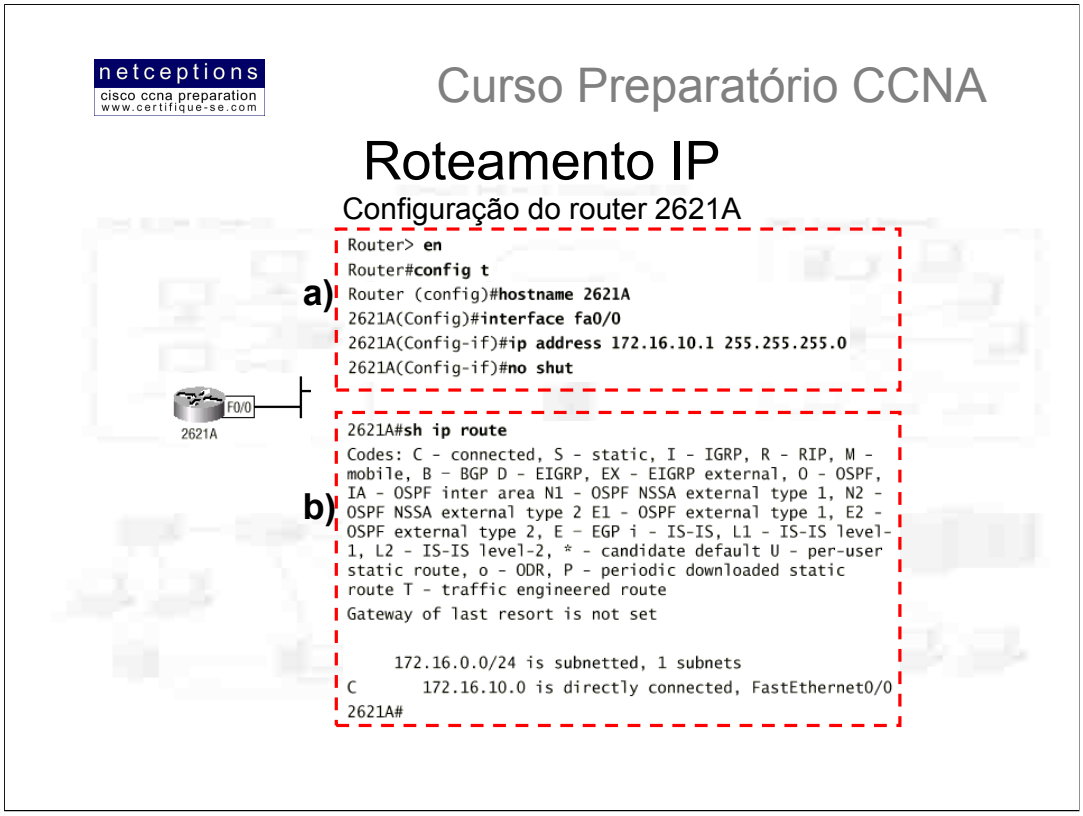


No exemplo ilustrado nas páginas anteriores, a tabela de roteamento (routing table) do router já possuía os endereços IP de ambas as redes, uma vez que ambas encontravam-se diretamente conectadas ao router em questão. O que acontece, então, se adicionarmos 3 outros routers? A figura acima ilustra uma rede composta de 4 routers: 2500A, 2500B, 2500C e 2621A. Estes routers, por default, contém em suas routing tables apenas os endereços IP de redes diretamente conectadas aos mesmos.

Na figura acima, observamos 3 routers da linha 2500 conectados através de uma WAN (conexões seriais S0-So e S1-S0), e o router 2621 conectado ao router 2500A através de uma rede Ethernet. Cada router possui, também, uma rede Ethernet conectada.

O primeiro passo é a configuração de cada interface ativa de cada router. A tabela abaixo nos mostra o esquema de endereçamento IP utilizado na configuração de cada rede (note que os endereços apresentados foram aleatoriamente escolhidos. Estes podem - e devem - variar caso-a-caso). Vamos primeiro acompanhar como cada interface é devidamente configurada, para depois verificarmos como configurar o roteamento IP. Cada endereço de rede apresentado na tabela abaixo possui uma máscara de rede de 24-bits (255.255.255.0):

Router	Network Address	Interface	Address
2621A	172.16.10.0	f0/0	172.16.10.1
2501A	172.16.10.0	e0	172.16.10.2
2501A	172.16.20.0	s0	172.16.20.1
2501B	172.16.20.0	s0	172.16.20.2
2501B	172.16.40.0	s1	172.16.40.1
2501B	172.16.30.0	e0	172.16.30.1
2501C	172.16.40.0	s0	172.16.40.2
2501C	172.16.50.0	e0	172.16.50.1



O processo de configuração de um router é relativamente simples, uma vez que basta configurar os endereços IP para cada interface (é importante, em um ambiente de produção, que você defina uma tabela como a apresentada na página anterior para auxiliá-lo no processo de configuração e para posterior documentação das redes criadas) e, logo em seguida, aplicar o comando **`no shut`** em cada interface configurada. O processo ficará um pouco mais complexo mais adiante, mas por hora, vamos configurar os endereços IP para cada interface.

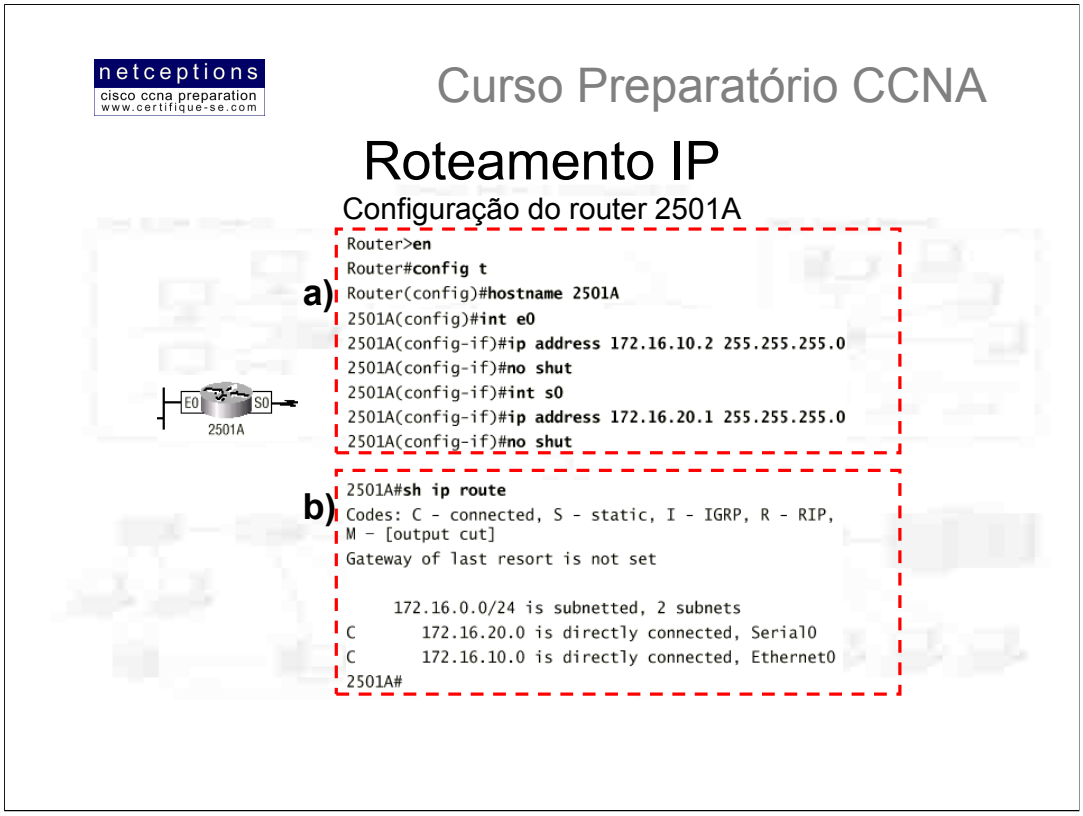
Configuração do router 2621A:

Para configurar o router 2621, basta definir um endereço IP para a interface FastEthernet 0/0. O processo de configuração de um nome para o router (**`hostname`**) facilita a identificação de cada um em uma grande rede. Observe nas ilustrações acima que o processo de configuração, em si **(a)** é bastante simples e se resume em algumas poucas linhas.

Para verificação da tabela de roteamento (routing table) criada, utilize o comando **`sh ip route`** (b). Note que apenas a rede configurada é apresentada na tabela, o que significa que o router 2621, até o momento, sabe como alcançar apenas a rede 172.16.10.0.

Observe também que a sigla “C” precede o endereço de rede apresentado, indicando que se trata de uma rede diretamente conectada ao router. Note os outros códigos disponíveis: S-Static; I-IGRP; R-RIP; M-mobile; B-BGP; D-EIGRP; EX-EIGRP external; O-OSPF; etc.

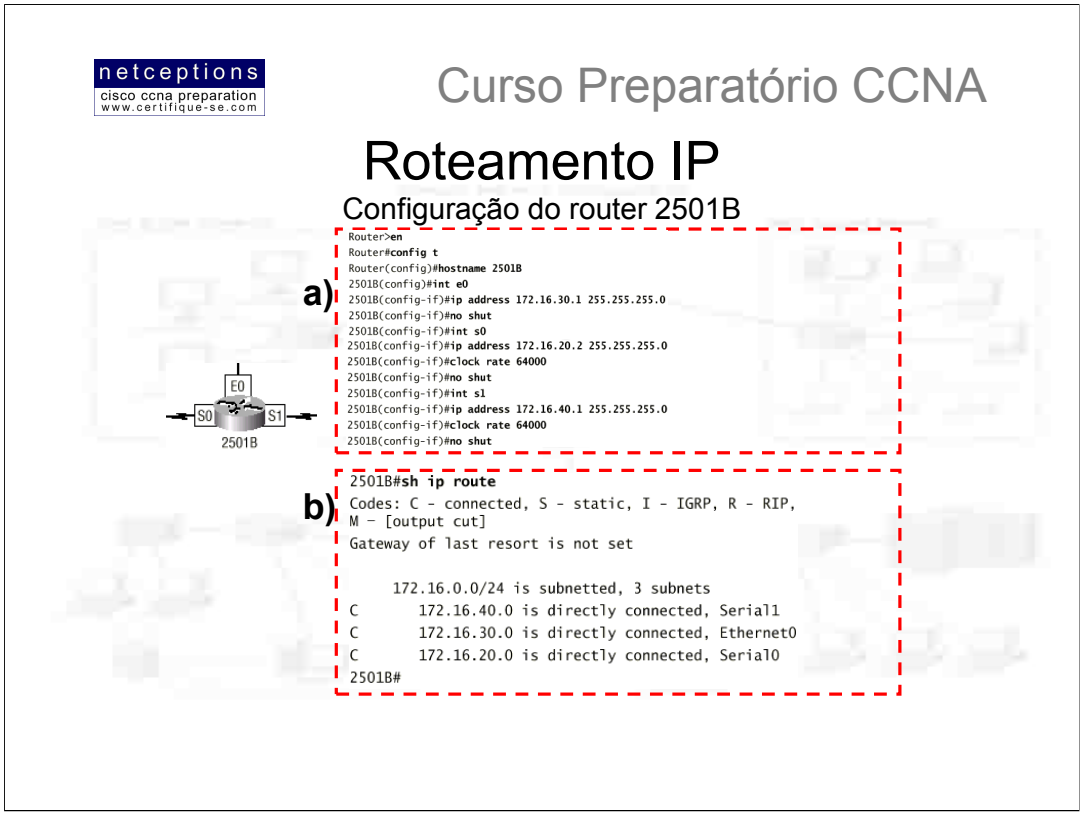
Note também que, mais uma vez, a informação da máscara de rede aparece no formato /24.



Configuração do router 2501A:

Para configurar o router 2501A, duas interfaces precisam ser configuradas: Ethernet0 e Serial0 **(a)**. A configuração ilustrada configura a interface S0 para a rede 172.16.20.0, e a interface E0 para a rede 172.16.10.0.

O comando **`sh ip route`** apresenta a saída ilustrada em **(b)**. Note que o router 2501A sabe como alcançar as redes 172.16.10.0 e 172.16.20.0. Os routers 2621 e 2501A já podem se comunicar pois encontram-se na mesma rede local (LAN) – não há conexões WAN entre os 2 routers.

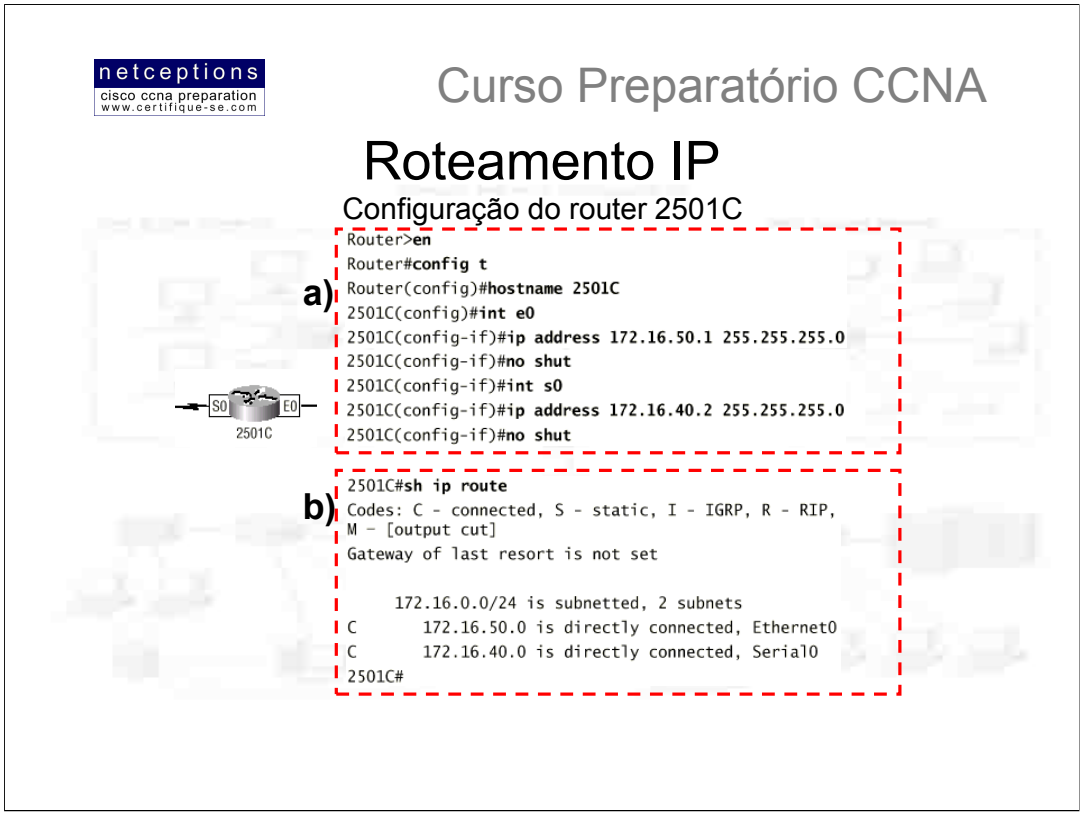


Configuração do router 2501B:

A configuração do router 2501B não é muito diferente, a não ser pelo fato que você precisa prover sincronização através do comando **`clock rate`** para ambas as interfaces DCE conectadas em ambas as interfaces seriais. Três interfaces precisam ser configuradas: Serial0, Ethernet0 e Serial1 **(a)**.

O comando **`sh ip route`** apresenta a saída ilustrada em **(b)**. Note que o router 2501B sabe como alcançar as redes 172.16.20.0, 172.16.30.0 e 172.16.40.0, que são as redes diretamente conectadas ao mesmo.

O router A e o router B podem se comunicar uma vez que se encontram na mesma rede WAN. Entretanto, o router B não pode se comunicar com o router 2621, uma vez que ele não tem informações em sua routing table de como alcançar a rede 172.16.10.0. O router A pode “pingar” ambos os routers 2621 e 2501B, entretanto, os routers 2501B e 2621 não “se enxergam”.



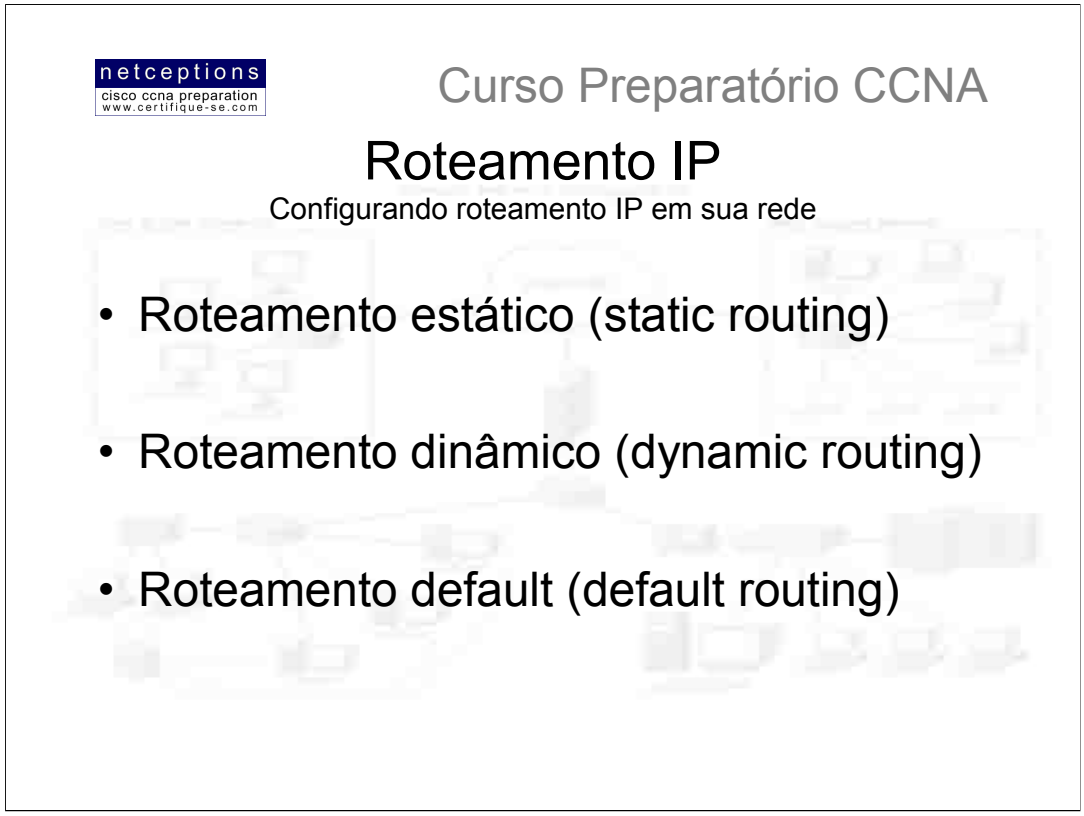
Configuração do router 2501C:

A configuração do router 2501C é muito parecida com a do router 2501A, apenas alterando-se os endereços de rede **(a)**.

A interface E0 é associada à rede 172.16.50.0, e a interface Serial0 é associada à rede WAN 172.16.40.0.

O comando **`sh ip route`** apresenta a saída ilustrada em **(b)**. Note que o router 2501C sabe como alcançar as redes 172.16.40.0 e 172.16.50.0, que são as redes diretamente conectadas ao mesmo.

O router C pode se comunicar diretamente com o router B, uma vez que participam da mesma rede WAN. Entretanto, por default, o router C não tem conhecimento de nenhum outro router ou rede.



A rede sugerida nas páginas anteriores está, agora, devidamente configurada, com relação ao endereçamento IP. As redes que não se encontram diretamente conectadas aos routers, entretanto, ainda não podem se comunicar. Os routers “aprendem” as rotas através da consulta às suas routing tables. Se um pacote é endereçado à uma rede cujo endereço não se encontra nessa tabela o pacote é simplesmente descartado. Não há envio de mensagens de broadcast ou qualquer outro esquema utilizado para se descobrir tal rota. Como, então, configurar os routers da rede sugerida para que suas tabelas incluam os endereços das redes remotas?

Existem diferentes maneiras de se conseguir isso. Diferentes maneiras, para diferentes situações. O entendimento dos diferentes modos de roteamento IP é essencial para que a escolha do melhor modo seja efetuada. Os diferentes modos de roteamento encontram-se listados acima. Iniciaremos com a implementação de roteamento estático na rede sugerida. O motivo de começarmos com esse método é simples: uma vez que seja entendido como proceder para definir rotas estaticamente e, efetivamente, fazê-las funcionar demonstra um grande entendimento da rede como um todo.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Roteamento IP

Roteamento estático

Benefícios:

- Redução do overhead na CPU do router
- Não há utilização de largura-de-banda entre os routers
- Segurança (uma vez que o administrador possui total controle do processo de roteamento)

Desvantagens:

- O administrador precisa, de fato, possuir um profundo conhecimento da rede como um todo
- Se uma rede for adicionada à internetwork, o administrador deve, manualmente, adicionar tal rota à cada um dos routers
- Não é viável em grandes redes

A sintaxe do comando utilizado para se configurar rotas estaticamente é a seguinte:

`ip route [rede_destino] [máscara] [endereço_do_próximo_ponto ou interface_de_saída] [distância_administrativa] [permanent]` onde:

▪ **ip route** = Comando utilizado para designar rotas estaticamente

▪ **rede_destino (destination network)** = a rede que você está adicionando à routing table

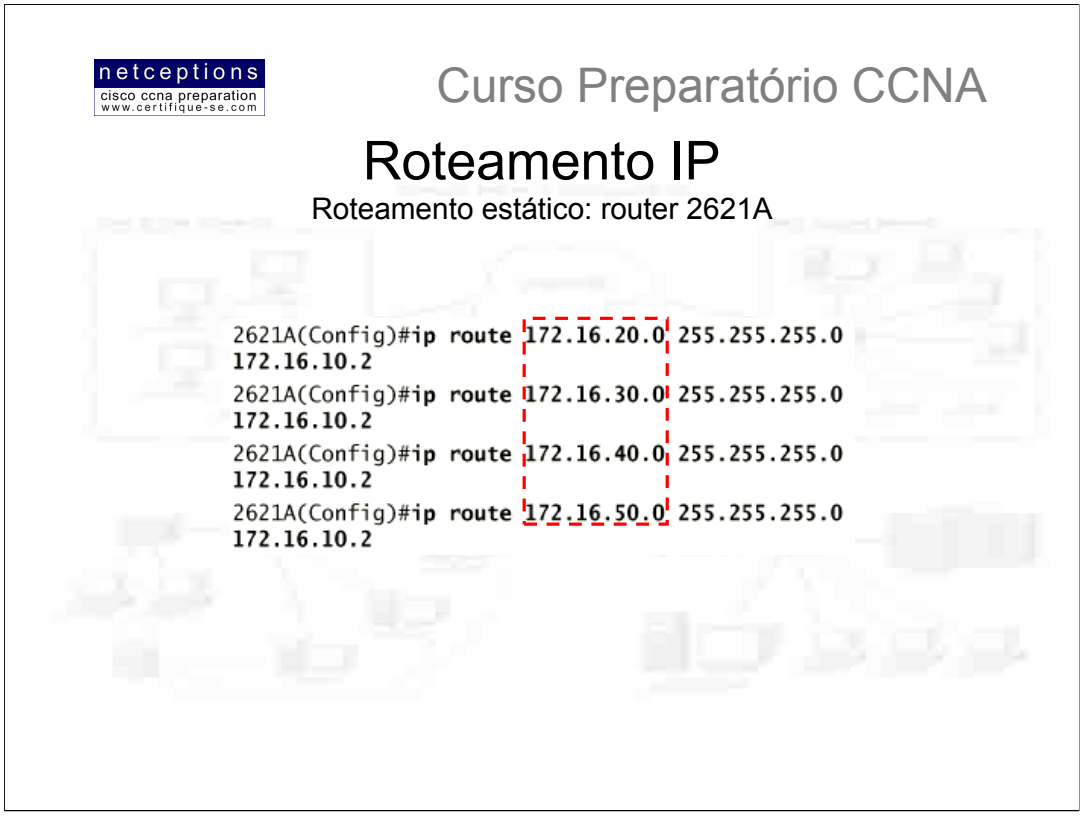
▪ **máscara (mask)** = Máscara de rede em uso na rede

▪ **endereço do próximo ponto (next hop address)** = Endereço do ponto que receberá o pacote e o enviará à rede remota. Trata-se da interface do router que encontra-se em uma rede diretamente conectada

▪ **interface de saída (exit interface)** = Utilizada em lugar do endereço do próximo ponto, caso desejado. Só pode ser utilizado em conexões ponto-à-ponto, como uma WAN. Esse comando não funciona em uma LAN, como uma interface Ethernet, por exemplo

▪ **distância administrativa (administrative distance / AD)** = Por default, rotas estáticas possuem uma distância administrativa de 1. Esse valor pode ser alterado adicionando-se um valor ao final do comando

▪ **permanent** = Caso uma interface encontre-se desativada, ou o router não possa se comunicar com o router no próximo ponto, a rota é automaticamente descartada da tabela de roteamento (routing table). Utilizando-se a opção permanent mantém os dados na tabela de roteamento, não importa o que aconteça.



Configuração de roteamento estático no router 2621A

Cada tabela de roteamento inclui, automaticamente, todas as redes diretamente conectadas. Para que seja possível o roteamento à todas as redes pertencentes à sua internetwork, a tabela de roteamento deve incluir informação que define onde as outras redes estão localizadas e como alcançá-las.

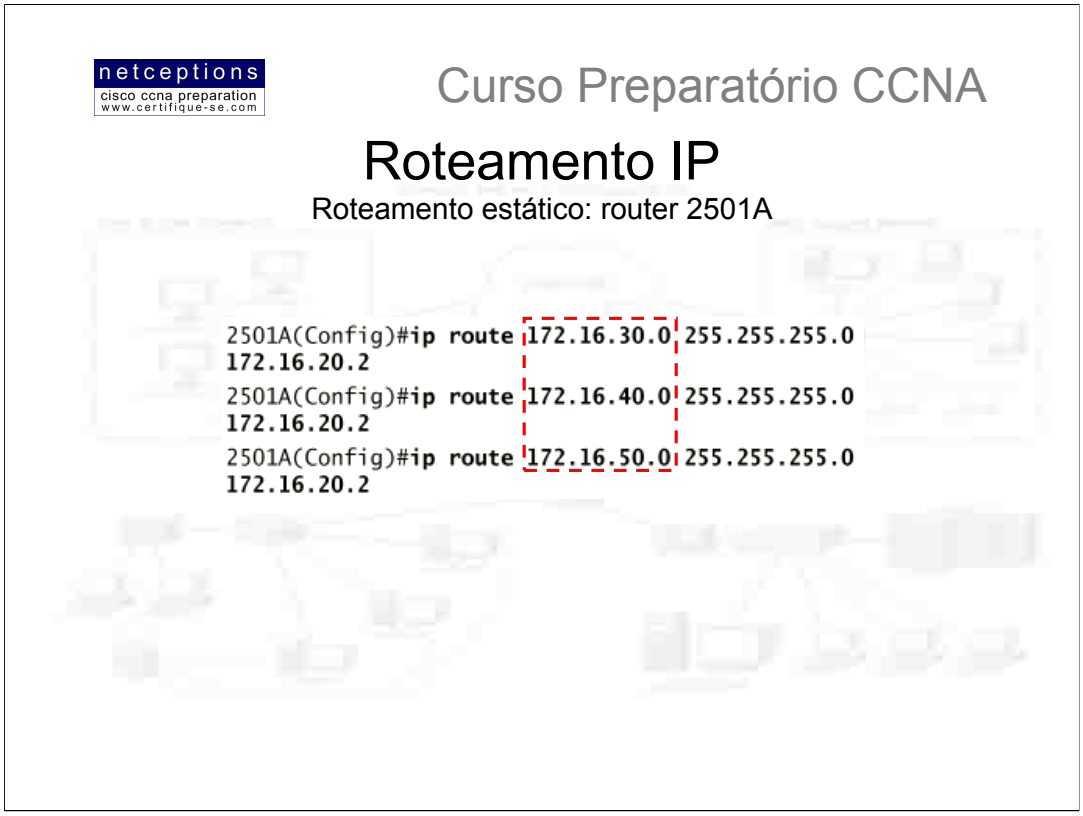
Em nossa rede sugerida, o router 2621A encontra-se conectado apenas à rede 172.16.10.0. Para o router 2621A ser capaz de rotear pacotes para todas as redes, os seguintes endereços de rede devem ser incluídos em sua tabela de roteamento:

172.16.20.0
172.16.30.0
172.16.40.0
172.16.50.0

Acima, ilustramos o processo de configuração de tais rotas no router 2621A. Para esse router ser capaz de encontrar redes remotamente conectadas, dados descrevendo tais redes, máscara de rede utilizada e para onde enviar os pacotes devem ser adicionadas à tabela de roteamento. Note que cada rota estática envia os pacotes para a rede 172.16.10.2, que é o endereço do próximo ponto do router 2621A.

Após a configuração do router, utilize o comando **`show ip route`** ou **`show running-config`** para verificar as rotas configuradas.

O router 2621A possui, agora, todas as informações requeridas para se comunicar com as redes remotamente conectadas. Entretanto, se os outros router da rede não possuírem essa mesma informação, os pacotes serão descartados ao alcançarem o router 2501A.



Configuração de roteamento estático no router 2501A

O router 2501A encontra-se conectado às redes 172.16.10.0 e 172.16.20.0. Para o router 2501A ser capaz de rotear pacotes para todas as redes, os seguintes endereços de rede devem ser incluídos em sua tabela de roteamento:

172.16.30.0

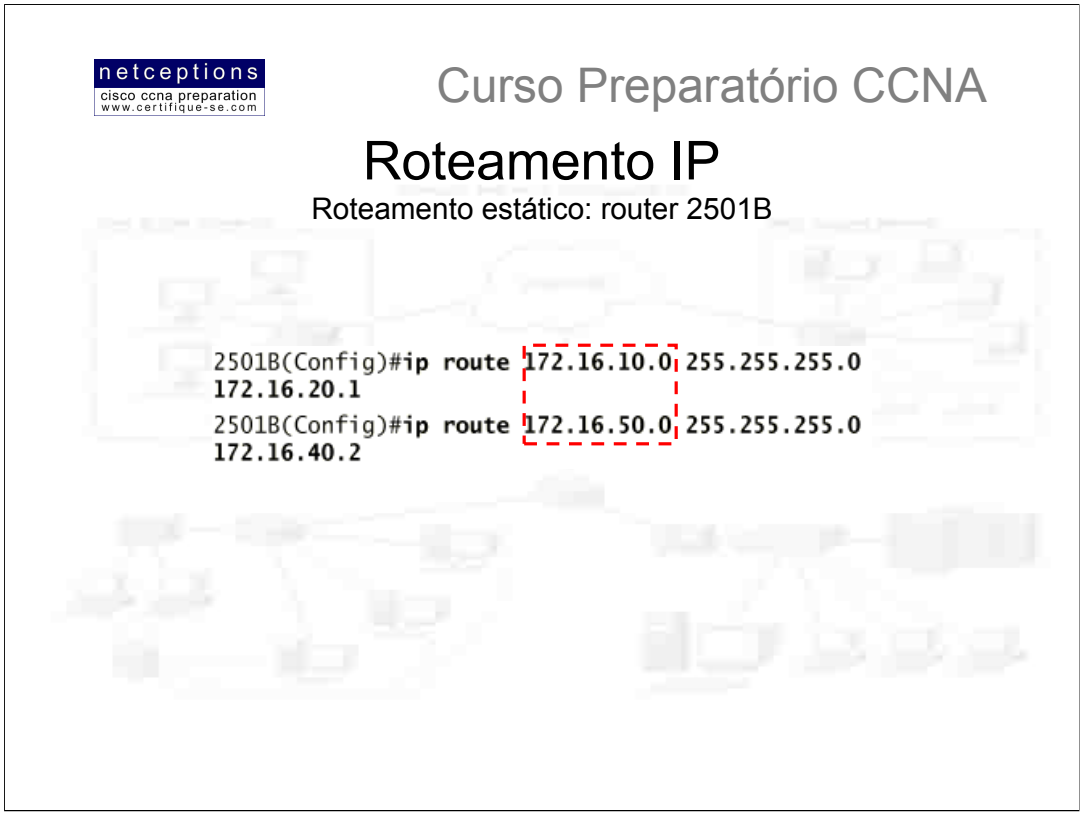
172.16.40.0

172.16.50.0

Acima, ilustramos o processo de configuração de tais rotas no router 2501A.

Após a configuração do router, utilize o comando **`show ip route`** ou **`show running-config`** para verificar as rotas configuradas.

O router 2501A possui, agora, todas as informações requeridas para se comunicar com as redes remotamente conectadas. Uma vez que todos os routers da rede possuam o mesmo conteúdo em suas tabelas de roteamento, o router 2501A poderá se comunicar com todas as redes remotamente conectadas.



Configuração de roteamento estático no router 2501B

O router 2501B encontra-se conectado às redes 172.16.20.0, 172.16.30.0 e 172.16.40.0. Para o router 2501B ser capaz de rotear pacotes para todas as redes, os seguintes endereços de rede devem ser incluídos em sua tabela de roteamento:

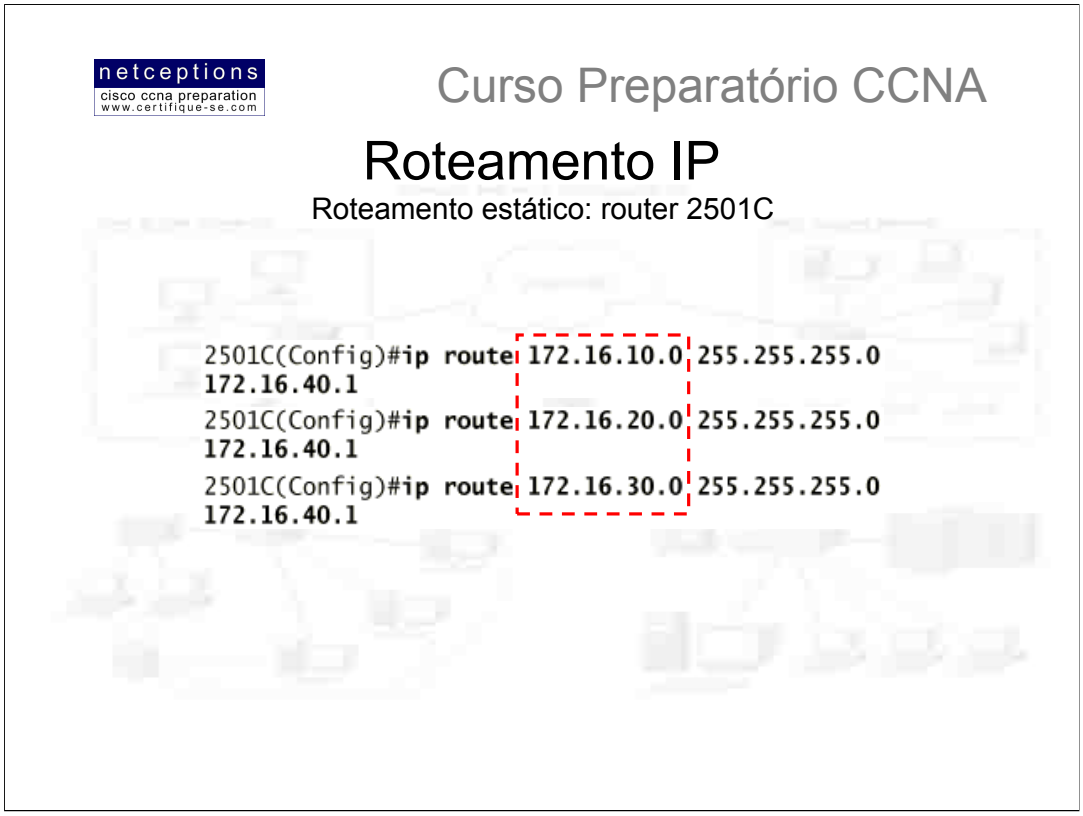
172.16.10.0

172.16.50.0

Acima, ilustramos o processo de configuração de tais rotas no router 2501B.

Após a configuração do router, utilize o comando **`show ip route`** ou **`show running-config`** para verificar as rotas configuradas.

O router 2501B possui, agora, todas as informações requeridas para se comunicar com as redes remotamente conectadas. Uma vez que todos os routers da rede possuam o mesmo conteúdo em suas tabelas de roteamento, o router 2501B poderá se comunicar com todas as redes remotamente conectadas.



Configuração de roteamento estático no router 2501C

O router 2501C encontra-se conectado às redes 172.16.40.0 e 172.16.50.0. Para o router 2501C ser capaz de rotear pacotes para todas as redes, os seguintes endereços de rede devem ser incluídos em sua tabela de roteamento:

172.16.10.0

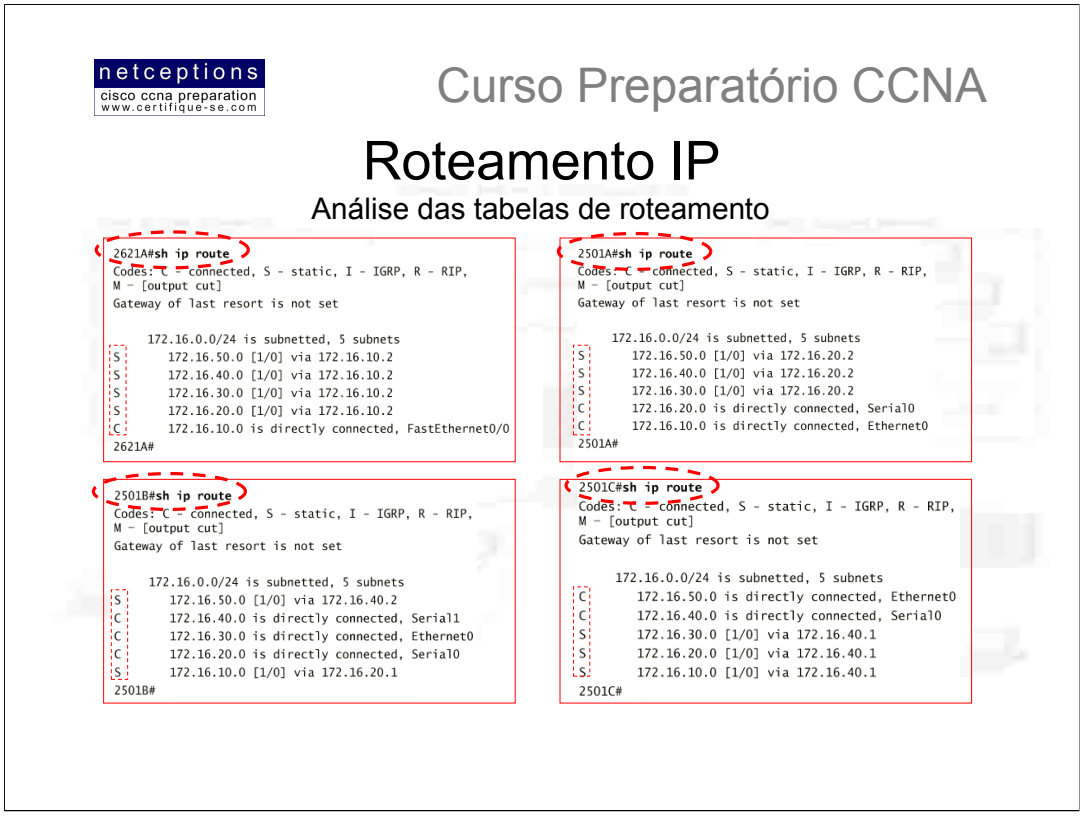
172.16.20.0

172.16.30.0

Acima, ilustramos o processo de configuração de tais rotas no router 2501C.

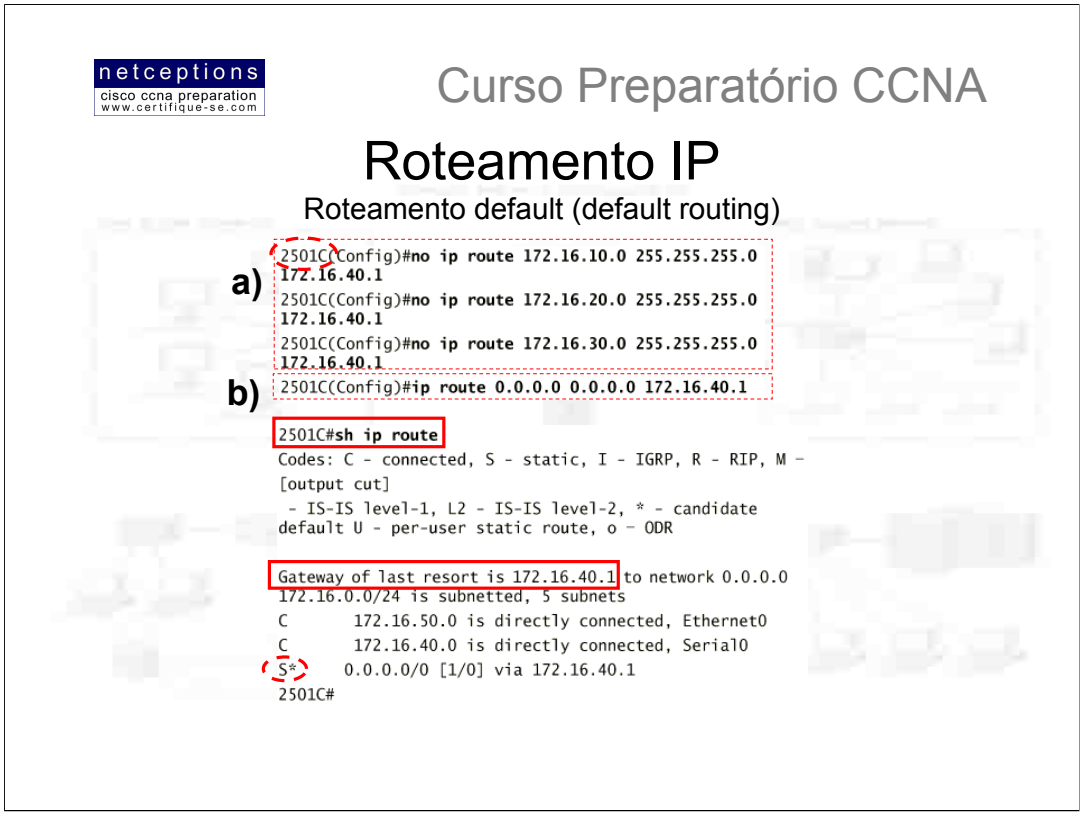
Após a configuração do router, utilize o comando **`show ip route`** ou **`show running-config`** para verificar as rotas configuradas.

Uma vez finalizada a configuração das rotas no router 2501C, todos os router da rede devem possuir em suas tabelas de roteamento exatamente o mesmo conteúdo. Isso significa que uma comunicação total entre os routers da rede pode ser atingida. Entretanto, caso apenas uma rede seja adicionada à internetwork, as tabelas de roteamento de todos os routers devem ser reconfiguradas, para que contenham o endereço da rede adicionada. Em uma rede de pequeno porte, como a sugerida, isso não seria problema. Em uma rede de grande porte, isso seria praticamente inviável.



Note, acima, que todas as tabelas de roteamento apresentadas contém as mesmas informações sobre as rotas pertencentes à internetwork. Observe que, apesar de os endereços em todas as tabelas serem exatamente os mesmos, o modo como os mesmos se encontram configurados é diferente de router para router.

Determinadas rotas foram estaticamente configuradas **(S)**, enquanto que outras, por se tratarem de redes diretamente conectadas, são incorporadas à tabela automaticamente, sem a necessidade de incluí-las manualmente **(C)**.



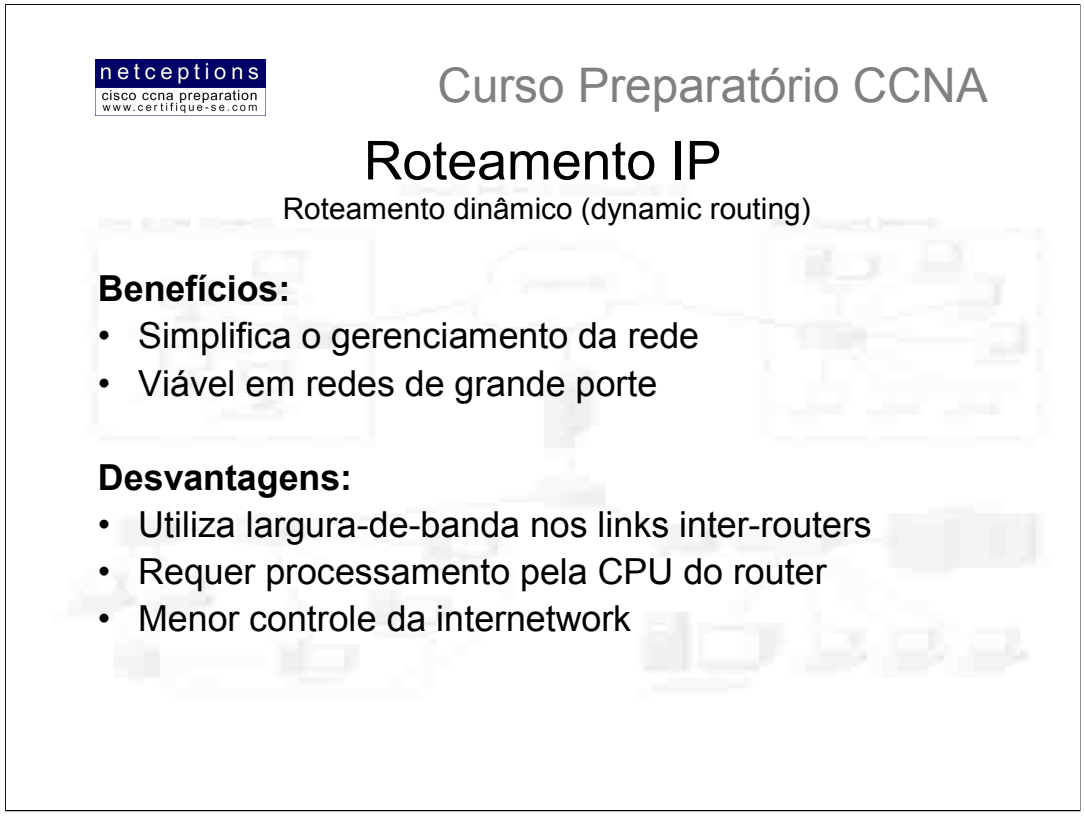
Roteamento default é usado no envio de pacotes para redes que não se encontrem nas tabelas de roteamento dos routers de próximo ponto. Rotas default apenas podem ser configuradas em redes chamadas "stub", ou seja, em redes que possuam apenas uma porta de saída da mesma. Em nossa rede sugerida, os routers que se encaixam nesta categoria são o 2621A e o 2501C. Se você tentar configurar rotas default em qualquer um dos outros routers, os pacotes não serão roteados corretamente, pois esses routers possuem mais de uma interface de saída para outros routers.

Embora o router 2501C possua 2 conexões, não há um router conectado à rede 172.16.50.x que necessite o envio de pacotes. O router 2501C apenas enviará pacotes para a rede 172.16.40.1, que é o endereço da interface do router 2501B. Já o router 2621A apenas enviará pacotes para o endereço 172.16.10.1, que é o endereço da interface do router 2501A.

Para a configuração de rotas default, você fará uso de "wildcards" no lugar do endereço e da máscara de rede. Pense na rota default como uma rota estática que utiliza wildcards no lugar das informações do endereço e da máscara de rede. No exemplo acima, ilustramos a criação de rotas default para o router 2501C.

O router 2501C encontra-se diretamente conectado às redes 172.16.40.0 e 172.16.50.0. A tabela de roteamento precisa conter os endereços das redes 172.16.10.0, 172.16.20.0 e 172.16.30.0. Para configurar o router para que o roteamento para as 3 redes mencionadas ocorram, configuramos, anteriormente, 3 rotas estáticas. Ao utilizar roteamento default, apenas uma rota precisa ser criada. Portanto, devemos, primeiramente, excluir as 3 rotas anteriormente configuradas. Para isso, utilizamos o comando **`no ip route`** **(a)**. Em seguida, configuramos a rota default utilizando os wildcards no lugar dos endereços de rede e da máscara **(b)**.

Note que, na saída do comando sh ip route ilustrada acima, o "gateway of last resort" agora aparece configurado. Note também que a rota aparece identificada por um **S***, demonstrando que trata-se de uma rota default. Mais um comando deve ser levado em conta quando rotas default são configuradas: o comando **`ip classless`**. Todos os routers Cisco são tidos como "classfull", ou seja, eles esperam que uma máscara de rede para cada interface seja configurada. Quando um router recebe um pacote para uma sub-rede destino que não se encontra na tabela de roteamento, ele descartará os pacotes, por default. Se você esta usando rotas default, você precisa utilizar o comando **`ip classless`** uma vez que nenhuma sub-rede remota constará na tabela de roteamento. Nos sistemas IOS 12.x em diante, o comando **`ip classless`** encontra-se ativado por default. Se você utilizar rotas default em routers rodando versões mais antigas do IOS, esse comando precisa ser digitado.



Como você deve ter imaginado, existe, sim, um modo mais prático de se gerenciar uma rede composta de vários routers. Este modo é conhecido como roteamento dinâmico (dynamic routing).

O processo de roteamento dinâmico utiliza protocolos para encontrar e atualizar tabelas de roteamento de routers. Esse modo é muito mais simples que roteamento estático, porém, você paga por essa simplicidade. Esse modo utiliza largura-de-banda (bandwidth) em links inter-routers, além de exigir que processamento seja feito pela CPU do router.

Um protocolo de roteamento (routing protocol) define as regras à serem utilizadas por um router quando esse se comunica com routers vizinhos. Os dois tipos de protocolos roteadores que estaremos discutindo são o RIP (Routing Information Protocol) e o IGRP (Interior Gateway Routing Protocol), uma vez que o exame CCNA não vai além desses 2 protocolos. Exemplos de outros protocolos existentes são: EIGRP (Enhanced Interior Gateway Routing Protocol) e OSPF (Open Shortest Path First).

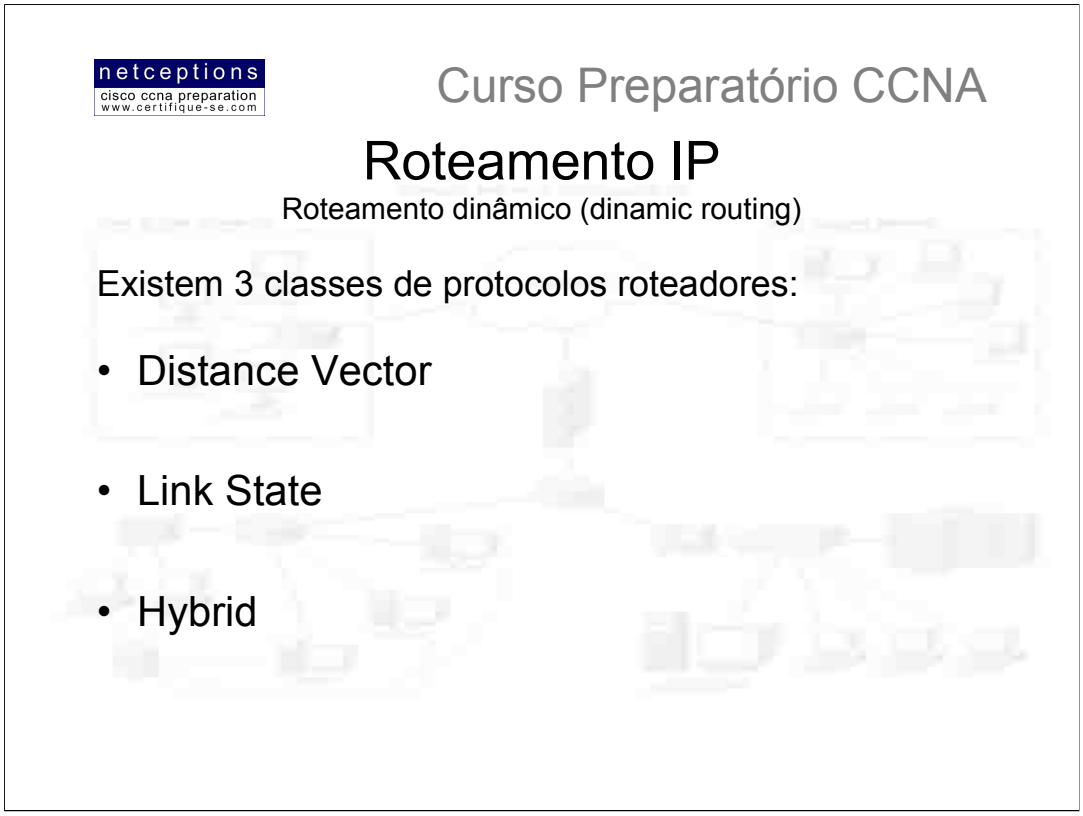
Os protocolos de roteamento utilizados em internetworks caem em 2 categorias: IGP (Interior Gateway Protocol) e EGP (Exterior Gateway Protocol). Protocolos IGP são usados para troca de informações entre routers de mesmo Sistema Autônomo (AS - Autonomous System). Um Sistema Autônomo é uma coleção de redes sob um mesmo domínio administrativo. Já os protocolos EGP são utilizados para comunicação entre routers pertencentes à Ass distintos. Um exemplo de um protocolo que se encaixa na categoria EGP seria o BGP (Border Gateway Protocol) - que não faz parte dos estudos para a prova CCNA, mas sim para o exame CCNP.

Distâncias Administrativas (Administrative Distances)

Quando configurando protocolos roteadores, você deve atentar para Distâncias Administrativas (ADs). Tratam-se de métricas utilizadas para classificar a confiabilidade das informações roteadas recebidas em um router vindas de um router vizinho. Distância Administrativa é um número inteiro compreendido entre 0 e 255, 0 sendo a rota mais confiável e 255 significando que nenhum tráfego passará por determinada rota. A tabela abaixo ilustra as Distâncias Administrativas que os routers Cisco utilizam para determinar qual rota utilizar para alcançar uma rede remota:

Rota Origem	Distância Padrão
Interface conectada	0
Rota estática	1
EIGRP	90
IGRP	100
OSPF	110
RIP	120
External EIGRP	170
Desconhecido	255

Se uma rede encontra-se diretamente conectada, esta sempre utilizará a interface conectada nesta rede. Se um administrador configurar rotas estáticas, o router “acreditará” nelas ao invés de rotas dinamicamente “aprendidas”. Os valores das ADs podem ser alterados. A tabela ilustra os valores default. No caso do valor de uma AD ser 255, essa rota nunca será escolhida.



Existem 3 classes quando falamos em protocolos de roteamento:

Distance Vector: Os protocolos de roteamento classificados nesta categoria utilizam a distância à rede remota para definição do melhor caminho. Cada vez que um pacote passa por um router, chamamos de "hop". No caso de protocolos de roteamento da classe distance vector, o menor número de "hops" até determinada rede remota determina a melhor rota. Ou seja, são protocolos que se baseiam na contagem de "hops" (hop count) para definição e escolha da melhor rota. Exemplos de protocolos que pertencem à esta classe são **RIP e IGRP**.

Link State: Tipicamente conhecidos como "caminho mais curto antes" (Shortest Path First), cada router cria 3 diferentes tabelas. Uma dessas tabelas mantém informações sobre redes diretamente conectadas, outra determina a topologia da rede como um todo e a última é a tabela de roteamento. Routers que utilizam protocolos link-state conhecem a rede como um todo mais profundamente que qualquer protocolo baseado em distance-vector. Um exemplo de protocolo de roteamento que pertence à essa classe é o **OSPF** (Open Shortest Path First).

Hybrid: tratam-se de protocolos de roteamento que possuem características de ambas as classes acima. Um exemplo de protocolo que pertence à essa classe é o**EIGRP** .

Não existe uma única solução que possa ser considerada a melhor para uso no dia-a-dia. A escolha do melhor protocolo à ser utilizado deve ser uma tarefa baseada em estudos de operações cotidianas e conhecimento das características de cada protocolo. Uma vez que você entenda como as diferentes classes de protocolo funcionam, você poderá, então, tomar a melhor decisão.

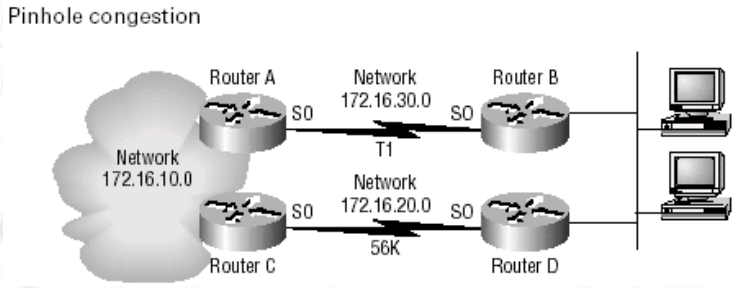
Para efeitos da prova CCNA, cobriremos apenas a primeira classe de protocolos (Distance Vector).

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Roteamento IP

Protocolos baseados em Distance Vector

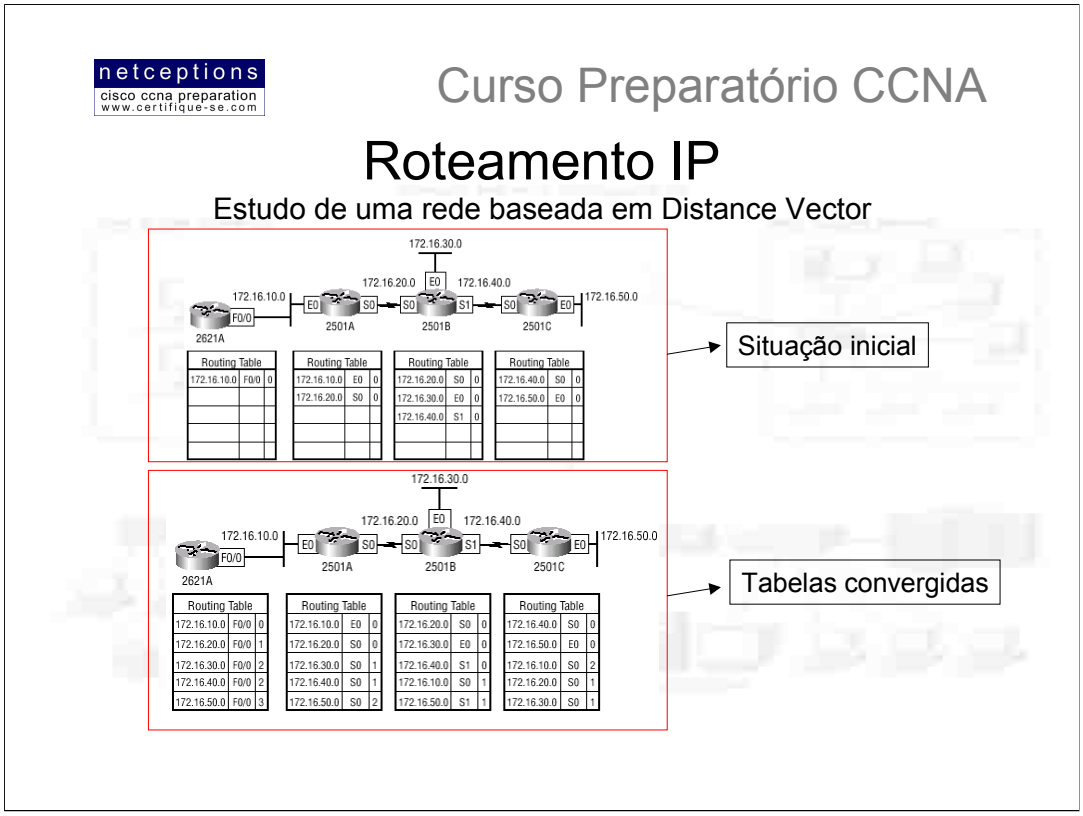


O algoritmo de roteamento distance vector envia as tabelas de roteamento completas para os routers vizinhos. Os router vizinhos, então, combinam as tabelas recebidas com as tabelas que já possuem e completam o mapa da rede. Esse processo é conhecido como “routing by rumour”, pois o router que recebe a atualização do router vizinho aceita a informação recebida como correta, sem verificar por si mesmo.

É possível encontrar uma rede que possua diversos links para uma mesma rede remota. Neste caso, a distância administrativa é o primeiro fator à ser checado. Se o valor das ADs forem os mesmos, outras métricas são utilizadas pelos protocolos roteadores para se determinar o melhor caminho para a rede remota.

O **RIP**, por exemplo, utiliza apenas a contagem de nós (hop count) para determinação da melhor rota para uma rede remota. Se RIP deparar-se com mais de um link para a mesma rede remota com a mesma contagem de nós, ele executará automaticamente o que chamamos de “round-robin load balance”, ou seja, distribuirá, alternadamente, a carga entre os links de igual custo (mesmo número de hops, no caso). RIP pode realizar balanceamento de carga para até 6 links com mesmo custo.

Entretanto, um problema com esse tipo de métrica aparece quando 2 links para uma mesma rede remota possuem diferentes largura-de-banda, porém, a mesma contagem de hops. A figura acima ilustra 2 links para a rede remota 172.16.10.0. Uma vez que a rede 172.16.30.0 encontra-se conectada à um link T1 com uma largura-de-banda de 1.544Mbps, e a rede 172.16.20.0 encontra-se conectada à um link de 56K, você desejaria que o router escolhesse o link T1 em vez do link 56K. Entretanto, uma vez que a contagem de hops é a única métrica utilizada pelo protocolo RIP, ambos os links serão vistos como tendo o mesmo custo. Isso é chamado de **pinhole congestion**.



É importante entender o que ocorre quando um protocolo de roteamento distance-vector é ativado. Na figura acima, vemos, em primeira instância, que os 4 routers, no início do processo, possuem em suas tabelas de roteamento apenas informações sobre redes diretamente conectadas. Uma vez que o protocolo de roteamento distance-vector é ativado em cada um dos routers, as tabelas de roteamento são atualizadas com todas as informações reunidas dos routers vizinhos. Cada router envia sua tabela de roteamento completa através de cada interface ativa no mesmo. As informações de cada tabela incluem o endereço da rede, a interface de saída para esse endereço e a contagem de hops para essa rede. Note que, para redes diretamente conectadas, o número da contagem é 0.

Na mesma figura, em segunda instância, temos as tabelas já atualizadas com informações sobre todas as redes de nossa pequena internetwork. Neste ponto, as tabelas de roteamento são tidas como convergidas. Quando os routers estão em convergência, nenhuma informação é transmitida. Eis o porque de o tempo de convergência ser crítico. Um dos maiores problemas com o protocolo RIP é seu tempo de convergência demasiado lento.

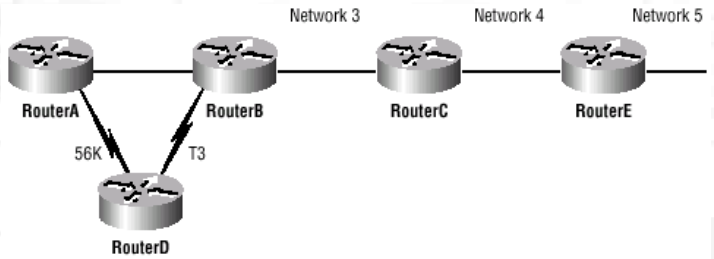
As tabelas de roteamento de cada router mantém informações sobre o endereço da rede remota, a interface pela qual o router enviará pacotes para alcançar essa rede e a métrica (hop count no caso).

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Roteamento IP

Routing Loops



Protocolos de roteamento distance-vector mantém registros de todas as mudanças ocorridas na rede através do broadcast periódico de atualizações das tabelas de roteamento para todas as interfaces ativas. Esse processo funciona bem, apesar de consumir largura-de-banda e utilização da CPU do router. Entretanto se uma queda na rede ocorre, problemas podem vir a acontecer. A lenta convergência dos protocolos de roteamento distance-vector pode causar atualizações inconsistentes nas tabelas de roteamento e loops podem vir a ocorrer.

Loops de roteamento (routing loops) podem ocorrer porque routers não são atualizados ao mesmo tempo. Imagine, na figura acima, que a interface para a rede 5, por algum motivo, falhe. Todos os routers na rede ilustrada sabem sobre a rede 5 pelo router E. O router A, em suas tabelas, possui as rotas para a rede 5 através dos routers B, C e E. Quando a rede 5 falha, o router E avisa o router C. Isso faz com que o router C pare de rotear pacotes para a rede 5 através do router E. Porém, os routers A, B e D ainda não sabem sobre a situação da rede 5, portanto, continuam enviando suas tabelas para atualização. O router C irá, eventualmente, enviar sua tabela atualizada e fará com que o router B pare de rotear pacotes para a rede 5, mas os routers A e D ainda não foram atualizados. Para eles, a rede 5 encontra-se disponível através do router B com uma métrica de 3 hops.

O router A envia uma mensagem regular a cada 30 segundos avisando que está ativo, e as rotas que ele conhece - que inclui o caminho para a rede 5. Os routers B e D, então, recebem as boas novas que a rede 5 pode ser alcançada através do router A, e então enviam mensagens avisando que a rede 5 está disponível. Qualquer pacote destinado à rede 5 irá então passar pelo router A, dele para o router B e depois, novamente para o router A. À isso chamamos de **routing loop**.

Esquemas adotados para evitar a ocorrência de loops

Maximum Hop Count

O problema descrito anteriormente é chamado de contagem ao infinito (counting to infinity) e é causado pela transmissão de informações distorcidas sobre a real situação da rede. Sem algum tipo de intervenção, a contagem de hops aumenta cada vez que um pacote passa por um router dentro do loop. Uma maneira de se resolver esse problema é definindo um número máximo de hops que um pacote de dados deve atravessar antes de ser descartado. Chamamos isso de **maximum hop count**. Protocolos distance-vector como RIP permitem uma contagem de hops até 15. Qualquer rede que requeira 16 hops é tida como inalcançável. Em outras palavras, após um loop de 15 hops, a rede 5 será considerada inativa. Essa é uma solução remediadora. Ela não elimina o loop. Os pacotes continuarão atravessando o loop, porém, agora, serão descartados após 15 hops, não permanecendo no loop indefinidamente.

Split Horizon

Outra solução para o problema de loops é chamado **split horizon**. Esse método reduz a transmissão de informações incorretas pela rede assim como reduz o overhead em redes baseadas em distance-vector através da imposição da regra que "informação não pode ser enviada de volta na mesma direção em que foi recebida". Isso preveniria o router A de enviar a atualização de tabela de roteamento recebida do router B de volta ao router B.

Route Poisoning

Outro modo de se prevenir a ocorrência de inconvenientes causados pela propagação de informações errôneas pela rede é conhecido como **route poisoning**. Por exemplo, quando a rede 5 falha, o router E inicia o "envenenamento da rota" (route poisoning) através da entrada em sua tabela de roteamento do valor 16 para a rede 5, ou seja, inalcançável. Uma vez efetuada essa operação de "envenenamento", o router C não mais esta suscetível à atualizações incorretas sobre a rota para a rede 5. Quando o router C recebe o envenenamento de rota do router E, ele envia uma atualização chamada **poison reverse** (veneno reverso) de volta ao router E. Isso assegura que todas as rotas no segmento tenham recebido a informação sobre a rota envenenada.

Holddowns

Finalmente, temos os chamados **holddowns**. Eles previnem que uma mensagem regular de atualização reative uma rota que, na verdade, encontra-se desativada. Também agem na prevenção de mudanças repentinas nas rotas, disponibilizando um certo tempo para que, ou uma rota que esteja desativada por algum motivo torne-se ativa, ou para que a rede se estabilize antes de decidir pela melhor rota. Holddowns também informam routers para restringir, por um específico período de tempo, quaisquer mudanças que possam afetar routers recém-removidos. Isso previne routers inoperantes de serem prematuramente restaurados nas tabelas de outros routers.

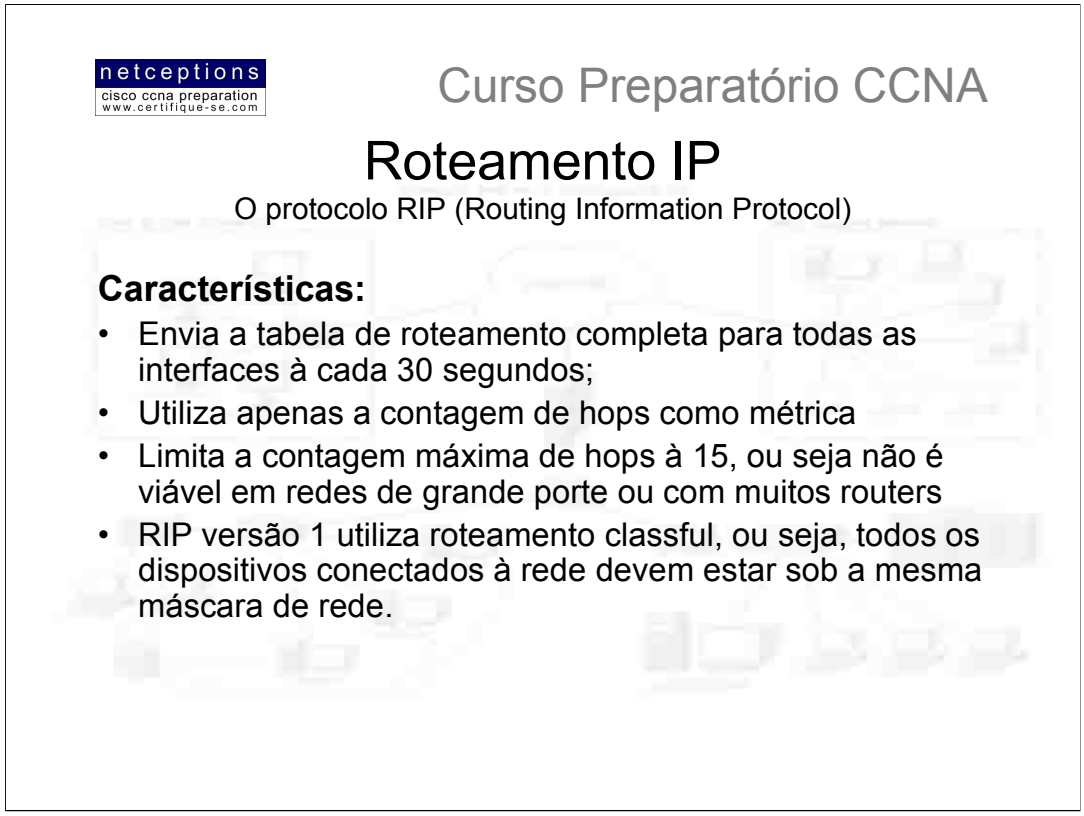
Quando um router recebe uma atualização de um router vizinho indicando que uma rede anteriormente acessível tornou-se inatingível, o timer do holddown se inicia. Se uma nova atualização chegar de um router vizinho com uma melhor métrica, o holddown é removido e os dados são passados. Entretanto, se uma atualização é recebida de um router vizinho antes da expiração do timer e esta possuir uma métrica inferior que a anterior, a atualização é ignorada e o timer continua funcionando. Isso permite mais tempo para a rede convergir. Holddowns utilizam o que chamamos de **triggered update** - que reseta o timer - para alertar routers vizinhos sobre mudanças na rede. Diferentemente de mensagens de atualização de routers vizinhos, triggered updates geram uma nova tabela de roteamento que é imediatamente enviada aos routers vizinhos uma vez que uma mudança foi detectada na rede como um todo. 3 são as ocasiões quando triggered updates resetam o timer do holddown:

1) O timer do holddown expira;

2) O router recebe uma requisição de processamento proporcional ao número de links na internetwork;

3) Outra atualização é recebida indicando que a situação da rede foi alterada

NOTA: O exame CCNA abrange os pontos acima com algum nível de detalhamento. É importante o entendimento de cada um dos esquemas de prevenção de loops.



RIP Timers:

RIP utiliza três diferentes tipos de timers para regular sua performance:

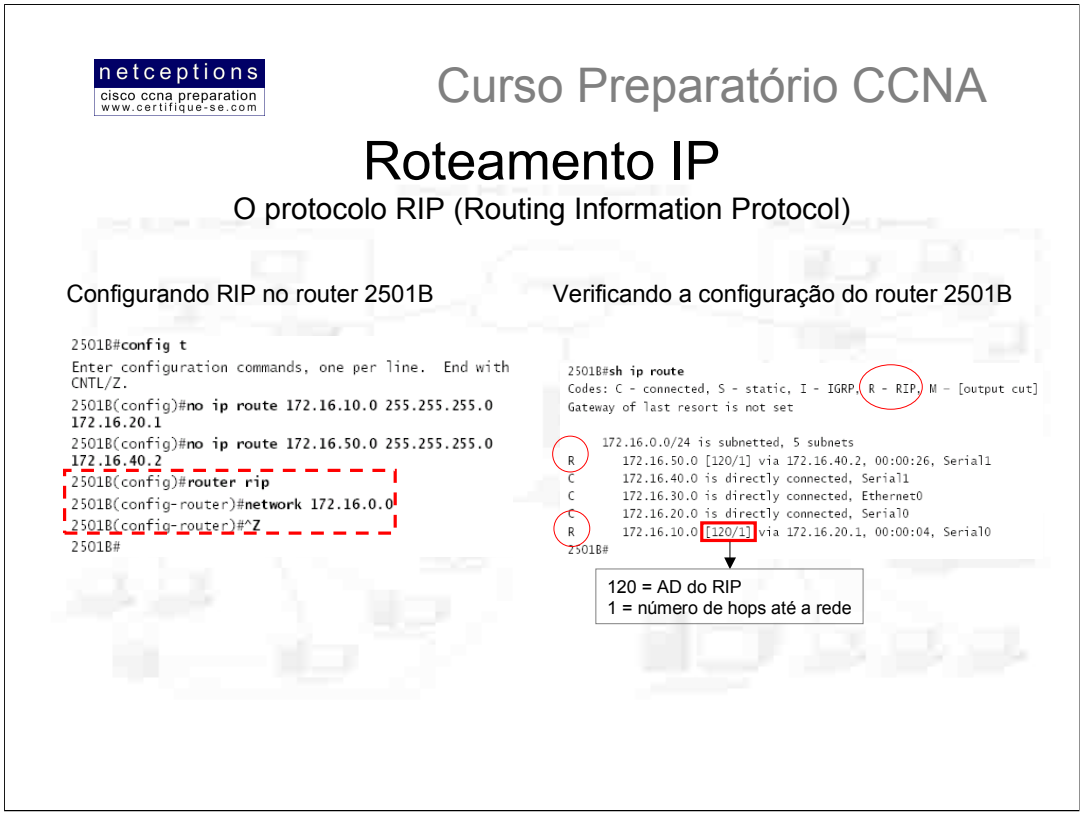
a) Route Update Timer - Estabelece um intervalo (geralmente **30 segundos**) entre as atualizações regulares, nas quais os routers enviam uma cópia completa de suas tabelas de roteamento para todos os routers vizinhos

b) Route Invalid Timer - Determina a quantidade de tempo que deve correr (normalmente **90 segundos**) antes de um router determinar que uma rota tornou-se inválida. Essa conclusão será atingida se não ocorrerem updates sobre uma determinada rota até o fim desse período.

c) Route Flush Timer - Estabelece o tempo (normalmente **240 segundos**) entre uma rota tornar-se inválida e sua remoção da tabela de roteamento. Antes de eliminar uma rota de sua tabela de roteamento, o router avisa os router vizinhos que determinada rota encontra-se inativa. O valor do Invalid Timer deve ser sempre menor que o do Flush Timer. Isso assegura ao router tempo suficiente para atualizar os routers vizinhos sobre a rota inválida, antes que sua tabela de roteamento seja atualizada.

OBS: Os valores padrão dos timers acima descritos devem ser decorados para a prova CCNA 2.0. Um modo fácil de memorizá-los é o seguinte:

RUT = 30 | RIT = RUT x 3 | RFT = RUT x 8



A configuração do RIP em um router é extremamente simples e direta. Eis o porque de termos estudado roteamento estático antes. Se você domina roteamento estático, a configuração de um router para roteamento dinâmico será extremamente fácil.

Na ilustração acima, configuramos RIP no router 2501B de nossa rede sugerida. Observe que, primeiramente devemos deletar as rotas estáticas anteriormente estabelecidas (comando **`no ip route`**) - caso isso não seja feito, o router continuará aceitando a configuração de rotas dinâmicas, porém, como rotas estáticas possuem uma AD de 1, estas sempre serão escolhidas pelo router.

Em seguida, utiliza-se o comando **`router rip`** para entrarmos no modo de configuração de roteamento (config-router). O comando **`network`** informa ao router qual rede à ser anunciada (172.16.0.0, no caso). Note que as subredes à serem anunciadas não são informadas, apenas a rede em si (classful). RIP encontrará todas as subredes e as anunciará, automaticamente.

O processo de configuração RIP não se altera para os outros routers, com exceção das rotas estáticas que devem ser deletadas. Como toda a rede participa da mesma máscara de rede, a única rede à ser informada será a 172.16.0.0.

Note que o comando **`CTRL+Z`** foi utilizado ao final do processo de configuração para retornar ao modo privilegiado (**`#`**).

Limitando a propagação do RIP

Você pode não desejar que sua rede RIP seja anunciada por toda a sua LAN ou WAN. Por exemplo, não há vantagens em anunciar sua rede RIP à Internet. Existem alguns mecanismos que evitam que indesejadas atualizações RIP se propaguem por toda a sua LAN ou WAN. O modo mais fácil de se fazer isso é através do comando **`passive-interface.`** Esse comando evita que uma atualização RIP seja propagada por uma determinada interface, porém, essa mesma interface pode receber atualizações RIP (torna-se passiva!). Eis um exemplo de como utilizar o comando:

```
RouterA#config t
RouterA(config)#router rip
RouterA(config-router)#network 10.0.0.0
RouterA(config-router)#passive-interface serial 0
```

O comando acima evitara que atualizações geradas pelo RIP sejam propagadas pela interface serial 0, porém, a interface ainda pode receber atualizações RIP.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Roteamento IP

O protocolo IGRP (Interior Gateway Routing Protocol)

Características:

- Proprietário Cisco (apenas routers Cisco podem utilizar IGRP);
- Contagem máxima de hops = 255 com default em 100 (útil em redes de grande porte)
- Utiliza largura de banda (bandwidth) e atraso da linha (delay of the line) como métricas default (composite metric)
- Permite que outras métricas como reliability, load e maximum transmit unit (MTU) também sejam utilizadas

O protocolo IGRP foi criado pela Cisco para superar as limitações impostas pelo RIP, como o limite de 15 para a contagem de hops. Apenas routers Cisco podem utilizar IGRP para roteamento, pois esse protocolo foi desenvolvido pela Cisco.

IGRP utiliza quatro diferentes tipos de timers para regular sua performance:

a) Route Update Timer - Estabelece um intervalo (default = **90 segundos**) entre as atualizações regulares, nas quais os routers enviam uma cópia completa de suas tabelas de roteamento para todos os routers vizinhos

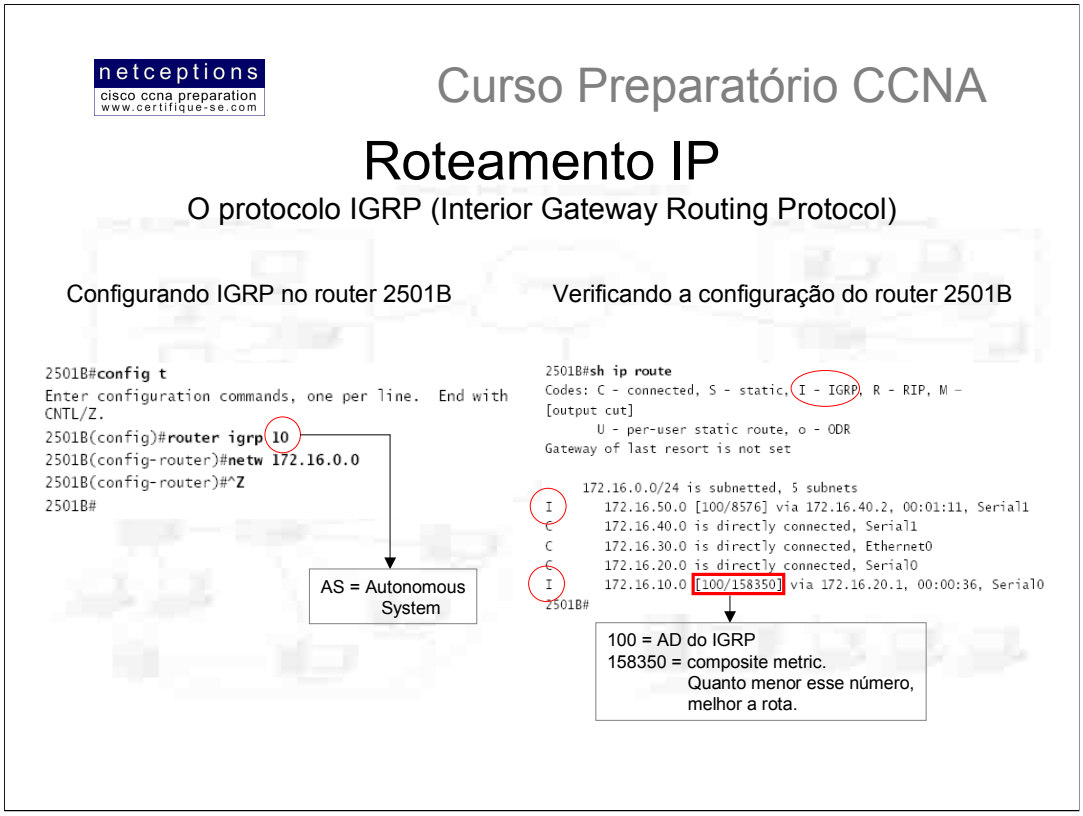
b) Route Invalid Timer - Determina a quantidade de tempo que deve correr (default = **3 x Update Timer**) antes de um router determinar que uma rota tornou-se inválida.

c) Holddown Timers - Especifica o período de holddown (default = **3 x Update Timer + 10 segundos**)

d) Route Flush Timer - Estabelece o tempo (default = **7 x Update Timer**) entre uma rota tornar-se inválida e sua remoção da tabela de roteamento. Antes de eliminar uma rota de sua tabela de roteamento, o router avisa os router vizinhos que determinada rota encontra-se inativa. O valor do Invalid Timer deve ser sempre menor que o do Flush Timer. Isso assegura ao router tempo suficiente para atualizar os routers vizinhos sobre a rota inválida, antes que sua tabela de roteamento seja atualizada.

OBS: Os valores padrão dos timers acima descritos devem ser decorados para a prova CCNA 2.0. Um modo mais fácil de memorizá-los é o seguinte:

RUT = 90 | RIT = RUT x 3 | HDT = RUT x 3 + 10 | RFT = RUT x 7



A configuração do IGRP em um router é bastante semelhante à configuração do RIP, com uma importante diferença: Você precisa informar o número do sistema autônomo (AS = Autonomous System). Todos os routers dentro de um mesmo sistema autônomo devem utilizar o mesmo número AS, ou eles não se comunicarão com informações de roteamento. Na ilustração acima, configuramos IGRP no router 2501B de nossa rede sugerida. Em seguida, utiliza-se o comando **`router igrp 10`** para entrarmos no modo de configuração de roteamento (config-router), onde 10 é o número do sistema autônomo. O comando **`network`** informa ao router qual rede à ser anunciada (172.16.0.0, no caso).

O processo de configuração IGRP não se altera para os outros routers.

Balanceando carga (load balancing) com IGRP

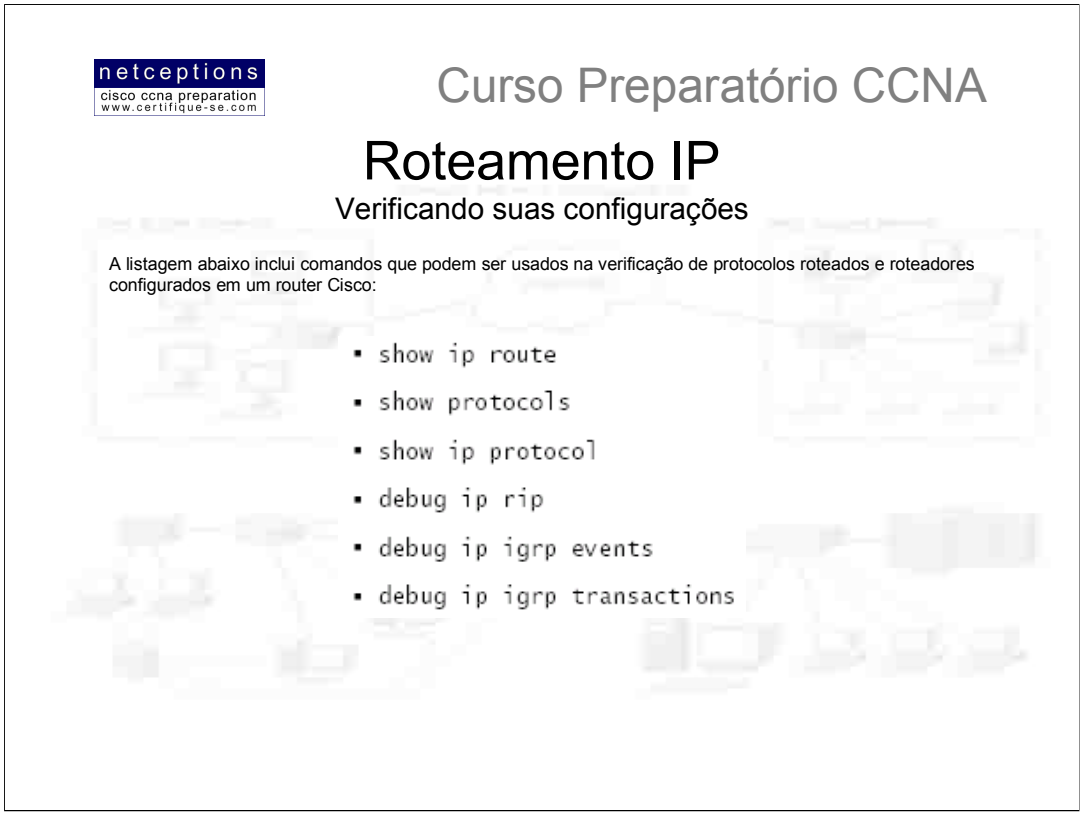
IGRP pode balancear a carga entre 6 links desiguais. Redes RIP devem ter a mesma contagem de hops para balancear carga. Já IGRP utiliza a largura-de-banda (bandwidth) para determinar como balancear a carga. No balanceamento de carga entre links desiguais, o comando **`variance`** controla o balanceamento entre a melhor métrica e a pior métrica aceitável. Outros dois comandos são utilizados para ajudar no controle da distribuição de tráfego entre rotas IGRP que dividem a carga:

`traffic-share balanced` e **`traffic-share min`**

```
Router(config-router)#variance ?
  <1-128>  Metric variance multiplier

Router(config-router)#traffic-share ?
  balanced  Share inversely proportional to metric
  min       All traffic shared among min metric paths
```

A saída acima ilustra o comando **`variance`**, que é o multiplicador de métrica. A saída do comando **`traffic-share`** nos mostra as 2 opções: **`balanced`** e **`min`**. A opção **`balanced`** informa o protocolo IGRP para compartilhar de modo proporcionalmente inverso às métricas, enquanto que a opção **`min`** informa o protocolo IGRP para utilizar no processo apenas rotas de menor custo.



O primeiro comando da lista acima, **`sh ip route`**, já foi ilustrado nas páginas anteriores. Portanto, não falaremos dele aqui.

O comando **`sh protocols`** é bastante útil, pois apresenta os endereços de rede configurados em cada interface:

2501B#**sh protocol**

Global values:

Internet Protocol routing is enabled

Ethernet0 is up, line protocol is up

Internet address is 172.16.30.1/24

.

Na saída acima, verificamos o endereço IP das interfaces configuradas. Caso IPX ou Appletalk também estivessem configuradas, seriam apresentadas da mesma forma.

O comando **`sh ip proto`** apresenta em sua saída os protocolos de roteamento configurados em seu router. O comando **`sh ip proto`** também apresenta os valores dos timers utilizados pelos protocolos roteadores configurados. Outras informações incluídas na saída do comando **`sh ip proto`** são: AS, redes sendo anunciadas, gateways, e ADs (distância administrativa).

O comando **`debug ip rip`** envia as atualizações propagadas e recebidas pelo router para a sessão de console (se você estiver efetuando uma sessão Telnet, você deverá digitar o comando **`terminal monitor`** para ser capaz de receber a saída dos comandos de debug). Essa é uma grande ferramenta para identificação de problemas. Para desligar o modo "debug", use o comando **`undebug all`** ou **`no debug all`**. A abreviação **`un all`** também pode ser usada.

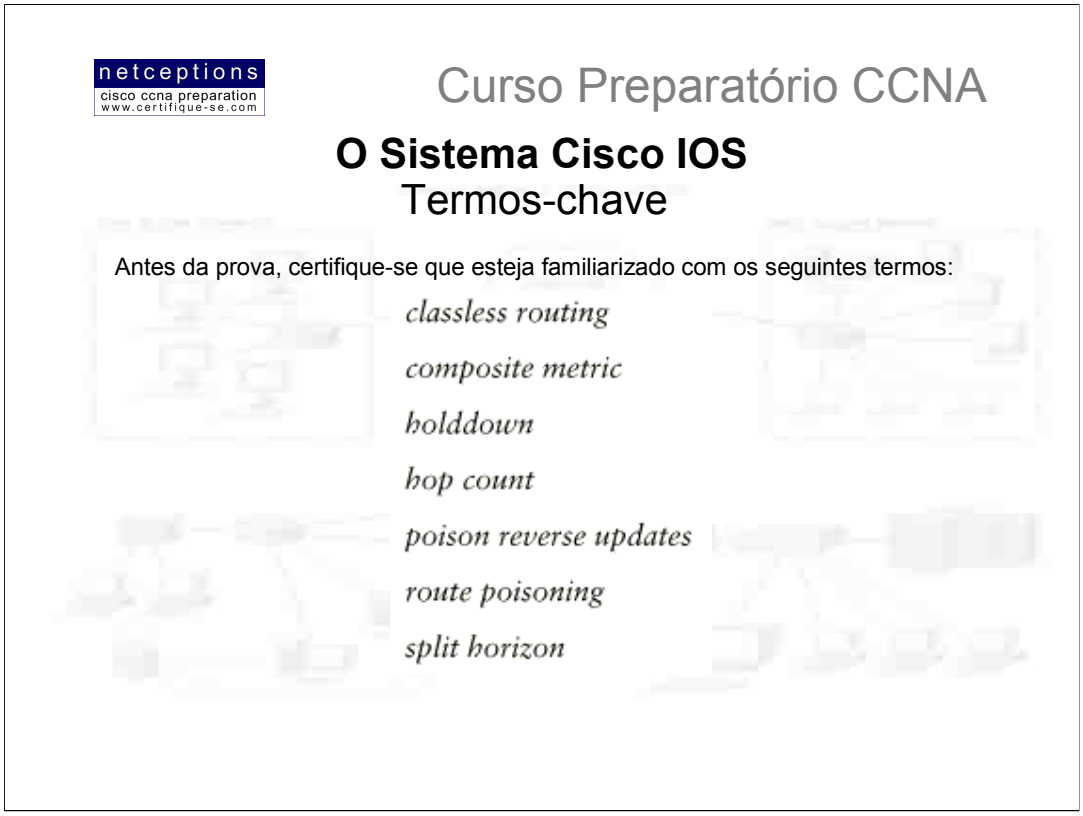
Com o comando **`debug ip igrp`** você tem 2 opções: **`events`** e **`transactions`**.

O comando **`debug ip igrp events`** apresenta um resumo das informações de roteamento IGRP que estão sendo propagadas pela rede. Dados como origem e destino de cada atualização, assim como o número de routers em cada uma são apresentadas. Informações sobre rotas individuais **NÃO** são apresentadas com esse comando.

Finalmente, o comando **`debug ip igrp transactions`** apresenta requisições por atualizações de routers vizinhos e as atualizações enviadas pelo seu router para esses routers.

Utilize **`un all`** para sair do modo debug.

NOTA: Ë muito importante saber como verificar as configurações de um router, as informações trazidas por cada comando e o que os comandos debug apresentam.



Resumo da aula 5:

Nesta aula cobrimos roteamento IP em detalhes. É importante que você entenda os conceitos abrangidos nesta aula uma vez que tudo o que é feito com um router Cisco, em algum momento, envolve a configuração de roteamento IP.

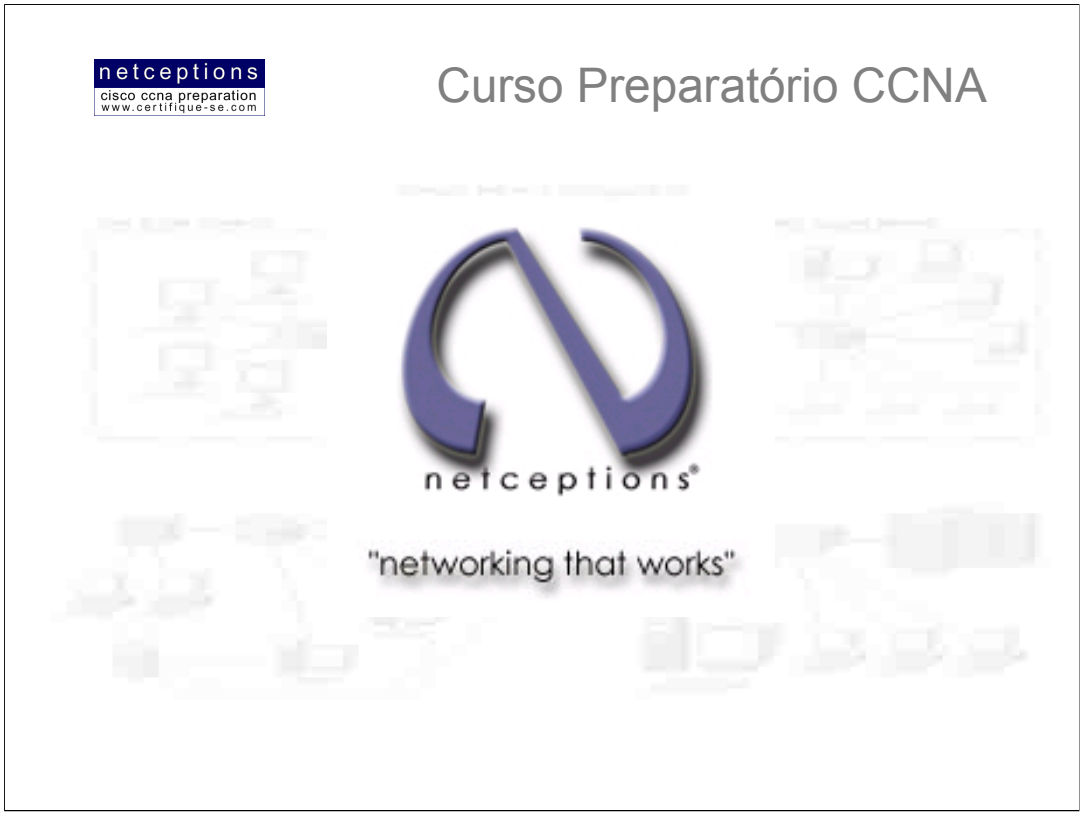
Nesta aula tratamos dos seguintes tópicos:

- Roteamento IP e como frames são utilizados para transportar pacotes de dados entre routers e para o destino;
- Roteamento estático;
- Roteamento default;
- Roteamento dinâmico (distance-vector routing)
- Routing loops
- Configuração e verificação de RIP
- Configuração e verificação de IGRP

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

FIM AULA 05



Apostila Aula 6

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Aula 6 / Módulo I
Gerenciando uma Rede Cisco

- Backup e Recuperação do Sistema IOS
- Backup e Recuperação da configuração do router
- Reunião de informações sobre dispositivos vizinhos através dos recursos CDP e Telnet
- Resolução de hostnames
- Teste da rede através dos recursos Ping e Trace

Neste módulo estaremos vendo como gerenciar routers Cisco em uma rede de grande porte.

O sistema IOS e arquivos de configuração residem em diferentes localizações em um dispositivo Cisco, e é importante o entendimento de onde estes arquivos se encontram e como os mesmos funcionam.

Analisaremos neste módulo, também, os componentes de um router, a sequência de inicialização (boot sequence) do mesmo, e o “configuration register” na recuperação de senhas “esquecidas” ou perdidas.

Os itens acima listados serão cobertos neste módulo.

Antes de configurar e atuar na resolução de problemas (troubleshooting) de uma internetwork Cisco, você deve conhecer os principais componentes de um router Cisco, assim como entender o que estes componentes fazem:

Bootstrap: Armazenado no microcode da ROM, o bootstrap é utilizado na inicialização de um router, para ativá-lo. Ele se encarrega do "boot" do router e do carregamento do IOS.

POST (Power-On Self Test): Também armazenado no microcódigo da ROM, o POST é utilizado na checagem básica de hardware do router e determina quais interfaces encontram-se presentes.

ROM Monitor: Armazenado no microcódigo da ROM, o ROM Monitor é usado na identificação de problemas e testes de fabricação.

Mini-IOS: Também chamado de RXBOOT ou bootloader, o Mini-IOS é uma versão reduzida do IOS alojada na ROM que pode ser usado na ativação de uma interface e no carregamento do sistema IOS na FLASH. O Mini-IOS também pode desempenhar outras tarefas de manutenção.

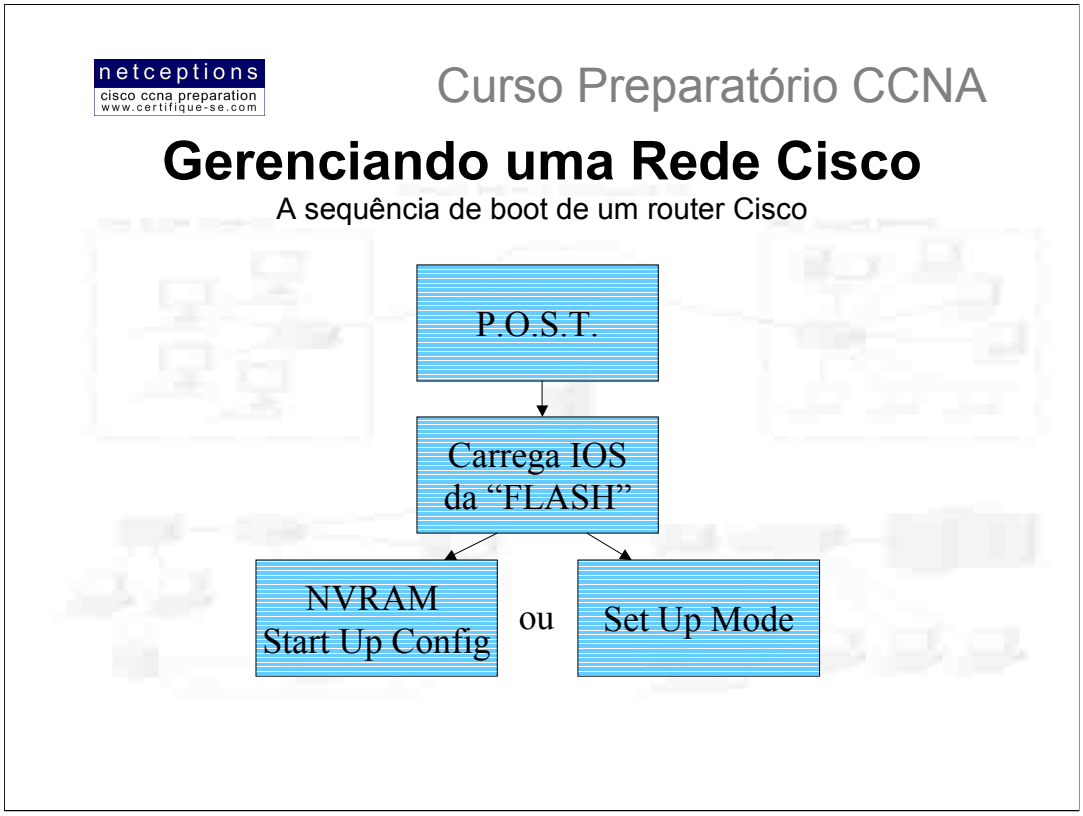
RAM: Usada no armazenamento (buffer) de pacotes, tabelas de roteamento, e outras estruturas de dados que permitem ao router funcionar adequadamente. A configuração ativa (Running-Config) é armazenada na RAM e, em alguns routers, o IOS pode ser rodado à partir da RAM.

ROM: Usada para inicializar o router e na sua manutenção.

FLASH: Usada para armazenamento do sistema IOS. O conteúdo da memória FLASH não é perdido quando um router é reiniciado.

NVRAM: Usada no armazenamento da configuração (Startup-Config) em routers e switches. Seu conteúdo também é mantido mesmo que um router seja desligado.

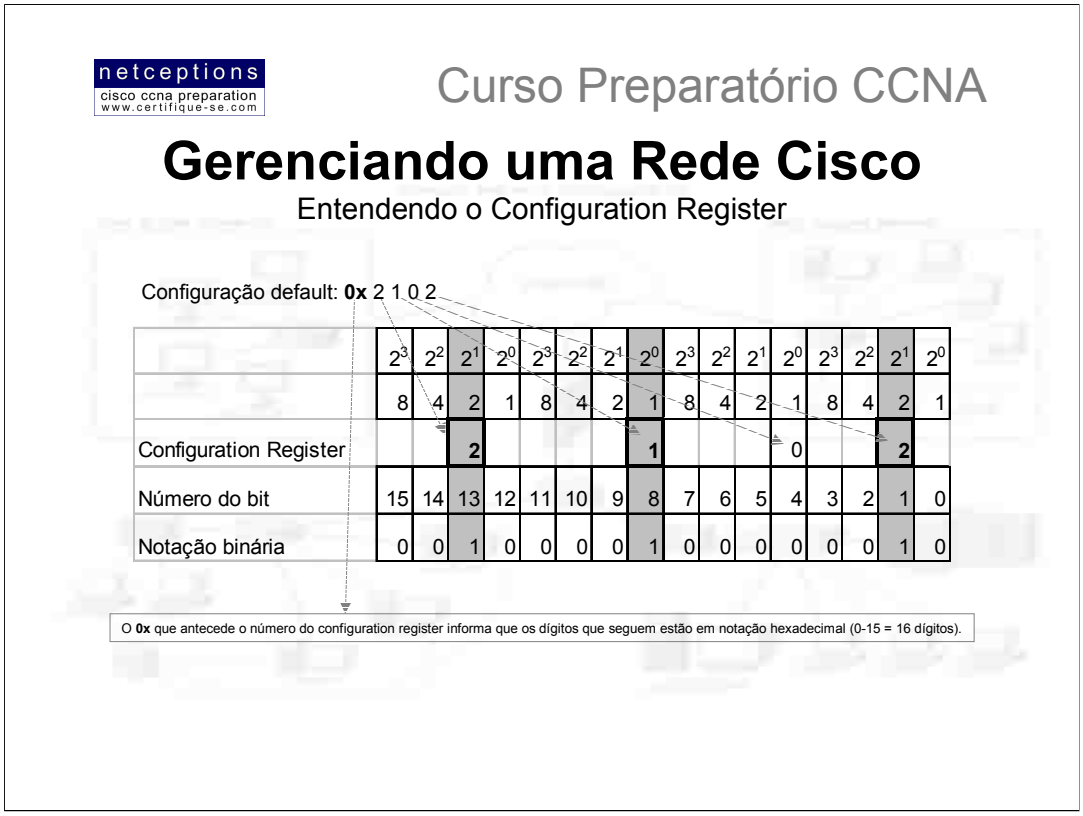
Configuration Register: Define como um router será inicializado. A configuração ativa pode ser vista através do comando **`show version`**.



Quando você liga um router Cisco pela primeira vez, ele executa uma checagem geral do hardware chamada POST (Power On Self Test) e, se caso não existam problemas, o software **bootstrap,** armazenado na ROM, irá procurar e carregar o sistema IOS da memória FLASH (default), ou outro local específico. A FLASH é um tipo de memória eletronicamente deletável, programável e acessível apenas para leitura (Erasable Programmable Read-Only Memory = EEPROM).

O IOS será carregado e então ele procurará por um arquivo de configuração chamado **startup-config**, que fica armazenado por default na memória RAM não volátil (NVRAM). Esse arquivo apenas encontrar-se-á armazenado na NVRAM se um administrador, previamente, efetuou o backup da configuração ativa na RAM, através do comando **`copy run start`**. Caso um arquivo de configuração encontre-se armazenado na NVRAM, o router irá carregá-lo e, em seguida, encontrar-se-á operacional.

Caso não exista nenhum arquivo de configuração na NVRAM (ex. router novo ou o arquivo foi deletado), o router irá trazer então o que chamamos de *setup mode* (vide ilustração). Este seria um modo que permite a configuração do router passo-a-passo. Você pode optar pela configuração via linha de comando a qualquer momento digitando o comando **setup** no modo de configuração global (global configuration mode). O modo setup cobre apenas alguns comandos genéricos, mas é bastante útil quando você não sabe como configurar determinados protocolos, como bridging ou DCnet, por exemplo.



Todos os routers Cisco possuem um software registrador de 16-bits, que fica armazenado na NVRAM. Por default, o configuration register é configurado para carregar o sistema IOS da FLASH e para procurar o startup-config na NVRAM.

Os 16 bits do configuration register correspondem ao intervalo 0-15, lidos da esquerda para a direita (veja esquema acima). A configuração default encontrada nos routers Cisco é 0x2102. Isso significa que os bits 13,8 e 1 encontram-se "ligados" (veja esquema). Note que cada grupo de 4 bits é lido em notação binária com valores 1, 2, 4 e 8, da direita para a esquerda.

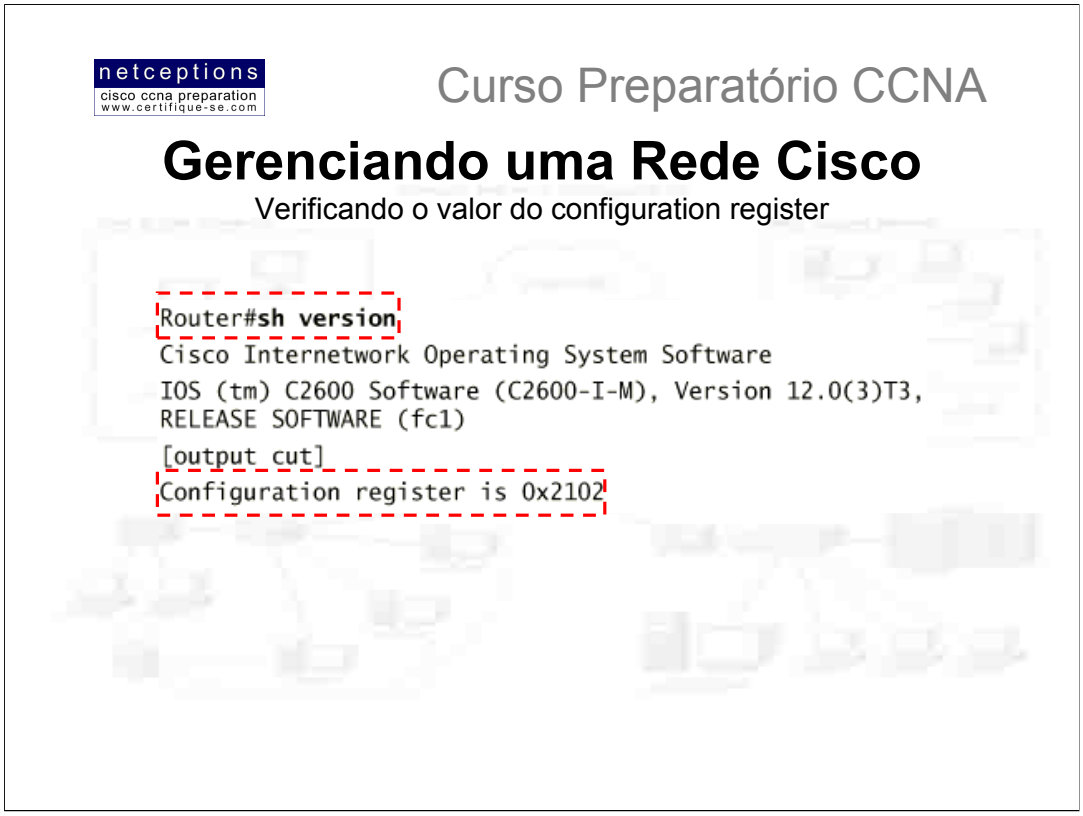
O **0x** que antecede o número do configuration register informa que os dígitos que seguem estão em notação hexadecimal (0-15 = 16 dígitos).

A tabela à seguir ilustra os significados dos bits. Note que o bit 6 pode ser utilizado para que se ignore o conteúdo da NVRAM. Esse recurso é utilizado na recuperação de senhas, que veremos mais adiante.

Bit	Hex	Descrição
0-3	0x0000-0x000F	Campo de boot (veja tabela abaixo)
6	0x0040	Ignora o conteúdo da NVRAM
7	0x0080	Habilita o bit OEM
8	0x0100	Disabilita o <BREAK>
10	0x0400	Broadcast IP com 0s
11-12	0x0800-0x1000	Velocidade da linha do console
13	0x2000	Inicializa via software presente na ROM, caso inicialização via rede falhe
14	0x4000	Broadcasts IP sem valores da rede
15	0x8000	Habilita mensagens de diagnóstico e ignora o conteúdo da NVRAM

O campo de boot (boot field), que consiste do intervalo de bits 0-3 no configuration register, controla a sequência de inicialização (boot) do router. Abaixo, descrevemos os bits do campo de boot:

Campo de boot	Significado	Utilização
0	Modo ROM monitor	Para inicialização em modo ROM monitor, configure o configuration register para 2100. O router deve ser manualmente inicializado através do comando `b`. O prompt `rommon>` será apresentado
1	Inicializa com imagem da ROM	Para inicializar o router à partir de uma imagem do IOS armazenada na ROM, configure o configuration register para 2101. O prompt `(boot)>` será apresentado
02-F	Especifica um nome de arquivo de boot default	Qualquer valor, de 2102 à 210F informa o router para utilizar os comando de inicialização especificados na NVRAM.



Você pode checar o valor em uso do configuration register através do comando **`show version`**, conforme ilustrado acima. A última informação (em destaque) é o valor do configuration register em uso. Nesse exemplo, o valor é 0x2102, que é o valor default. Note também que a saída do comando **`show version`** nos informa a versão do sistema IOS em uso (12.0(3)T3).

Alterando o configuration register

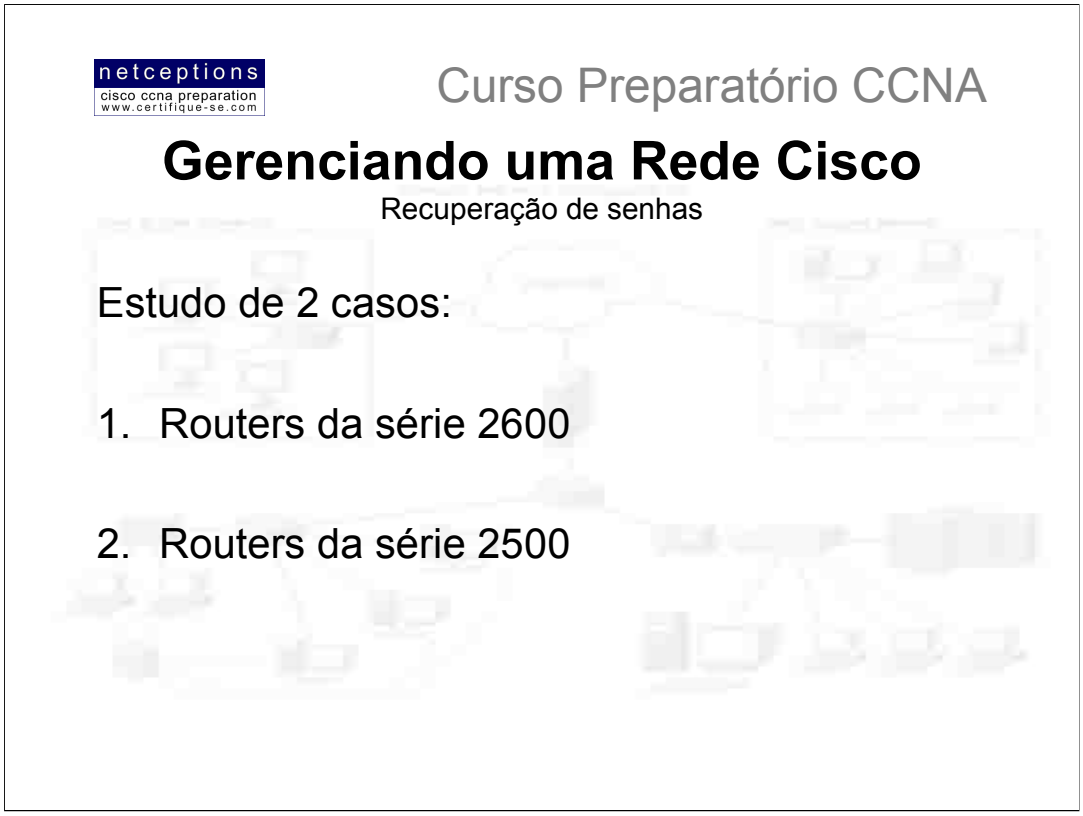
Você pode alterar o valor do configuration register para modificar o modo como o router inicializa e opera, como segue:

- Colocar o sistema para Modo Monitor
- Selecionar uma fonte para inicialização e um nome de arquivo boot default
- Habilitar e desabilitar o recurso <BREAK>
- Controlar endereços de broadcast
- Definir a velocidade (baud rate) da linha Console
- Carregar o sistema IOS da ROM
- Habilitar inicialização via servidor TFTP

NOTA: Antes de alterar os valores do configuration register, certifique-se que a configuração atual esteja anotada. Use o comando **`show version`** para obter esta informação.

Para alterar o valor do configuration register, utilize o comando **`config-register`**.No exemplo abaixo, os comandos digitados informam ao router para inicializar a partir da imagem existente na ROM. Em seguida, o valor do configuration register (que apenas terá efeito após reinicialização do router) é apresentado:

```
Router(config)#config-register 0x0101
Router(config)#^Z
Router#sh ver
[cut]
Configuration register is 0x2102 (will be 0x0101 at next
reload)
```



Caso 1: Routers da série 2600:

Para recuperar o acesso ao router cuja senha foi perdida, deve-se, antes de mais nada, no modo EXEC (prompt "**>**") digitar o comando **`config-register 0x01`**, para permitir que um "break" seja executado na inicialização do router.

Feito isso, desligue o router, ligue-o novamente, e pressione a tecla "BREAK" (CTRL+C) nos 60 segundos iniciais.

No prompt apresentado (algo como **`rommon>`**), digite o comando **`confreg 0x2142`**, que fará com que o router ignore a configuração na NVRAM, indo direto para a RAM.

Digite o comando "reset", para reinicializar o router. Como nenhum arquivo de configuração encontra-se armazenado na RAM, o router começará do ZERO (setup mode). Opte por não entrar no modo setup e, uma vez no modo de comando, digite **`enable`** para entrar em modo privilegiado. Neste ponto, você tem 2 opções: Se a senha perdida for a enable, basta digitar o comando **`show startup-config`** e identificar a senha na sadia apresentada, uma vez que ela não é criptografada. Se esse for o caso, anote a senha, mude o registrador de volta para o valor original, reinicie o router e caso encerrado. Caso você tenha configurado a senha enable secret, isso não resolverá, uma vez que a mesma é criptografada. Neste caso, copie a configuração da NVRAM para a RAM (**`copy start run`**), entre no modo de configuração global (**`config t`**) e defina uma nova senha enable secret. Mude, então, o registrador para o valor inicial (para procurar a configuração na NVRAM), copie a configuração da RAM para a NVRAM (**`copy run start`**), reinicie o router e pronto.

Caso 2: Routers da série 2500:

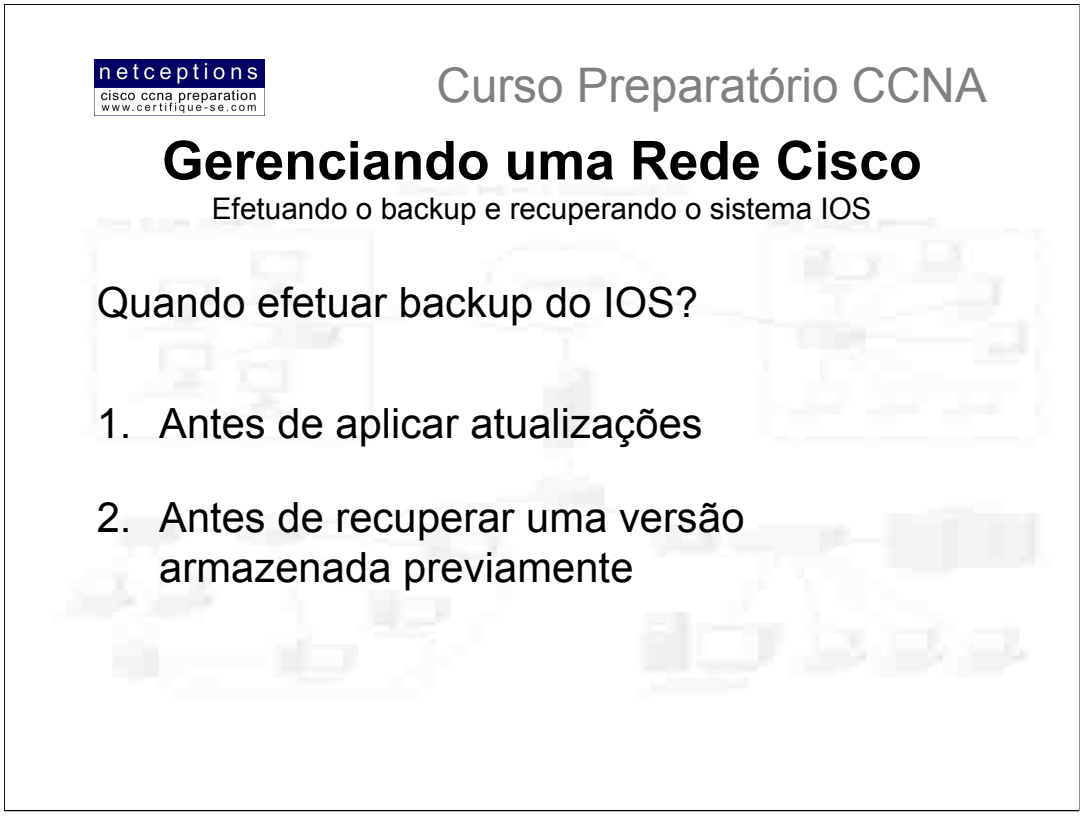
Para routers da série 2500, os procedimentos para recuperação de senha são muito parecidos com os descritos acima, com algumas exceções:

Na linha 2500, ao se efetuar o "BREAK", deve-se, no prompt apresentado (algo como **>** somente) digitar o comando **`o`**. Feito isso, um menu será apresentado na tela listando as opções para configuração do configuration register. Para alterar a configuração, utilize o comando **`o/r`**, seguido do novo valor:

```
>o/r 0x2142
```

Após alterado o valor do configuration register, utilize o comando **`I`** para reinicializar o router. A partir deste ponto, os passos à seguir são os mesmos descritos para a linha 2600.

Não se esqueça de configurar o configuration register com o valor original após os procedimentos para recuperação de senha terem sido efetuados.



Antes de efetuar um upgrade no sistema IOS, uma cópia da versão atual deve ser feita caso existam problemas com a imagem à ser instalada. Normalmente, backups são feitos em hosts TFTP. Por default, o sistema IOS encontra-se armazenado na FLASH do router. Descreveremos nesta sessão como analisar a quantidade de memória disponível na FLASH, os procedimentos para se copiar o sistema IOS da FLASH para um host TFTP e, finalmente, como recuperar o sistema IOS de um host TFTP para a FLASH.

Antes de efetuar um upgrade no IOS de um router, devemos nos certificar que há espaço suficiente na FLASH do mesmo para tal operação. Você pode verificar a quantidade de memória disponível na FLASH, assim como os arquivos armazenados na mesma através do comando **`show flash`**:

```
Router#sh flash
System flash directory:
File  Length   Name/status
  1   8121000  c2500-js-l.112-18.bin
[8121064 bytes used, 8656152 available, 16777216 total]
16384K bytes of processor board System flash (Read ONLY)
Router#
```

Note que o nome do arquivo, no exemplo acima, é `c2500-js-l.112-18.bin`. O nome do arquivo é específico à cada plataforma, e tem o seguinte significado:

`C2500` – indica a plataforma

`j` – indica que o arquivo é uma enterprise image (versão corporativa)

`s` – indica que o arquivo contém capabilidades estendidas

`l` – indica que o arquivo pode ser movido da FLASH se necessário e que o mesmo não se encontra comprimido

`112.18` - número de versão / revisão do arquivo (versão 11.2, revisão 18)

`.bin` - indica que o Cisco IOS é um binário executável

A última linha da saída apresentada indica que trata-se de uma FLASH com capacidade de 16MB (16.384KB). Portanto, se o arquivo que você deseja copiar para a mesma tem, vamos supor, um tamanho de 10MB, você saberia que tem espaço suficiente para o mesmo. Uma vez verificado que a FLASH possui espaço suficiente para acomodar a nova imagem à ser copiada, o processo de backup pode prosseguir.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Gerenciando uma Rede Cisco

Efetuando o backup do sistema IOS para um TFTP host

```
Router#copy flash tftp
System flash directory:
File  Length   Name/status
  1   8121000  c2500-js-l.112-18.bin
[8121064 bytes used, 8656152 available, 16777216 total]
Address or name of remote host [255.255.255.255]?
192.168.0.120
Source file name? c2500-js-l.112-18.bin
Destination file name [c2500-js-l.112-18.bin]? (press
enter)
Verifying checksum for 'c2500-js-l.112-18.bin')file
#1)...OK
Copy '/c2500-js-l.112-18' from Flash to server
  as '/c2500-js-l.112-18'? [yes/no]y
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!! [output cut]
Upload to server done
Flash copy took 00:02:30 [hh:mm:ss]
Router#
```

Para copiar o sistema IOS para um host TFTP, utilize o comando **copy flash tftp**. Os únicos dados que lhe serão pedidos são: 1) nome do arquivo fonte e 2) endereço IP do host TFTP.

Antes de iniciar a operação de backup, é uma boa idéia testar a conexão entre o router e o TFTP host. Isso pode ser feito através do comando **ping**. No exemplo abaixo, ilustramos esse procedimento para um TFTP host com endereço IP 192.168.0.120:

```
Router#ping 192.168.0.120
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.120, timeout
is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max
= 4/4/8 ms
```

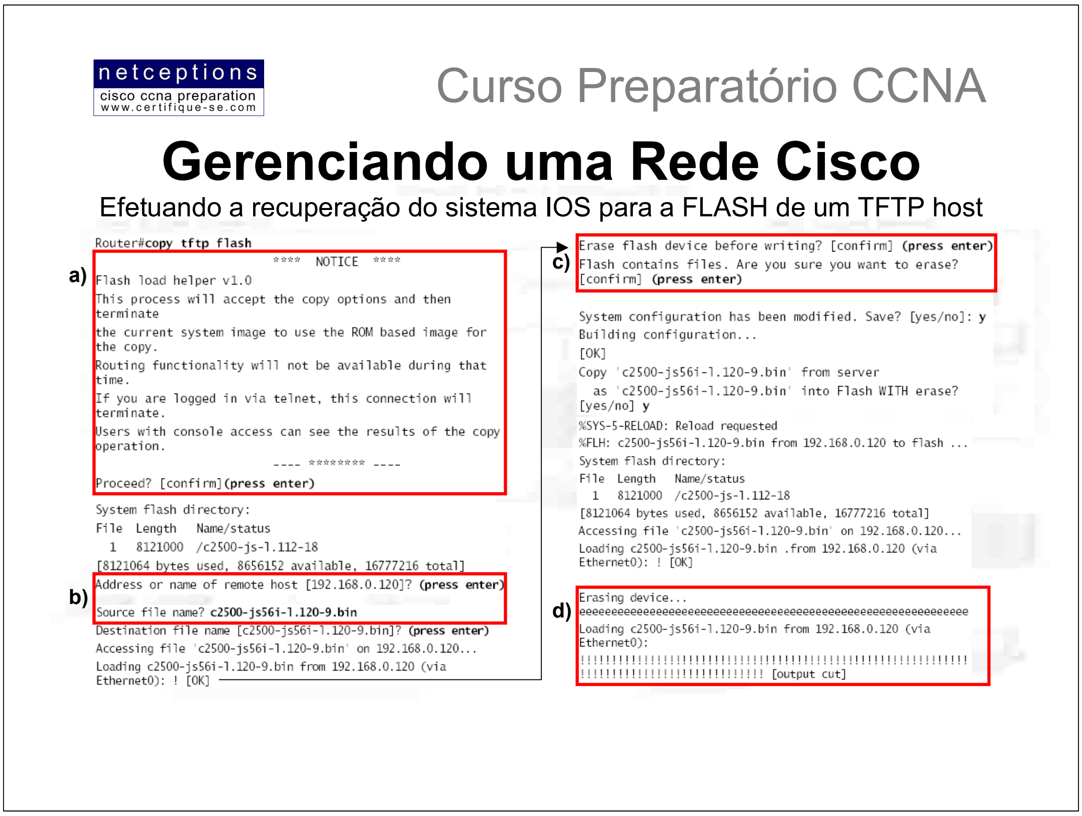
Após certificar-se que a conectividade entre as pontas é satisfatória, efetue o processo de backup utilizando o comando **copy flash tftp**, conforme ilustrado na figura acima. Note que, logo após a digitação do comando o nome do arquivo armazenado na FLASH é apresentado, facilitando as coisas para você. Você pode, simplesmente, copiar o nome do arquivo apresentado e colá-lo, quando requisitado.

Lembre-se:

Source file name = nome do arquivo apresentado após a digitação do comando

Address of remote host = endereço IP do TFTP host

O comando copy flash tftp não pede que você entre com a localização de qualquer arquivo, ou pede que você escolha onde colocar o arquivo copiado. Ele simplesmente transfere o arquivo para um diretório padrão no host TFTP. Caso este diretório não exista, o processo falhará.



Você pode precisar recuperar um arquivo IOS armazenado em um host TFTP para a FLASH, para substituir um arquivo que tenha sido corrompido ou para substituir a versão presente na FLASH por uma mais nova. Para recuperar um arquivo armazenado em um TFTP host, utilize o comando **`copy tftp flash`**. Você será prontificado à fornecer o endereço IP do TFTP host e o nome do arquivo que você deseja copiar para a FLASH **(b)**.

Antes do iniciar o processo, certifique-se que o arquivo que você deseja copiar para a FLASH se encontra no diretório default do host TFTP. Uma vez executado o comando, TFTP não irá perguntar à você onde se encontra o arquivo. Se o arquivo que você deseja copiar para a FLASH não se encontrar no diretório default do host TFTP, o processo não irá funcionar.

Uma vez executado o comando, uma mensagem surgirá na tela **(a)** informando que o router irá reinicializar e utilizar o IOS presente na ROM para efetuar essa operação.

O próximo passo é informar o endereço IP do host TFTP e o nome do arquivo à ser copiado **(b)**. Uma vez que o router já tenha utilizado um host FTP, ele “lembrará” do endereço IP do mesmo **(b)**.

Uma vez informado os dados requisitados, o router irá pedir que você confirme o entendimento de que o conteúdo da memória FLASH será apagado durante o processo **(c)**.

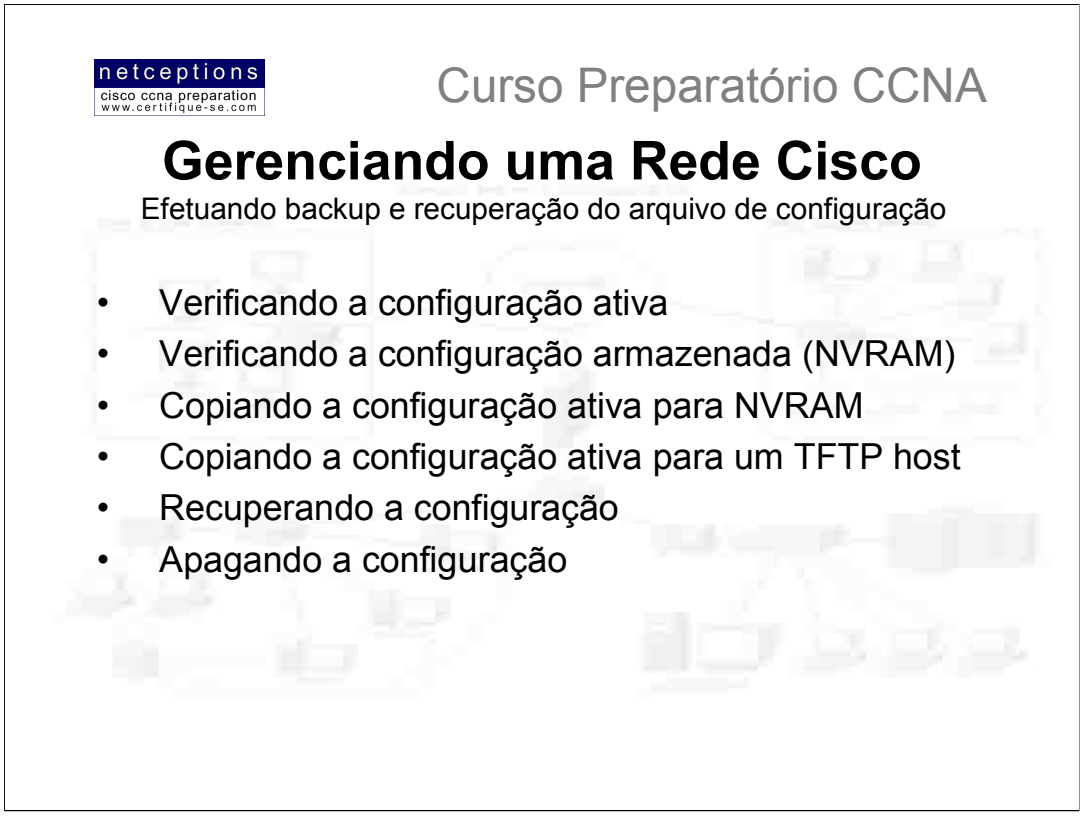
Uma vez confirmado (3 vezes), o router irá reiniciar e carregar uma versão simplificada do IOS presente na ROM, uma vez que o IOS da FLASH não pode ser alterado se estiver em uso. Feito isso, o conteúdo da FLASH é apagado e o arquivo presente no TFTP host é copiado para a FLASH. A fileira de “e”s indica que o conteúdo da FLASH está sendo apagado **(d)**. Cada ponto de exclamação (!) indica que um segmento UDP foi transferido com sucesso **(d)**.

Uma vez completada a operação, a seguinte mensagem deve ser apresentada:

```
[OK - 10935532/16777216 bytes]
Verifying checksum... OK (0x2E3A)
Flash copy took 0:06:14 [hh:mm:ss]
%FLH: Re-booting system after download
```

Uma vez que o novo arquivo tenha sido copiado para a FLASH e que a checagem de erro (checksum) tenha ocorrida sem problemas, o router é reiniciado para que o novo IOS seja executado.

NOTA: Routers Cisco podem agir como hosts TFTP para uma imagem do IOS que esteja armazenada na FLASH. O comando para isso é: **`(config)#tftp-server system [nome-do-arquivo-IOS]`**



Qualquer mudança que você efetua na configuração de um router fica armazenada no arquivo running-config, que é a configuração ativa, armazenada na RAM. Caso você não execute o comando **`copy run start`**, toda a configuração será perdida caso o router seja desligado, ou reiniciado. Você pode desejar efetuar um backup adicional do seu arquivo de configuração, na eventualidade do router "pifar" de vez, ou para documentação. Descreveremos, à seguir, como proceder para copiar a configuração ativa para a NVRAM e para um host TFTP, e como recuperar essa configuração.

Para verificar a configuração ativa (running-config), utilize o comando **`sh run`**. Esse comando informa, entre outras coisas, a versão do IOS ativa no router.

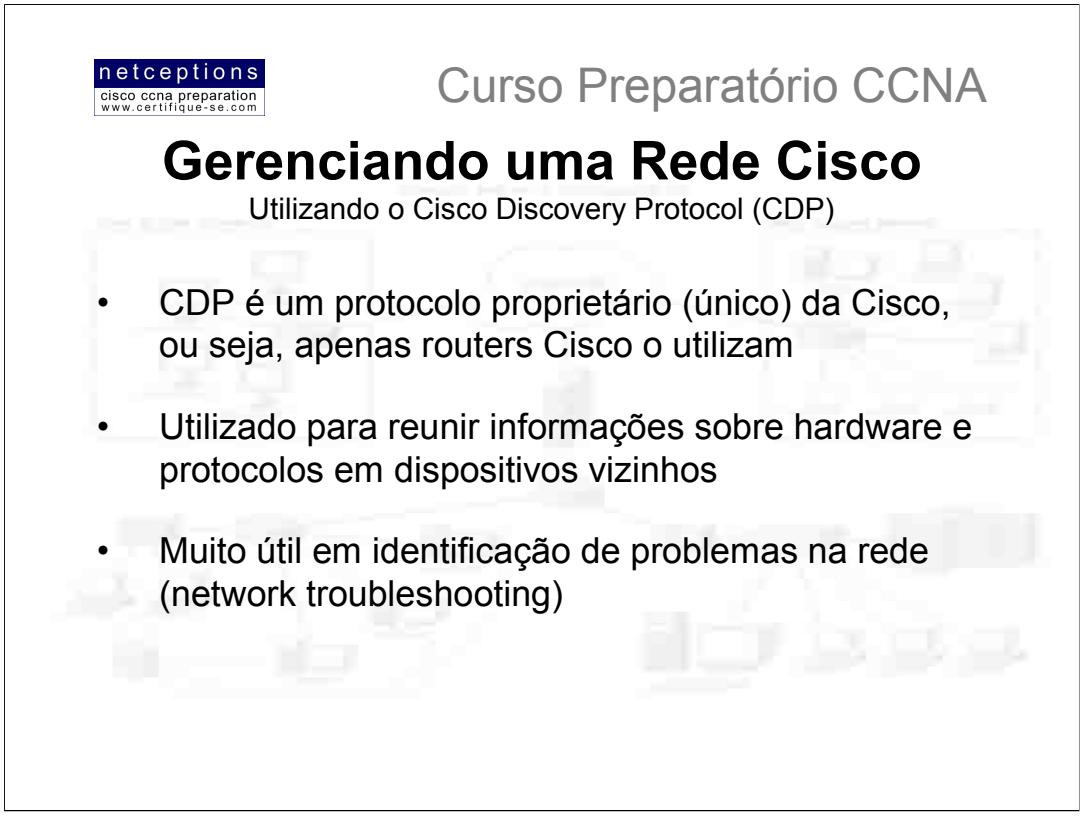
Para verificar a configuração armazenada na NVRAM (startup-config), utilize o comando **`sh start`**. Dentre as informações apresentadas, você obterá o espaço de memória utilizado pelo arquivo. Se você não tem certeza se os arquivos running-config e startup-config são os mesmos, e é o running-config que você deseja utilizar e manter, utilize o comando **`copy run start`** para copiá-lo da RAM para a NVRAM. Desta forma, na próxima vez que o router for inicializado, essa será a configuração carregada.

Você pode copiar a configuração ativa para um host TFTP, como um segundo backup da running-config. Para tal, utilize o comando **`copy run tftp`**. Conforme discutido nas páginas anteriores, 2 informações lhe serão pedidas: o endereço IP do TFTP host e o nome do arquivo destino (destination filename). Para nome do arquivo, qualquer nome pode ser escolhido, desde que o router não tenha um hostname configurado. Neste caso, o nome do arquivo será, automaticamente, o nome do router (hostname) acrescido da extensão "**`-confg`**".

Para ativar a configuração armazenada na NVRAM, utilize o comando **`copy start run`**. O conteúdo da NVRAM (startup-config) será copiado para a RAM, substituindo a running-config anteriormente utilizada. Um comando mais antigo também pode ser utilizado para executar essa operação: **`config mem`**.

Para recuperar uma configuração copiada para um TFTP host, utilize o comando **`copy tftp run`** (para copiar para a RAM) ou **`copy tftp start`** (para copiar para a NVRAM). Um comando mais antigo também pode ser utilizado para executar essa operação: **`config net`** (equivale ao comando **`copy tftp run`**)

Para apagar a configuração armazenada na NVRAM (startup-config), utilize o comando erase start. Esse comando apaga a startup-config, ou seja, na próxima vez que o router inicializar, ele irá para o modo setup.



O protocolo CDP foi criado pela Cisco para ajudar administradores de rede na coleta de informações sobre dispositivos local e remotamente conectados.

Obtendo os valores dos timers CDP e informações sobre holdtime

O comando **`show cdp (sh cdp)`** apresenta informações dobre 2 parâmetros globais CDP que podem ser configurados em dispositivos Cisco:

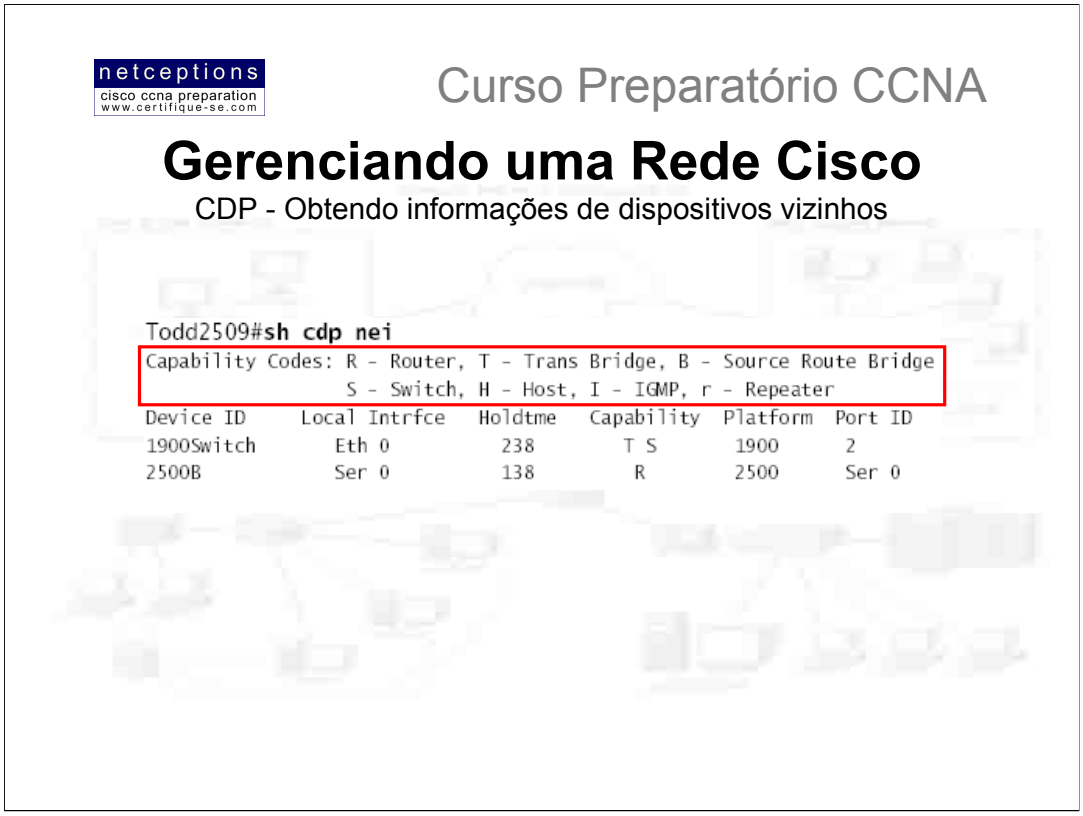
• **CDP Timer** registra a frequência com a qual pacotes CDP são transmitidos para todas as interfaces ativas;

• **CDP Holdtime** registra a quantidade de tempo que um dispositivo deve reter pacotes recebidos de dispositivos vizinhos.

Ambos router e switches Cisco utilizam estes parâmetros, e a saída em um router é ilustrada abaixo:

```
Router#sh cdp
Global CDP information:
Sending CDP packets every 60 seconds
Sending a holdtime value of 180 seconds
Router#
```

Você pode utilizar os comandos **`(config)#cdp timer [valor]`** e **`(config)#cdp holdtime [valor]`** para configurar estes parâmetros em um router, ou pode ativar e desativar esse recurso em interfaces específicas através dos comandos **`cdp enable`** e **`no cdp enable`**. Veremos como fazer isso mais adiante.



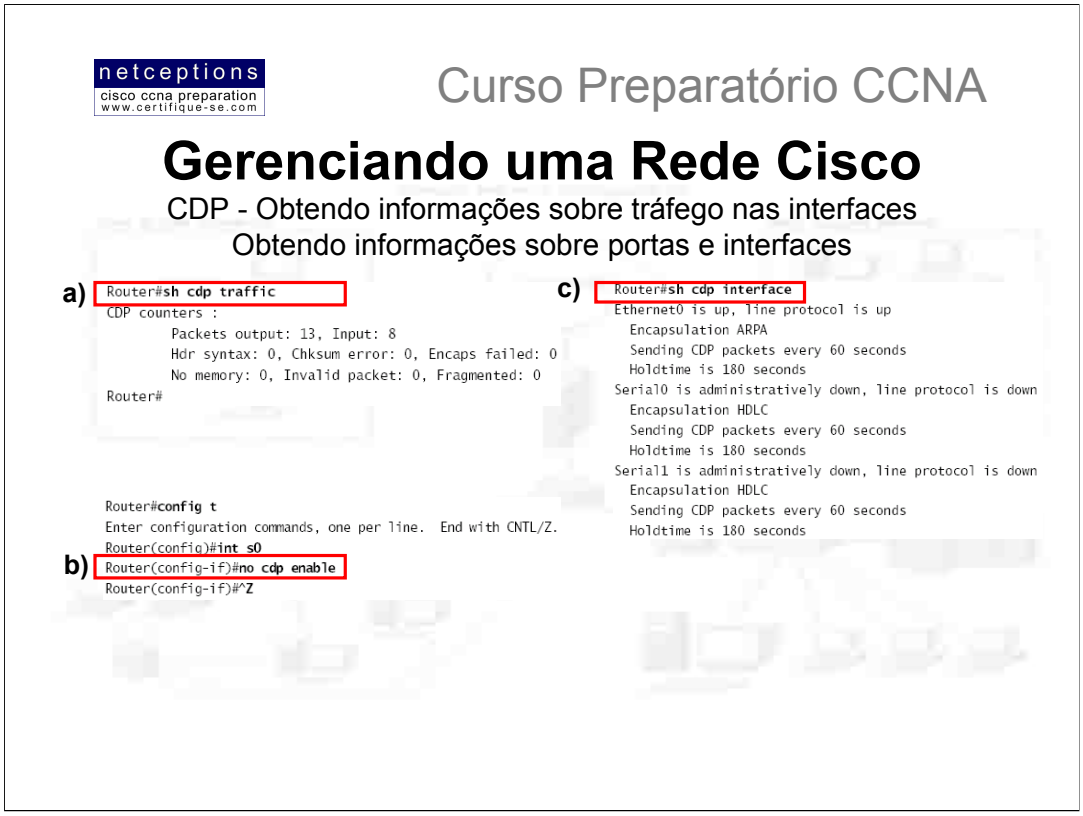
O comando sh cdp neighbor (sh cdp nei) apresenta informações sobre dispositivos diretamente conectados. É importante lembrar que pacotes CDP não são passados através de um switch Cisco, e você apenas vê aquilo que encontra-se diretamente conectado. No caso de um router conectado à um switch, você não obterá informações sobre os dispositivos conectados ao switch.

Acima ilustramos uma saída do comando **`sh cdp nei`**, executado em um router modelo 2509. A tabela abaixo sumariza as informações obtidas através do comando **`sh cdp nei`** para cada dispositivo:

Campo	Descrição
Device ID	O nome (hostname) do dispositivo diretamente conectado
Local Interface	A porta ou interface na qual os pacotes CDP estão sendo recebidos
Holdtime	Tempo que o router deve reter pacotes recebidos de dispositivos vizinhos antes de descartá-los, caso pacotes CDP não sejam mais recebidos
Capability	A capabilidade do dispositivo vizinho, como um router ou um switch. Os códigos de capabilidade encontram-se listados no topo da saída do comando
Platform	Identifica o tipo de dispositivo Cisco conectado
Port ID	A porta ou interface do dispositivo vizinho pela qual os pacotes CDP são enviados

Outro comando utilizado na provisão de informações sobre dispositivos vizinhos é o **`sh cdp nei detail`** (**`sh cdp nei de`**), que também pode ser executado em um router ou switch. Esse comando exibe informações detalhadas sobre cada dispositivo conectado ao dispositivo em questão (um router 2509, no caso). Dentre as informações obtidas na saída deste comando - em adição às informações obtidas através do comando **`sh cdp nei`** - estão: hostname e endereço IP de dispositivos diretamente conectados e versão do sistema IOS em atividade no dispositivo vizinho.

O comando **`sh cdp entry *`** apresenta exatamente as mesmas informações obtidas através do comando **`sh cdp nei de`**.

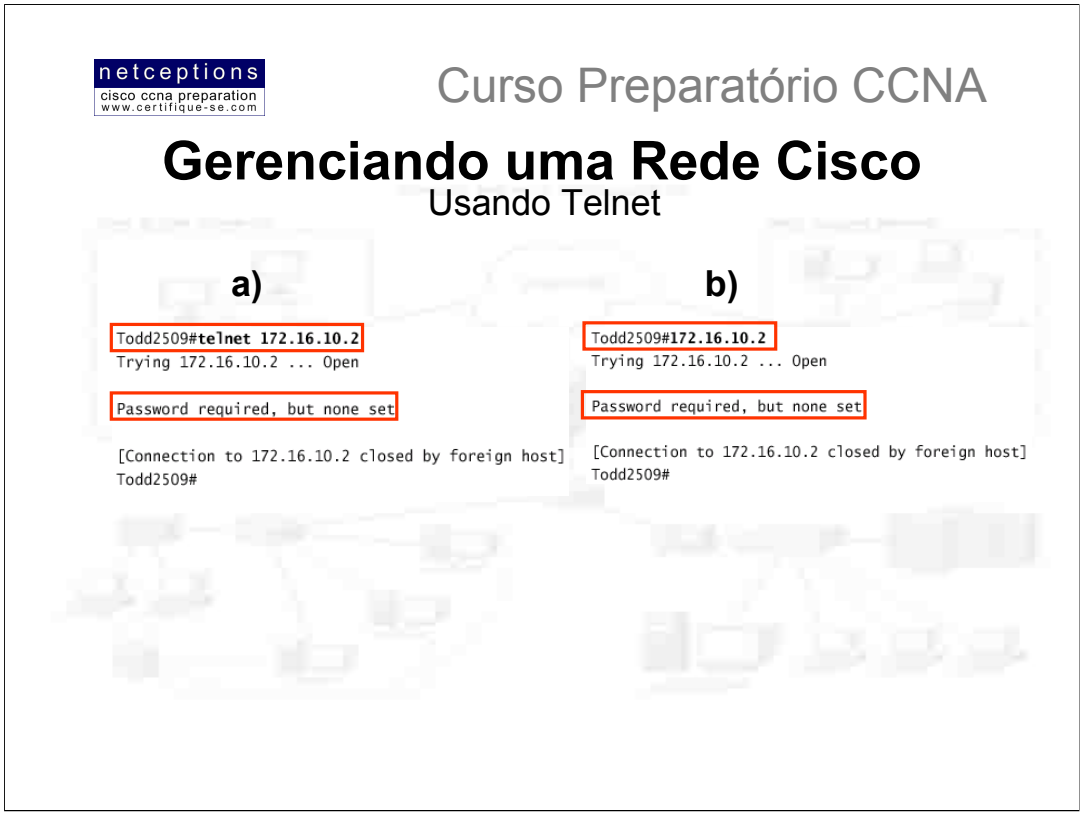


O comando **`sh cdp traffic`** apresenta informações sobre o tráfego em interfaces, incluindo o número de pacotes CDP enviados e recebidos e os erros relacionados ao CDP. No exemplo **(a)** ilustrado acima temos a saída do comando executado em um router.

O comando **`sh cdp interface`** (**`sh cdp int`**) apresenta o status do CDP nas interfaces de um router ou nas portas de um switch. Conforme mencionado anteriormente, é possível desativar completamente o recurso CDP através do comando **`no cdp enable`**. Outro comando que pode ser usado para esse fim é o **`no cdp run`**. Para habilitar CDP em portas ou interfaces específicas, utilize o comando **`cdp enable`**. Todas as portas e interfaces tem, como default, CDP habilitado. Em um router, o comando **`sh cdp int`** apresenta informações sobre cada interface utilizando CDP, incluindo o encapsulamento na linha, o timer, e o holdtime para cada interface. O caso **(c)**, ilustrado acima, exemplifica uma saída do comando **`sh cdp int`**.

Para desativar o CDP em uma interface específica no router, utilize o comando **`no cdp enable`**, no modo de configuração de interface (**`config-if`**). O caso **(b)**, ilustrado acima, exemplifica como proceder para desativar o CDP na interface serial 0 de um router.

Verifique a desativação utilizando o comando **`sh cdp int`**. A interface serial 0 (S0) não deve constar na saída deste comando.



Telnet é um protocolo de terminal virtual, parte do conjunto de protocolos TCP/IP. Telnet permite que você se conecte à dispositivos remotos, reuna informações sobre os mesmos, os configure, e rode aplicações.

Uma vez que seus routers e switches encontrem-se configurados, você pode utilizar um programa Telnet para checagem de configuração e para configuração dos mesmos sem a necessidade do uso de cabos de console.

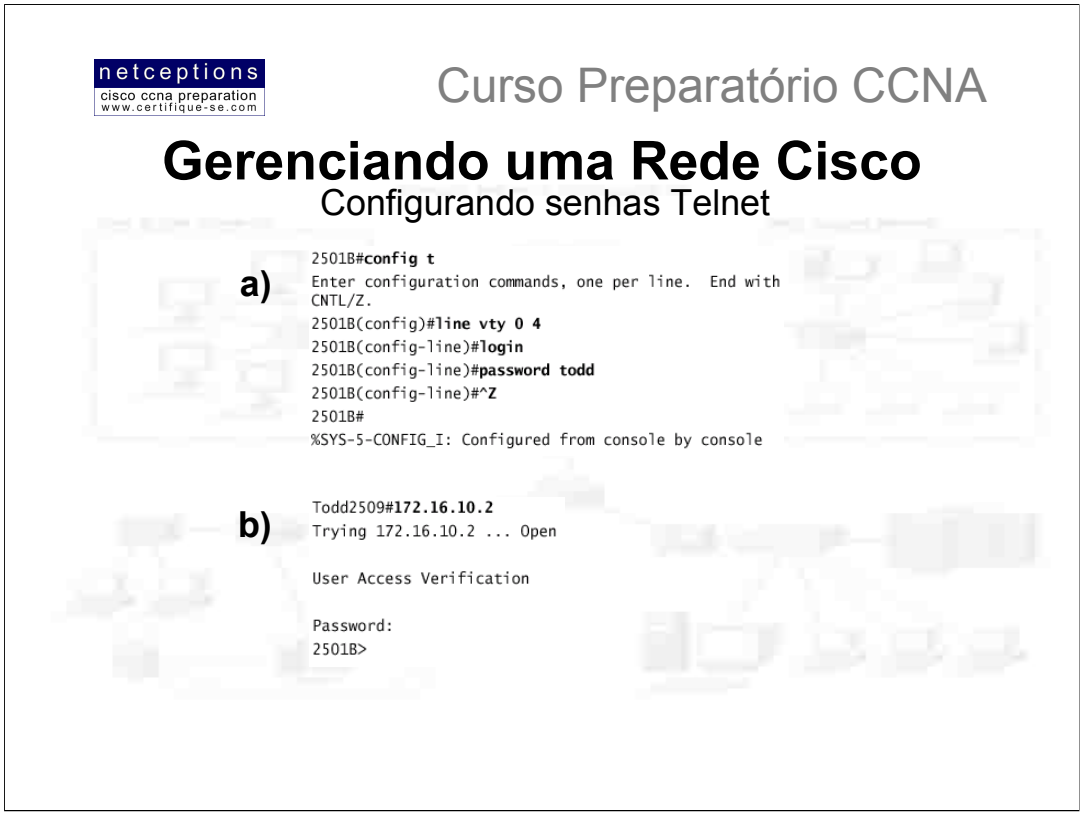
Para executar um programa Telnet, normalmente basta que se digite telnet no prompt de comando em qualquer ambiente CLI (DOS, UNIX, IOS). Entretanto, para acessar routers através desse recurso, senhas VTY devem estar configuradas nos mesmos.

Você não pode utilizar CDP para reunir informações sobre dispositivos que não estejam diretamente conectados ao seu dispositivo. Entretanto, Telnet pode ser utilizado para esse fim. Você pode se conectar à um dispositivo vizinho utilizando Telnet e rodar, remotamente, CDP nesse dispositivo para reunir informações sobre dispositivos diretamente conectados ao mesmo.

Na ilustração **(a)** acima, exemplificamos como utilizar o recurso telnet à partir de um router Cisco. É importante ressaltar que o comando telnet funciona em qualquer prompt do IOS. Note que, no exemplo **(a)** acima a senha VTY não foi configurada, o que ocasionou a mensagem de erro seguida da desconexão com o host.

Lembre-se que portas VTY em um router são configuradas por default como login, o que significa que você deve ou definir uma senha para a porta VTY, ou usar o comando **`no login`** na porta VTY (veja aula 4 para maiores detalhes).

Em um router Cisco, o comando **`telnet`** não precisa ser utilizado. Uma vez que você saiba o endereço IP do dispositivo-alvo, basta digitá-lo diretamente no prompt, conforme ilustração **(b)**, acima.



Vamos definir uma senha para o router que estávamos tentando nos conectar na página anterior, para que, assim, a conexão possa ser estabelecida via Telnet. A ilustração **(a)** acima ilustra como proceder.

Em seguida **(b)**, tentamos novamente uma conexão via Telnet com o host 172.16.10.2, da página anterior. A senha definida é pedida e, após digitada, a conexão é estabelecida com sucesso.

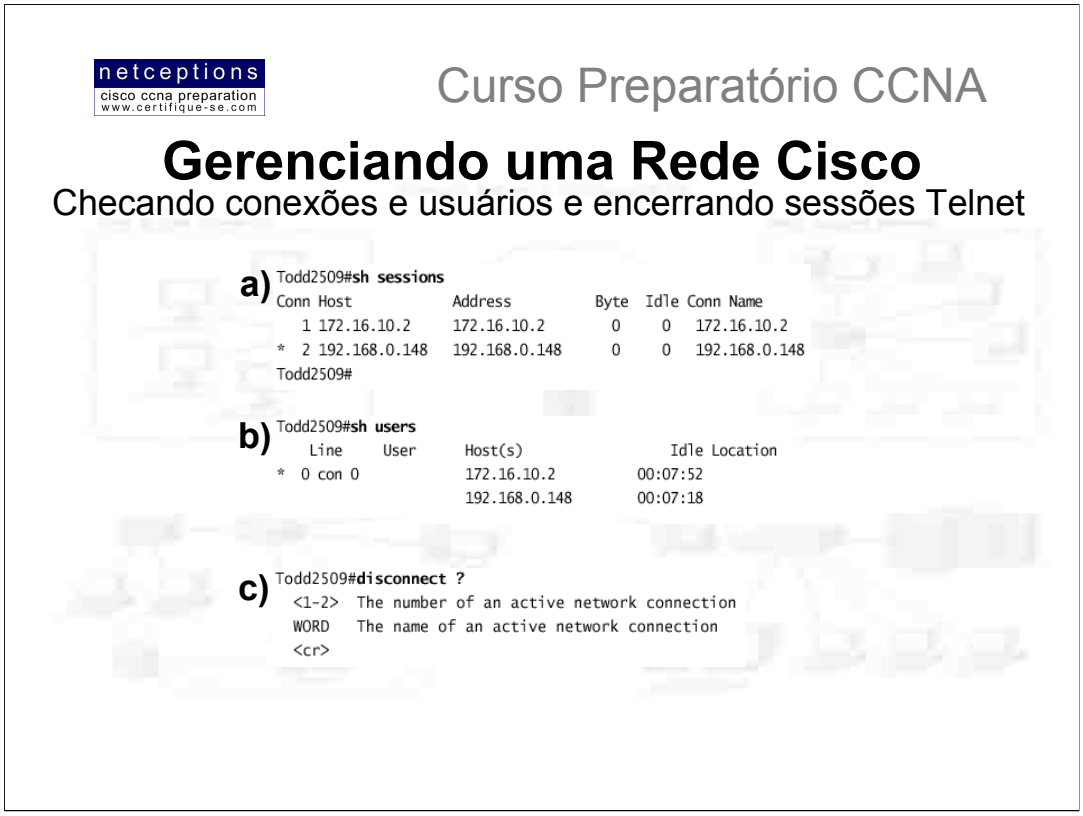
Lembre-se que a senha VTY é uma senha de modo usuário. Caso você tente entrar em modo privilegiado (comando enable) no prompt do dispositivo remotamente conectado, o seguinte ocorrerá:

```
2501B>en
%No password set
2501B>
```

Isso é um bom recurso. Você não gostaria que qualquer pessoa se conectasse remotamente via Telnet à seu router e, depois, simplesmente digitasse “enable” e entrasse em modo privilegiado... .

A senha enable ou enable secret deve estar configurada no dispositivo-alvo para que o mesmo possa ser remotamente configurado. No caso acima, nenhuma senha de modo privilegiado estava configurada.

Para se conectar remotamente à múltiplos dispositivos simultaneamente, utilize a combinação de teclas **CTRL+SHIFT+6** e logo após, pressione “**X**” após encontrar-se em modo usuário no dispositivo remoto. Fazendo isso, você terá o prompt de seu router de volta na tela, permitindo que outra sessão Telnet seja iniciada, e assim, sucessivamente.

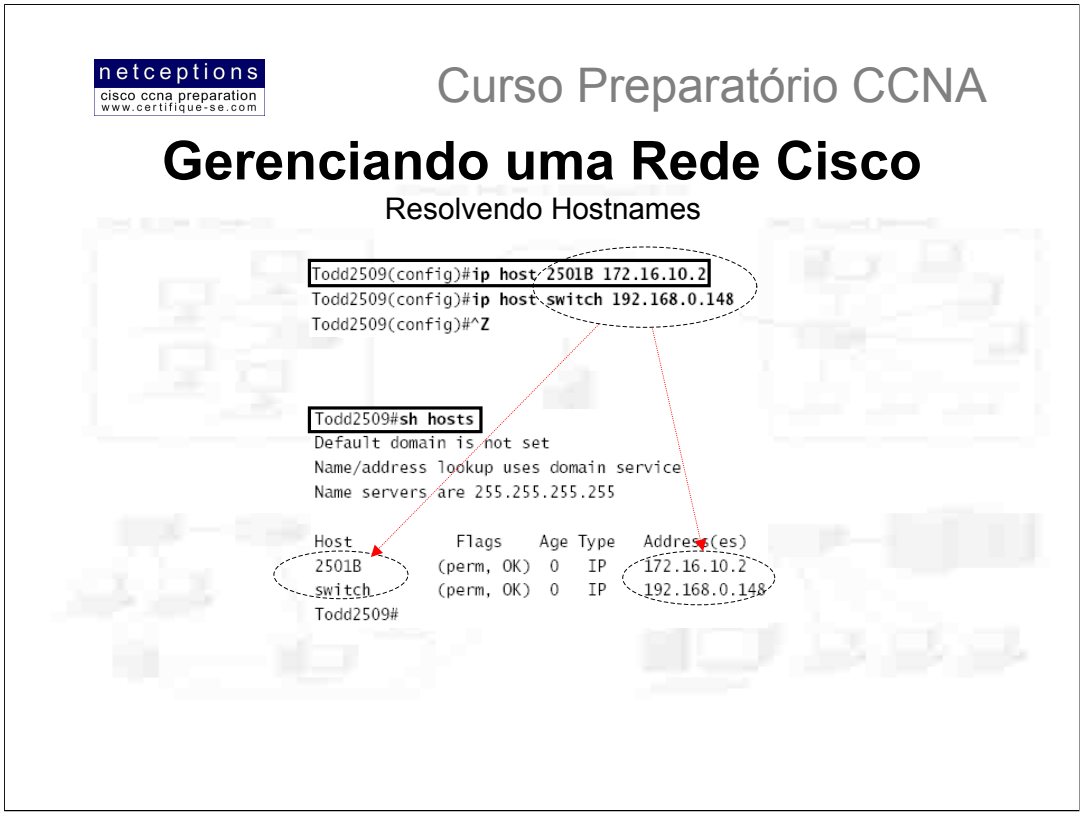


Para checar conexões realizadas do seu router para dispositivos remotos, utilize o comando **`sh sessions` (a)**. Note o asterisco (*) ao lado da conexão 2. Isso significa que a sessão 2 foi a última à ser efetivada. Você pode retornar à sua última sessão pressionando-se <ENTER> 2 vezes seguidas. Outro modo de se retornar à conexão desejada é digitando-se o número da mesma e pressionando-se <ENTER> 2 vezes.

Para listar todos os consoles ativos e portas VTY em uso no seu router, utilize o comando **`sh users` (b)**. O “con” na saída ilustrada representa o console local. No exemplo acima, o console encontra-se conectado à 2 dispositivos (endereços IP apresentados).

Para encerrar uma sessão Telnet **(c)**, meios diferentes podem ser utilizados. Digitando o comando **`exit`** ou **`disconnect`** talvez seja o mais simples de todos. Usando o comando **`disconnect`**, você pode especificar qual sessão deseja encerrar informando o número da mesma como atributo.

Caso você deseje encerrar uma sessão Telnet de um dispositivo conectado ao seu router, primeiro certifique-se de quais dispositivos encontram-se conectados (utilize o comando **`sh users`**). Identifique qual porta (line) **(exemplo b)** da saída apresentada possui a conexão que você deseja encerrar. Identificado o número da porta (line), utilize o comando **`clear line [número da porta].`** Certifique-se que a conexão foi desfeita através do comando **`sh users`**.



Para utilizar um nome (hostname) no lugar de um endereço IP para se conectar à um dispositivo remoto, o dispositivo que você está utilizando para efetuar esta conexão deve ser capaz de "traduzir", ou melhor, mapear este nome para um endereço IP (façamos uma analogia ao modo de endereçamento da Web, como conhecemos hoje).

Existem dois modos para mapear nomes para endereços IP: criando - manualmente - uma tabela de nomes (chamada de host table), ou criando um servidor de mapeamento de nomes (DNS - Domain Name Server), o que seria o equivalente à uma tabela de nomes dinâmica.

A host table irá prover o mapeamento de nomes para IP apenas no router onde a mesma se encontra. A sintaxe do comando à ser usado na criação de uma host table em um router é a seguinte:

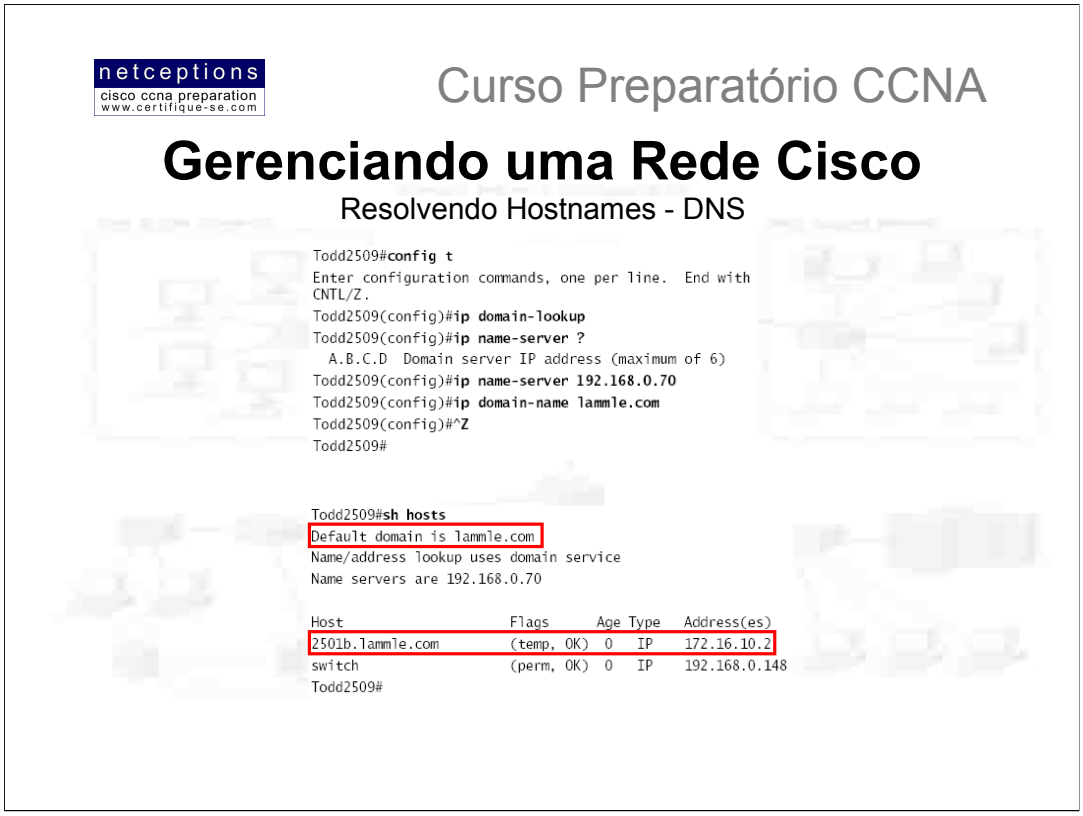
`ip host [nome] [porta_tcp] [endereço_ip]`

A porta default é a 23 (Telnet). Acima ilustramos um exemplo de como o comando deve ser utilizado. No exemplo, foi feita a configuração da host table com 2 entradas, para o mapeamento dos nomes do router 2501B e do switch.

Para ver a tabela formada, utilize o comando sh hosts. Acima ilustramos a saída deste comando. O termo "perm" que aparece na coluna "Flags" significa que os dados apresentados foram manualmente adicionados. Caso o termo encontrado nessa coluna fosse "temp", os dados teriam sido adicionados através de um servidor DNS.

Para testar a funcionalidade da tabela apresentada, tente digitar apenas o nome do dispositivo remoto no prompt do IOS. Caso a conexão seja estabelecida, a tabela encontra-se operacional.

Para remover uma entrada da tabela host (host table), utilize o comando **`no ip host [nome]`**. O problema com o método apresentado é que os nomes e endereços IP correspondentes precisam ser manualmente adicionados à tabela. Se houver muitos dispositivos que você deseje ter seus nomes mapeados, utilizar o método DNS pode ser mais produtivo.



Se você possui muitos dispositivos à serem mapeados, utilize DNS para o mapeamento de nomes. Toda a vez que um dispositivo Cisco recebe um comando que não é tido como válido para o IOS, ele tenta resolver o comando (ou nome) digitado através do DNS (procedimento default). Eis o que acontece quando um comando não reconhecido é digitado:

```
Todd2509#nome
Translating "nome"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find
computer address
Todd2509#
```

Você pode desabilitar o procedimento de resolução padrão através do comando **`no ip domain-lookup`**, digitado no modo de configuração global.

Caso você, de fato, tenha um servidor DNS operando em sua rede, alguns comandos devem ser digitados para que a resolução de nomes via DNS funcione de acordo:

`ip domain-lookup` (este comando encontra-se ativo, por default)

`ip name-server` - utilizado para definir o endereço IP do servidor DNS

`Ip domain-name` - opcional, mas sua utilização é recomendada. Acrescenta o nome do domínio ao nome digitado. Uma vez que DNS é um sistema de domínios totalmente qualificados (Fully Qualified Domain Name System), é aconselhável a adoção de nomes DNS completos, no estilo **domínio.com**.

Acima ilustramos a utilização destes 3 comandos.

Uma vez que a configuração DNS esteja OK, sua funcionalidade pode ser testada através dos comandos **`ping`**, **`trace`** e **`telnet`**. Se você conseguir "pingar" um dispositivo utilizando seu nome, ao invés de seu endereço IP, seu sistema DNS está funcionando.

Utilize o comando **`sh hosts`** para visualizar a host table atualizada. Note que o router 2501B aparece com seu nome completo (com a extensão **lammle.com**), assim como, agora, temos um "default domain" configurado (**lammle.com**).

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Relação dos comandos analisados:

Comando	Descrição
cdp enable	Ativa CDP em uma interface específica
cdp holdtime	Altera a frequência do holdtime
cdp run	Ativa CDP em um router
cdp timer	Altera a frequência do timer do CDP
clear line	Encerra uma conexão Telnet ao seu router
config-register	Informa ao router como inicializar e altera a configuração do registro
copy flash tftp	Copia arquivos da FLASH para um servidor TFTP
copy run start	Copia a configuração ativa (running-config) para a NVRAM (startup-config)
copy run tftp	Copia a configuração ativa para um servidor TFTP
copy tftp flash	Copia um arquivo do servidor TFTP para a FLASH
copy tftp run	Copia a configuração armazenada no servidor TFTP para a RAM
Ctrl+Shift+6, depois **X**	Retorna a tela para a última conexão
disconnect	Encerra uma conexão à um dispositivo remoto
erase startup-config	Apaga o conteúdo da NVRAM (startup-config) em um router
exit	Encerra uma conexão à um dispositivo remoto
ip domain-lookup	Ativa DNS lookup
ip domain-name	Adiciona um nome de domínio ao DNS lookup
ip host	Cria uma tabela host (host table) em um router
ip name-server	Define o endereço IP para até 6 servidores DNS
no cdp enable	Desativa CDP em uma determinada interface
no cdp run	Desativa CDP no router
no ip domain-lookup	Desativa DNS lookup
no ip host	Remove um nome da host table
o/r 0x2142	Altera o modo como um router 2501 inicializa
show cdp	Apresenta os timers CDP e frequência do holdtime
show cdp entry *	Apresenta os endereços IP e versão do IOS, em adição às informações apresentadas pelo comando **sh cdp nei**
show cdp interface	Apresenta as interfaces com CDP ativo
show cdp neighbor	Apresenta os dispositivos diretamente conectados e detalhes sobre os mesmos
show cdp neighbor detail	Mesma função do comando **show cdp entry ***
show cdp traffic	Apresenta os pacotes CDP enviados e recebidos, e erros decorrentes
show flash	Apresenta o conteúdo da FLASH
show hosts	Apresenta o conteúdo da tabela host
show run	Apresenta o arquivo de configuração ativo (running-config)
show sessions	Apresenta as conexões via Telnet ativas
show start	Apresenta o arquivo de configuração armazenado na NVRAM (startup-config)
show version	Apresenta o tipo e versão do IOS ativo, assim como os valores do registrador (configuration register)
tftp-server system ios-name	Cria um servidor TFTP para uma imagem do IOS armazenada na FLASH, para acesso por outros dispositivos

Resumo módulo 6-a:

Nesta aula analisamos como routers Cisco são configurados e como gerenciar essa configuração. Os seguintes tópicos foram abordados:

- Backup e Recuperação do Sistema IOS
- Backup e Recuperação da configuração do router
- Reunião de informações sobre dispositivos vizinhos através dos recursos CDP e Telnet
- Resolução de hostnames
- Teste da rede através dos recursos Ping e Trace

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Aula 6 / Módulo II
Configurando Novell IPX

- Identificação das porções de rede e de host em um endereço IPX
- Configuração do IPX em routers Cisco
- Configuração de múltiplos métodos de encapsulamento em uma interface através do recurso de sub-interfaces
- Monitoração e verificação de IPX no router

A maioria dos administradores de rede já se depararam com o protocolo IPX por 2 motivos: primeiro, IPX é o protocolo default do NOS (Network Operating System) Novell Netware; segundo porque esse sistema foi o sistema operacional de rede (NOS) mais popular entre o final dos anos 80 e início dos anos 90. Como resultado, milhões de redes IPX foram implantadas. No entanto, a Novell vem acompanhando as tendências. Sua última versão do Netware já é baseado no protocolo IP, apesar de ainda suportar IPX.

O protocolo IPX (Internetwork Packet eXchange) vem sendo usado desde o início dos anos 80. Ele se assemelha em muitos aspectos ao TCP/IP, e como tal, é composto por uma família de protocolos que coexistem e interagem entre si.

Não há sombra de dúvida que o protocolo IPX ainda continuará ativo por algum tempo, ainda. Basta considerar sua base instalada. O sistema IOS suporta inteiramente o protocolo IPX. Para aproveitar as vantagens desse protocolo, devemos entender como o mesmo funciona, como é seu esquema de endereçamento, entre outras coisas.

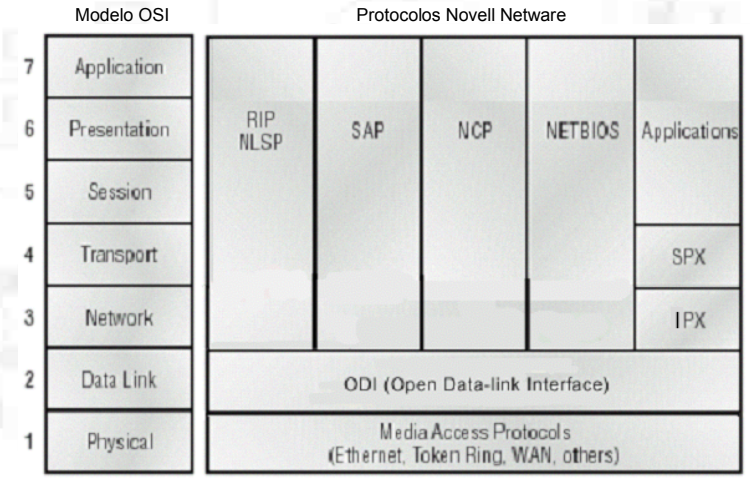
É isso o que estaremos fazendo nesta aula.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Configurando Novell IPX

A pilha de protocolos Novell IPX



IPX não espelha diretamente o modelo OSI de camadas, mas seus protocolos também funcionam em camadas. Quando foi desenvolvido, a preocupação com o IPX era performance, e não em estar de acordo com padrões ou modelos existentes. A figura acima ilustra os protocolos IPX, suas camadas e funções comparadas ao modelo OSI.

IPX: IPX realiza funções nas camadas 3 e 4 do modelo OSI. Ele controla a designação dos endereços IPX (software) aos dispositivos, gerencia o transporte de pacotes através da rede e toma decisões sobre rotas baseadas em informações obtidas através dos protocolos de roteamento RIP ou NLSP. IPX é um protocolo não-orientado à conexão (connectionless), similar ao protocolo IP, do modelo TCP/IP. Para a comunicação com protocolos de camada superior, o IPX utiliza “sockets”. Esses são análogos às portas no modelo TCP/IP.

SPX: SPX (Sequenced Packet eXchange) faz as vezes do TCP no modelo TCP/IP. Ele faz com que a comunicação seja orientada-à-conexão. SPX age criando circuitos virtuais entre dispositivos, com cada conexão tendo seu identificador incluso no cabeçalho SPX.

RIP: RIP (Routing Information Protocol) é um protocolo de roteamento baseado em distance-vector, usado pelo IPX para descobrir rotas através de internetworks. Ele utiliza “ticks” (1/18 segundos) e contagem de hops como métricas para identificar melhores rotas.

SAP: SAP (Service Advertising Protocol) é usado para propagar e requisitar serviços. Servidores o usam para propagar os serviços disponibilizados pelos mesmos, e workstations o utilizam para requisitar tais serviços.

NLSP: NLSP (Netware Link Services Protocol) é um protocolo de roteamento avançado, baseado no estado do link (link state protocol). A intenção da Novell é utilizá-lo em substituição ao RIP e ao SAP.

NCP: NCP (Netware Core Protocol) provê às workstations acesso aos recursos dos servidores. Funções como acesso à arquivos, impressão, sincronização e segurança são gerenciados pelo NCP.

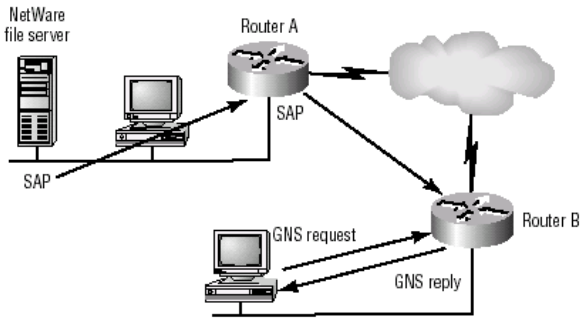
Como já deve ter sido notado, a presença de protocolos de roteamento, protocolos orientados-à-conexão e protocolos de aplicação indicam que IPX é um protocolo capaz de suportar redes de grande porte, rodando um grande volume de aplicações.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Configurando Novell IPX

Comunicação Cliente-Servidor



O sistema Novell Netware segue à risca o modelo cliente-servidor. Um dispositivo em uma rede Netware ou é um cliente, ou um servidor, e ponto. Não existem dispositivos que simultaneamente provêem e consomem recursos. Clientes podem ser máquinas rodando sistemas como MacOS, DOS, MS Windows, NT, UNIX ou VMS. Servidores, exclusivamente, rodam Novell Netware. Servidores Novell Netware provêem o seguinte às máquinas cliente: arquivos, impressão, mensagens, aplicações e bancos de dados.

Como você deve imaginar, clientes Netware necessitam dos servidores para localizar todos os recursos disponíveis. Todo servidor Netware cria uma tabela SAP que é composta de todos os recursos que ele tenha conhecimento. Quando clientes necessitam de um determinado recurso, eles enviam uma mensagem de broadcast IPX chamada GNS (Get Nearest Server - "Me Dê o Servidor Mais Próximo"), para assim localizar o servidor Netware mais próximo que oferece o recurso requisitado. Do outro lado, servidores que recebem a requisição GNS checam suas tabelas SAP para localizar o servidor Netware que possui o recurso solicitado. Uma vez encontrado, uma mensagem chamada GNS Reply - contendo informações sobre o(s) servidor(es) que possui(em) o serviço solicitado, assim como acessá-lo - é enviada ao cliente. Caso nenhum servidor com o recurso solicitado seja encontrado, o servidor simplesmente não responde, deixando o cliente impossibilitado de acessar o recurso.

Routers Cisco também criam tabelas SAP e podem responder à requisições GNS como se fosse servidores Netware. Isso não significa, no entanto, que routers Cisco ofereçam os serviços que servidores Netware oferecem, mas apenas que suas respostas são idênticas à de um servidor Netware quando se trata de localizar recursos e serviços em uma rede IPX. No caso de haver servidores Netware na rede local, esses seriam os primeiros à responder as requisições GNS. No caso de não haver nenhum servidor local, um router Cisco que conecte o segmento onde se encontra o cliente requisitante à rede IPX pode responder ao pedido GNS emitido pelo cliente. Isso poupa tempo pois evita a espera de se alcançar um servidor Netware remoto para que esse responda ao pedido GNS. Outra vantagem desse esquema é a economia de banda, conforme ilustrado na figura acima. Na figura, observamos workstations (clientes) localizados em um site remoto requisitar acesso aos recursos do servidor localizado no escritório central. Nesse caso, o router B responde aos pedido GNS do cliente baseado nas informações contidas em sua tabela SAP. Para os clientes, essa operação é transparente, uma vez que, de sua perspectiva, todas as respostas aos seus pedidos são feitas localmente, independente da localização física da rede como um todo.

Comunicação Servidor-Servidor

A comunicação entre 2 servidores Netware é um pouco mais complexa que a comunicação cliente-servidor. Conforme mencionado, servidores são responsáveis pela criação e gerenciamento das tabelas SAP, independentemente dos recursos encontrarem-se ou não localmente no servidor. Outro fato que deve ser lembrado é que o servidor Netware deve ser capaz de localizar qualquer recurso através da rede.

Servidores trocam 2 tipos de informação utilizando 2 protocolos distintos: SAP e RIP. SAP transmite informações sobre serviços, enquanto que o RIP transmite informações de roteamento.

NOTA: Não confunda o protocolo RIP do TCP/IP com o protocolo RIP do IPX. Ambos são protocolos de roteamento, porém, não são o mesmo protocolo.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Configurando Novell IPX

Service Advertising Protocol (SAP)

```
Flags:          0x00
  Status:       0x00
  Packet Length:306
  Timestamp:    23:48:36.362000 06/28/1998
Ethernet Header
  Destination:  ff:ff:ff:ff:ff:ff Ethernet Brdcast
  Source:       00:80:5f:ad:14:e4
  Protocol Type:81-37  NetWare
IPX - NetWare Protocol
  Checksum:          0xffff
  Length:            288
  Transport Control:
    Reserved:        %0000
    Hop Count:       %0000
  Packet Type:       4  PEP
  Destination Network:  0xcc715b00
  Destination Node:     ff:ff:ff:ff:ff:ff Ethernet Brdcast
  Destination Socket:   0x0452  Service Advertising
Protocol
  Source Network:       0xcc715b00
  Source Node:          00:80:5f:ad:14:e4
  Source Socket:        0x0452  Service Advertising
Protocol
SAP - Service Advertising Protocol
  Operation:        2  NetWare General Service Response
Service Advertising Set #1
  Service Type:     263  NetWare 386
  Service Name:
```

```
BORDER3.....................................
  Network Number:   0x12db8494
  Node Number:      00:00:00:00:00:01
  Socket Number:    0x8104
  Hops to Server:   1
Service Advertising Set #2
  Service Type:     4  File Server
  Service Name:
BORDER3.....................................
  Network Number:   0x12db8494
  Node Number:      00:00:00:00:00:01
  Socket Number:    0x0451
  Hops to Server:   1
Service Advertising Set #3
  Service Type:     632
  Service Name:     BORDER_____________
R.S.I@@@@@D.P]..
  Network Number:   0x12db8494
  Node Number:      00:00:00:00:00:01
  Socket Number:    0x4006
  Hops to Server:   1
```

broadcast SAP capturado com um analisador de rede

Os servidores Netware usam o protocolo SAP na propagação dos serviços disponíveis pelos mesmos em intervalos de 60 segundos. As mensagens de broadcast propagadas incluem todos os serviços que o servidor sabe sobre outros servidores, e não apenas os serviços oferecidos por ele. Todos os servidores que recebem essa mensagem SAP incorporam a informação contida na mesma às suas próprias tabelas SAP. Uma vez que informações SAP são trocadas entre todos os servidores, cedo ou tarde, todos os servidores estarão cientes de todos os serviços disponíveis na rede como um todo, estando, portanto, habilitados à responder pedidos GNS de clientes. Conforme novos serviços são introduzidos, eles são adicionados às tabelas SAP nos servidores locais, e são então re-propagadas até que todos os servidores possuam as mesmas informações em suas tabelas SAP.

Para o protocolo SAP, routers Cisco são vistos como um servidor Netware qualquer. Por default, um broadcast SAP não atravessa um router Cisco. O router adiciona todas as mensagens SAP recebidas em todas as suas interfaces habilitadas com IPX à sua tabela SAP. À menos que você altere a configuração padrão, o router, então, passa a propagar essa tabela através de cada uma dessas interfaces em intervalos de 60 segundos (como um verdadeiro servidor Netware). O router isola as mensagens SAP em segmentos locais, e transmite apenas um sumário dessa informação para cada segmento.

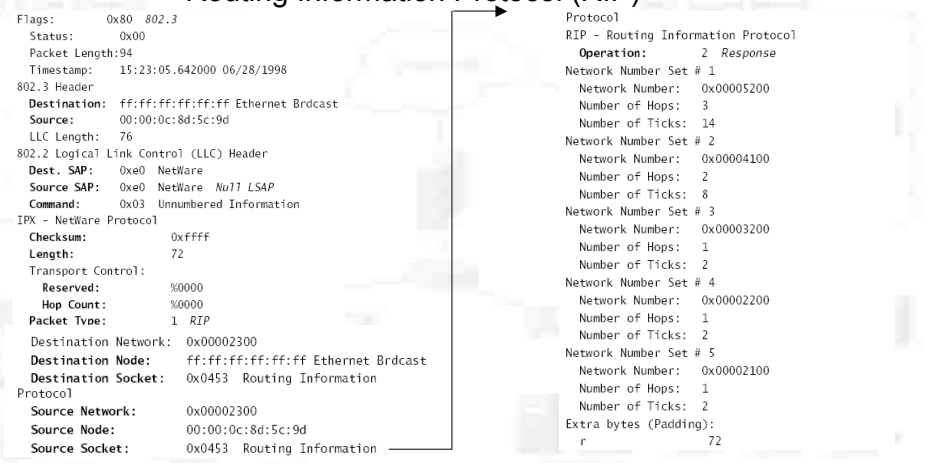
Observe a figura acima. Trata-se de um broadcast SAP capturado com um analisador de rede. Essa mensagem SAP veio de um servidor Netware chamado BORDER3. Note como ele lista 3 diferentes serviços que oferece. Esses serviços - seus endereços e informações referentes ao “socket” - serão adicionadas nas tabelas SAP de todos os dispositivos IPX conectados à essa rede - incluindo routers - e serão, então, re-propagadas pela rede como um todo.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Configurando Novell IPX

Routing Information Protocol (RIP)

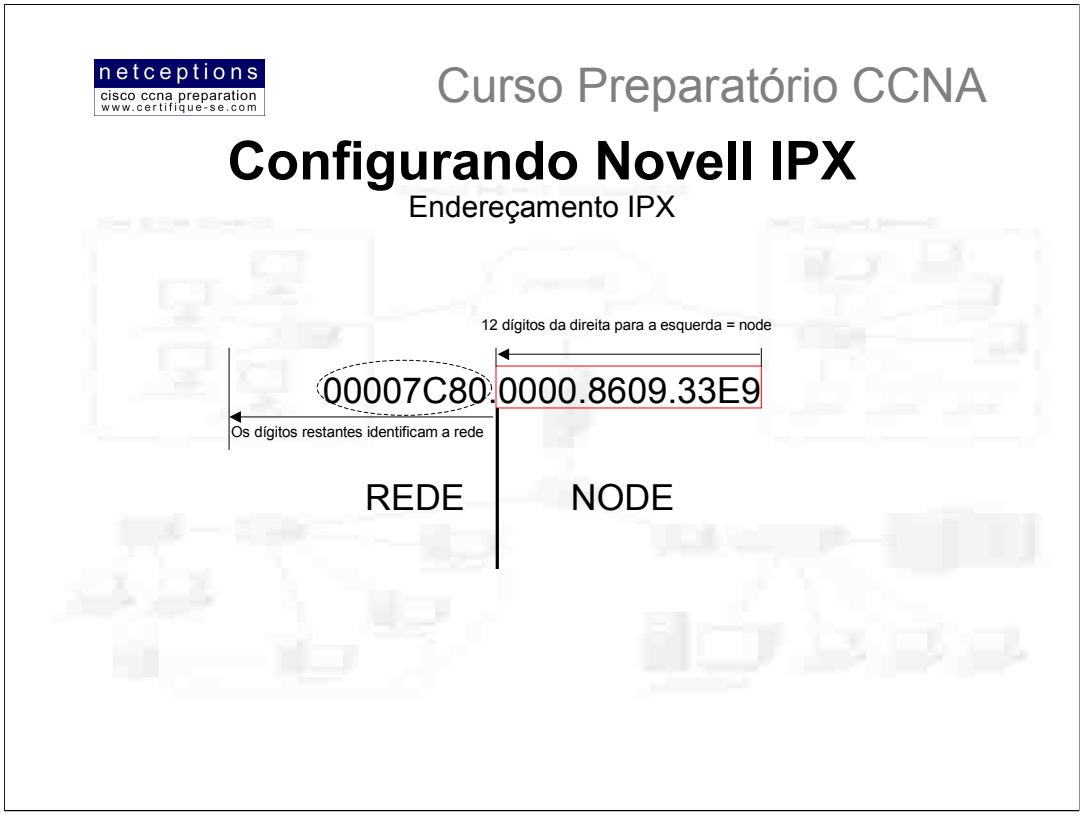


Pacote RIP IPX capturado com um analisador de rede

Informações RIP são trocadas entre servidores do mesmo modo que informações SAP. Servidores criam tabelas de roteamento contendo informações sobre as redes às quais os mesmos encontram-se diretamente conectados. Essas tabelas são, então, propagadas através de todas as interfaces habilitadas para IPX. Outros servidores presentes nesse segmento recebem essas atualizações e propagam suas tabelas RIP através de interfaces IPX. Assim como informações SAP são transmitidas de servidor à servidor até que todos convirjam com as mesmas informações, informações RIP são propagadas até que todos os servidores e routers tenham informações sobre todas as rotas disponíveis para redes remotas. Assim como informações SAP, informações RIP são propagadas em intervalos de 60 segundos.

Acima observamos um pacote IPX RIP, capturado com um analisador de rede. Repare na semelhança com um pacote RIP IP. A diferença clara está na falta dos endereços IP. Em seu lugar, aparecem endereços IPX e números de rede (network numbers). Note, também, que aparecem campos com número de ticks (number of ticks) e número de hops (number of hops) nas informações apresentadas.

Ticks são quantos 1/18 de segundo são necessários para se alcançar uma rede remota. Esse é o modo como IPX utiliza o atraso do link (link delay) para identificar a melhor rota para uma rede remota. No exemplo, existem apenas 3 routers, e esse pacote é transmitido à cada 60 segundos. Imagine isso acontecendo em uma rede de grande porte, com centenas de routers... .



Após ter estudado o esquema de endereçamento IP, você irá achar IPX extremamente fácil. O esquema de endereçamento utilizado pelo IPX possui uma série de características que o torna muito mais fácil de compreender e gerenciar quando comparado com o esquema utilizado pelo protocolo IP.

Endereços IPX são formados por 80 bits (10 bytes) de dados. Assim como TCP/IP, eles são hierárquicos e divididos em 2 porções: rede e nó (node). Veja ilustração acima para entender como identificar cada parte em um endereço IPX (**ATENÇÃO**: ISSO SEMPRE CAI NA PROVA CCNA!). Em IPX não existe classes, ou seja, não há endereços de classe A, B ou C. As porções de rede e do nó sempre têm o mesmo tamanho.

Assim como em endereçamento IP, a porção de rede do endereço IPX deve ser definida por um administrador e deve ser a mesma para toda a rede IPX. O endereçamento dos nodes é realizado automaticamente, uma vez definido o endereço de rede. Na maior parte dos casos, o endereço MAC do dispositivo é utilizado como endereço do nó. Esse esquema de endereçamento apresenta uma série de vantagens, se comparado com TCP/IP. Uma vez que o endereçamento de dispositivos ocorre automaticamente, você não precisa se preocupar com servidores DHCP ou com a configuração de dispositivo por dispositivo com um endereço IPX. Outra grande vantagem é que, uma vez que o endereço MAC já é parte do endereço IPX, não há necessidade de algo equivalente ao ARP do TCP/IP em IPX.

Assim como endereços IP, endereços IPX podem ser escritos sob uma variedade de notações. A mais usual, entretanto, é a notação hexadecimal. Lembre-se sempre que os 12 primeiros dígitos contados da direita para a esquerda representam o node. O que restar, representa a rede.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

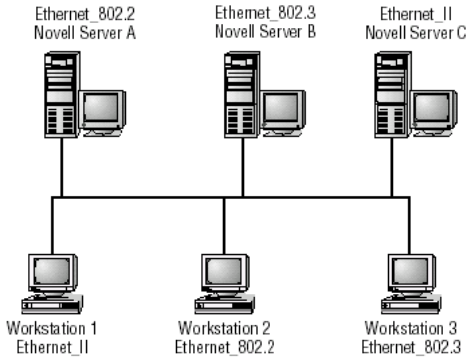
Configurando Novell IPX

Encapsulamento

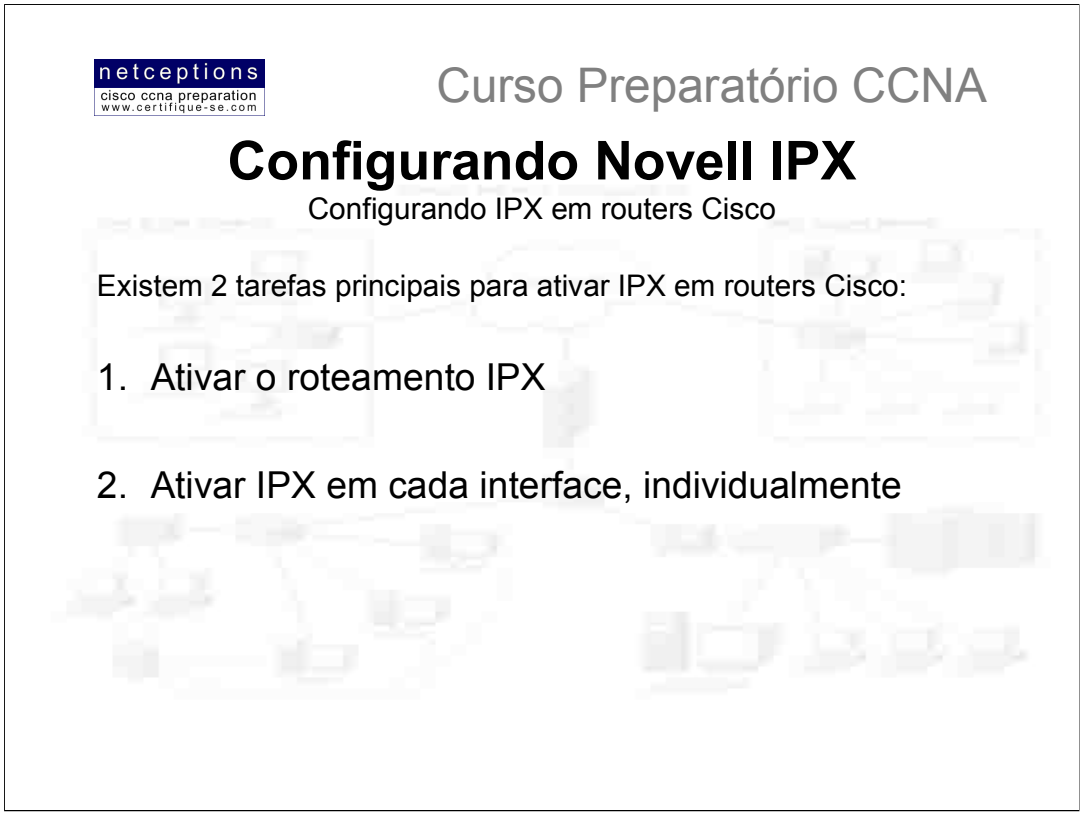
Tipo de frame Netware	Nome utilizado por dispositivos Cisco	Características
Ethernet_802.3	novell-ether (default)	Default até o Netware 3.11
Ethernet_802.2	sap	Default à partir do Netware 3.12
Ethernet_II	arpa	Suporta ambos TCP/IP e IPX
Ethernet_SNAP	snap	Suporta AppleTalk, IPX e TCP/IP
Token-Ring	sap	
Token-Ring_snap	snap	
fddi_snap	snap (default)	
fddi_802.2	sap	
fddi_raw	novell-fddi	

Encapsulamento ou framing é o processo de se pegar pacotes de protocolos de camadas superiores e embutí-los em frames para a transmissão através da rede. Como você deve se lembrar, frames são definidos na camada 2 do modelo OSI. Quando falamos de IPX, encapsulamento é o processo específico de se pegar datagramas IPX (camada 3) e embutí-los em frames (camada 2) que uma determinada mídia suporte. Nesta aula falaremos sobre os seguintes padrões de camada física: Ethernet, Token Ring e FDDI.

Qual a importância do encapsulamento de dados? Novell Netware suporta múltiplos métodos de encapsulamento, incompatíveis entre si, e os suporta sob a mesma mídia. Por exemplo, Ethernet. Netware utiliza 4 diferentes tipos de encapsulamento (veja tabela acima), à serem escolhidos de acordo com sua necessidade. Cada um deles é incompatível com o próximo. Eis o que pode ocorrer: Suponha que seus servidores utilizam o método de encapsulamento Ethernet_802.2, enquanto que seus clientes utilizam o método Ethernet_II. Se eles estão se comunicando através de um router que suporte os 2 tipos de encapsulamento, nenhum problema. Caso contrário, eles simplesmente não se comunicarão. Quando configurando IPX em sua rede, certifique-se de que exista consistência no tipo de frame escolhido. Em alguns caso, entretanto, você pode ter múltiplos tipos de frames (encapsulamento) configurados em uma mesma rede.



Na figura acima, cada tipo de encapsulamento possui um endereço de rede IPX diferente. Mesmo em se tratando de um único segmento Ethernet, existem 3 redes IPX virtuais e, portanto, 3 endereços de rede IPX distintos. Cada rede será propagada através da internetwork em intervalos de 60 segundos. Na figura, a workstation 1 pode se comunicar com o servidor C, pois ambas têm configuradas em suas interfaces o método Ethernet_II de encapsulamento. Workstation 2 comunica-se com o servidor A e a workstation 3 com o servidor B. Para que todas as workstations se comuniquem com todos os servidores existem algumas possibilidades: Uma delas adicionar à rede um router que suporte os 3 tipos de frames ilustrados. Esse router, porém, teria de rotear pacotes para todos os servidores e clientes com tipos de frames distintos. Adicionar múltiplos tipos de frames à servidores e routers não é uma boa solução. Talvez, a melhor solução seja eleger um tipo de frame (provavelmente 802.2) e configurar toda a rede com ele. Netware 5 já é IP-nativo, ou seja, tudo o que falamos é desnecessário, à não ser que você tenha de suportar servidores legados. Quando configurar um router Cisco, você deverá saber o tipo de frame e o endereço da rede IPX para cada segmento à ser conectado ao router.



Ativando roteamento IPX

Para configurar o roteamento IPX, utilize o comando **`ipx routing`**, conforme exemplo abaixo:

```
RouterA#config t
RouterA(config)#ipx routing
```

Uma vez que ipx esteja ativado em seu router, RIP e SAP são automaticamente ativados, também. Nada acontecerá, porém, até que cada interface seja configurada com endereços IPX.

Ativando IPX em cada interface

Uma vez que IPX esteja ativo em seu router,o próximo passo é a configuração individual de interfaces. Primeiro entre no modo de configuração de interface, e em seguida, digite o comando ilustrado abaixo:

`ipx network` *`number`* `[encapsulation encapsulation-type][secondary]`

Onde:

`number` = Endereço da rede IPX

`[encapsulation encapsulation-type]`= Opcional. Veja tabela na página anterior para os tipos de frames default para diferentes tipos de mídia.

`[secondary]`= Define o segundo tipo de frame e endereço de rede na mesma interface

Abaixo, um exemplo de configuração de IPX no router 2501A:

```
2501A#config t
2501A(config)#ipx routing
2501A(config)#int e0
2501A(config-if)#ipx network 10
```

Isso é tudo! O resto é feito para você. IPX é um protocolo de roteamento extremamente auto-suficiente, pois envia mensagens broadcast para quase tudo. Isso explica o porque dos problemas quando se aplica IPX em redes de porte muito grande.

Qual o tipo de frame utilizado no exemplo acima pela interface e0? Por default, é Novell-ether (802.3).

Para alterar ou adicionar outro tipo de frame, utilize o comando **`encapsulation`** na configuração da interface:

```
2501A(config-if)#ipx network 10 encapsulation sap
```

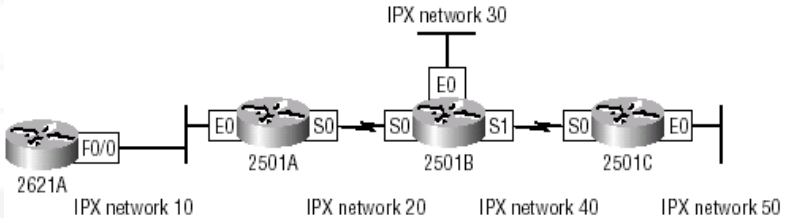
Para adicionar múltiplos frames, utilize o comando **`secondary`**, ou crie sub-interfaces.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Configurando Novell IPX

Configurando IPX em nossa rede sugerida



Vamos começar adicionando o tipo de frame novell-ether (802.3) às redes Ethernet de nossa pequena rede. Uma vez que novell-ether é o tipo de frame default, a configuração é muito simples. O método de encapsulamento default para links seriais é o HDLC. Esse método será discutido na aula 7 de nosso curso.

Configurando IPX no router 2621A:

```
2621A(config)#ipx routing
2621A(config)#int f0/0
2621A(config-if)#ipx network 10
```

Configurando IPX no router 2501A:

```
2501A(config)#ipx routing
2501A(config)#int e0
2501A(config-if)#ipx network 10
2501A(config-if)#int s0
2501A(config-if)#ipx network 20
```

Configurando IPX no router 2501B:

```
2501B(config)#ipx routing
2501B(config)#int e0
2501B(config-if)#ipx network 30
2501B(config-if)#int s0
2501B(config-if)#ipx network 20
2501B(config-if)#int s1
2501B(config-if)#ipx network 40
```

Configurando IPX no router 2501C:

```
2501C(config)#ipx routing
2501C(config)#int e0
2501C(config-if)#ipx network 50
2501C(config-if)#int s0
2501C(config-if)#ipx network 20
```

Para verificar as tabelas de roteamento IPX, utilizamos o comando **`sh ipx route`**, analogamente ao modo utilizado com IP. Como IP, routers IPX apenas conhecem redes diretamente conectadas, por default. Entretanto, ao se ativar o roteamento IPX nas configurações efetuadas na página anterior, IPX RIP foi automaticamente iniciado em todos os routers configurados. IPX RIP irá encontrar todas as redes em nossa internetwork e irá cuidar da atualização das tabelas de roteamento, em cada router. Abaixo ilustramos exemplos do conteúdo das tabelas de roteamento de cada router em nossa rede:

2621A:

```
2621A#sh ipx route
Codes: C - Connected primary network, c - Connected
secondary network
[output cut]
5 Total IPX routes. Up to 1 parallel paths and 16 hops
allowed.
No default route known.
C 10 (NOVELL-ETHER), Fa0/0
R 20 [07/01] via 10.0000.0c8d.3a7b, 16s, Fa0/0
R 30 [07/02] via 10.0000.0c8d.3a7c, 17s, Fa0/0
R 40 [07/02] via 10.0000.0c8d.3a7c, 17s, Fa0/0
R 50 [13/03] via 10.0000.0c8d.3a7c, 17s, Fa0/0
2621A#
```

Ticks (7) e hops (1) até a rede remota

C - Diretamente conectado
R - Redes encontradas pelo IPX RIP

2501A:

```
2501A#sh ipx route
Codes: C - Connected primary network, c - Connected
secondary network
[output cut]
5 Total IPX routes. Up to 1 parallel paths and 16 hops
allowed.
No default route known.
C 20 (HDLC), Se0
C 10 (NOVELL-ETHER), Et0
R 30 [13/02] via 20.0000.0c8d.2b8c, 16s, Se0
R 40 [07/02] via 20.0000.0c8d.2b8c, 17s, Se0
R 50 [07/03] via 20.0000.0c8d.2b8c, 17s, Se0
2501A#
```

2501B:

```
2501B#sh ipx route
Codes: C - Connected primary network, c - Connected
secondary network
[output cut]
5 Total IPX routes. Up to 1 parallel paths and 16 hops
allowed.
No default route known.
C 20 (HDLC), Se0
C 40 (HDLC), Se1
C 30 (NOVELL-ETHER), Et0
R 10 [07/01] via 20.0000.0c8d.3d8e, 16s, Se0
R 50 [07/01] via 40.0000.0c8d.5c9d, 17s, Se1
2501B#
```

2501C:

```
2501C#sh ipx route
Codes: C - Connected primary network, c - Connected
secondary network
[output cut]
5 Total IPX routes. Up to 1 parallel paths and 16 hops
allowed.
No default route known.
C 40 (HDLC), Se0
C 50 (NOVELL-ETHER), Et0
R 10 [13/02] via 40.0000.0c8d.5c9d, 16s, Se0
R 20 [07/01] via 40.0000.0c8d.5c9d, 17s, Se0
R 30 [07/01] via 40.0000.0c8d.5c9d, 17s, Se0
2501C#
```

Novell-ether (802.3) é o tipo de frame Ethernet (encapsulamento) padrão em uma rede IPX. Quando o comando **encapsulation** não é utilizado, o tipo de frame default (novell-ether) é usado. À seguir, veremos como configurar múltiplos tipos de frames em nossas redes Ethernet. Lembre-se, no entanto, que em um ambiente de produção essa não é uma prática saudável.

Para configurar múltiplos tipos de frames em uma única interface, você pode usar o comando secondary. Não há diferenças funcionais em como os comandos **secondary** ou **subinterface** operam em uma internetwork. A diferença é apenas à nível administrativo.

Configuração de endereços secundários

Para configurar endereços secundários em uma LAN Ethernet para que a mesma suporte múltiplos tipos de frames, utilize o comando **ipx network** com o parâmetro **secondary** no final. O exemplo abaixo ilustra o procedimento:

```
2501A#config t
Enter configuration commands, one per line. End with
CNTL/Z.
2501A(config)#int e0
2501A(config-if)#ipx network 10a encap sap sec
```

Caso o comando sec não seja adicionado ao final da linha, o comando digitado irá substituir o anterior (10 por 10a). O mais importante à ser entendido aqui é que cada tipo de frame deve ter um endereço IPX de rede diferente.

Subinterfaces

Para definir subinterfaces, utilize o comando interface número da porta Ethernet. Qualquer número compreendido entre e.0.0 e e.0.4292967295 pode ser usado na criação de subinterfaces. No exemplo abaixo, o tipo de frame 802.2 (sap) é adicionado:

```
2621A(config)#int e0.10
2621A(config-subif)#ipx network 10a encap sap
2621A(config-subif)#^Z
2621A#
```

Conforme mencionado anteriormente, não há diferenças funcionais entre a criação de subinterfaces ou a utilização do comando **sec**. A diferença existe apenas em caráter administrativo. Subinterfaces permitem um maior poder gerencial, uma vez que comandos podem ser aplicados à subinterface. Quando se utiliza o comando **secondary**, a rede fica dependente da interface física, e qualquer alteração que se faça na mesma afetará a rede como um todo.

Configuração de múltiplos tipos de frame em uma mesma interface

Lembre-se mais uma vez. Isso não é recomendável em ambiente de produção. O único caso em que se deve fazer isso é quando existem clientes na rede que, simplesmente, não suportam o tipo de frame 802.3 (novell-ether), e você precisa que a rede suporte, também, 802.2 (sap). Lembre-se: a melhor rede IPX é aquela que roda apenas 1 tipo de frame.

É importante entender que isso é aplicado somente às interfaces LAN, e que você não utiliza frames LAN em interfaces WAN.

Múltiplos frames no router 2621A

Para configuração de múltiplos frames no router 2621A, você precisará adicionar 3 novos números de rede, um para cada tipo de frame que você irá adicionar. No exemplo abaixo, criaremos um endereço secundário (comando sec) e 2 subinterfaces, para adição dos 3 tipos de frame faltantes. Em um ambiente de produção, aconselhamos apenas o uso de subinterfaces, uma vez que endereços secundários deixarão de ser suportados pela Cisco em breve.

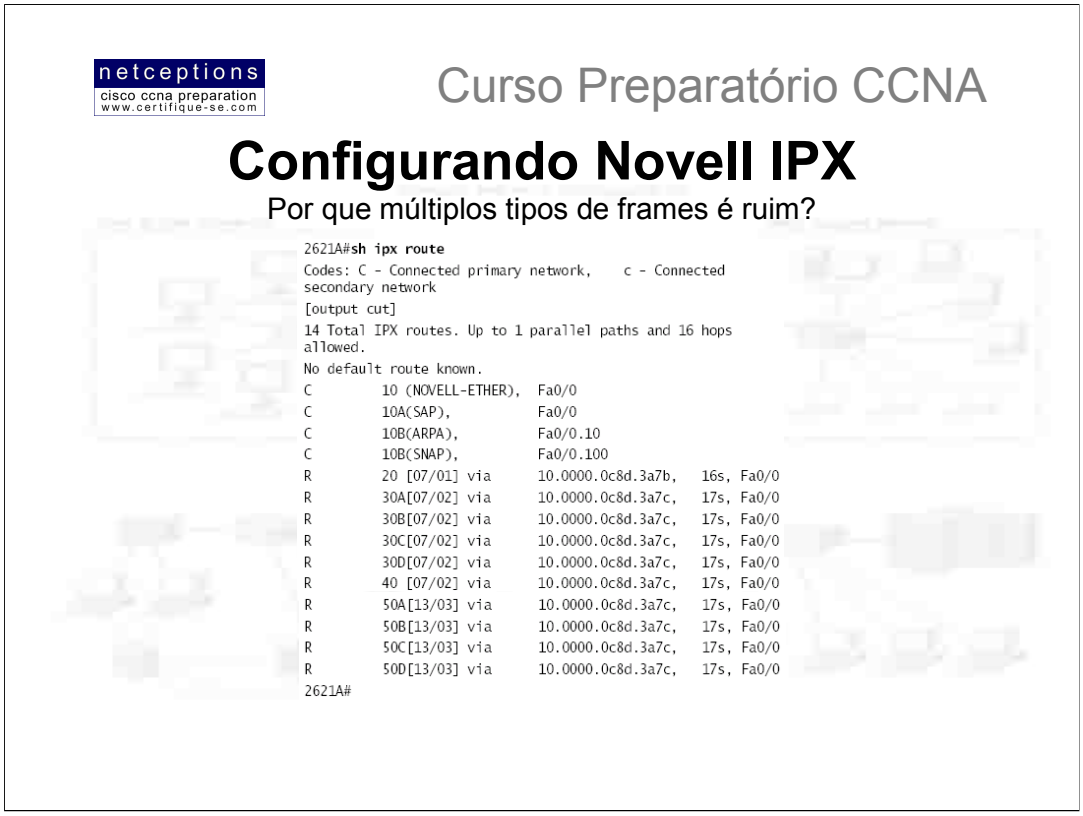
```
2621A(config-if)#ipx network 10a encap sap sec

2621A(config)#int f0/0.10
2621A(config-if)#ipx network 10b encap arpa

2621A(config)#int f0/0.100
2621A(config-if)#ipx network 10c encap snap
```

Os 4 tipos de frames estão agora configurados na interface FastEthernet0/0 do router 2621A. Para qualquer dispositivo ser capaz de se comunicar com o router 2621A usando IPX, ele deverá suportar os mesmos números de rede configurados para cada tipo de frame.

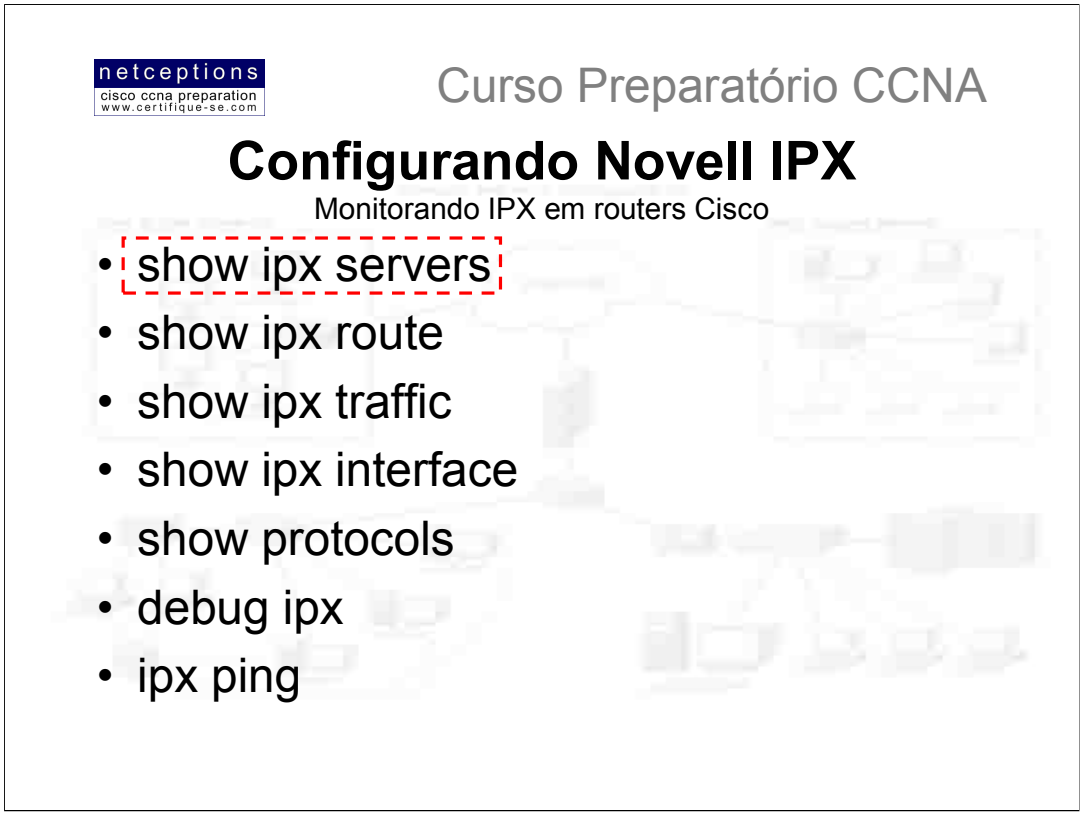
Não ilustraremos o processo de configuração de tipos de frames para os outros routers, visto que a metodologia é exatamente a mesma. Apenas devemos lembrar que os números de rede devem ser iguais para cada tipo de frame configurado.



Quando executamos o comando **`sh ipx route`** anteriormente, existiam apenas uma conexão para cada rede IPX nas tabelas de roteamento de cada router. A ilustração acima apresenta a saída do mesmo comando após todos os tipos de Ethernet frame terem sido configurados no router.

Note que a tabela de roteamento, agora, possui 14 rotas IPX, no lugar das apenas 5 anteriores. Nenhuma rede física foi adicionada à nossa rede. Cada uma das 3 LANs propagam 4 redes IPX criadas à intervalos de 60 segundos, através de cada interface. Imagine, agora, a adição de todos os tipos de frames em uma rede com mais de 20 routers...! Essa tabela seria gigantesca. E isso ocupa uma preciosa largura-de-banda.

Existe mais uma consideração à ser feita quanto à questão de se adicionar múltiplos tipos de frames à uma LAN: A atividade SAP. SAP (Service Advertisement Protocol) é propagado através de cada interface ativa em intervalos de 60 segundos. Caso sua LAN tenha múltiplos tipos de frames configurados, a propagação é enviada através de todos os tipos de frames disponíveis. Ou seja, um único pacote SAP seria enviado 4 vezes. Resumindo, os pacotes SAP seriam enviados 4 vezes à cada 60 segundos. Mais uma vez, largura-de-banda sendo desperdiçada.

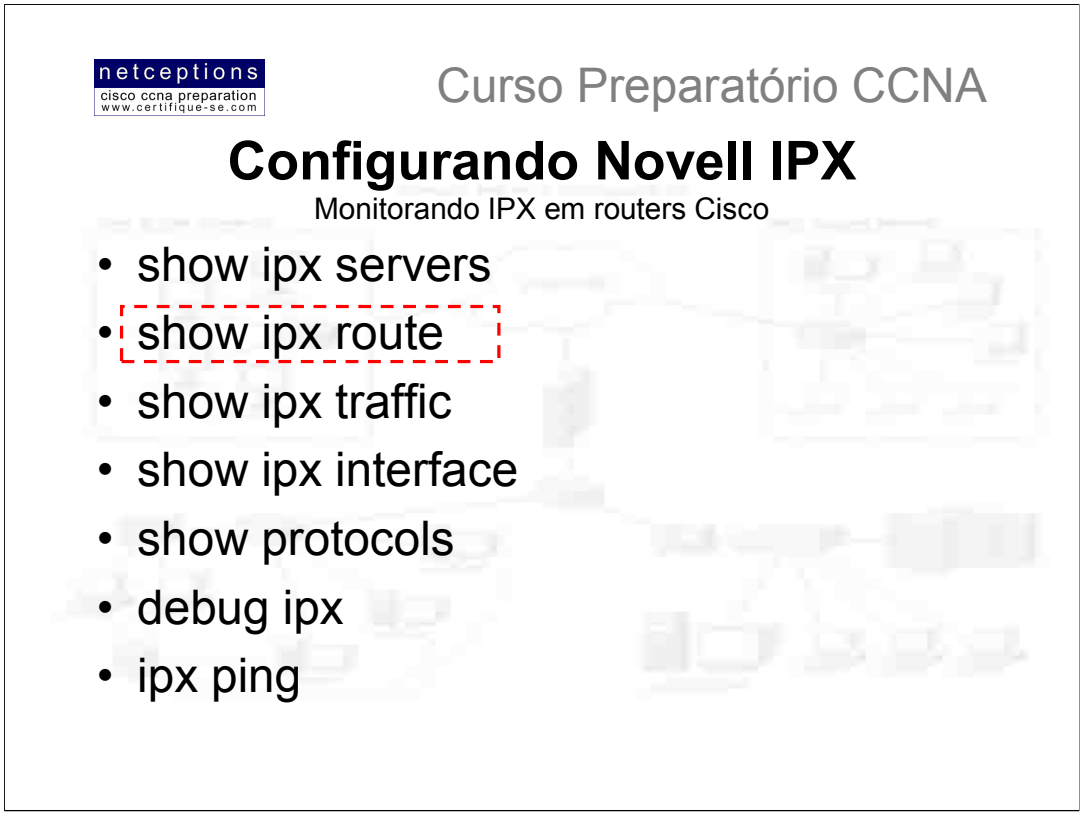


sh ipx servers

O comando **`sh ipx servers`** lembra o comando display servers, no Netware. Ele apresenta o conteúdo da tabela SAP em um router Cisco, ou seja, você será capaz de ver os nomes de todos os serviços SAP com este comando. Se houver servidores faltando na tabela apresentada que não deveriam estar, cheque os endereços IPX de rede e as configurações de encapsulamento.

```
2501A#sho ipx servers
Codes: S - Static, P - Periodic, E - EIGRP, N - NLSP,  H - Holddown, + = detail
9 Total IPX Servers
Table ordering is based on routing and server info
   Type     Name     Net      Address              Port   Route   Hops     Itf
P    4 BORDER1     350ED6D2.0000.0000.0001:0451     2/01    1     Et0
P    4 BORDER3     12DB8494.0000.0000.0001:0451     2/01    1     Et0
P    107 BORDER1   350ED6D2.0000.0000.0001:8104     2/01    1     Et0
P    107 BORDER3   12DB8494.0000.0000.0001:8104     2/01    1     Et0
P    26B BORDER    350ED6D2.0000.0000.0001:0005     2/01    1     Et0
P    278 BORDER    12DB8494.0000.0000.0001:4006     2/01    1      t0
P    278 BORDER    350ED6D2.0000.0000.0001:4006     2/01    1     Et0
P    3E1 BORDER1   350ED6D2.0000.0000.0001:9056     2/01    1     Et0
P    3E1 BORDER3   12DB8494.0000.0000.0001:9056     2/01    1     Et0
```

A saída apresentada permite que se identifique todos os servidores IPX descobertos através das propagações SAP. O campo Type identifica o tipo de serviço SAP sendo propagado, com o valor 4 sendo serviço de arquivo (file service) e 7 sendo um serviço de impressão (print service). O campo Net Address lista os endereços IPX de rede configurados em cada servidor. O campo Port identifica a aplicação de camada superior. O número do socket para o Netware Control Protocol (NCP) é 451.

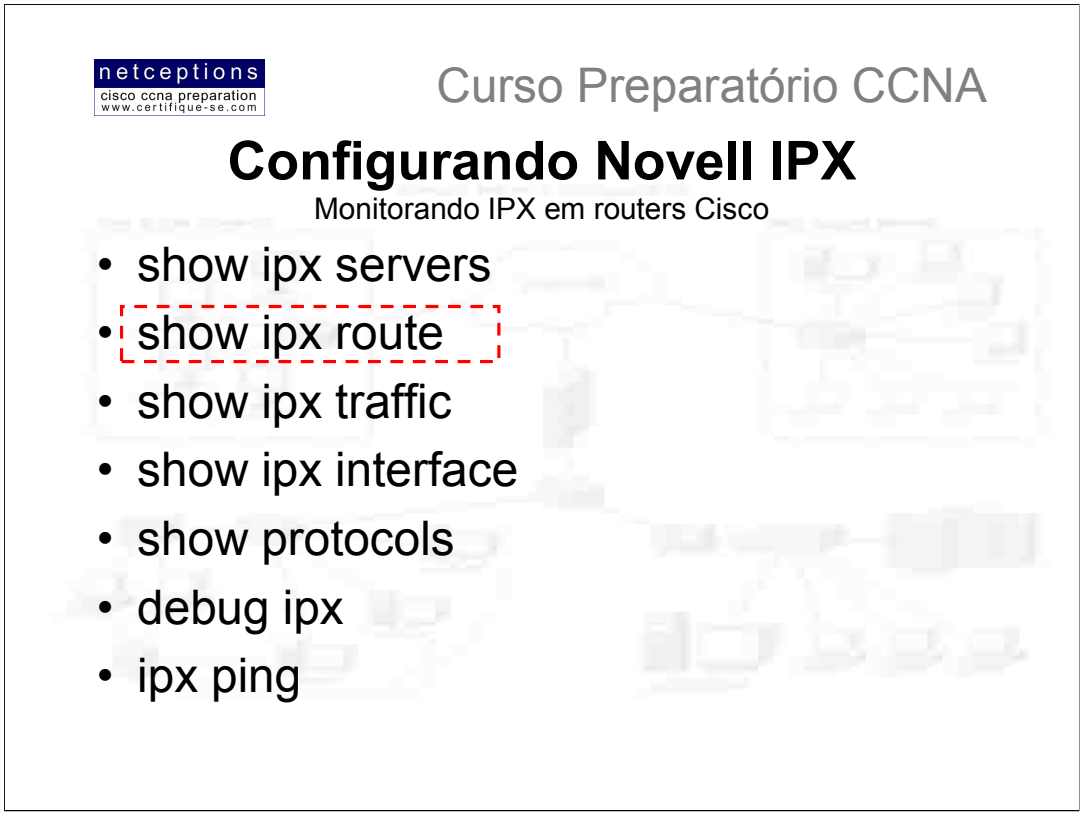


sh ipx route

O comando **`sh ipx route`** apresenta o conteúdo da tabela de roteamento IPX, com as rotas que o router conhece. O router propaga as redes que encontram-se diretamente conectadas, e, após algum tempo, propaga também as redes que foram "aprendidas", desde que o mesmo foi inicializado.

```
2501A#sh ipx route
Codes: C - Connected primary network,     c - Connected
secondary network, S - Static, F - Floating static, L -
Local (internal), W - IPXWAN, R - RIP, E - EIGRP, N -
NLSP, X - External, A - Aggregate, s - seconds, u - uses
6 Total IPX routes. Up to 1 parallel paths and 16 hops
allowed.
No default route known.

C       10 (NOVELL-ETHER),  Et0
C       20 (HDLC),          Se0
c       10a (sap),          Et0
C       10b (ARPA),         Et0.10
R       40 [07/01] via     20.00e0.1ea9.c418,    13s, Se0
R       50 [13/02] via     20.00e0.1ea9.c418,    13s, Se0
RouterA#
```

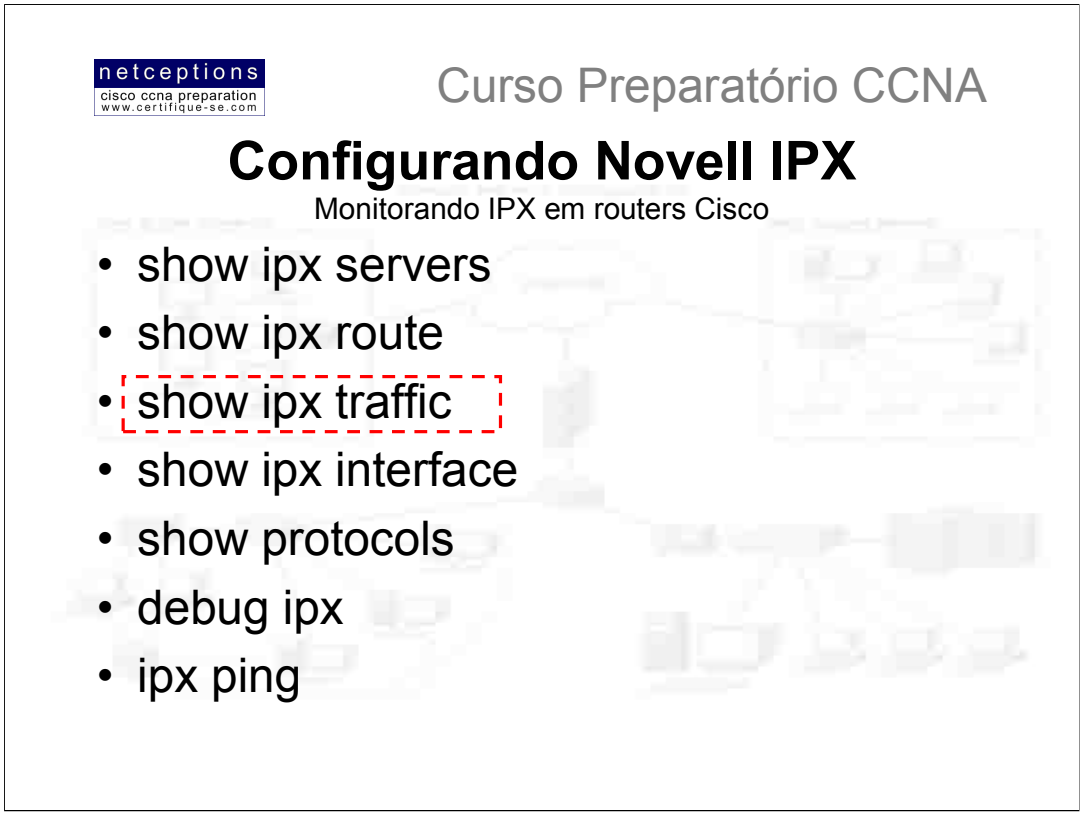


Balanceando carga com IPX

Se você configurar rotas IPX paralelas entre routers Cisco, o sistema IOS não "aprenderá" sobre essas rotas, por default. O router irá aprender uma única rota para o destino e descartará a informação sobre rotas alternativas, paralelas ou de igual custo. Na saída do comando **`sh ipx route`** , a frase "`up to 1 paralell paths and 16 hops are allowed`". Para ser capaz de realizar round-robin load balance (balanceamento de carga alternado) através de múltiplos links de igual custo, o comando **`ipx maximum-paths [#]`** (com # sendo um número até 64) deve ser utilizado. Este comando permitirá que o router aceite a possibilidade de que, talvez, exista outra rota para o mesmo destino.

Por default, o router Cisco irá realizar um compartilhamento de carga por pacote através dessas rotas paralelas. Pacotes serão enviados alternadamente (round-robin) entre todos os links de igual custo, independentemente do destino. Entretanto, caso você deseje que todos os pacotes enviados para um destino ou host específico sempre utilize a mesma rota, o comando **`ipx per-host-load-share`** deve ser utilizado. Abaixo, ilustramos um exemplo de utilização do comando ipx maximum-paths. Ele informa ao IPX RIP para alternar o balanceamento de carga entre 2 links de igual custo.

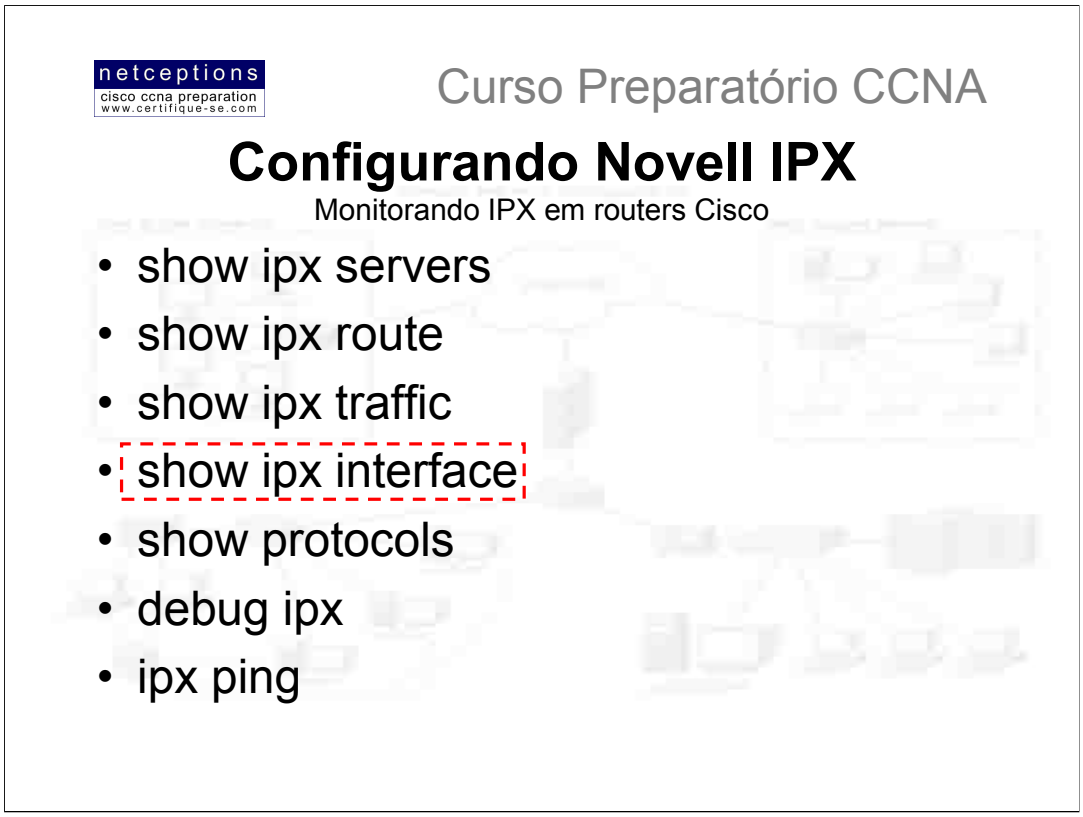
```
Router#config t
Router(config)#ipx maximum-paths 2
Router(config)#^Z
Router#sh ipx route
Codes: C - Connected primary network,     c - Connected
[output cut]
5 Total IPX routes. Up to 2 parallel paths and 16 hops
allowed.
[output cut]
```



sh ipx traffic

O comando **`sh ipx traffic`** apresenta um sumário do número e tipo dos pacotes IPX recebidos e enviados pelo router. Note que este comando irá apresentar estatísticas sobre pacotes IPX RIP e SAP. Para verificar as estatísticas de pacotes RIP e SAP em apenas uma determinada interface, utilize o comando **`sh ipx interface`**

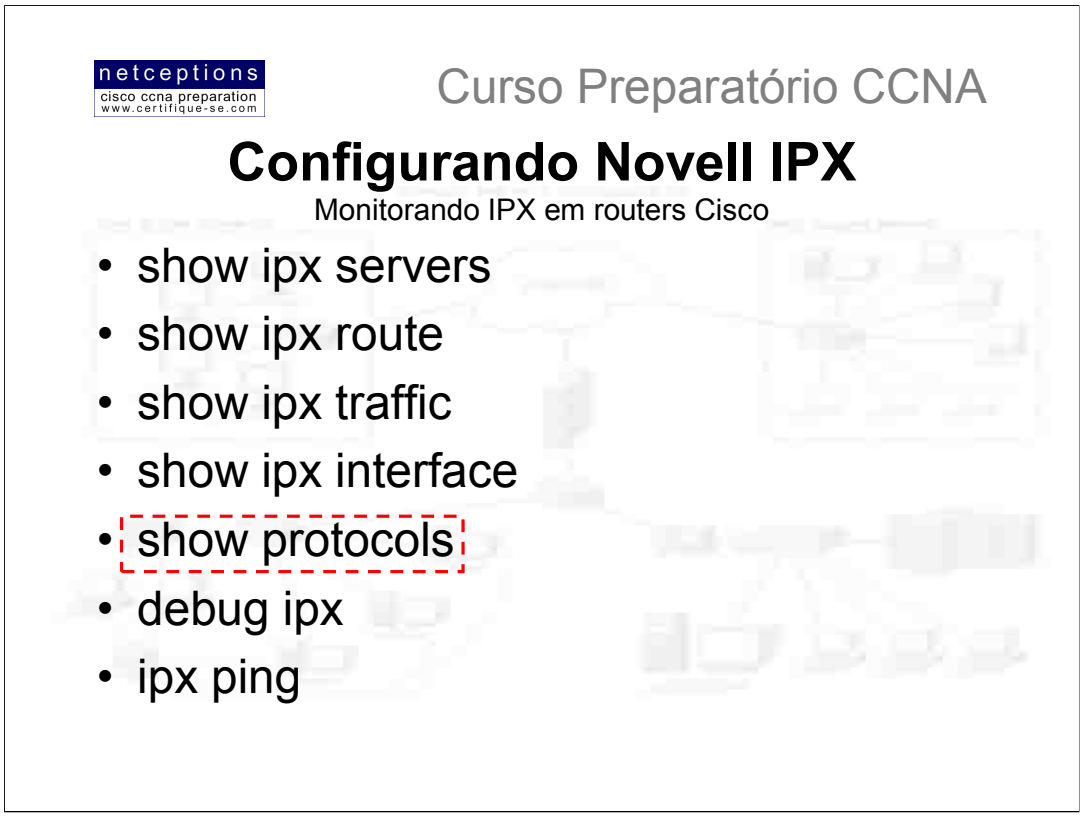
```
2501A#sh ipx traffic
System Traffic for 0.0000.0000.0001 System-Name: RouterA
Rcvd:   15 total, 0 format errors, 0 checksum errors, 0
bad hop count, 0 packets pitched, 15 local destination, 0
multicast
Bcast:  10 received, 249 sent
Sent:   255 generated, 0 forwarded
        0 encapsulation failed, 0 no route
SAP:    1 SAP requests, 0 SAP replies, 0 servers
        0 SAP Nearest Name requests, 0 replies
        0 SAP General Name requests, 0 replies
        0 SAP advertisements received, 0 sent
        0 SAP flash updates sent, 0 SAP format errors
RIP:    1 RIP requests, 0 RIP replies, 6 routes
        8 RIP advertisements received, 230 sent
        12 RIP flash updates sent, 0 RIP format errors
Echo:   Rcvd 0 requests, 5 replies
        Sent 5 requests, 0 replies
        0 unknown: 0 no socket, 0 filtered, 0 no helper
        0 SAPs throttled, freed NDB len 0
Watchdog:
        0 packets received, 0 replies spoofed
Queue lengths:
        IPX input: 0, SAP 0, RIP 0, GNS 0
        SAP throttling length: 0/(no limit), 0 nets
pending lost route reply
 --More-
```



sh ipx interface

O comando **`sh ipx interface`** apresenta o status das interfaces IPX e os parâmetros configurados nas mesmas. O comando **`sh ipx int e0`**, por exemplo, apresenta o endereço IPX e o tipo de encapsulamento da interface e0. Lembre-se que o comando **`sh int e0`**, somente, apresenta o endereço IP, e não o IPX.

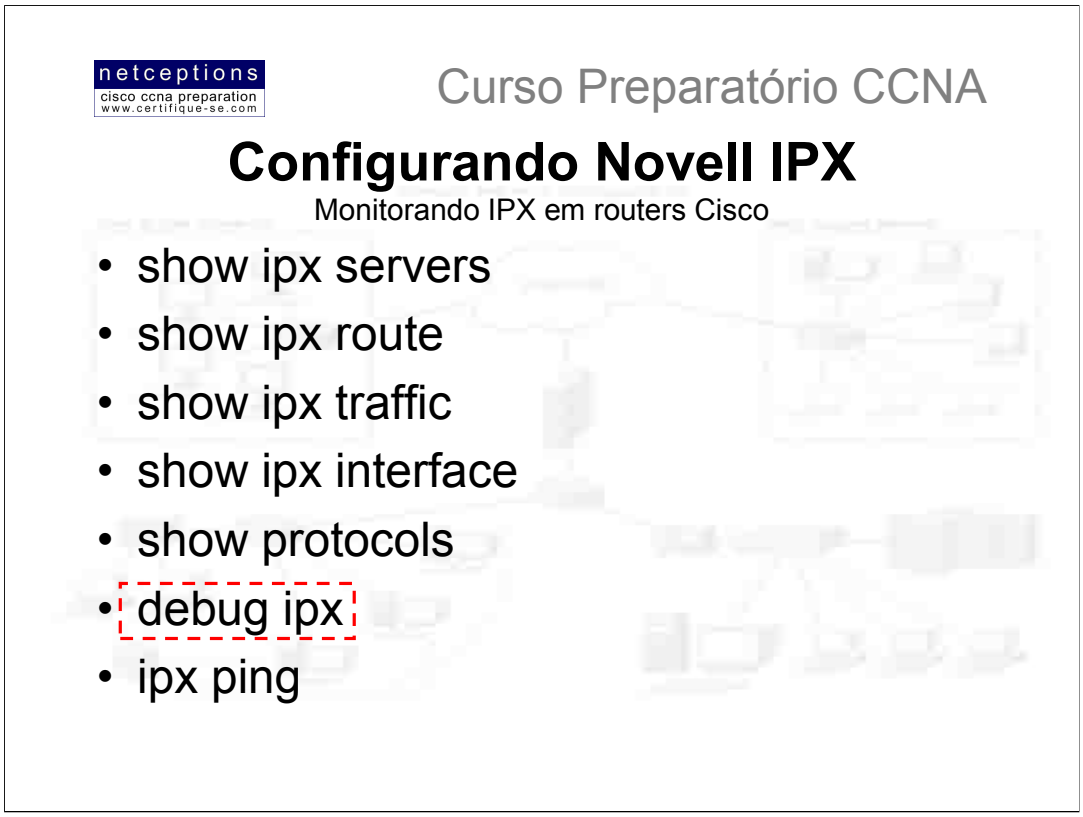
```
2501A#sh ipx int e0
Ethernet0 is up, line protocol is up
  IPX address is 10.0000.0c8d.5c9d, NOVELL-ETHER [up]
  Delay of this IPX network, in ticks is 1 throughput 0
link delay 0
  IPXWAN processing not enabled on this interface.
  IPX SAP update interval is 1 minute(s)
  IPX type 20 propagation packet forwarding is disabled
  Incoming access list is not set
  Outgoing access list is not set
  IPX helper access list is not set
  SAP GNS processing enabled, delay 0 ms, output filter
list is not set
  SAP Input filter list is not set
  SAP Output filter list is not set
  SAP Router filter list is not set
  Input filter list is not set
  Output filter list is not set
  Router filter list is not set
  Netbios Input host access list is not set
  Netbios Input bytes access list is not set
  Netbios Output host access list is not set
  Netbios Output bytes access list is not set
  Updates each 60 seconds, aging multiples RIP: 3 SAP: 3
  SAP interpacket delay is 55 ms, maximum size is 480
bytes
  RIP interpacket delay is 55 ms, maximum size is 432
bytes
 --More-
```



sh protocols

O comando **`sh protocols`** também apresenta o endereço IPX e o tipo de encapsulamento de uma interface. Este comando também apresenta os protocolos roteados configurados no router e os endereços IP das interfaces. Lembre-se: há apenas 2 comandos que apresentam o endereço IPX de uma interface: **`sh proto`** e **`sh ipx interface`**.

```
2501A#sh protocols
Global values:
  Internet Protocol routing is enabled
  IPX routing is enabled
Ethernet0 is up, line protocol is up
  Internet address is 172.16.10.1/24
  IPX address is 10.0060.7015.63d6 (NOVELL-ETHER)
  IPX address is 10A.0060.7015.63d6 (SAP)
Ethernet0.10 is up, line protocol is up
  IPX address is 10B.0060.7015.63d6
Ethernet0.100 is up, line protocol is up
  IPX address is 10C.0060.7015.63d6
Serial0 is up, line protocol is up
  Internet address is 172.16.20.1/24
  IPX address is 20.0060.7015.63d6
```



debug ipx

Os comandos **debug ipx** (**debug ipx routing activity** e **debug ipx sap activity**) apresentam uma saída ilustrando o comportamento do IPX em sua rede. Atualizações IPX SAP e IPX RIP podem ser verificadas através deste comando. Deve ser usado com atenção, uma vez que consome muita CPU.

debug ipx routing activity

O comando **debug ipx routing activity** apresenta informações sobre atualizações IPX que são transmitidas ou recebidas pelo router. Para desativar esse recurso, digite: **undebug ipx routing act**

```
RouterA#debug ipx routing act
IPX routing debugging is on
RouterA#
IPXRIP: update from 20.00e0.1ea9.c418
50 in 2 hops, delay 13
40 in 1 hops, delay 7
IPXRIP: positing full update to 10.ffff.ffff.ffff via
Ethernet0 (broadcast)
IPXRIP: src=10.0000.0c8d.5c9d, dst=20.ffff.ffff.ffff,
packet sent
network 50, hops 3, delay 14
network 40, hops 2, delay 8
network 30, hops 1, delay 2
network 20, hops 1, delay 2
network 10, hops 1, delay 2
```

debug ipx sap activity

O comando **debug ipx sap activity** apresenta os pacotes IPX SAP transmitidos ou recebidos pelo router. Cada pacote SAP é apresentado como múltiplas linhas na saída do comando. Digite o comando **undebug ipx sap act** para desativar esse recurso.

```
RouterA#debug ipx sap activity
05:31:18: IPXSAP: positing update to 1111.ffff.ffff.ffff
via Ethernet0 (broadcast) (full)
02:31:18: IPXSAP: Update type 0x2 len 288
src:1111.00e0.2f5d.bf2e dest:1111.ffff.ffff.ffff(452)
02:31:18: type 0x7, ” MarketingPrint ",
10.0000.0000.0001(451), 2 hops
02:31:18: type 0x4, "SalesFS", 30.0000.0000.0001(451),
2 hops
02:31:18: type 0x4, "MarketingFS",
30.0000.0000.0001(451), 2 hops
02:31:18: type 0x7, "SalesFS", 50.0000.0000.0001(451),
2 hops
```

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Configurando Novell IPX

Monitorando IPX em routers Cisco

- show ipx servers
- show ipx route
- show ipx traffic
- show ipx interface
- show protocols
- debug ipx
- ipx ping

ipx ping

Você pode ou conectar-se à um host remoto via Telnet ou utilizar o comando sh cdp neighbor detail (ou sh cdp entry *) para identificar o endereço IPX de um router vizinho. Isso permitirá à você "pingar" o endereço identificado de um router através da utilização do comando ping (normal ou estendido).

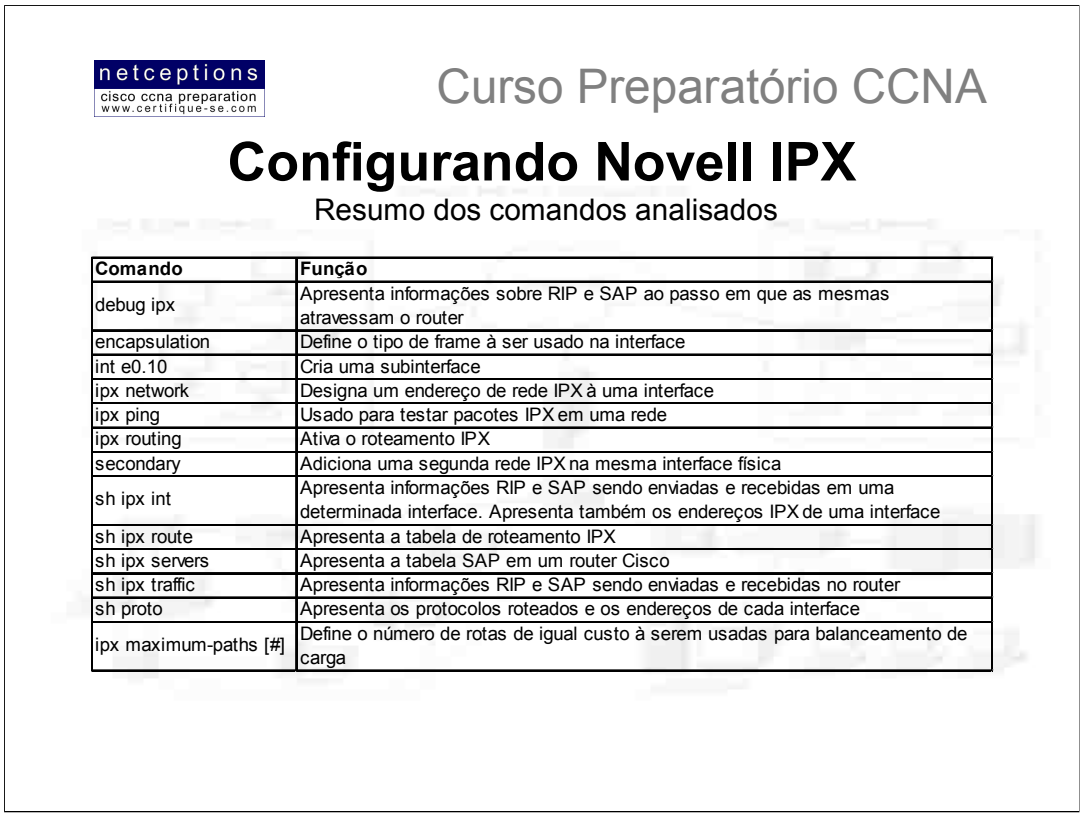
```
RouterC#sh cdp entry *
-------------------------
Device ID: RouterB
Entry address(es):
  IP address: 172.16.40.1
  Novell address: 40.0000.0c8d.5c9d
Platform: cisco 2500,  Capabilities: Router
Interface: Serial0,  Port ID (outgoing port): Serial1
Holdtime : 155 sec

RouterC#ping ipx 40.0000.0c8d.5c9d
Sending 5, 100-byte IPX Novell Echoes to 40.0000.0c8d.5c9d
, timeout is 2 seconds:
!!!!!

RouterC#ping
Protocol [ip]: ipx
Target IPX address: 40.0000.0c8d.5c9d
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Verbose [n]:
Novell Standard Echo [n]: y
Type escape sequence to abort.
Sending 5, 100-byte IPX Novell Echoes to 40.0000.0c8d.5c9d
, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max
= 4/7/12 ms
```

ping regular

ping estendido



Comando	Função
debug ipx	Apresenta informações sobre RIP e SAP ao passo em que as mesmas atravessam o router
encapsulation	Define o tipo de frame à ser usado na interface
int e0.10	Cria uma subinterface
ipx network	Designa um endereço de rede IPX à uma interface
ipx ping	Usado para testar pacotes IPX em uma rede
ipx routing	Ativa o roteamento IPX
secondary	Adiciona uma segunda rede IPX na mesma interface física
sh ipx int	Apresenta informações RIP e SAP sendo enviadas e recebidas em uma determinada interface. Apresenta também os endereços IPX de uma interface
sh ipx route	Apresenta a tabela de roteamento IPX
sh ipx servers	Apresenta a tabela SAP em um router Cisco
sh ipx traffic	Apresenta informações RIP e SAP sendo enviadas e recebidas no router
sh proto	Apresenta os protocolos roteados e os endereços de cada interface
ipx maximum-paths [#]	Define o número de rotas de igual custo à serem usadas para balanceamento de carga

Resumo módulo 6-b:

Nesta aula discutimos em detalhes o protocolo IPX, criado pela Novell. Eis os tópicos abordados:

- Endereçamento IPX e tipos de frames (encapsulamento)
- Como ativar o protocolo IPX e configurá-lo nas interfaces de um router
- Como monitorar as operações do protocolo IPX em um router
- Porção de nó e de rede de um endereço IPX

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Configurando Novell IPX

Termos-chave

Antes da prova, certifique-se que esteja familiarizado com os seguintes termos:

connection ID

encapsulation

framing

socket

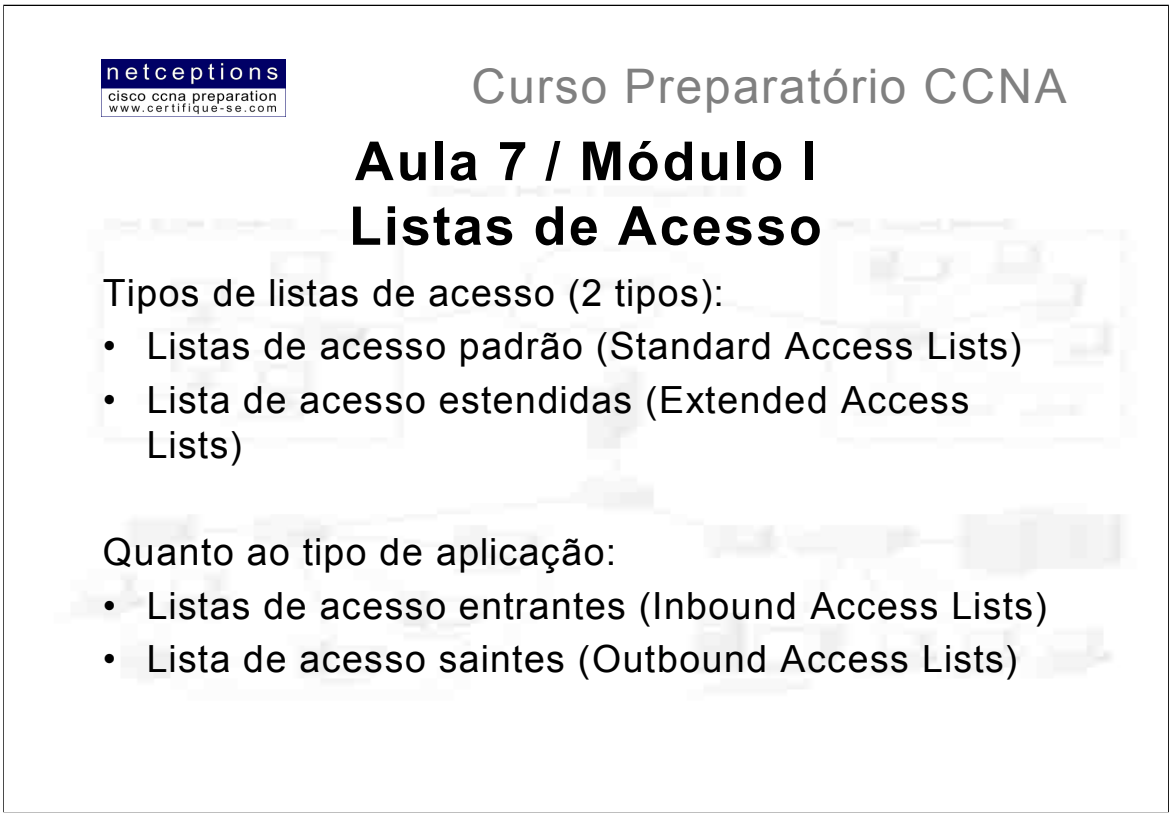
virtual circuit

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

FIM AULA 06

Apostila Aula 7



A apropriada configuração e uso de listas de acesso é um procedimento vital no processo de configuração de um router. Listas de acesso permitem aos administradores de rede o gerenciamento de um grande fluxo através da rede como um todo. Aplicando listas de acesso, administradores podem obter estatísticas sobre o fluxo de pacotes e, então, implementar políticas de segurança apropriadas.

Listas de acesso podem ser utilizadas para permitir ou negar o fluxo de pacotes através de um router, permitir ou negar acesso via Telnet (VTY) para ou de um router, proteger dispositivos críticos de acessos não autorizados, e determinar o que é considerado "tráfego interessante (interesting traffic) em uma rede, que em um ambiente de discagem sob demanda (dial-on-demand - DDR) iniciará o processo de discagem para um local remoto.

Listas de acesso são, essencialmente, listas de condições que controlam o acesso. Listas de acesso IP e IPX funcionam de maneira análoga, não havendo grandes diferenças quanto às suas implementações. Uma vez criadas, listas de acesso podem ser aplicadas tanto ao tráfego entrante (inbound traffic) quanto ao tráfego sainte (outbound traffic), em qualquer interface. A aplicação de listas de acesso fará com que o router examine cada pacote atravessando uma determinada interface em uma determinada direção, e tome providências apropriadas.

Algumas regras que um pacote segue quando comparado com listas de acesso:

• A comparação com cada linha da lista de acesso sempre ocorre sequencialmente, ou seja, sempre se inicia na linha 1, seguindo para a linha 2, e assim sucessivamente.

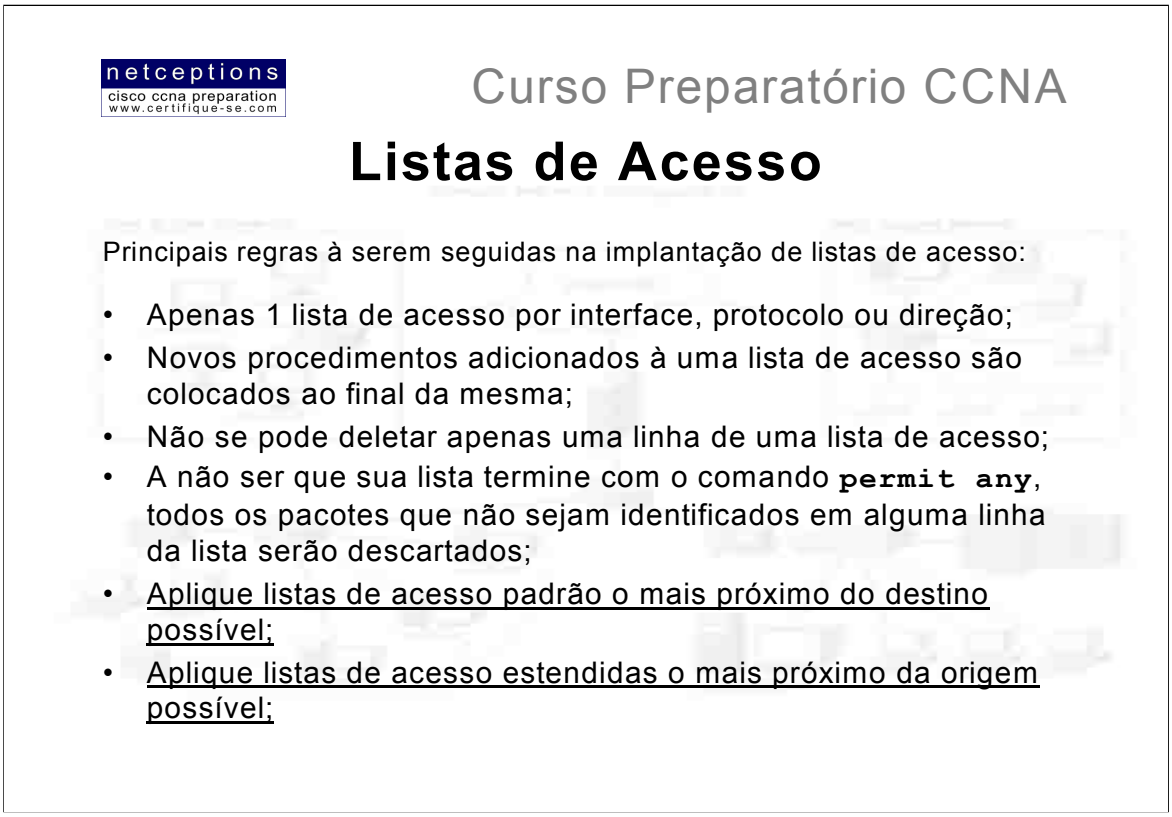
• A comparação é realizada apenas até ocorra a identificação de uma linha da lista de acesso com o pacote. Uma vez que essa identificação ocorra, ações específicas são tomadas, e nenhuma comparação adicional é feita.

• Existe um comando "negue" (**`deny`**) implícito (ele não aparece, mas o router o entende) no final de cada lista de acesso. Isso significa que, caso não ocorra nenhuma identificação positiva de um determinado pacote com alguma linha da lista de acesso, o mesmo será descartado.

Existem 2 tipos de lista de acesso: standard (padrão) e extended (estendida). Uma vez criada, a lista de acesso deve ser aplicada à uma interface como entrante (inbound), ou sainte (outbound).

• **Inbound**: Os pacotes são processados pela lista de acesso antes de serem encaminhados para a interface de saída

• **Outbound**: Os pacotes são primeiro encaminhados à interface de saída para depois serem processados pela lista de acesso.



Algumas regras devem ser seguidas na criação e implementação de listas de acesso em um router:

• Apenas 1 lista de acesso pode ser designada por interface, protocolo ou direção. Isso significa que, se você estiver criando listas de acesso IP, apenas 1 lista entrante e 1 sainte é permitida por interface.

• Organize suas listas de acesso para que os procedimentos mais específicos e críticos encontrem-se no início das mesmas.

• Novas listas são sempre adicionadas ao final de listas existentes.

• Não se pode remover apenas uma linha de uma lista de acesso. Ao se tentar faze-lo, toda a lista será deletada. É melhor copiar a lista de acesso inteira para um editor de textos antes de tentar editá-la. A única exceção é no caso de listas de acesso nomeadas.

• A menos que sua lista de acesso termine com o comando **`permit any`**, todos os pacotes que não sejam identificados com algum procedimento da lista ativa serão descartados. Por esse motivo, toda lista deve conter ao menos um comando **`permit`**, ou você pode, sem saber, estar desativando sua interface.

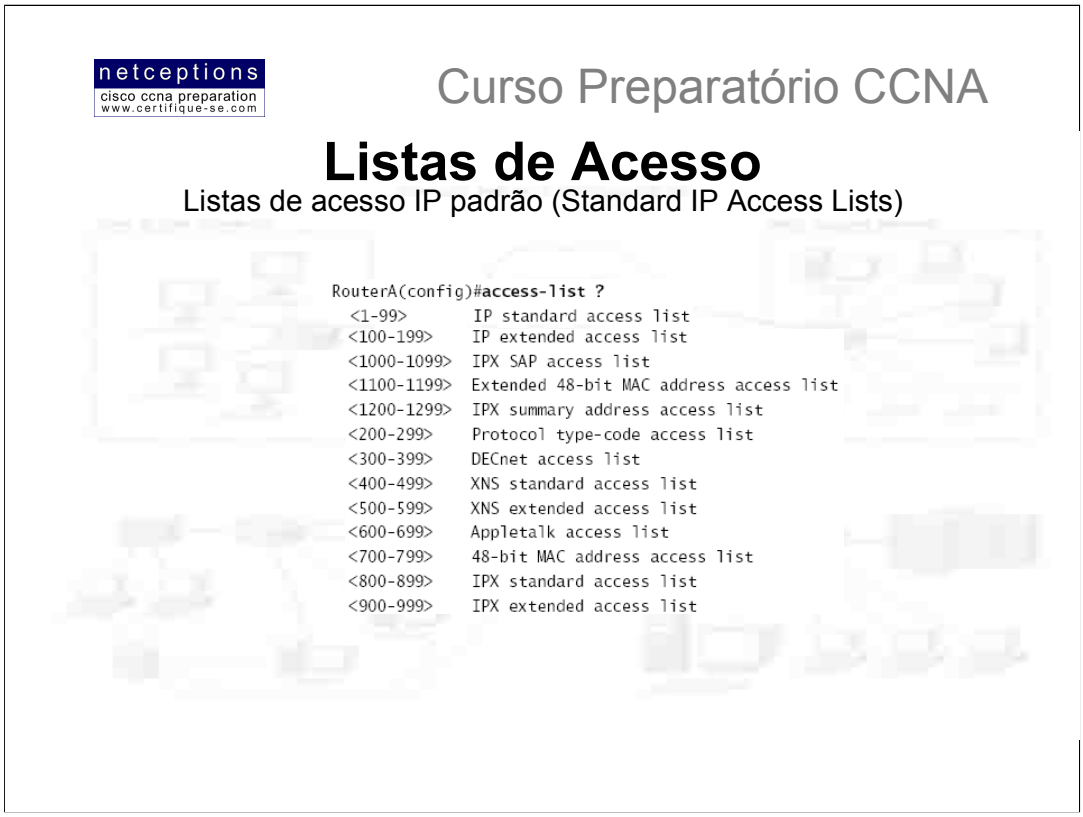
• Primeiro crie listas de acesso para depois aplicá-las às interfaces. De nada adianta a aplicação de listas de acesso que não estejam presentes.

• Listas de acesso foram idealizadas e concebidas para filtrar o tráfego que atravessa um router. Elas não filtrarão o tráfego originado pelo router onde encontram-se aplicadas.

• Listas de acesso padrão (standard) devem ser aplicadas o mais próximo do destino possível(*).

• Listas de acesso estendidas devem ser aplicadas o mais próximo da origem possível(*).

(*)**NOTA:** Essas 2 últimas regras são de extrema importância e caem no exame CCNA com frequência.



Listas de acesso IP padrão (standard IP access lists) filtram a rede utilizando o endereço IP de origem em um pacote IP. Listas de acesso IP padrão são identificadas por números compreendidos no intervalo 1-99 (veja a ilustração acima). É muito importante lembrar-se disso. 1-99: listas de acesso IP padrão, 100-199: listas de acesso IP estendida, 800-899: listas de acesso IPX padrão, 900-999: listas de acesso IPX estendidas. Para o exame CCNA, apenas o conhecimento destas listas é o suficiente. Memorize estes intervalos!

Eis o procedimento para se criar uma lista de acesso IP padrão:

```
RouterA(config)#
access-list 10 ?
deny Specify packets to reject
permit Specify packets to forward
```

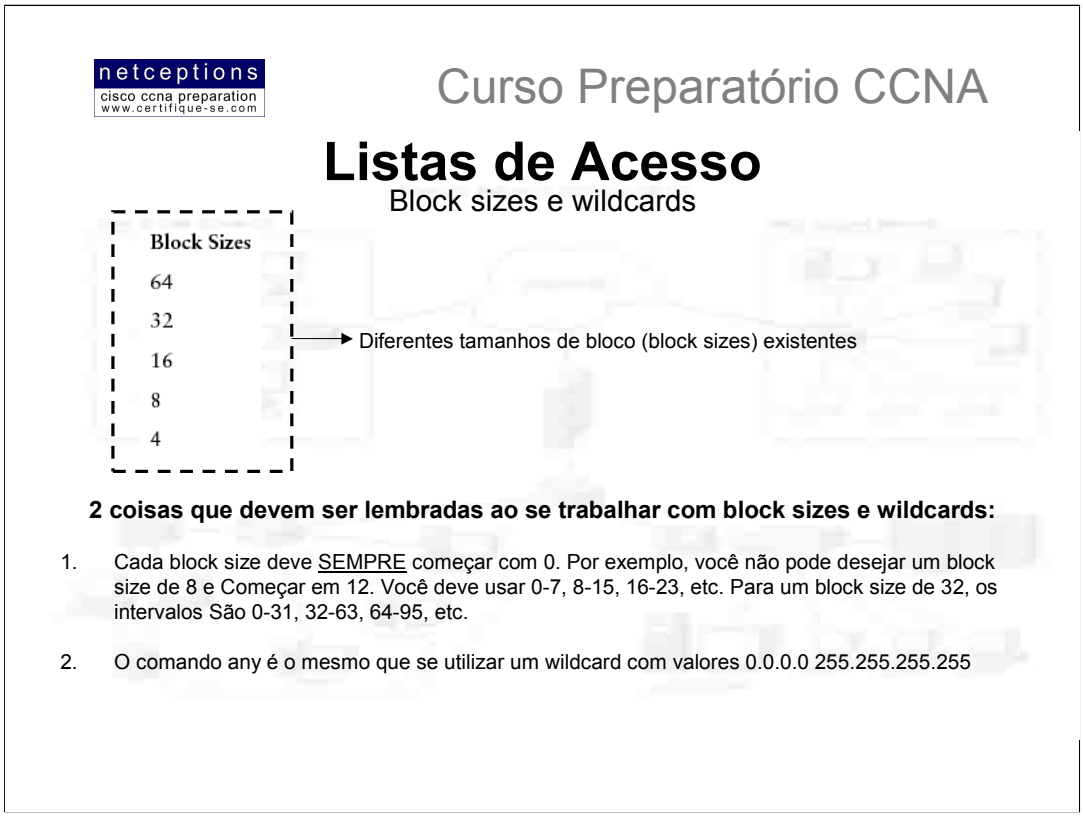
Após escolher o número desejado para a lista de acesso à ser criada (10 no nosso caso), deve-se definir se esta será uma lista do tipo permit ou deny (permitir / negar acesso). Suponhamos que seja uma lista de acesso deny:

```
RouterA(config)#
access-list 10 deny ?
Hostname or A.B.C.D Address to match
any Any source host
host A single host address
```

Nos deparamos agora com 3 opções: pode-se utilizar o comando **any** para permitir ou negar o acesso à qualquer host ou rede, pode-se especificar o endereço IP para um host ou rede específico, ou pode-se ainda utilizar o comando **host** para especificar apenas um determinado host. Eis um exemplo de uma entrada que instrui a lista de acesso à negar qualquer pacote que tenha originado do host 172.16.30.2:

```
RouterA(config)# access-list 10 deny host 172.16.30.2
```

Host é o comando default, ou seja, se você simplesmente digitar **access-list 10 deny 172.16.30.2** o router entenderá como se o comando **host** tivesse sido digitado.



Existe ainda um outro modo de se especificar um host específico: utilizando-se wildcards. Na verdade, para se especificar uma rede ou sub-rede, não há outro modo. Deve-se utilizar wildcards nas listas de acesso.

Wildcards são utilizados em listas de acesso para especificar um host, uma rede, ou parte de uma rede. O primeiro passo no entendimento de wildcards é o entendimento de block sizes (tamanhos de bloco). Block sizes são utilizados para especificar um intervalo de endereços. A lista acima apresenta alguns dos diferentes tamanhos de bloco existentes.

Quando você precisa especificar um intervalo de endereços, você deve escolher o tamanho de bloco (block size) que mais se aproxima de suas necessidades. Por exemplo: se você precisar especificar 34 redes, você precisa de um block size tamanho 64 (mais próximo de 34).

Wildcards são usados em conjunto com o endereço do host ou da rede para informar ao router o intervalo de endereços existentes para filtragem. Para especificar um host, o formato do endereço dever ser algo como:

172.16.30.5 **0.0.0.0**

Os quatro zeros representam cada octeto do endereço. Cada vez que um 0 aparece, significa que o octeto correspondente no endereço deve ser exatamente igual ao informado. Para especificar que um determinado octeto pode ter qualquer valor, o número 255 é utilizado. No exemplo abaixo, especificamos uma sub-rede inteira:

172.16.30.0 **0.0.0.255**

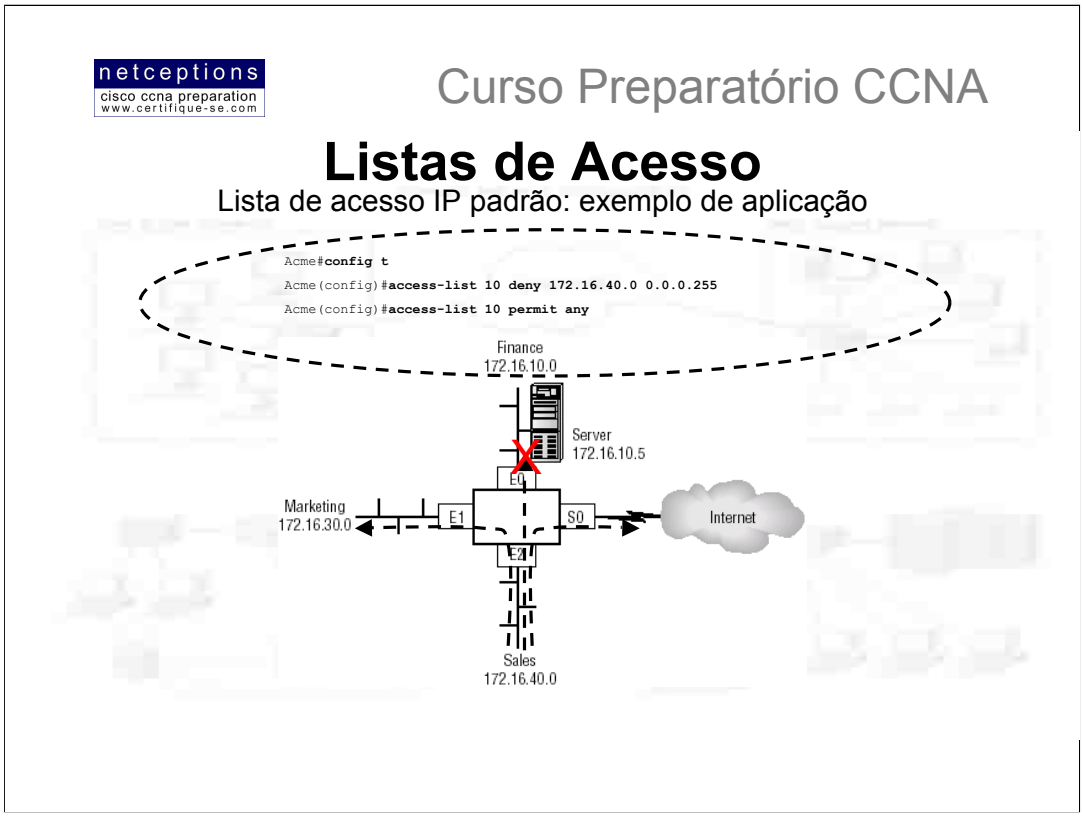
Isso informa ao router que os 3 primeiros octetos (172.16.30) dever ser idênticos aos informados, o quarto octeto, porém, pode conter qualquer valor.

Para especificar um intervalo específico de subredes, block sizes são utilizados. O intervalo de valores deve ser especificado com base em um block size. Em outras palavras, você não pode especificar 20 subredes, por exemplo. Você pode apenas especificar a quantidade de redes que um block size permite, exatamente. Por exemplo, o intervalo será 16 ou 32, mas nunca 20.

Vamos supor que você queira bloquear o acesso à uma parte da rede compreendida entre o intervalo 172.16.8.0 à 172.16.15.0. O tamanho de bloco à ser utilizado, neste caso, é de 8 (15-8=7 -> block size=8). Seu endereço de rede, portanto, seria 172.16.8.0 e o wildcard seria 0.0.7.255. **Sim, 7 e não 8!** Lembre-se que o wildcard sempre será o número de bloco (block number) menos 1 (8-1=7, no nosso caso). Se você usar um block size de 16, seu wildcard trará o número 15. E assim por diante. Eis um exemplo:

```
RouterA(config)#access-list 10 deny 172.16.16.0 0.0.3.255
```

A configuração acima informa ao router para iniciar no endereço de rede 172.16.16.0 e utilizar um block size de 4. Portanto, o intervalo seria de 172.16.16.0 até 172.16.19.0. Muito simples!



Vamos discutir agora como aplicar listas de acesso IP padrão para impedir o acesso de certos usuários a LAN do departamento de finanças. Na figura acima, um router tem 3 conexões LAN e uma conexão WAN, para a Internet. Usuários do departamento de Vendas não devem ter acesso à LAN do departamento de Finanças, mas eles devem ter acesso à Internet e à LAN do departamento de Marketing. A LAN do depto. de Marketing precisa de acesso à LAN do depto. de Finanças.

No router em questão, a seguinte lista de acesso IP padrão é criada:

```
Acme#config t
Acme(config)#access-list 10 deny 172.16.40.0 0.0.0.255
Acme(config)#access-list 10 permit any
```

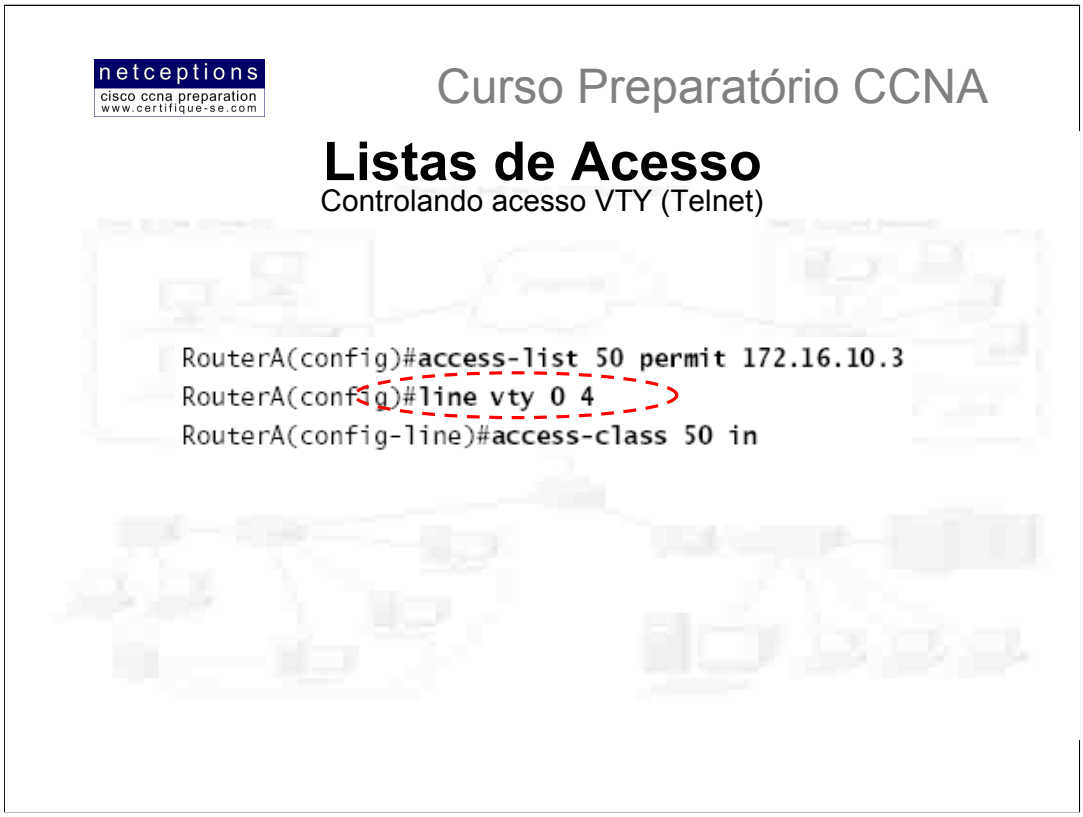
É de extrema importância o entendimento que o comando any, utilizado acima, tem o mesmo efeito que a linha abaixo:

```
Acme(config)#access-list 10 permit 0.0.0.0 255.255.255.255
```

Nesta altura, a lista de acesso está negando acesso à LAN de Vendas, e permitindo o acesso de todas as outras LANs. A questão agora é: ONDE está lista de acesso deve ser aplicada? Caso a mesma seja aplicada como uma lista entrante (inbound) na interface e2, por exemplo, você poderá estar desativando a interface e2, uma vez que toda a LAN de Vendas teve seu acesso negado às outras LANs conectadas ao router. Portanto, o melhor lugar para se aplicar a lista seria na interface e0, como uma lista sainte (outbound):

```
Acme(config)#int e0
Acme(config-if)#ip access-group 10 out
```

Isso impedirá completamente que a rede 172.16.40.0 (Vendas) atravesse a interface e0 (Finanças), porém, a LAN de Vendas ainda terá acesso à LAN de Marketing, e à Internet.



Você terá dificuldades ao tentar impedir usuários de conectar-se à um router via Telnet. Isso porque qualquer porta ativa em um router é passível de acesso VTY.

Entretanto, listas de acesso IP padrão podem ser usadas para controlar o acesso Telnet, através da aplicação das mesmas diretamente às linhas VTY.

Para realizar essa operação:

1) Crie uma lista de acesso IP padrão que permita que apenas o host ou os hosts que você deseje possam conectar-se via Telnet ao router;

2) Aplique a lista de acesso criada diretamente às portas VTY, utilizando o comando **`access-class`**, como ilustrado acima.

No exemplo acima, por causa do comando **`deny any`**, implícito no final da lista, a lista de acesso impede que qualquer host tenha acesso ao router via Telnet, exceto o host com endereço IP 172.16.10.3.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

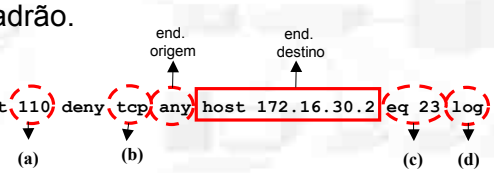
Listas de Acesso

Listas de acesso IP estendidas (IP Extended Access List)

- Listas de acesso IP estendidas permitem que se filtre a rede não apenas através do endereço IP de origem e destino, mas também através do protocolo e número de porta

- Listas de acesso IP estendidas podem ser usadas para permitir que usuários acessem determinada LAN, porém, barra o acesso à serviços específicos. Isso não é possível de se conseguir com listas IP padrão.

- EX: `RouterA(config)#access-list 110 deny tcp any host 172.16.30.2 eq 23 log`



No exemplo acima, eis o que temos:

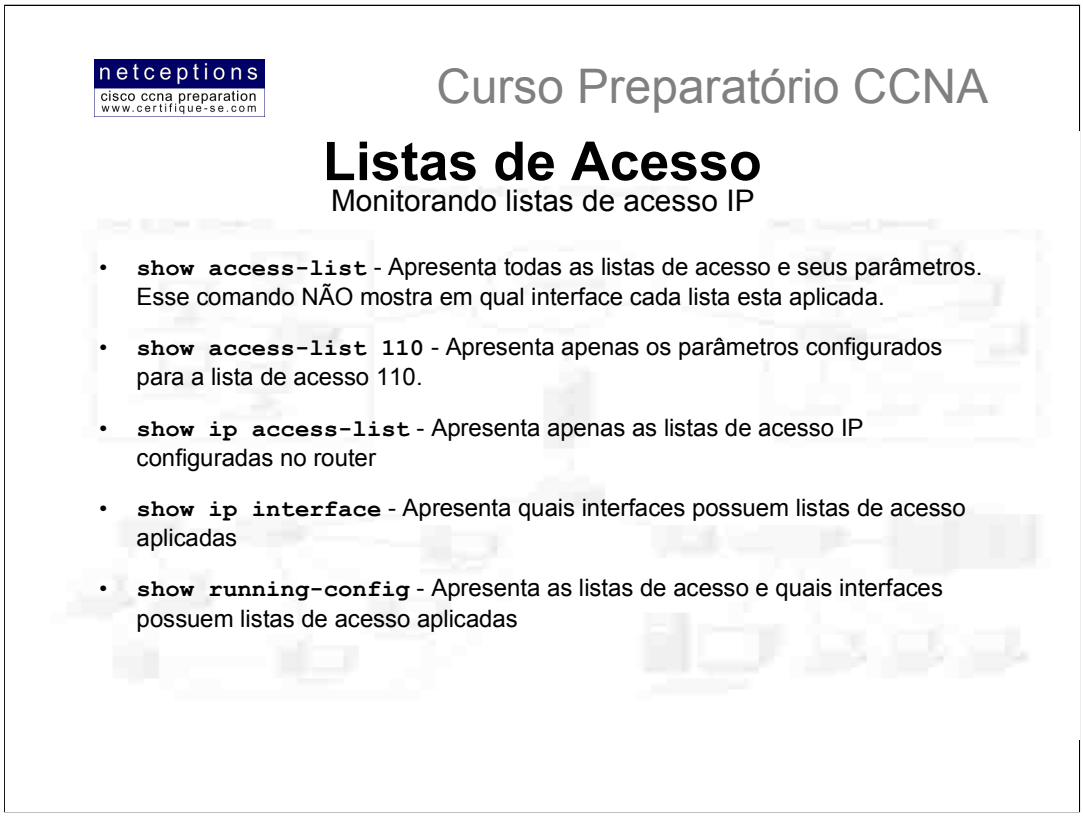
(a) **`110`** - informa o comando **`access-list`** que se trata de uma lista IP estendida (100-199)

(b) **`tcp`** - informa o protocolo que será utilizado como filtro. No caso, utilizamos o protocolo TCP. Lembre-se que, para filtragem através da camada de aplicação, o protocolo escolhido aqui deve permitir que você "suba" no modelo OSI até a camada 7 (Application). Por esse motivo, TCP foi escolhido. Por exemplo, para filtragem da rede através de aplicações como Telnet ou FTP, TCP deve ser utilizado neste campo.

(c) **`eq 23`** - o atributo **`eq`** informa que pacotes serão verificados e comparados à lista apenas se originados na porta TCP especificada (23). No nosso caso, utilizamos a porta **`23`**, que é o número de porta TCP utilizado pela aplicação Telnet. O nome da aplicação (**`telnet`**) também poderia ter sido utilizado, em lugar ao número da porta. Outras opções aqui poderiam ser: eigrp, icmp, ip, udp, entre outras. Para a prova CCNA, TCP - e suas portas - é o mais importante. Memorize que porta 23 = Telnet; 21 = FTP e 80 = www. Essas são as mais importantes e as únicas que o exame CCNA pede.

(d) **`log`** - esse comando é utilizado para geração de um arquivo (log file) que é enviado ao console toda vez que uma tentativa de acesso é efetuada. Esse recurso não seria muito produtivo em um ambiente com tráfego intenso, mas é muito útil para redes de pequeno porte.

Resumindo, a lista acima criada, uma vez aplicada, bloqueia a porta Telnet (23) para o host 172.16.30.2. Caso este host deseje acesso através de alguma outra aplicação, como FTP, por exemplo, lhe será permitido.



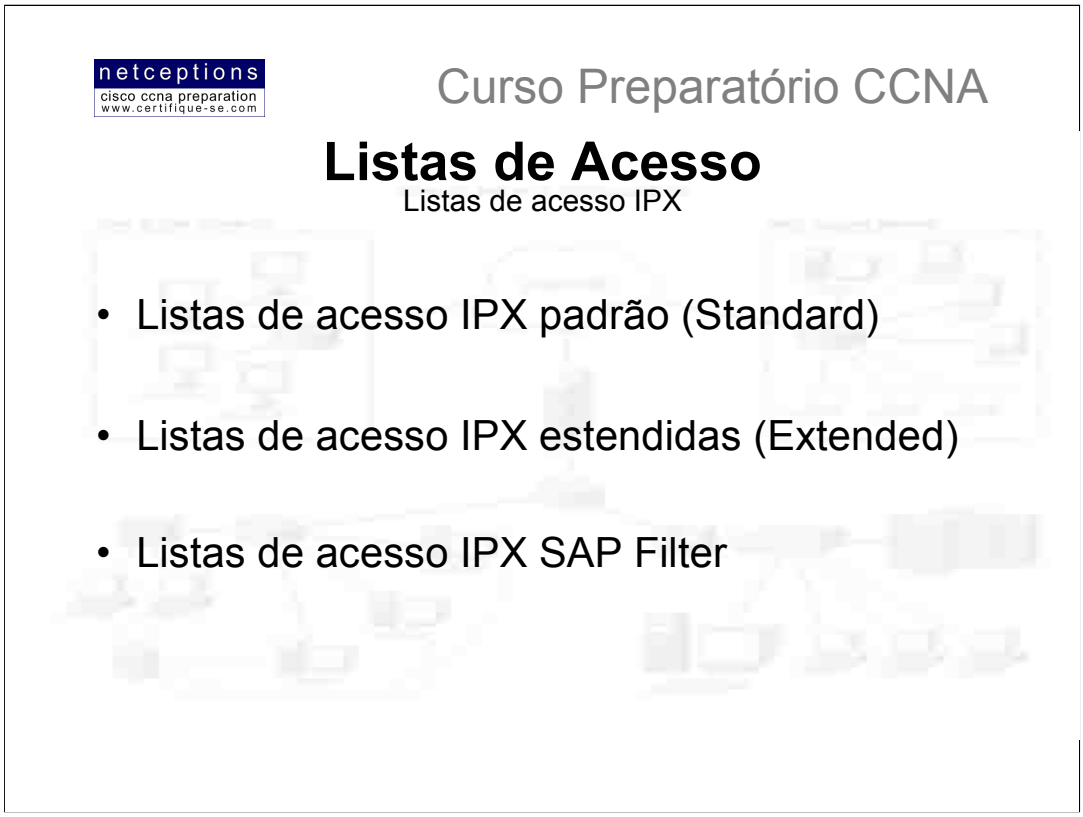
Eis um exemplo um pouco mais complexo de uma lista de acesso IP estendida:

```
Acme#config t
Acme(config)#access-list 110 deny tcp any host 172.16.10.5 eq 21
Acme(config)#access-list 110 deny tcp any host 172.16.10.5 eq 23
Acme(config)#access-list 110 permit ip any any
Acme(config)#int e0
Acme(config-int)#ip access-group 110 out
```

Nesse exemplo, utilizando o diagrama presente na página 6, negamos o acesso aos recursos de FTP (21) e Telnet (23) no servidor 172.16.10.5, presente na LAN Financeira. Todos os outros serviços encontram-se disponíveis para o acesso pelas LANs de Marketing e Vendas.

É importante entender porque as linhas **`deny`** foram configuradas primeiro na lista. O motivo é que, se você configurasse **`permit`** primeiro e **`deny`** depois, a LAN do depto de finanças não seria capaz de se comunicar com nenhuma outra LAN, ou com a Internet, devido ao **`deny`** implícito no final de TODA lista de acesso. A configuração apresentada é o modo como deve ser feito. Qualquer outra maneira seria extremamente complicada e menos funcional.

Uma vez que as 3 outras LANs em nosso router precisam ser capazes de acessar a LAN do depto Financeiro, a lista deve ser aplicada como sainte (**`out`**) na interface **e0**. Se a lista, entretanto, tivesse sido criada com o intuito de bloquear, por exemplo, o acesso ao depto de Vendas somente, então, deveríamos aplicá-la próximo à origem, ou seja, na interface **e2.**



Listas de acesso IPX são configuradas da mesma forma que listas IP: utiliza-se o comando access-list para criar as listas e o comando access-group para aplicá-las. Os seguintes tipos de lista IPX serão discutidos:

IPX padrão (standard) - Uma lista IPX padrão filtra à partir dos endereços IPX de origem e de destino (similar às listas de acesso IP padrão). São definidas pelos valores compreendidos entre o intervalo 800-899 (incluindo os mesmos).

IPX estendida (extended) - Este tipo de lista IPX faz a filtragem nos endereços IPX de origem e de destino, no campo protocol do cabeçalho de camada de rede e no número do socket no cabeçalho de camada de transporte. São definidas pelos valores compreendidos entre 900-999 (incluindo os mesmos).

IPX SAP Filter - Tratam-se de filtros usados no controle do tráfego SAP em LANs e WANs. São definidas por valores compreendidos entre 1000-1099 (incluindo os mesmos). Administradores de rede podem configurar listas de acesso IPX para controlar o volume de tráfego IPX, incluindo IPX SAPs através de links WAN.

Listas de acesso IPX padrão funcionam de maneira análoga às listas de acesso IP padrão. Eis a sintaxe do comando de configuração de uma lista de acesso IPX padrão:

```
access-list [800-899] [deny or permit] [source_address destination_address]
```

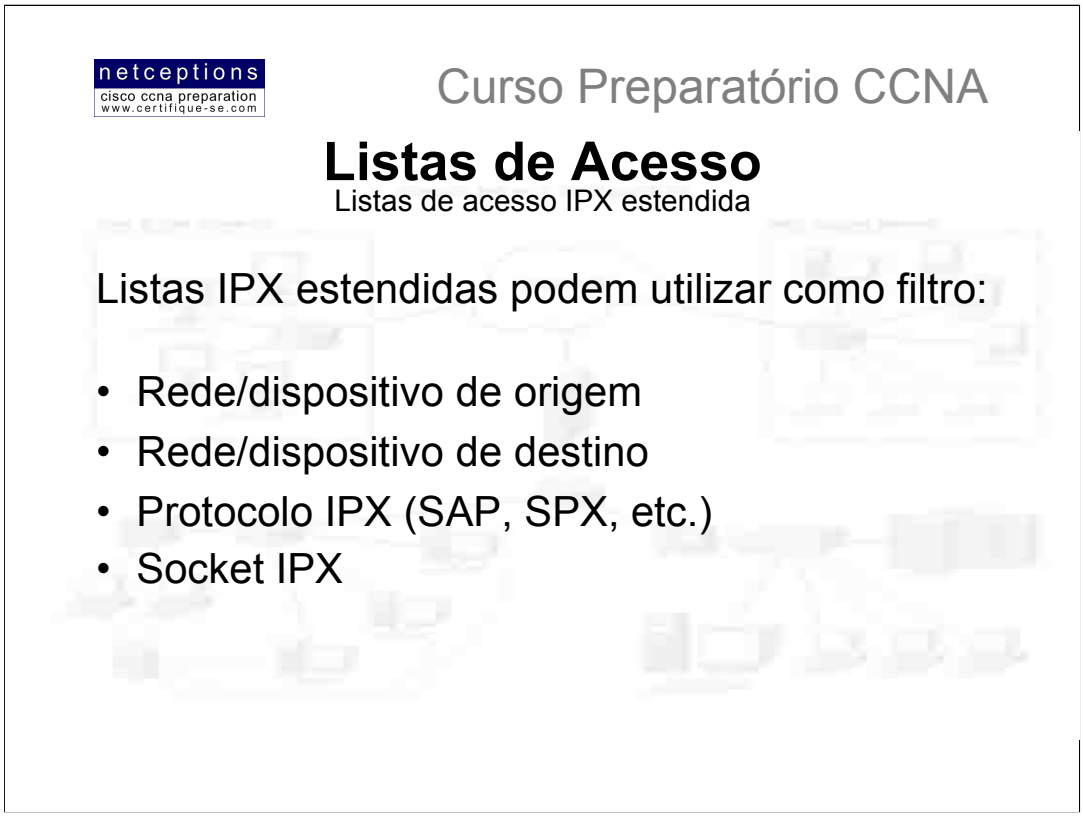
Wildcards podem ser utilizados para os endereços IPX de origem e destino, entretanto, o wildcard é -1, o que significa igual à qualquer host ou rede **(-1 = any)**. A figura acima ilustra um exemplo de uma rede IPX e como são configuradas listas IPX padrão.

A seguinte configuração é utilizada na rede proposta acima: a interface e0 encontra-se na rede 40, a interface e1 na rede 10, a interface e2 na rede 20 e a interface e3 na rede 30. A lista de acesso abaixo é criada e aplicada conforme ilustrado:

```
Router(config)#access-list 810 permit 20 40
Router(config)#int e0
Router(config-if)#ipx access-group 810 out
```

Essa lista IPX permite que pacotes gerados pela rede 20 atravesse a interface e0 até a rede 40. Vamos analisar com mais cuidado o que essa lista implica: primeiramente, qualquer dispositivo na rede 20 que atravesse a interface e2 pode se comunicar com o servidor na rede 40, conectado à interface e0. Eis o que mais essa lista implica, em apenas uma linha:

- Hosts pertencentes à rede 10 não podem se comunicar com o servidor na rede 40;
- Hosts pertencentes à rede 40 podem comunicar-se com a rede 10, porém, os pacotes enviados não podem retornar;
- Hosts pertencentes à rede 30 não se comunicam com o servidor na rede 40;
- Hosts pertencentes à rede 40 podem comunicar-se com hosts na rede 30, porém, os pacotes enviados não podem retornar;
- Hosts pertencentes à rede 20 podem se comunicar com qualquer dispositivo da rede.

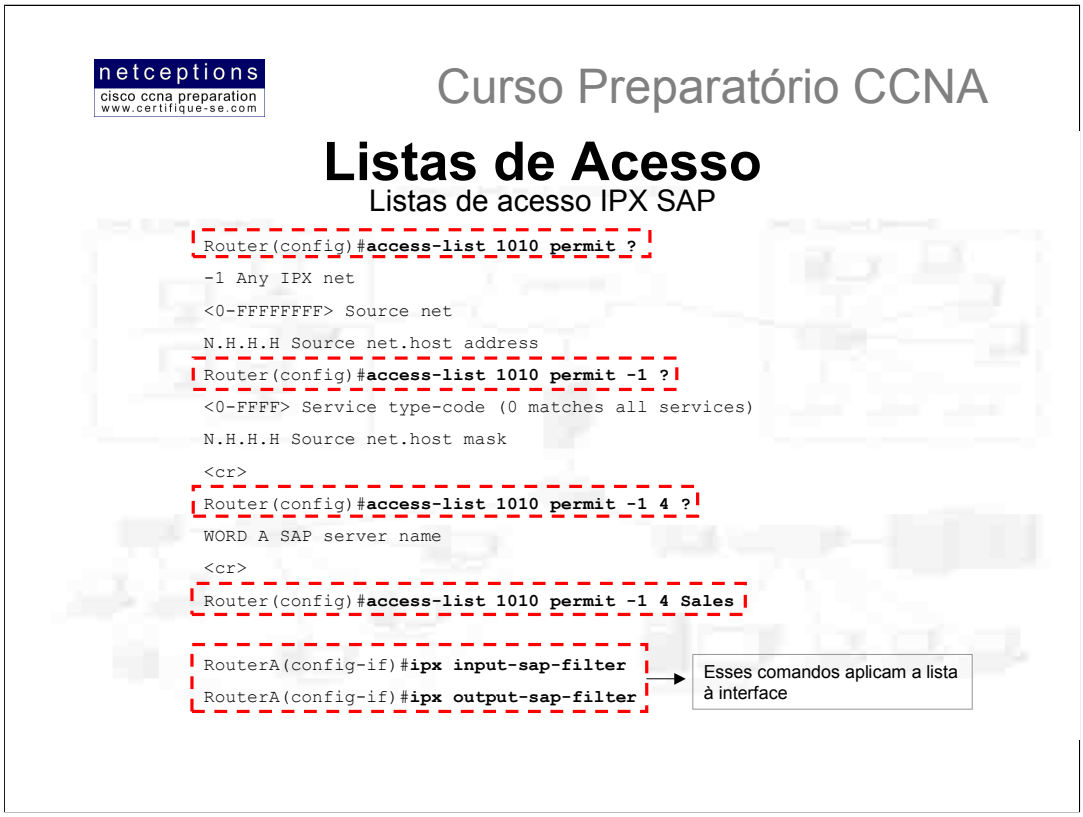


Listas IPX estendidas são definidas pelo intervalo 900-999 e são configuradas de modo similar às listas IPX padrão, com a adição dos parâmetros do protocolo e socket. Eis a sintaxe de uma lista IPX estendida:

```
access-list {number} {permit/deny} {protocol} {source}
{socket} {destination} {socket}
```

Mais uma vez, a escolha da aplicação de uma lista estendida em lugar à uma padrão deve-se ao fato de se poder filtrar a rede baseada em protocolos e sockets, em adição aos endereços IPX de origem e destino.

OBS: Listas de acesso IPX estendidas não costumam cair no exame CCNA. Concentre-se em listas IP padrão e estendidas e listas IPX padrão e SAP.



Filtros IPX SAP são implementados da mesma forma dos outros filtros discutidos anteriormente. Eles possuem um importante papel no controle do tráfego IPX SAP. Isso é importante pois, se você puder controlar o SAP, você poderá controlar o acesso à dispositivos IPX. Filtros IPX SAP são definidos entre o intervalo 1000-1099. Esses filtros devem ser aplicados o mais próximo possível à origem dos broadcasts (propagações SAP). Isso evitará que tráfego SAP indesejado atravesse a rede. Existem 2 tipos de filtros IPX SAP:

IPX input SAP filter - Usado para barrar o acesso de certos pacotes SAP ao router e atualizar sua tabela SAP;

IPX output SAP filter - Usado para impedir que certas atualizações SAP sejam transmitidas pelo router em intervalos regulares de 60 segundos.

Acima ilustramos um exemplo completo de uma lista IPX SAP, que permite serviços de tipo 4 (file services) de um servidor Netware chamado Sales. Repare no **-1** usado. O **-1** é um wildcard com o mesmo significado que **any** nas listas IP (0.0.0.0). Significa qualquer rede e qualquer host.

O comando **input-sap-filter** é usado para impedir que informações SAP sejam adicionadas à tabela SAP do router. Já o comando **output-sap-filter** foi utilizado para impedir que informações SAP sejam propagadas pelo router em questão.

Verificando listas de acesso IPX

Para verificar as listas de acesso IPX implementadas em um router, use o comando **show ipx interface** ou o comando **show ipx access-list.** Na saída apresentada, você notará linhas como:

```
Router#sh ipx access-list
IPX access list 810
permit FFFFFFFF 30
```

Os **Fs** são hexadecimais e são equivalente à 1s em notação binária. Significam **permit any**. Uma vez que foi utilizado **-1** , eles aparecem representados por **Fs**, na saída.

Resumo Aula 7 - módulo I - Listas de Acesso:

Nesse módulo analisamos o funcionamento das listas de acesso IP e IPX, como criá-las, para que criá-las, suas funções e como aplicá-las às interfaces de um router.

Lembre-se de focar seus estudos no seguinte:

Intervalos que definem cada tipo de lista (**MUITO IMPORTANTE!!!**):

IP Standard: 100-199

IP Extended: 200-299

IPX Standard: 800-899

IPX Extended: 900-999

IPX SAP: 1000-1099

Saiba as portas de aplicações mais comuns, como FTP (21), Telnet (23) e www (80)

Não estude demasiado listas IPX estendidas. Concentre-se em listas IP padrão e estendidas e listas IPX padrão e SAP.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Listas de Acesso

Resumo dos comandos analisados

Comando	Descrição
0.0.0.0 255.255.255.255	Wildcard, o mesmo que o comando any
access-class	Aplica uma lista de acesso IP padrão à uma linha VTY
Access-list	Cria uma lista de acesso
Any	Especifica qualquer host e qualquer rede. O mesmo que 0.0.0.0 255.255.255.255
Host	Especifica o endereço de um único host
ip access-group	Aplica uma lista de acesso IP à uma interface
ipx access-group	Aplica uma lista de acesso IPX à uma interface
ipx input-sap-filter	Aplica um filtro IPX SAP entrante à uma interface
ipx output-sap-filter	Aplica um filtro IPX SAP sainte à uma interface
show access-list	Apresenta todas as listas de acesso configuradas no router
show access-list 110	Apresenta apenas os parâmetros configurados para a lista 110
show ip access-list	Apresenta apenas listas de acesso IP
show ip interface	Apresenta quais interfaces possuem listas de acesso IP aplicadas
show ipx access-list	Apresenta apenas listas de acesso IPX
show ipx interface	Apresenta quais interfaces possuem listas de acesso IPX aplicadas

O sistema Cisco IOS é capaz de suportar diversos protocolos WAN (Wide Area Protocol) diferentes, que podem ajudá-lo à estender suas LANs para outras LANs, remotamente localizadas. A inter-conexão de diversos sites dentro de uma corporação para troca de informações é imperativo na nova ordem econômica.

Entretanto, pense nos custos que isso traria se sua empresa precisasse implantar seus próprios cabos ou conexões para a inter-conexão de seus sites. Provedores de serviço permitem que conexões já instaladas pelos mesmos sejam “arrendadas” (leased) ou compartilhadas, reduzindo enormemente os custos e o tempo de implantação.

É importante o entendimento dos diferentes tipos de protocolos e serviços WAN suportados pela Cisco. Não cobriremos aqui todos os protocolos suportados, apenas os abrangidos pelo exame CCNA como: HDLC, PPP, Frame Relay e ISDN. Outros exemplos populares seriam: ATM e X.25.

Termos WAN

Para o entendimento das tecnologias WAN, é necessário o entendimento dos diferentes termos utilizados nesse tópico, assim como tipos de conexão que podem ser utilizados na inter-conexão de redes. Eis os termos mais comuns:

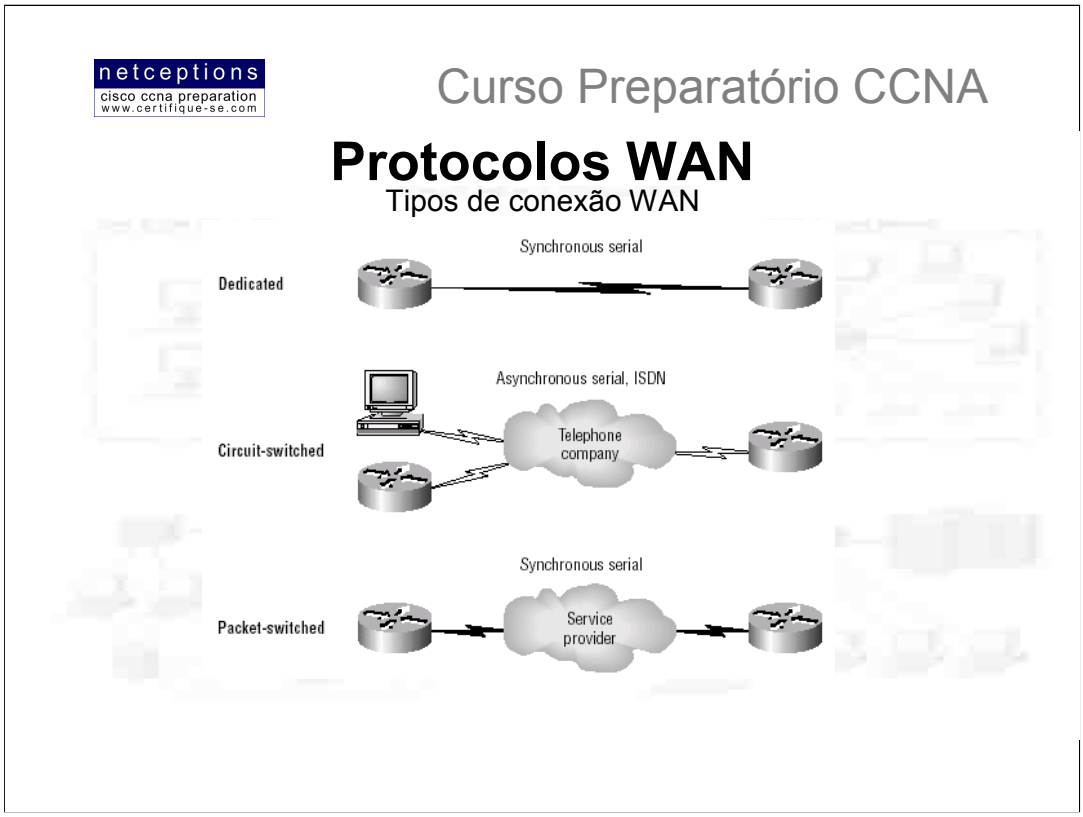
CPE (Customer Premisses Equipment) - Definem os equipamentos pertencentes e ao assinante do serviço, e localizados em suas premissas.

Demarcation (demarc) - O último ponto sob a responsabilidade do provedor de serviço. Comumente uma conexão RJ-45 localizada próxima ao CPE. O CPE nesse ponto deve ser um CSU/DSU ou uma interface ISDN que conecta diretamente ao demarc.

Local loop - Conecta o demarc à estação central da operadora de serviço comutado (switching office) mais próxima.

Central Office (CO) - Conecta o assinante à rede comutada do provedor (provider’s switching network). O CO também é referido, às vezes, por POP (Point of Presence)

Toll Network - Links de transporte (trunk lines) dentro da rede do provedor. Trata-se de uma coleção de estruturas e switches.



A figura acima ilustra os diferentes tipos de tipos de conexão WAN que podem ser usados na inter-conexão de LANs, através de uma rede DCE.

A lista à seguir explica os tipos de conexão WAN:

Leased Lines - Normalmente conhecidas como conexões ponto-à-ponto ou conexões dedicadas. Trata-se de um caminho WAN pré-estabelecido do CPE do site local, através de um switch DCE, até o CPE do site remoto, permitindo a comunicação ininterrupta entre redes DTE, sem que procedimentos de ativação ou autenticação sejam necessários antes da transmissão de dados. São utilizadas linhas de transmissão seriais Síncronas de até 45Mbps.

Circuit Switching - Utiliza um procedimento de estabelecimento de link análogo à uma chamada telefônica. Nenhum dado pode ser transmitido antes de uma conexão ponto-à-ponto ser estabelecida. Esse tipo de conexão é utilizado por modems comuns e ISDN. Utilizado em transmissões que requeiram baixa largura-de-banda.

Packet Switching - Método de comutação WAN que permite o compartilhamento de largura-de-banda com outros usuários, resultando em grande redução de custos. Imagine uma rede packet switched como uma linha telefônica comunitária. Uma vez que você não transmita dados constantemente mas sim o faça esporadicamente, esse método pode reduzir seus custos drasticamente. Entretanto, se você transfere dados de forma constante, a melhor solução é o arrendamento de uma linha (leased line). Frame Relay, X.25 e ATM são exemplos de tecnologias que utilizam o método packet switching. As velocidades de transmissão variam de 56Kbps à 2Mbps.

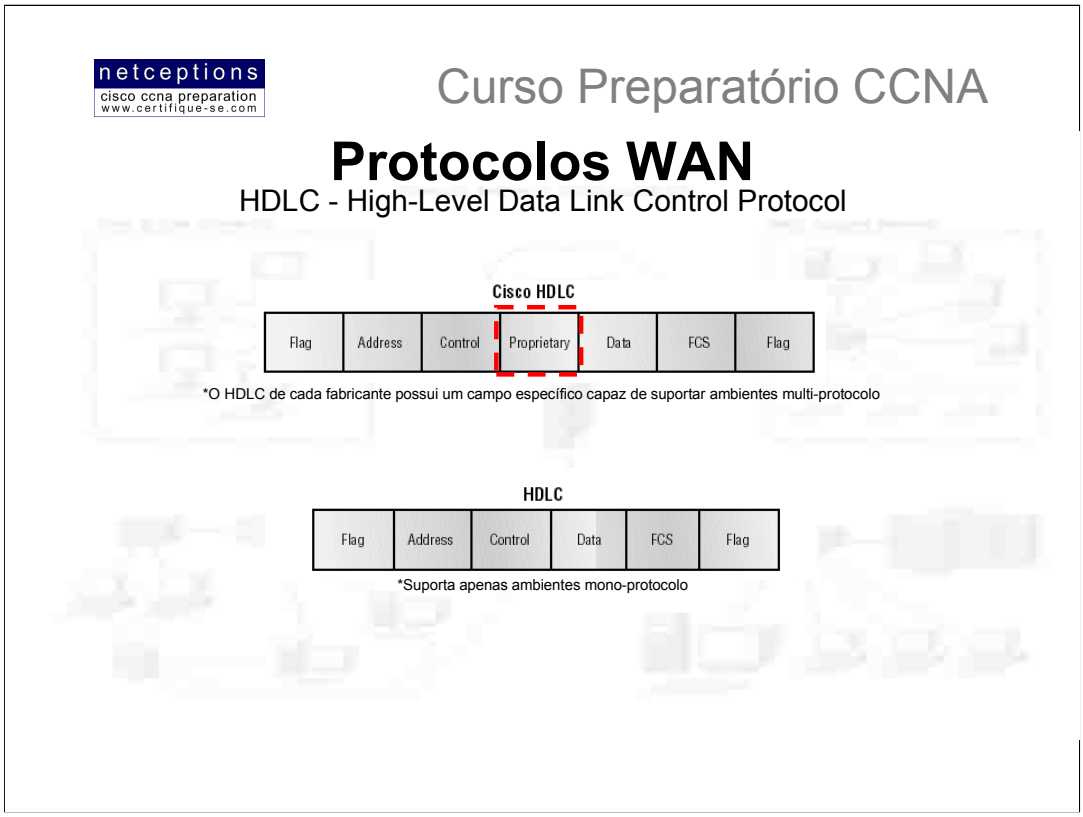
Frame Relay - Tecnologia de comutação de pacotes (packet-switched) que surgiu nos anos 90. Frame Relay é definido nas camadas física e de enlace (camadas 2 e 1), e é um protocolo de alta-performance. Frame Relay assume que as estruturas utilizadas hoje são menos sujeitas à falhas do que quando o protocolo X.25 (do qual Frame Relay é derivado) foi criado. Por esse motivo, o overhead foi reduzido, aumentando sua performance. Frame Relay é mais custo-eficiente que conexões ponto-à-ponto e suas velocidades variam de 64Kbps à 1.544 Kbps. Frame Relay disponibiliza recursos que possibilitam a alocação dinâmica de banda, assim como mecanismos para controle de congestionamento de dados.

ISDN - Trata-se de uma série de serviços digitais que tornam possível a transmissão de voz e dados através de uma linha telefônica ordinária. ISDN oferece uma solução de baixo custo para usuários remotos que necessitam de uma conexão relativamente rápida, se comparada à velocidade atingida via modems comuns. ISDN é também uma boa escolha para o estabelecimento de links de backup para outros tipos de conexões, como Frame Relay ou T-1 (conexão dedicada - leased line).

LAPB - Esse protocolo orientado-à-conexão foi criado para ser utilizado na camada de enlace, juntamente com o protocolo X.25. LAPB possui um overhead volumoso devido aos recursos de windowing e time-out que utiliza. Esse protocolo pode ser utilizado em lugar ao HDLC se os links em questão forem extremamente sujeitos à falhas (error-prone). Como isso não é um problema real nos dias de hoje, LAPB não é muito utilizado.

HDLC - Protocolo orientado à conexão definido na camada de enlace. Possui um overhead muito pequeno, se comparado ao protocolo LAPB. HDLC não foi criado com a intenção de encapsular múltiplos protocolos de camada de rede através de um mesmo link. O header HDLC não contém informações sobre o tipo de protocolo sendo transportado. Por esse motivo, cada fabricante que utiliza HDLC possui sua própria maneira de identificar o protocolo de camada de rede, o que significa que o HDLC utilizado por cada fabricante é proprietário (exclusivo) aos equipamentos que fabricam.

PPP - Protocolo padrão da indústria. Uma vez que muitas versões do HDLC são proprietárias, PPP pode ser utilizado para criação de conexões ponto-à-ponto entre equipamentos de diferentes fabricantes. PPP utiliza o campo Network Control Protocol para identificação do protocolo de camada de rede. Permite autenticação e conexões multilink, e pode ser utilizado em links síncronos e assíncronos.



HDLC é um popular protocolo de camada de enlace, derivado do protocolo SDLC, padrão ISO, com orientação bit-à-bit. Ele especifica um método de encapsulamento de dados em links seriais síncronos. HDLC é um protocolo ponto-à-ponto utilizado em leased lines. Não é utilizado qualquer método de autenticação com o protocolo HDLC.

Em protocolos com orientação byte-à-byte, informações de controle são codificadas usando-se bytes inteiros. Já em protocolos com orientação bit-à-bit (como é o caso do HDLC, SDLC, TCP, IP, entre outros), um único bit pode representar uma informação de controle.

HDLC é o método de encapsulamento padrão utilizado em routers Cisco para conexões através de links seriais síncronos. O HDLC utilizado pela Cisco, como comentamos, é proprietário ao fabricante, ou seja, apenas equipamentos Cisco são capazes de compreendê-lo.

Conforme a ilustração acima, a razão pela qual cada fabricante possui um método de encapsulamento HDLC único é que cada fabricante adota uma metodologia diferente para fazer com que o protocolo HDLC se comunique com protocolos de camada de rede. Caso os fabricantes não implementassem uma solução para HDLC se comunicar com os diferentes protocolos definidos na camada de rede, HDLC seria capaz, então, de transportar apenas 1 protocolo. Esse cabeçalho proprietário é inserido no campo “data” do frame HDLC.

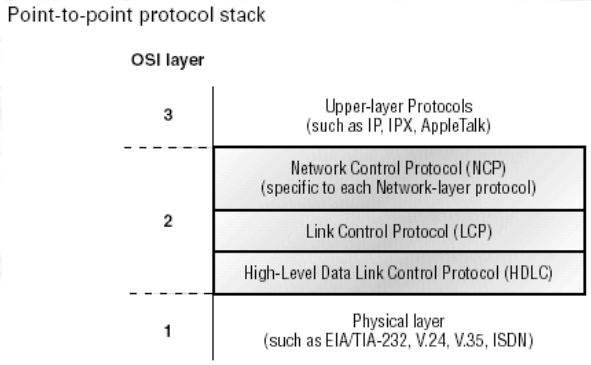
Caso você deseje conectar um router Cisco à um router de outro fabricante, o método padrão de encapsulamento HDLC não poderia ser utilizado. Nesse caso, uma solução padrão alternativa, como o protocolo PPP, que é padronizado pela ISO, deveria ser utilizada.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Protocolos WAN

PPP - Point-to-Point Protocol



PPP é um protocolo de camada de enlace que pode ser usado através de links seriais síncronos (ex. ISDN) e assíncronos (dial-up) que utilizam LCP (Link Control Protocol) para estabelecer e gerenciar conexões na camada de enlace.

A função básica do PPP é transportar pacotes de camada de rede através de um link ponto-à-ponto de camada de enlace. A figura acima ilustra o conjunto (stack) de protocolos PPP comparado ao modelo OSI.

PPP é constituído de 4 componentes principais:

EIA/TIA-232-C - Padrão internacional de camada física para comunicação serial

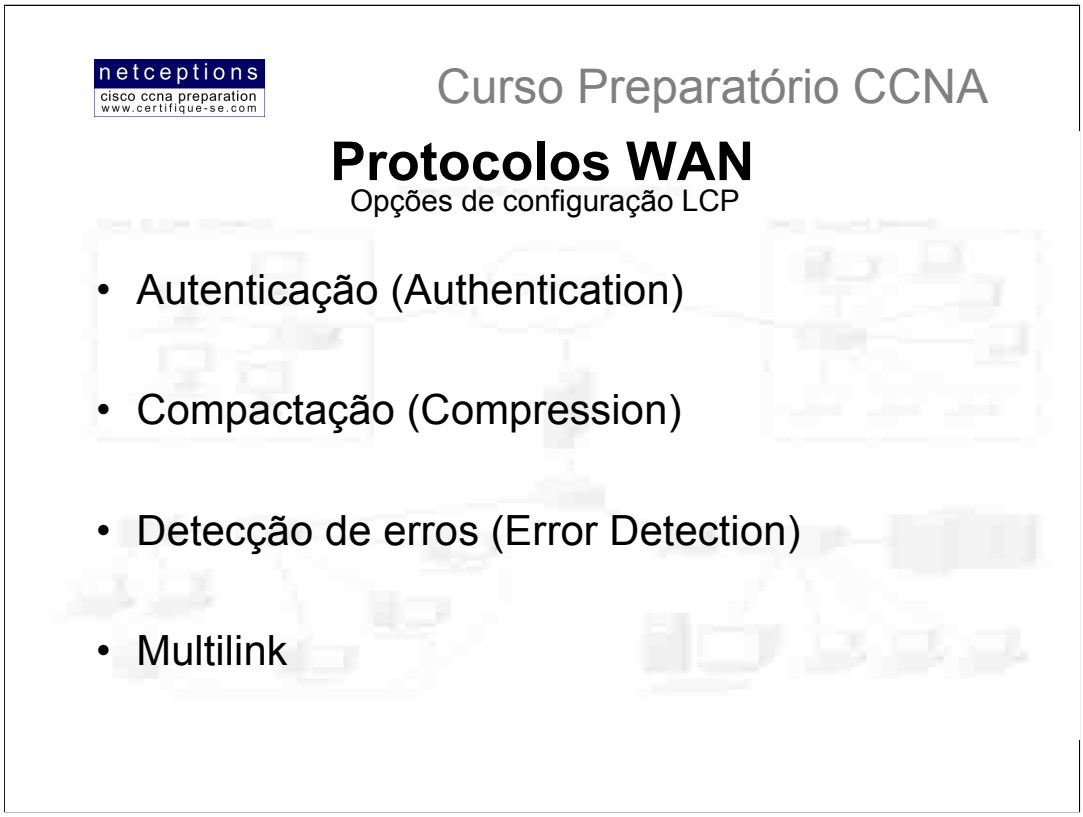
HDLC - Método de encapsulamento de datagramas através de links seriais

LCP - Protocolo utilizado no estabelecimento, configuração, manutenção, e terminação de conexões ponto-à-ponto.

NCP - Protocolo responsável pelo estabelecimento e configuração de diferentes protocolos de camada de rede. O protocolo PPP foi desenhado para permitir o uso simultâneo de múltiplos protocolos de camada de rede. Os protocolos usados aqui são específicos para cada protocolo de camada de rede. Alguns exemplos de protocolos usados: IPCP (IP Control Protocol) e IPXCP (IPX Control Protocol).

É importante entender que o conjunto de protocolos PPP é definido nas camadas de enlace e física, somente. NCP é utilizado para permitir a comunicação de múltiplos protocolos de camada de rede através do encapsulamento desses protocolos através de um link PPP.

Você DEVE conhecer os protocolos PPP!



O protocolo LCP (Link Control Protocol) oferece ao encapsulamento PPP diferentes opções, incluindo as seguintes:

Autenticação - Essa opção demanda ao lado que está chamando o envio informações para identificação do usuário. Os dois métodos que iremos discutir são PAP e CHAP.

Compactação - Usado para maximizar o fluxo de dados (throughput) entre conexões PPP. PPP descompacta o frame de dados na ponta receptora.

Detecção de Erros - PPP utiliza os recursos Quality e Magic Number para garantir o estabelecimento de uma conexão e fluxo de dados confiável.

Multilink - À partir da versão 11.1 do sistema IOS, multilink é suportado em links PPP nos routers Cisco. Isso divide a carga PPP para 2 ou mais circuitos paralelos, chamados “bundle”.

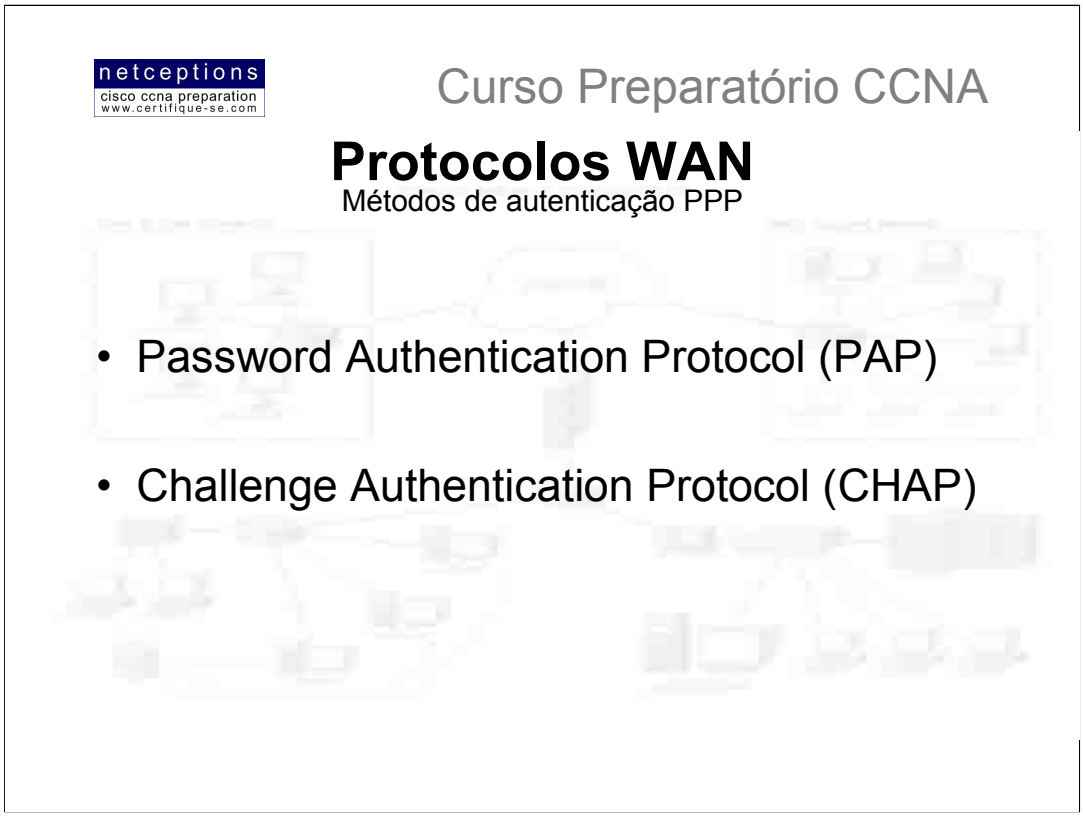
Estabelecimento de uma sessão PPP

PPP pode ser utilizado com autenticação. Isso significa que a comunicação entre 2 routers deve prover informações que identifiquem o link como válido para comunicação. Quando conexões PPP são iniciadas, os links passam por 3 fases antes do estabelecimento da sessão:

Link-establishment phase - Pacotes LCP são enviados por cada dispositivo PPP para configurar e testar o link. Os pacotes LCP contém um campo chamado “Configuration Option” que permite à cada dispositivo identificar o tamanho da compactação de dados e autenticação. Se não houver um campo “Configuration Option” presente, as configurações padrão são adotadas.

Authentication Phase - Caso configurados, CHAP ou PAP podem ser utilizados para autenticar um link. O processo de autenticação acontece antes das informações sobre protocolos de camada de rede serem processadas.

Network-Layer Protocol Phase - PPP utiliza NCP (Network Control Protocol) para permitir que múltiplos protocolos de camada de rede sejam encapsulados e enviados através de um link PPP.

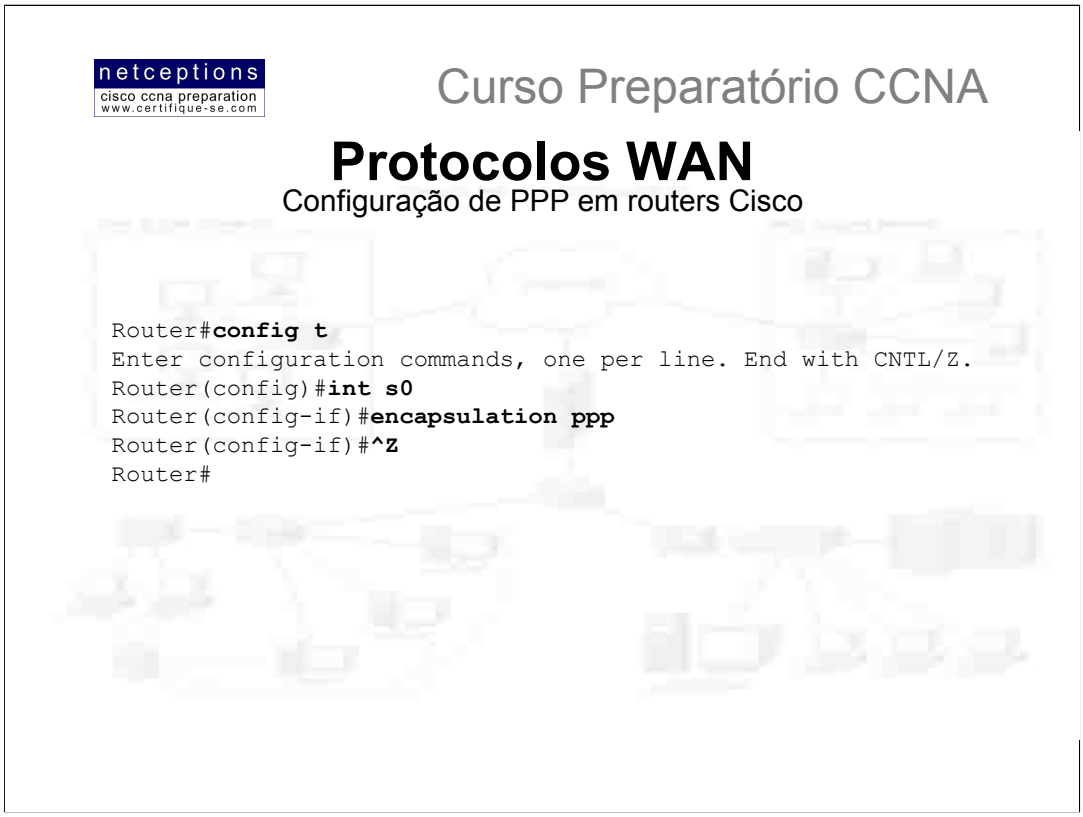


Existem 2 métodos de autenticação que podem ser utilizados em links PPP:

Password Authentication Protocol (PAP) - PAP é o menos seguro dos 2 métodos. Senhas (passwords) são enviadas como texto puro, sem que esquemas de criptografia sejam utilizados. Além disso, PAP entra em ação apenas depois do estabelecimento inicial do link. Logo que um link PPP é estabelecido o dispositivo remoto envia de volta ao router origem dados contendo o nome do usuário (username) e senha (password), até que os mesmos sejam aceitos. Simplesmente isso.

Challenge Authentication Protocol (CHAP) - CHAP é ativado logo que um link PPP é estabelecido, e periodicamente, na checagem do mesmo, para certificar-se que o router ainda encontra-se em comunicação com o mesmo dispositivo.

Após PPP ter concluído a fase inicial, o router local envia uma requisição challenge (challenge request) ao dispositivo remoto. Esse dispositivo envia ao router um valor calculado utilizando uma função especial de apenas um sentido (one-way) chamada MD5. O router efetua, então, a comparação desse valor com o gerado por ele. Caso existam divergências, a conexão é imediatamente encerrada.



O processo de configuração PPP em uma interface é bastante simples. Para configurar PPP, basta seguir os passos ilustrados acima. O encapsulamento PPP deverá estar configurado em ambas as interfaces conectadas através de um link serial para que PPP funcione. Existem algumas outras configurações adicionais, que podem ser vistas ao se utilizar o comando **help**.

Configurando autenticação PPP

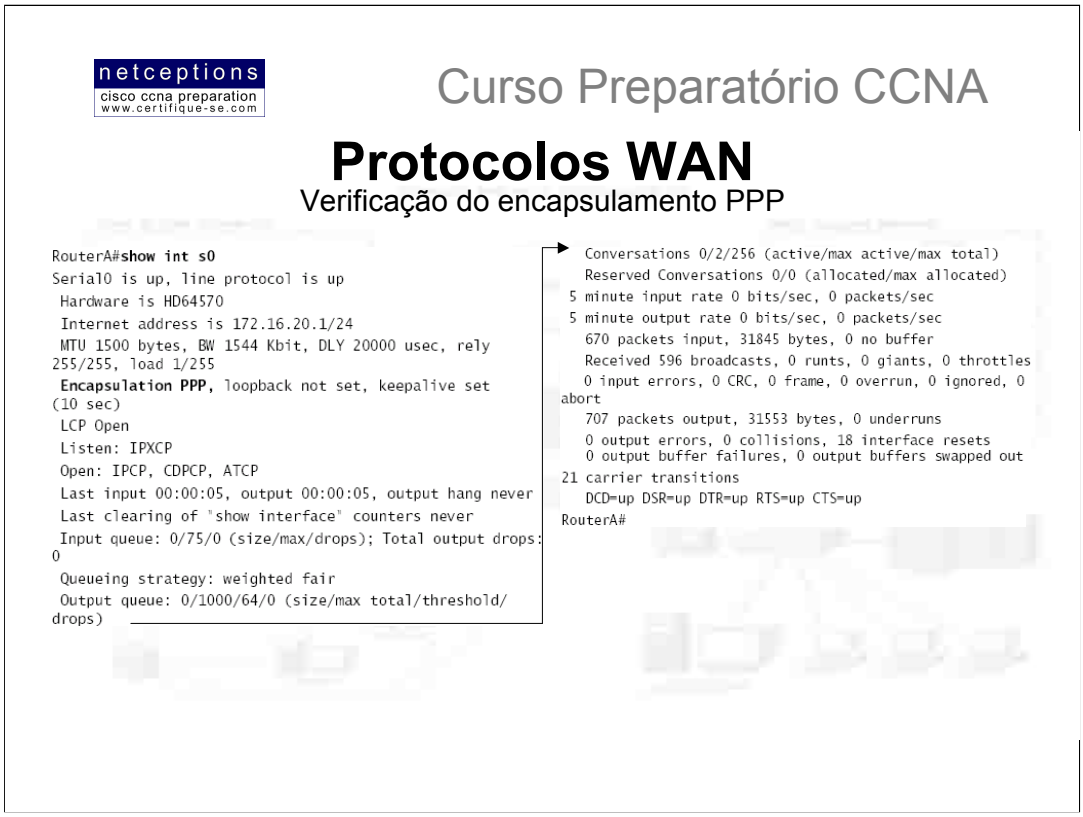
Após configurar sua interface serial para suportar encapsulamento PPP, você pode então configurar o método de autenticação à ser utilizado por PPP entre 2 routers. Primeiro você deve configurar um hostname para o router, caso isso já não tenha sido feito. Em seguida, defina um username e senha para o router localizado remotamente, que irá conectar-se ao seu router:

```
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# hostname RouterA
RouterA(config)#username todd password cisco
```

Ao utilizar o comando **hostname**, lembre-se que o username é o hostname do router localizado remotamente, que irá conectar-se ao seu router. No caso ilustrado, todd é o hostname do router remoto. A senha definida para ambos os routers também deve ser a mesma. Trata-se de uma senha em formato texto, que pode ser visualizada ao se digitar o comando **sh run**. A senha pode ser criptografada com a utilização do comando **service password-config**, antes da definição do username e senha. Um username e uma senha devem ser configurados para cada dispositivo remoto à ser conectado. Os routers remotos também devem ser configurados com senhas e usernames. Uma vez que o hostname, usernames e senhas tenham sido configurados, escolha o método de autenticação à ser utilizado - CHAP ou PAP:

```
RouterA#config t
Enter configuration commands, one per line. End with CNTL/Z.
RouterA(config)#int s0
RouterA(config-if)#ppp authentication chap
RouterA(config-if)#ppp authentication pap
RouterA(config-if)#^Z
RouterA#
```

Caso ambos os métodos sejam configurados, como ilustrado no exemplo acima, então apenas o primeiro método será utilizado durante a “negociação” do link. Caso o primeiro método venha a falhar, o segundo método será, então, utilizado.



Uma vez que o encapsulamento PPP esteja devidamente configurado, utilize o comando **`sh int`** para verificar se PPP encontra-se, de fato, ativado.

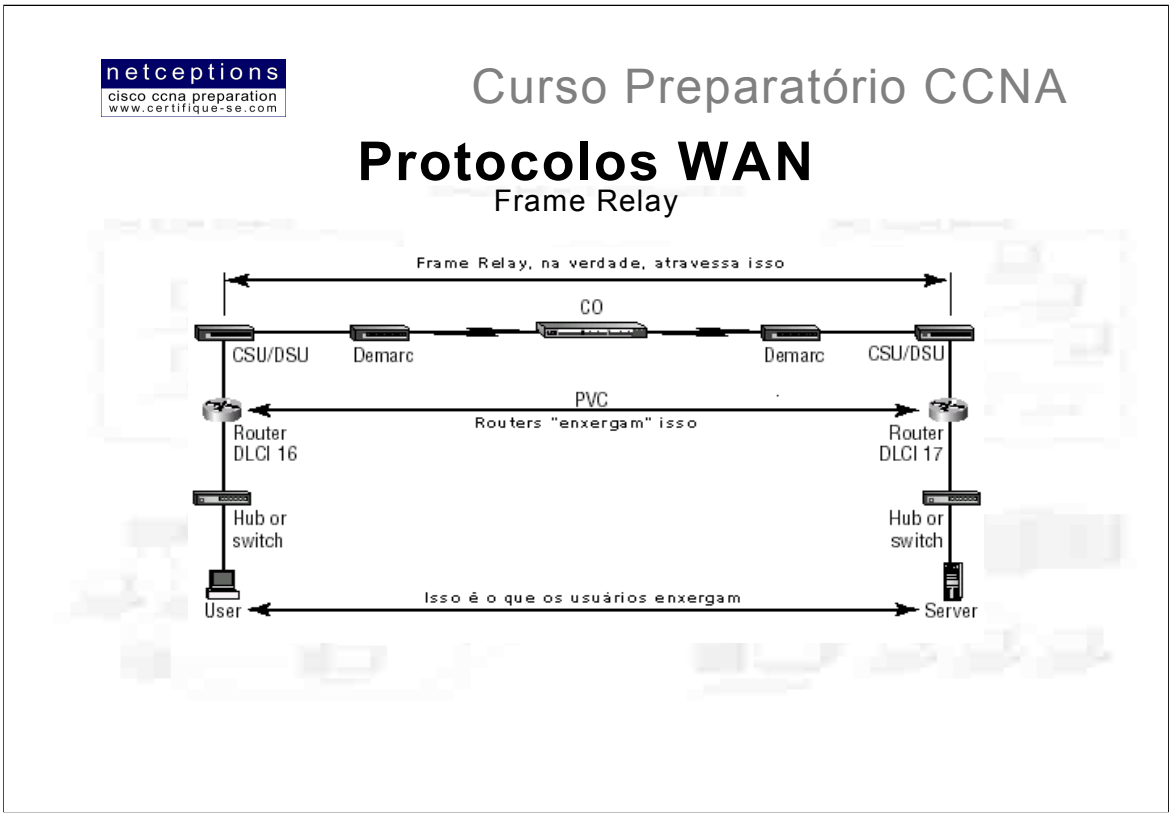
Note que a quinta linha lista encapsulamento PPP (**`Encapsulation PPP`**, `loopback not set, keepalive set`).

A sexta linha indica que LCP está aberto (`LCP Open`). Lembre-se que a função do LCP é estabelecer e manter conexões.

A oitava linha nos mostra que IPCP, CDPCP e ATCP encontram-se abertos (`Open: IPCP, CDPCP, ATCP`). Isso indica que os protocolos IP, CDP e AppleTalk são suportados pelo NCP.

A sétima linha reporta que IPXCP está sendo monitorado (`Listen: IPXCP`)

A configuração de autenticação PPP também pode ser realizada através do comando **`debug ppp authentication`**.



O método de encapsulamento de alta-performance conhecido como Frame-Relay é definido nas camadas física e de enlace do modelo OSI. Frame Relay foi originalmente idealizado e desenvolvido para ser usado em interfaces ISDN. Atualmente, Frame Relay suporta uma grande variedade de interfaces. O Frame Relay adotado pela Cisco suporta os seguintes protocolos: IP, DECnet, AppleTalk, XNS, IPX, CLNS, ISO, Banyan Vines, e Transparent Bridging.

Frame Relay provê uma interface de comunicação entre dispositivos DTE e DCE. Como já estudamos, DTEs englobam terminais, PCs, routers e bridges - equipamentos localizados no lado cliente. DCE geralmente consiste de equipamentos de propriedade da operadora (carrier).

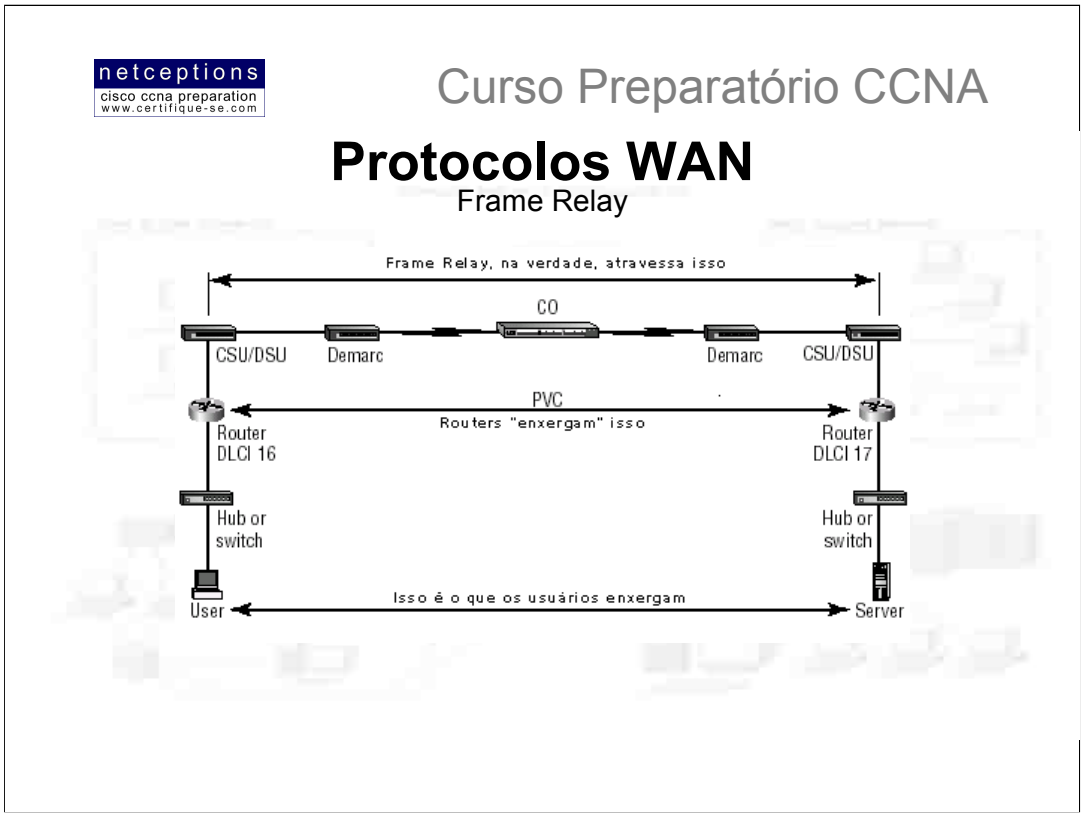
Frame Relay é mais eficiente que X.25, pois assume uma infra-estrutura menos sujeita à erros. Isso possibilita a redução do overhead utilizado.

Frame Relay provê comunicação orientada-à-conexão, na camada de enlace, através do estabelecimento de circuitos virtuais (Permanent Virtual Circuits - PVCs). Esses circuitos virtuais são conexões lógicas criadas entre 2 dispositivos DTE através de uma rede “packet-switched”. Essas conexões são identificadas por um DLCI (Data Link Connection Identifier). Frame Relay pode usar circuitos virtuais permanentes (PVCs) ou comutados (SVCs - Switched Virtual Connections), porém, grande maioria das redes Frame Relay existentes utilizam apenas PVCs. Esse tipo de circuito virtual estabelece o caminho completo até o destino antes de iniciar a transmissão de qualquer informação.

Para entender a terminologia utilizada é necessário, antes, que se entenda como Frame Relay funciona. A figura acima contém vários termos utilizados na descrição das diferentes partes de uma rede Frame Relay.

A idéia básica por trás do Frame Relay é possibilitar a comunicação de usuários entre dois dispositivos DTE, através de dispositivos DCE. Para os usuários, a comunicação ocorre de forma transparente.

A figura acima ilustra tudo o que deve ocorrer para que 2 dispositivos DTE possam se comunicar. À seguir, detalharemos o processo passo à passo.



1) O dispositivo de rede do usuário envia um frame através da rede local. O endereço de hardware (MAC) do router encontrar-se-á no cabeçalho do frame enviado.

2) O router captura o frame, extrai o pacote e descarta o frame. Ele, então, analisa o endereço IP de destino contido no pacote e analisa se a rota até o referido endereço é conhecida. Através de uma checagem na tabela de roteamento.

3) O router, então, encaminha o pacote pela interface que, à princípio, pode alcançar a rede remota (se a rota até a rede remota não estiver na tabela de roteamento, o pacote será descartado). Uma vez que essa interface será uma interface serial com encapsulamento Frame Relay, o router irá inserir o pacote na rede Frame Relay encapsulado em um frame Frame Relay. Será, então, adicionado à esse frame o número DLCI associado à interface serial em questão. DLCIs identificam o circuito virtual (PVC) para os routers e switches da operadora participantes da rede frame Relay.

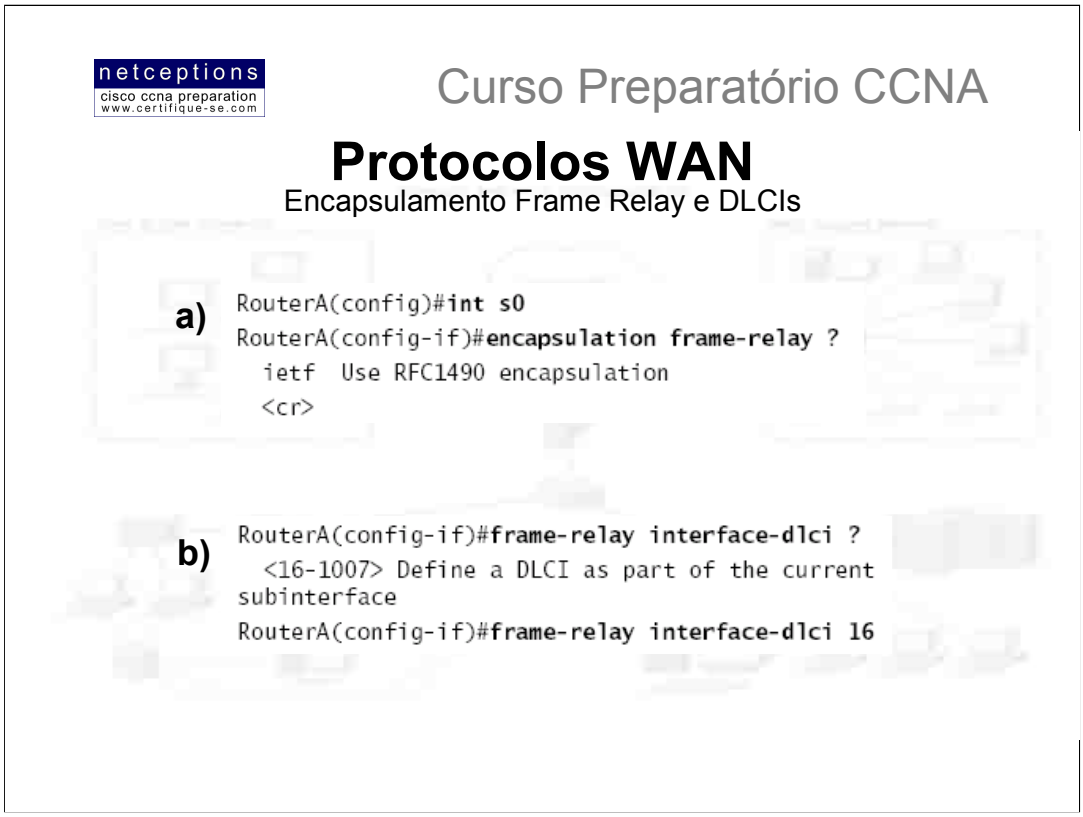
4) O dispositivo CSU/DSU (Channel Service Unit/Data Service Unit) recebe o sinal digital e o codifica em um tipo de sinal que o switch localizado no Packet Switch Exchange (PSE) possa entender. O PSE recebe o sinal e extrai a sequência de 1s e 0s da linha.

5) O CSU/DSU encontra-se conectado à um demarc instalado pelo provedor de serviço. O demarc, normalmente, é uma “tomada” RJ-45 localizada próxima ao CSU/DSU.

6) O demarc consiste de um par de cabos trançados (twisted pair cable) que se conecta ao local loop. O local loop se conecta ao CO (Central Office). O modo como o local loop se conecta ao SO pode englobar uma variedade de meios físicos. O mais comum, no entanto, é o par de fibra trançado (twisted pair fiber).

7) O CO recebe o frame e o envia através da “nuvem” Frame Relay para o seu destino. Essa “nuvem” pode ser composta por dezenas de switching offices, ou mais. O endereço IP de destino e o número DLCI correspondente são analisados. Normalmente, o número DLCI da rede remota é obtido através do mapeamento IP-para-DLCI. A base de dados para esse mapeamento normalmente é criada manualmente pelo provedor do serviço, porém, pode ser dinamicamente criada através do uso de protocolo IARP (Inverse ARP). Lembre-se que, antes de dados serem enviados através da “nuvem”, um circuito virtual ponto-à-ponto é estabelecido.

8) Uma vez que o frame alcance o switching office mais próximo do destination office, ele é enviado através do local loop. O frame é recebido no demarc e é, então, enviado ao dispositivo CSU/DSU. Finalmente, o router na ponta receptora extrai o pacote do frame e o insere na nova LAN, para que o mesmo seja enviado ao dispositivo ao qual se destina.



Ao configurar Frame Relay em routers Cisco, você deve especifica-lo como um método de encapsulamento nas interfaces seriais. Existem apenas 2 tipos de encapsulamento Frame Relay: Cisco e IETF. Acima ilustramos as 2 opções ao se configurar Frame Relay em um router Cisco **(a)**.

O método default é Cisco, à não ser que IETF seja manualmente escolhido. Cisco é o método que deve ser usado na conexão entre 2 routers Cisco. IETF deve ser escolhido na conexão entre um router Cisco e um de outro fabricante. Portanto, antes de optar por um método de encapsulamento, cheque com seu provedor qual equipamento eles utilizam.

DLCI - Data Link Connection Identifiers

Os circuitos virtuais criados pelo Frame Relay são identificados pelo DLCI. Normalmente o provedor de serviço Frame Relay, como uma operadora de telefonia, designa os números DLCI, que são utilizados pelo Frame Relay para distinguir entre diferentes circuitos virtuais em uma rede. Como muitos circuitos virtuais podem terminar em apenas uma interface Frame Relay multi-ponto, muitos DLCIs encontram-se associados à mesma.

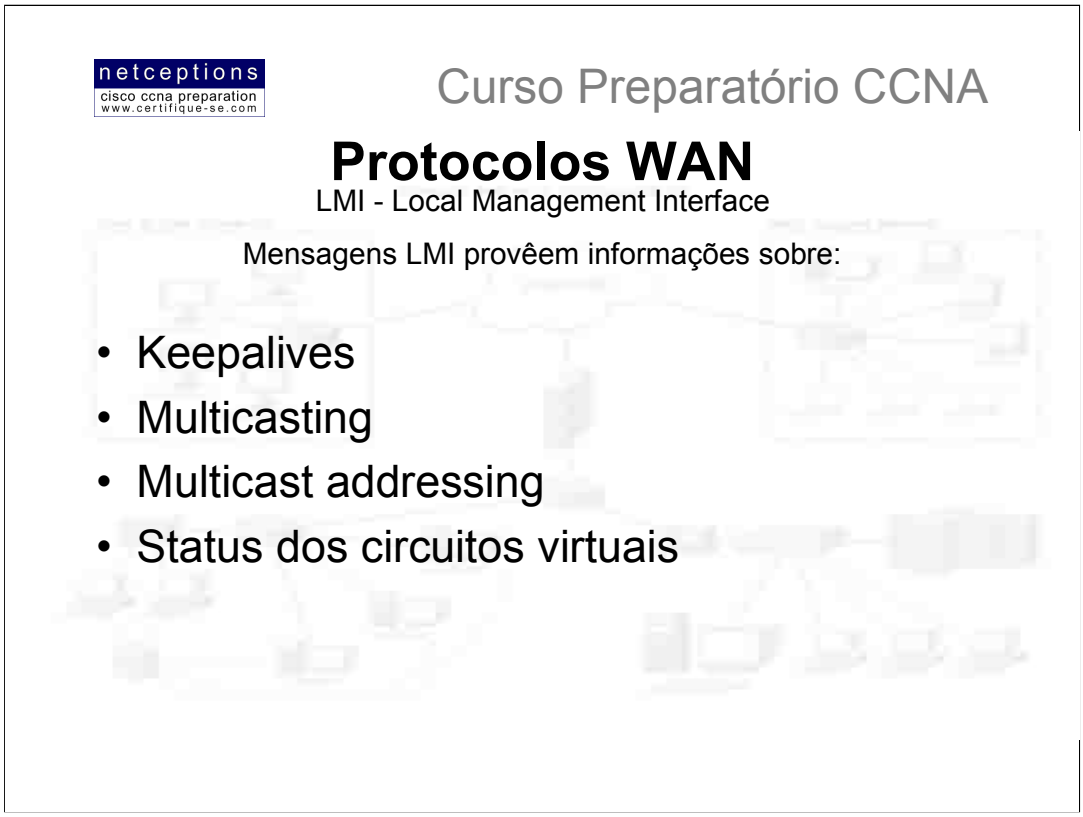
Para que dispositivos IP em cada ponta do circuito virtual possam se comunicar, seus endereços IP devem ser mapeados para números DLCI. Esse mapeamento pode ser realizado dinamicamente através do protocolo IARP (Inverse Address Resolution Protocol), ou manualmente, através do comando Frame Relay **`map`**.

Cada número DLCI pode ter um significado local ou global em qualquer ponto da rede Frame Relay. Algumas vezes, um provedor pode designar à um site um número DLCI que é propagado para todos os sites remotos que utilizam o mesmo PVC. Nesse caso, o PVC possui significância global (global meaning). Eis um exemplo: O escritório central de uma empresa pode ter o número DLCI 20 designado ao mesmo. Todos os sites remotos deverão saber que o DLCI do escritório central é 20, e poderão usar esse PVC para se comunicar com o mesmo.

Entretanto, o mais comum é dar ao DLCI um significado local (local meaning). Isso significa que os números DLCI não precisam, necessariamente, serem únicos. 2 números DLCI podem ser o mesmo em diferentes pontas de um link pois Frame Relay mapea um número DLCI local para um circuito virtual em cada interface do switch. Cada escritório remoto pode ter seu próprio número DLCI e comunicar-se com o escritório central utilizando números DLCI distintos.

Números DLCI são tipicamente designados pelo provedor, e começam no número 16.

Acima ilustramos como configurar o número DLCI para ser aplicado à uma interface **(b)**.



A interface de gerenciamento local (LMI) foi desenvolvida em 1990 pela Cisco, StrataCom, Northern Telecom e Digital Equipment Corporation (DEC), e ficou conhecida como “Gang-of-Four LMI”, ou Cisco LMI. Essa “gang” pegou o protocolo Frame Relay básico, definido pela CCITT, e adicionou extensões aos recursos do protocolo que permitiam à dispositivos de rede se comunicarem mais facilmente através de uma rede Frame Relay.

O LMI é um padrão de sinalização entre um dispositivo CPE (como um router) e um frame switch. O LMI é responsável pelo gerenciamento e manutenção do status entre esses dispositivos. Mensagens LMI provêem informações sobre:

Keepalives - Verifica que dados estão fluindo

Multicasting - Provê um DLCI PVC local

Endereçamento Multicasting - Provê significância global

Status dos Circuitos Virtuais - Provê o status do DLCI

À partir do sistema IOS 11.2, o tipo de LMI é automaticamente detectado (auto-sensed). Isso possibilita à uma interface determinar o tipo de LMI suportado pelo switch.

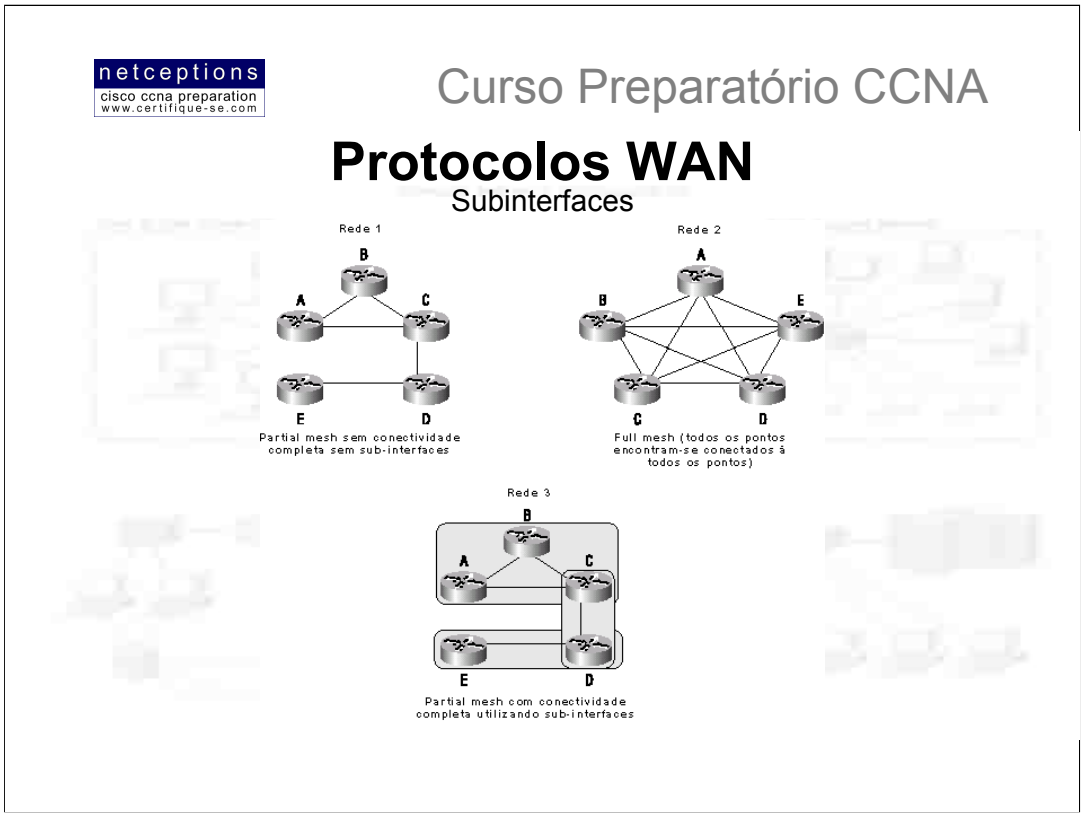
Se você não dispõe do recurso “auto-sense”, você deverá checar com seu provedor qual o tipo de LMI à ser usado. Os 3 diferentes tipos de LMI disponíveis são: cisco, ansi e q933a. O tipo default é Cisco, mas você poderá ter que mudar para ANSI ou Q.933A.

Routers recebem informações LMI em uma interface encapsulada Frame Relay, e atualiza o status dos circuitos virtuais para um dos 3 diferentes estados:

Ativo (active state) - Tudo encontra-se ativo e os routers podem trocar informações

Inativo (inactive state) - A interface do router encontra-se ativa e conectada ao switching office, porém, o router na outra ponta não encontra-se ativo.

Deleted (deleted state) - Isso significa que nenhuma informação LMI transmitida pelo switch está sendo recebida na interface do router. Isso pode ser devido à um problema de mapeamento, ou do próprio link.



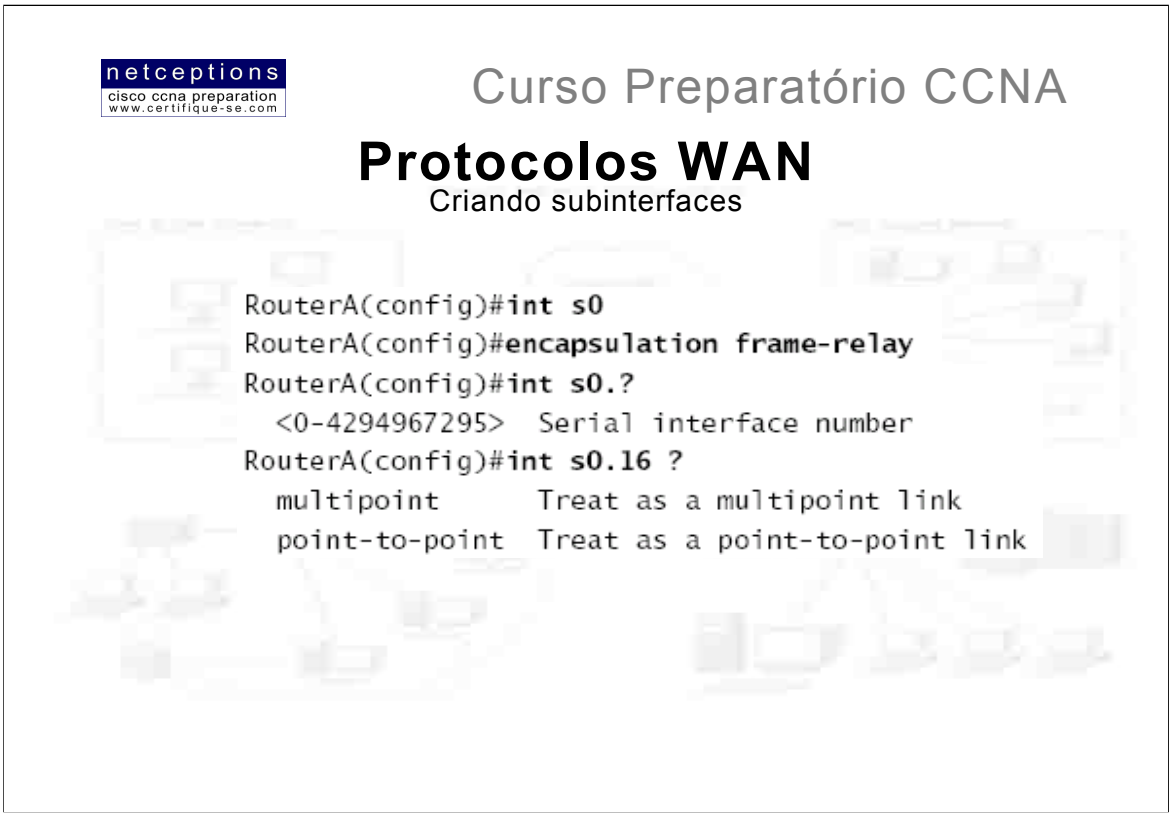
Você pode ter múltiplos circuitos virtuais em uma única interface serial e, ainda assim, tratar cada um como uma interface diferente. À isso chamamos sub-interfaces. Pense em uma subinterface como uma interface física definida pelo IOS. Uma vantagem de se criar subinterfaces é a habilidade atingida de se designar diferentes características de camada de rede à cada subinterface e circuito virtual, como roteamento IP em uma e IPX em outra.

Você pode criar subinterfaces para amenizar os problemas causados por redes constituídas parcialmente interconectadas (partial meshed), como na figura acima. Por exemplo, digamos que você esteja adotando o protocolo IP em uma rede LAN. Se, em uma mesma rede física, o router A pode se comunicar com o router B e esse com o router C, você normalmente assumiria que o router C pode se comunicar com o router A. Embora essa premissa seja verdadeira para uma LAN, não é necessariamente verdadeira para uma rede Frame Relay, à não ser que o router A tenha um PVC definido até o router C.

Na figura acima, a rede 1 encontra-se configurada com 5 sites. Para que essa rede funcione, uma rede totalmente interconectada (fully meshed), como a ilustrada na rede 2, teria de ser criada, a princípio. Entretanto, mesmo que o exemplo ilustrado na rede 2 seja totalmente funcional, sua implantação é extremamente cara. A solução apresentada na rede 3 - utilizando subinterfaces - é a mais custo-efetiva.

Na rede 3, a configuração de subinterfaces é um modo de subdividir a rede Frame Relay em subredes de menores proporções - cada uma com seu próprio endereço de rede. Portanto, os sites A, B e C encontram-se totalmente interconectados (fully meshed network), enquanto que os sites C e D, e D e E encontram-se conectados através de conexões ponto-à-ponto.

A criação de subinterfaces também resolvem o problema com protocolos de roteamento que utilizam o método split horizon. Como estudamos, protocolos que utilizam split horizon não propagam atualizações pela mesma interface onde essas foram recebidas. Isso pode ser um problema em uma rede Frame Relay totalmente interconectada. Entretanto, criando-se subinterfaces, protocolos de roteamento que recebem atualizações em uma subinterface podem propagar a mesma atualização por uma outra subinterface.



Subinterfaces são definidas através do comando int s0.{número da subinterface}, como ilustrado acima.

Você pode definir um número virtualmente ilimitado de subinterfaces em uma determinada interface física (considerando a memória disponível do router). No exemplo acima, escolhemos utilizar a subinterface 16, já que esse é o número que representa o DLCI designado àquela interface.

Existem 2 tipos de subinterface:

Point-to-point - Usadas quando um único circuito virtual conecta um router à outro. Cada interface point-to-point requer sua própria subrede.

Multipoint - Usadas quando o router é o centro de uma estrela de circuitos virtuais. Utiliza uma única subrede para todas as interfaces dos routers conectadas ao switch.

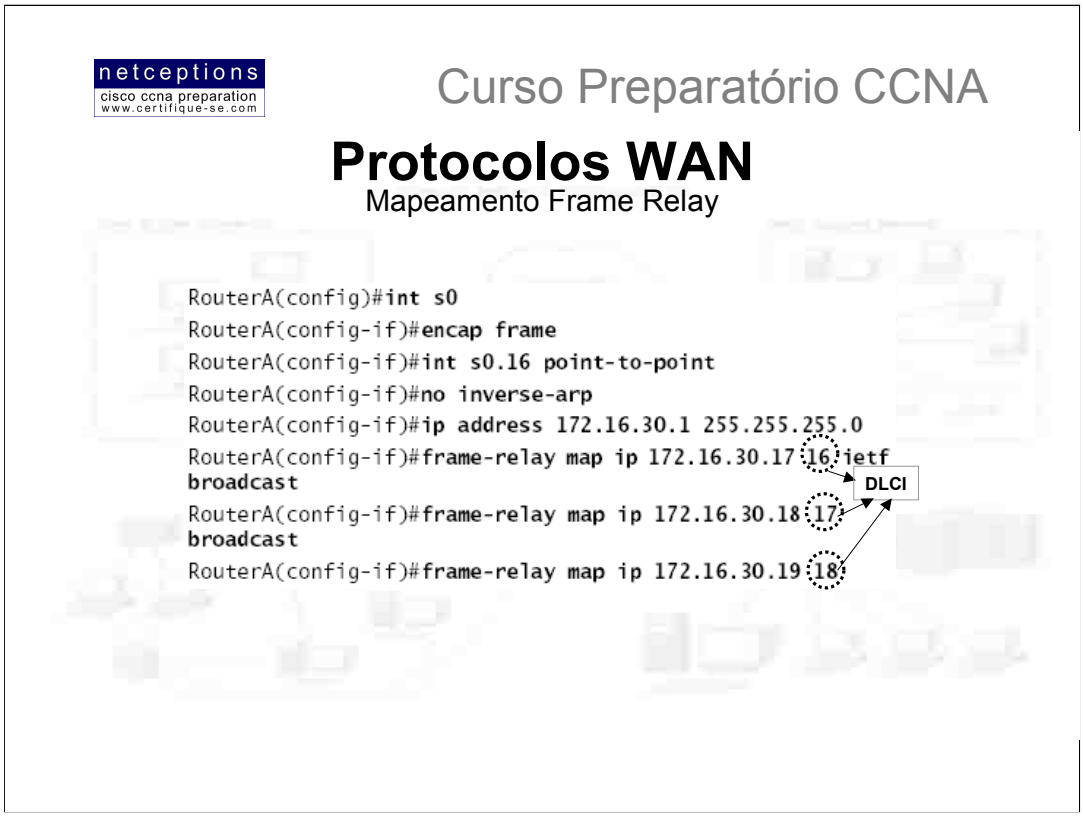
Ilustramos na próxima página uma saída de um router em ambiente de produção configurado com múltiplas subinterfaces. Note que, cada subinterface tem seu número baseado no DLCI designado à interface. Isso ajuda na administração das interfaces. Note também que não há um tipo de LMI definido, o que significa que esta sendo adotado o tipo padrão (Cisco) ou que o modo de detecção automática está ativo (no caso de o IOS ser versão 11.2 ou mais recente). Note ainda que cada subinterface é definida como uma subrede distinta, rede IPX distinta, e alcance do cabo AppleTalk distinto.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Exemplo de subinterfaces configuradas:

```
interface Serial0
no ip address
no ip directed-broadcast
encapsulation frame-relay
!
interface Serial0.102 point-to-point
ip address 10.1.12.1 255.255.255.0
no ip directed-broadcast
appletalk cable-range 12-12 12.65
appletalk zone wan2
appletalk protocol eigrp
no appletalk protocol rtmp
ipx network 12
frame-relay interface-dlci 102
!
interface Serial0.103 point-to-point
ip address 10.1.13.1 255.255.255.0
no ip directed-broadcast
appletalk cable-range 13-13 13.174
appletalk zone wan3
appletalk protocol eigrp
no appletalk protocol rtmp
ipx network 13
frame-relay interface-dlci 103
!
interface Serial0.104 point-to-point
ip address 10.1.14.1 255.255.255.0
no ip directed-broadcast
appletalk cable-range 14-14 14.131
appletalk zone wan4
appletalk protocol eigrp
no appletalk protocol rtmp
ipx network 14
frame-relay interface-dlci 104
!
interface Serial0.105 point-to-point
ip address 10.1.15.1 255.255.255.0
no ip directed-broadcast
appletalk cable-range 15-15 15.184
appletalk zone wan5
appletalk protocol eigrp
no appletalk protocol rtmp
ipx network 15
frame-relay interface-dlci 105
!
(...)
```



Conforme explicado anteriormente, para que dispositivos IP possam se comunicar através de uma rede Frame Relay, seus endereços IP devem ser mapeados para números DLCI. Existem 2 modos de se efetuar esse mapeamento: utilizando o comando Frame Relay **`map`** ou usando o recurso inverse-arp.

Acima ilustramos um exemplo de uso do comando **`map`** . Eis o que foi feito:

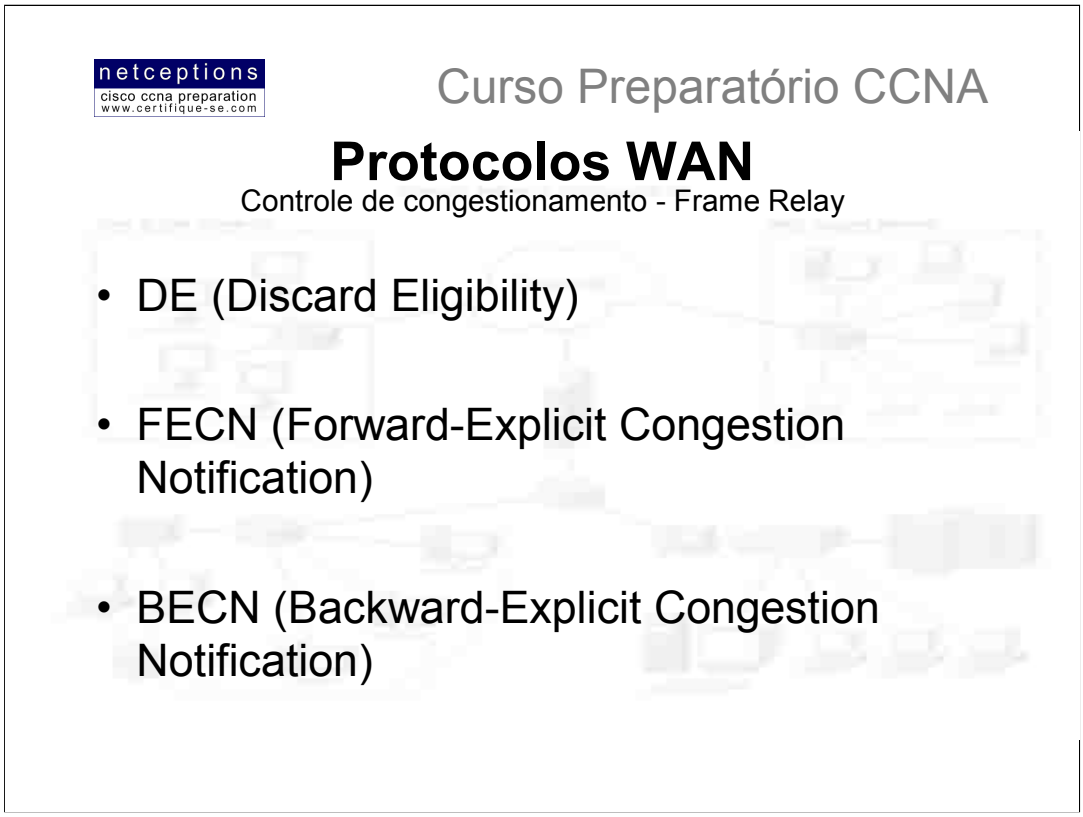
Primeiro, configuramos a interface serial 0 para utilizar o encapsulamento Frame Relay default (cisco). Criamos, então, uma subinterface. Em seguida, desativamos o recurso inverse-arp e mapeamos 3 circuitos virtuais e seus números DLCI correspondentes. Note que alteramos o tipo de encapsulamento (ietf) para a primeira subinterface. O comando frame map é a única maneira de se configurar múltiplos tipos de encapsulamento em uma interface.

A palavra "**`broadcast`**" que aparece no final da linha de comando informa ao router para encaminhar mensagens broadcast destinadas à interface em questão para o circuito virtual especificado. Lembre-se que frame Relay é um método de encapsulamento não-broadcast por default, o que significa que ele não propagará protocolos de roteamento. Para que Frame Relay efetue a propagação de broadcasts, o palavra **`broadcast`** juntamente com o comando **`frame map`** deve ser usada.

Em vez de aplicar o comando map à cada circuito virtual, você pode utilizar o recurso inverse-arp para que o mapeamento seja feito dinamicamente. Nesse caso, a configuração acima ficaria assim:

```
RouterA(config)#int s0.16 point-to-point
RouterA(config-if)#encap frame-relay ietf
RouterA(config-if)#ip address 172.16.30.1 255.255.255.0
```

Como se pode observar, esse método é muito mais fácil. Porém, não é tão estável quanto o método manual.



Frame Relay utiliza 3 métodos para lidar com problemas de congestionamento:

• **DE (Discard Eligibility)** - Quando um router Frame Relay detecta congestionamento na rede Frame relay, ele ativará o bit DE no cabeçalho do pacote Frame Relay (passará de 0 para 1). Se o switch Frame Relay estiver congestionado, ele começará a descartar os pacotes que tenham o bit DE ativado, primeiro. Se sua largura de banda estiver configurada com um CIR (Commited nformation Rate) de zero, o bit DE encontrar-se-à sempre ativado.

• **FECN (Forward-Explicit Congestion Notification)** - Quando a rede Frame Relay identifica um congestionamento na "nuvem", o switch ativará o bit FECN no cabeçalho do pacote Frame Relay. Isso informará ao DCE destino que a rota atravessada pelo pacote em questão encontra-se congestionada.

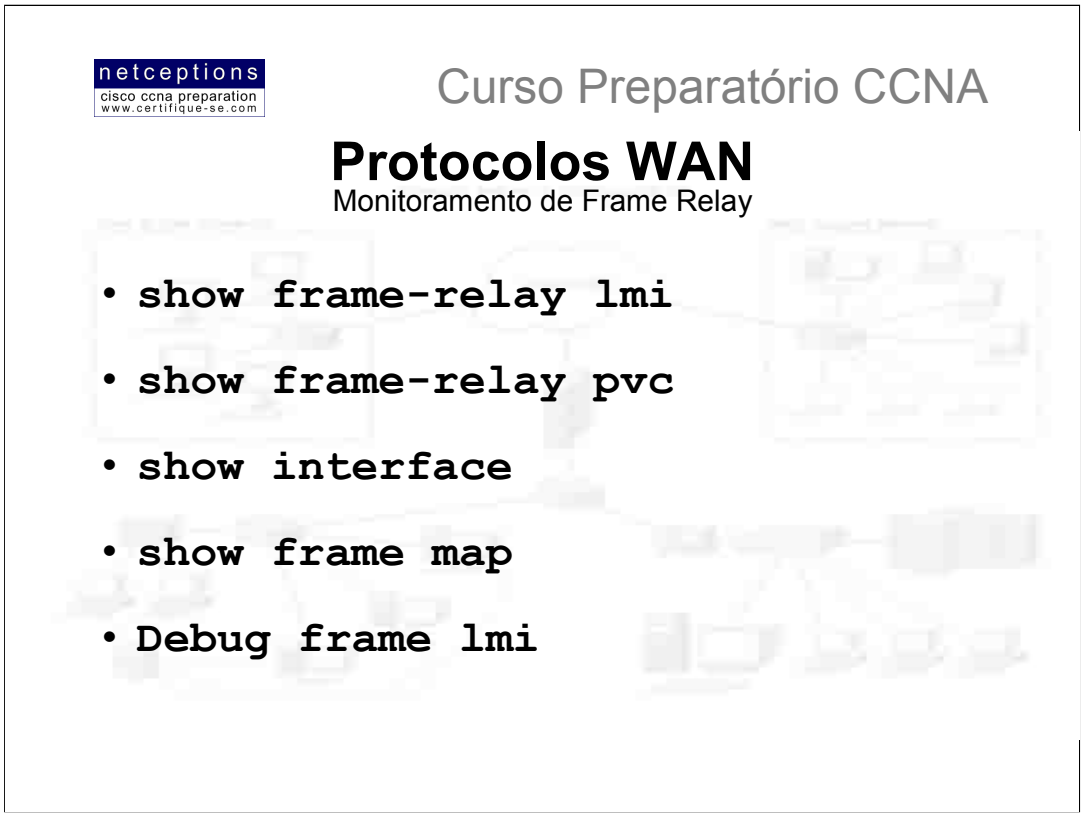
• **BECN (Backward-Explicit Congestion Notification)** - Quando o switch detecta um congestionamento na rede Frame Relay, ele ativará o bit BECN no cabeçalho do pacote Frame Relay e o enviará de volta ao router origem, informado-o que reduza o fluxo de pacotes.

Commited Information Rate (CIR)

Frame Relay permite que múltiplos usuários compartilhem uma rede de pacotes (packet-switched network) simultaneamente. Isso é positivo, uma vez que divide o custo da utilização dos switches entre os usuários. Entretanto, o conceito Frame Relay se baseia na premissa de os usuários da rede não enviarão dados de forma constante simultaneamente. Frame Relay funciona melhor com tráfego em rajadas.

Frame Relay funciona provendo uma largura-de-banda dedicada para cada usuário, que fica comprometido com aquela largura-de-banda todo o tempo. Provedores de serviço, normalmente, permitem que usuários adquiram uma quantidade de largura-de-banda menor do que àquela que realmente necessitam. À isso chamamos de CIR. O que isso implica é que um usuário pode adquirir uma largura-de-banda de, por exemplo, 256Kbps, mas será possível que o mesmo atinja velocidades em rajada do equivalente à uma T-1. O CIR especifica que enquanto a transmissão de dados feita por dispositivo em uma rede Frame relay não exceda o CIR, a rede continuará a encaminhar os pacotes ao PVC. Entretanto, se o fluxo de dados exceder o CIR, não há garantias.

O CIR deve ser escolhido baseado em projeções realísticas. Alguns provedores permitem que a aquisição de um CIR de zero. Isso pode ser uma opção quando custo é um problema e o reenvio constante de pacotes é aceitável. Entretanto, deve-se entender que o bit DE encontrar-se-á SEMPRE ativado.



• **show frame-relay lmi**

Apresenta estatísticas sobre o tráfego LMI ocorrido entre um router local e um switch Frame relay

• **show frame-relay pvc**

Relaciona todos os circuitos virtuais (PVCs) configurados (interfaces) e respectivos números DLCI. Apresenta o status de cada conexão PVC e estatísticas de tráfego. Também informa o número de pacotes BECN e FECN recebidos pelo router.

• **show interface**

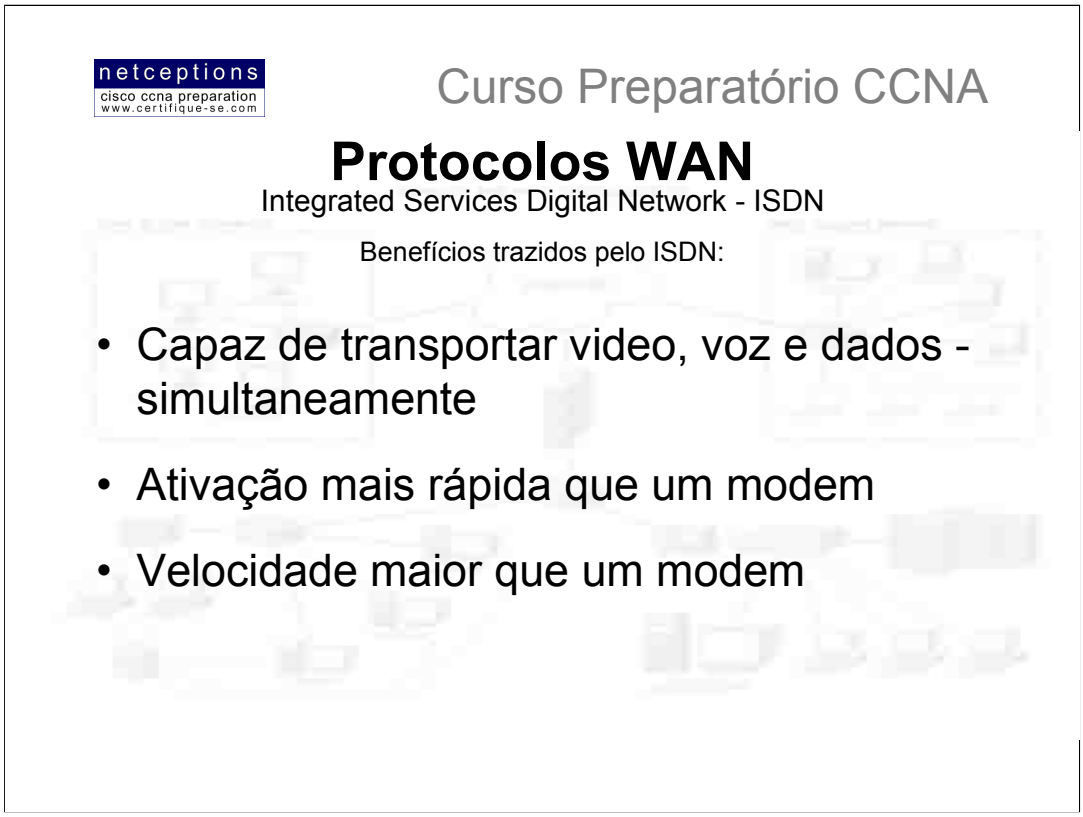
O comando **sh interface** pode ser usado para checagem de tráfego LMI. Apresenta informações sobre encapsulamento utilizado, assim como informações sobre camadas 2 (data-link) e 3 (rede). A informação sobre o tipo de LMI sendo usado é apresentada como LMI DLCI 1023 (Cisco) ou LMI DLCI 0 (ANSI).

• **show frame map**

Apresenta o mapeamento IP/IPX-para-DLCI

• **Debug frame lmi**

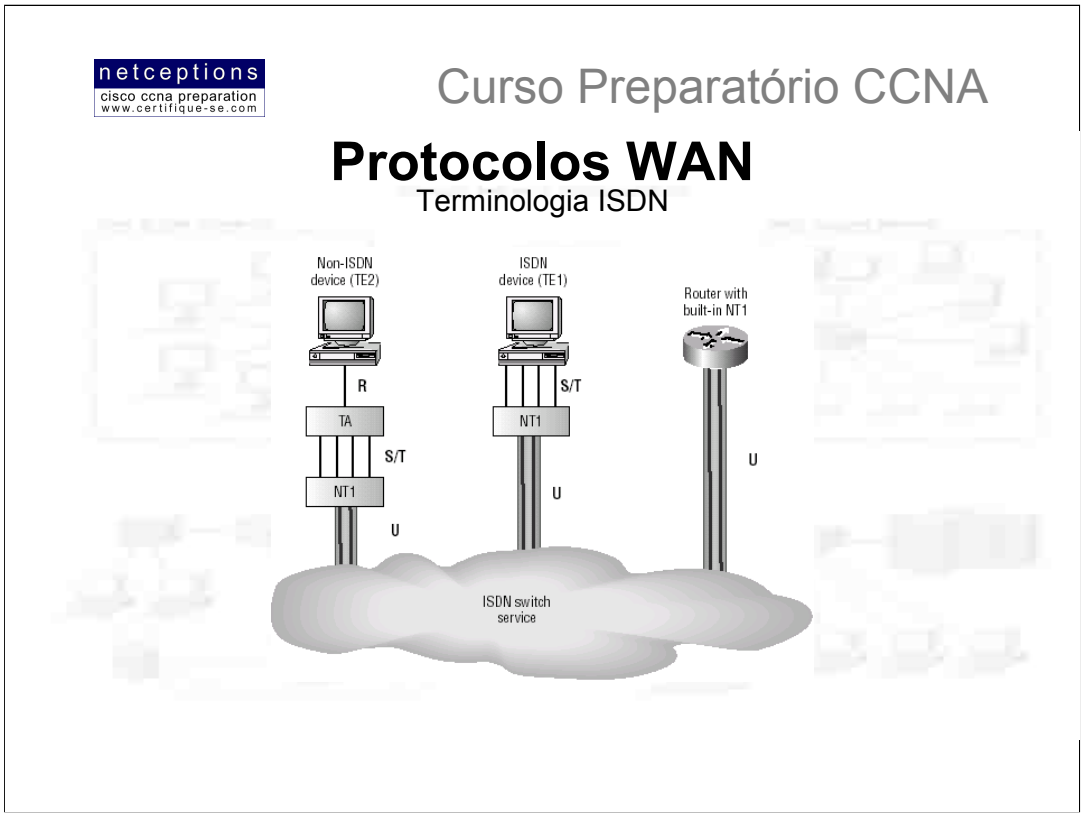
A informação originada desse comando permite que você verifique e identifique problemas em conexões Frame Relay, ajudando-o a determinar se a comunicação router-switch Frame Relay esta ocorrendo sem problemas. A saída deste comando é apresentada no console do router, por default.



ISDN é um serviço digital desenhado para ser usado sobre redes telefônicas legadas. ISDN suporta voz e dados, simultaneamente, porém, aplicações ISDN requerem largura-de-banda.

Aplicações ISDN típicas incluem transmissão de imagens em alta-velocidade, transferência de arquivos em alta-velocidade, serviços de video-conferência, entre outras.

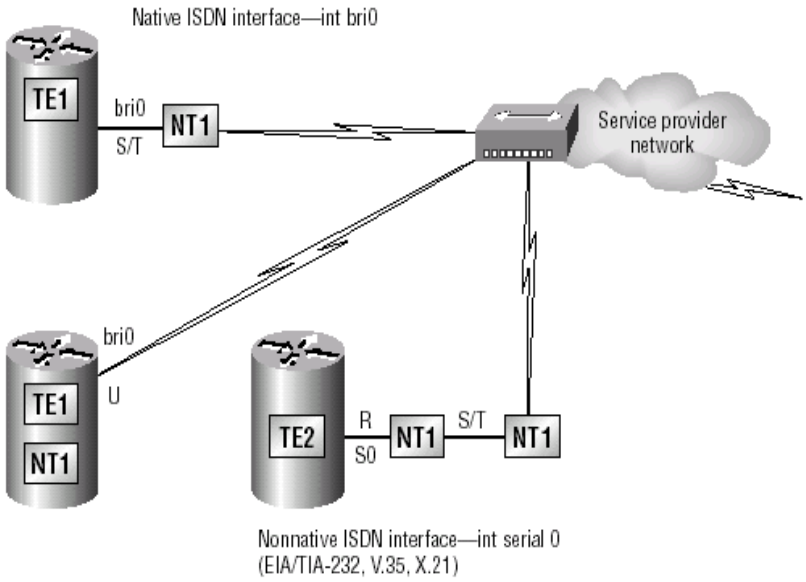
ISDN é, na verdade, um conjunto de protocolos de comunicação proposto por operadoras do sistema de telefonia permitindo que as mesmas transportem um grupo de serviços digitais que possibilitam a convergência de voz, texto, música, gráficos e vídeo aos seus usuários. ISDN é referenciado por uma série de padrões ITU-T que englobam as camadas de rede, enlace e física do modelo de referência OSI. Os padrões ISDN definem o hardware e esquemas de ativação de chamadas para estabelecimento de comunicação digital ponto-à-ponto.

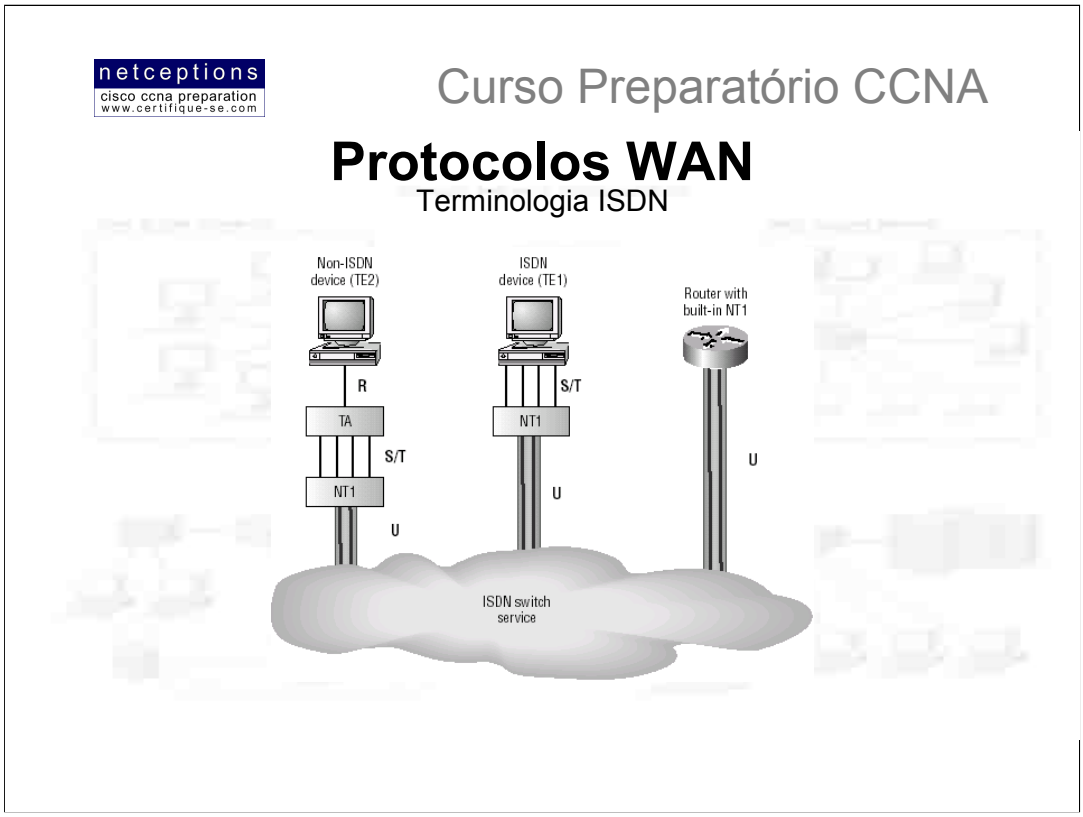


Os componentes utilizados com ISDN incluem funções e pontos de referência (reference points). A figura acima ilustra os diferentes tipos de terminais e pontos de referencia que podem ser usados em uma rede ISDN.

Nos EUA, ISDN adota uma conexão de 2 fios (two-wire connection) para o usuário final (casa ou escritório). Isso é chamado de ponto de referência "U". O dispositivo NT1 é usado na conversão de uma conexão 2 fios para uma conexão 4 fios, utilizada por telefones ISDN e adaptadores terminais (terminal adapters - TA). Grande parte dos routers existentes hoje podem ser adquiridos com uma interface NT1 (U) embutida.

A figura abaixo ilustra os diferentes pontos de referência e equipamentos terminais que podem ser utilizados com interfaces BRI ISDN Cisco:





Dispositivos conectados à uma rede ISDN são chamados de equipamentos terminais (Terminal Equipments - **TE**) e equipamentos de terminação de rede (Network Termination Equipments - **NT**). Existem 2 tipos de cada:

TE1 - Terminal Endpoint tipo 1. Referem-se aos terminais que entendem os padrões ISDN e podem ser conectados diretamente à uma rede ISDN.

TE2 - Terminal Endpoint tipo 2. Referem-se aos terminais que não seguem os padrões ISDN, pois foram concebidos antes dos mesmos. Para esses terminais poderem se conectar à uma rede ISDN, um adaptador terminal (Terminal Adapter - TA) deve ser usado.

NT1 - Network Termination 1. Implementa as especificações ISDN na camada física e conecta os dispositivos dos usuários à rede ISDN

NT2 - Network Termination 2. Refere-se, tipicamente, aos equipamentos do provedor, como um switch ou um PABX. Também provê implementações de camada de enlace e de rede. Muito raro nas premissas do usuário.

TA - Terminal Adapter. Converte a fiação TE2 para TE1, que então deve ser conectada à um dispositivo NT1 para conversão para 2 fios, usada na rede ISDN. (veja ilustrações na página anterior).

Pontos de referência ISDN (ISDN reference points)

R- Define o ponto de referência entre um equipamento não-ISDN (TE2) e um TA (Terminal Adapter)

S - Define o ponto de referência entre o router do usuário e um dispositivo NT2 (Network Termination 2)

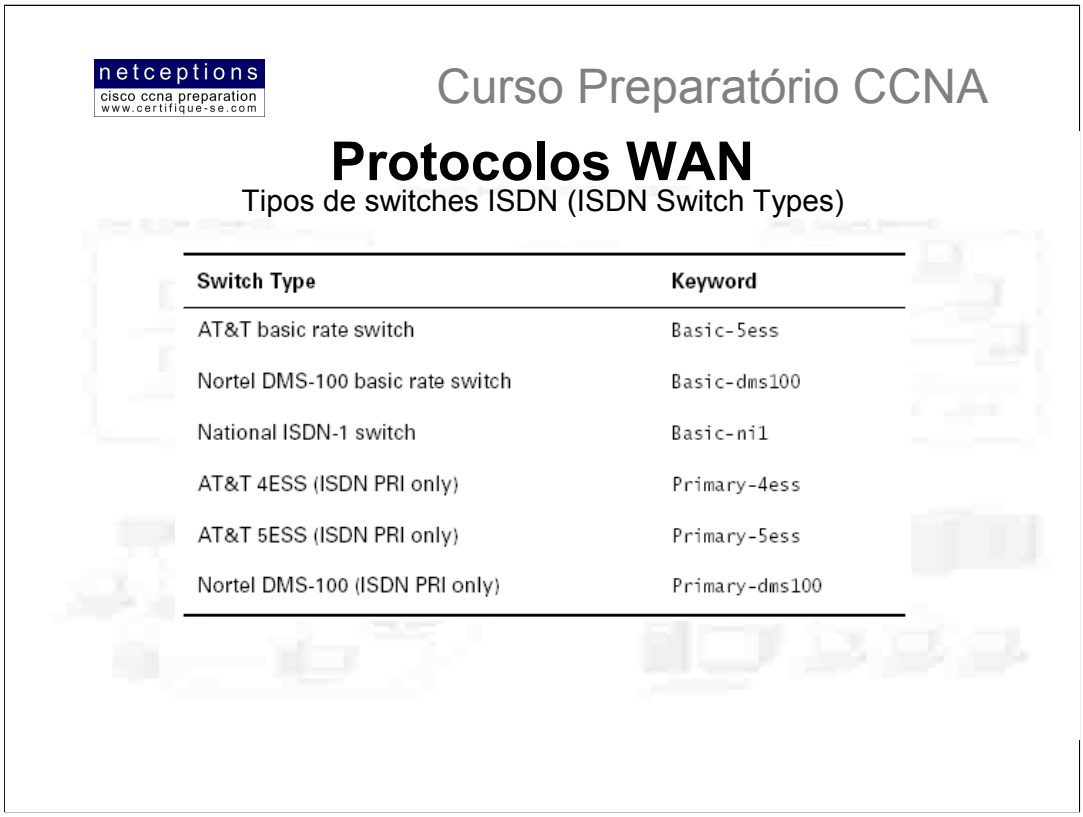
T - Define o ponto de referência entre um dispositivo NT1 e um dispositivo NT2. Os pontos de referência S e T são eletricamente iguais e, por essa razão, são também conhecidos como ponto de referência **S/T**.

U - define o ponto de referência entre um dispositivo NT1 e o equipamento de terminação de linha localizado em uma operadora de telefonia (isso é válido apenas para a América do Norte, onde a funcionalidade NT1 não é provida pela rede da operadora).

Prefixos ISDN

E - telefonia
I - conceitos, aspectos e serviços
Q - sinalização e comutação (switching)

NOTA: É MUITO IMPORTANTE SABER CADA UM DOS ÍTENS ACIMA LISTADOS PARA O EXAME.

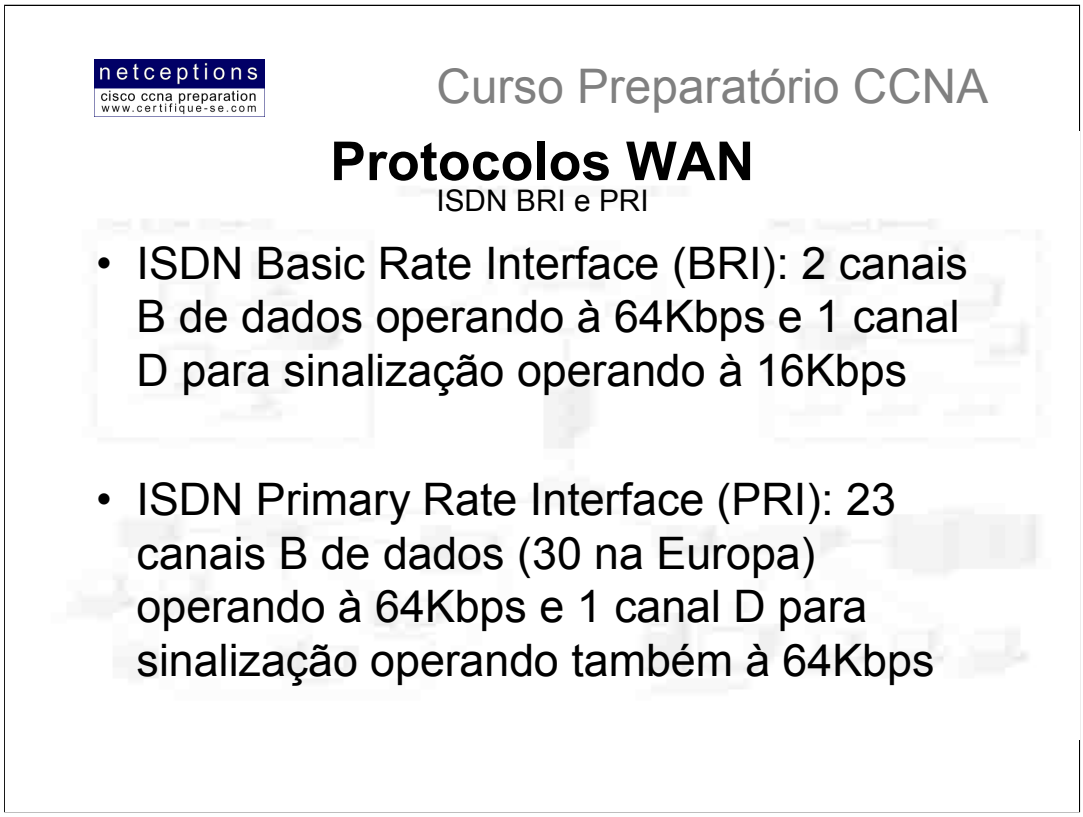


Devemos dar o crédito à AT&T e Nortel pela maioria dos switches ISDN existentes hoje. Outras companhias também os fabricam.

Na tabela acima, sob a palavra “Keyword”, você irá encontrar a palavra-chave adequada para utilizar com o comando **`isdn switch-type`** na configuração do router para uma variedade de switches aos quais o mesmo irá se conectar.

Caso não saiba qual switch sua operadora utiliza, simplesmente ligue e pergunte.

NOTA: *Isso NÃO costuma cair no exame CCNA.*



Serviços ISDN BRI, também conhecido como 2B+D, provêem 2 canais B de 64Kbps cada e 1 canal D de 16Kbps. Os canais B transportam dados, enquanto que o canal D transporta informações de sinalização e controle. O canal D pode ser usado para outras funções, como sistemas de alarme, ou qualquer outro serviço que não necessite de muita largura-de-banda. Pode-se, até mesmo, utilizá-lo para transporte de dados e somá-lo aos 2 canais B existentes, totalizando uma banda de 144Kbps para transporte de dados.

Ao se configurar ISDN BRI você deverá obter os SPIDs (Service Profile Identifiers)'- análogos aos números de telefone - e você deverá ter um SPID para cada canal B.

O dispositivo ISDN envia o SPID ao switch ISDN que, então, permite que o dispositivo acesse a rede ISDN. Sem um SPID, a maioria dos switches ISDN não permitirão que o dispositivo ISDN acesse a rede.

Para estabelecer uma conexão BRI, 4 eventos devem ocorrer:

1) O canal D entre o router e o switch ISDN local é ativado

2) O switch ISDN local utiliza a técnica de sinalização SS7 para estabelecer uma rota até o switch remoto

3) O switch remoto ativa o canal D até o router remoto

4) Os canais B são então conectados pontæ- ponta

ISDN PRI

Na América do Norte e no Japão, ISDN PRI (23B+D) oferece 23 canais B de 64Kbps e 1 canal D de 64Kbps, totalizando uma largura-de-banda de 1.544Mbps (T1). Já na Europa, Austrália e América do Sul, são 30 canais B e 1 D, totalizando uma largura-de-banda de 2.048Mbps (E1).

Acessar uma rede ISDN através de um router Cisco implica que você terá de adquirir um router com uma interface NT1 embutida ou um modem ISDN (TA). Se o seu router possui uma interface BRI, você esta pronto. Do contrário, você pode utilizar uma das interfaces seriais do router para conectar um modem ISDN (TA). Um router com uma interface BRI é conhecido como TE1 (Terminal Endpoint 1), e um que necessite de um modem acoplado é conhecido como TE2.

ISDN suporta virtualmente todos os protocolos de camada superior (IP, IPX, AppleTalk, etc.), e você pode optar por PPP, HDLC or LAPD como protocolo de encapsulamento.

Quando configurando ISDN você deverá saber o tipo de switch que sua operadora utiliza. Para ver os tipos de switches que seu router suporta, utilize o comando **`isdn switch-type ?`**. Você deve saber isso pois cada fabricante adota uma técnica diferente de sinalização.

Para cada interface ISDN BRI você deve especificar o SPID. Essa informação é fornecida pelo provedor de serviço e o identifica no switch da operadora, como um número de telefone. Alguns provedores não mais requerem que SPIDs sejam configurados. A segunda parte da configuração do SPID é o número de discagem local para aquele SPID. É opcional, mas alguns switches precisam dessa informação configurada na router para que ambos os canais B possam ser usados simultaneamente.

Acima ilustramos um exemplo de configuração ISDN BRI em um router Cisco.

NOTA: O comando **`isdn switch-type`** pode ser digitado tanto em modo de configuração global quanto no modo de configuração de interface. Digitando o comando em modo global fará com que todas as interfaces ISDN no router adotem o tipo de swich especificado. Caso seu router tenha apenas 1 interface ISDN, não faz diferença em que modo você digite o comando.

Dial-on-Demand Routing (DDR)

DDR é usado para permitir que 2 ou mais routers Cisco estabeleçam uma conexão ISDN sob demanda. DDR é usado para conexões periódicas, com baixo volume, utilizando tanto a Rede Pública Comutada (PSTN) ou ISDN. Isso foi desenhado visando a redução dos custos com links WAN. DDR é ativado quando um pacote recebido em uma interface se enquadra nos requerimentos definidos pelo administrador, que define "tráfego interessante" (interesting traffic). Os 5 passos seguintes descrevem brevemente o funcionamento do DDR quando um pacote "interessante" é recebido em uma interface do router:

1) A rota até a rede destino é determinada;

2) Pacotes interessantes determinam o estabelecimento da conexão (DDR call);

3) A informação do discador (dialer) é verificada;

4) Informação é transmitida;

5) A conexão é desfeita assim que o tráfego de dados cessa e o período limite de espera (timeout) é atingido.

Configurando DDR

Para configurar DDR, os seguintes passos devem ser seguidos:

1) Definir rotas estáticas, que definam como alcançar redes remotas e qual interface usar para isso.

2) Especificar o tráfego considerado interessante ao router

3) Configurar as informações do discador (dialer) que serão usadas para ativar a interface e alcançar a rede remota.

Configurando rotas estáticas

Para encaminhar tráfego através de um link ISDN, rotas estáticas devem ser configuradas nos routers das 2 pontas. Rotas dinâmicas também podem ser configuradas, porém, nesse caso, o link nunca será desfeito. Default routing pode ser usado se o router encontrar-se um uma rede "stub" (apenas uma saída). Abaixo, um exemplo de configuração de rotas estáticas com ISDN:

```
RouterA(config)#ip route 172.16.50.0 255.255.255.0 172.16.60.2
RouterA(config)#ip route 172.16.60.2 255.255.255.255 bri0
```

A primeira linha informa o router como alcançar a rede 172.16.50.0, que é através da rede 172.16.60.2. A segunda linha informa o router como chegar à rede 172.16.60.2.

Definindo tráfego interessante

Uma vez que as tabelas de roteamento estejam definidas, você deve configurar o router para determinar que tipo de pacote ativará a linha ISDN. Um administrador utilizando o comando **dialer-list** define pacotes interessantes. Os comandos que ativam a linha ISDN para qualquer pacote IP são ilustrados abaixo:

```
804A(config)#dialer-list 1 protocol ip permit
804A(config)#int bri0
804A(config-if)#dialer-group 1
```

O comando dialer-group aplica a lista de acesso à interface BRI. Listas de acesso estendidas podem ser utilizadas para restringir tráfego interessante à aplicações específicas.

Dial-on-Demand Routing (DDR)

5 passos devem ser seguidos na configuração da informação do discador (dialer):

1) Escolha a interface
2) Defina o endereço IP
3) Configure o tipo de encapsulamento
4) Associe tráfego interessante à interface
5) Configure o número ou números à serem discados

Eis um exemplo de como aplicar os 5 passos:

```
804A#config t
804A(config)#int bri0
804A(config-if)#ip address 172.16.60.1 255.255.255.0
804A(config-if)#no shut
804A(config-if)#encapsulation ppp
804A(config-if)#dialer-group 1
804A(config-if)#dialer-string 8350661
```

O comando **dialer map** pode ser usado no lugar do comando dialer string, oferecendo mais segurança:

```
804A(config-if)#dialer map ip 172.16.60.2 name 804B 8350661
```

O comando **dialer map** pode ser usado com o comando **dialer-group** e sua lista de acesso associada para iniciar a discagem. O comando **dialer map** usa o endereço IP do router do próximo hop, o hostname do router remoto para autenticação e, então, o número à ser discado para se alcançá-lo.

Comandos Opcionais

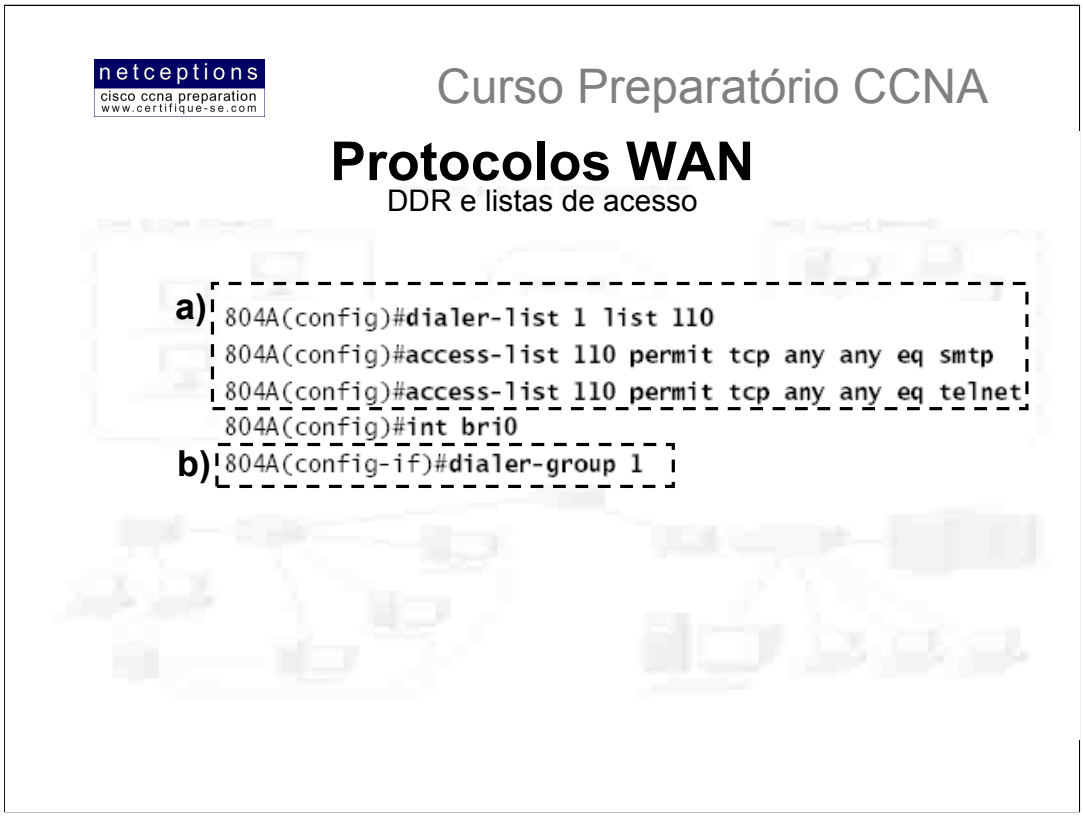
Existem 2 outros comandos que você pode usar na configuração de uma interface BRI:
dialer load-threshold e **dialer idle-timeout**

O primeiro informa à interface BRI quando o segundo canal deve ser ativado. O primeiro parâmetro pode ser um número de 1 à 255, onde 255 informa a interface para ativar o segundo canal apenas quando o primeiro canal estiver com sua capacidade em 100%. O segundo parâmetro pode ser **in, out** ou **either**. Isso calcula a carga atual da interface para tráfego entrante (in), sainte (out), ou uma combinação (either). O default é **out**.

O segundo comando (**dialer idle-timeout**) especifica o número de segundos antes de uma conexão ser desfeita, após o último pacote interessante ter sido transmitido. O valor default é 120 segundos. Eis um exemplo de cada:

```
RouterA(config-if)#dialer load-threshold 125 either
RouterA(config-if)#dialer idle-timeout 180
```

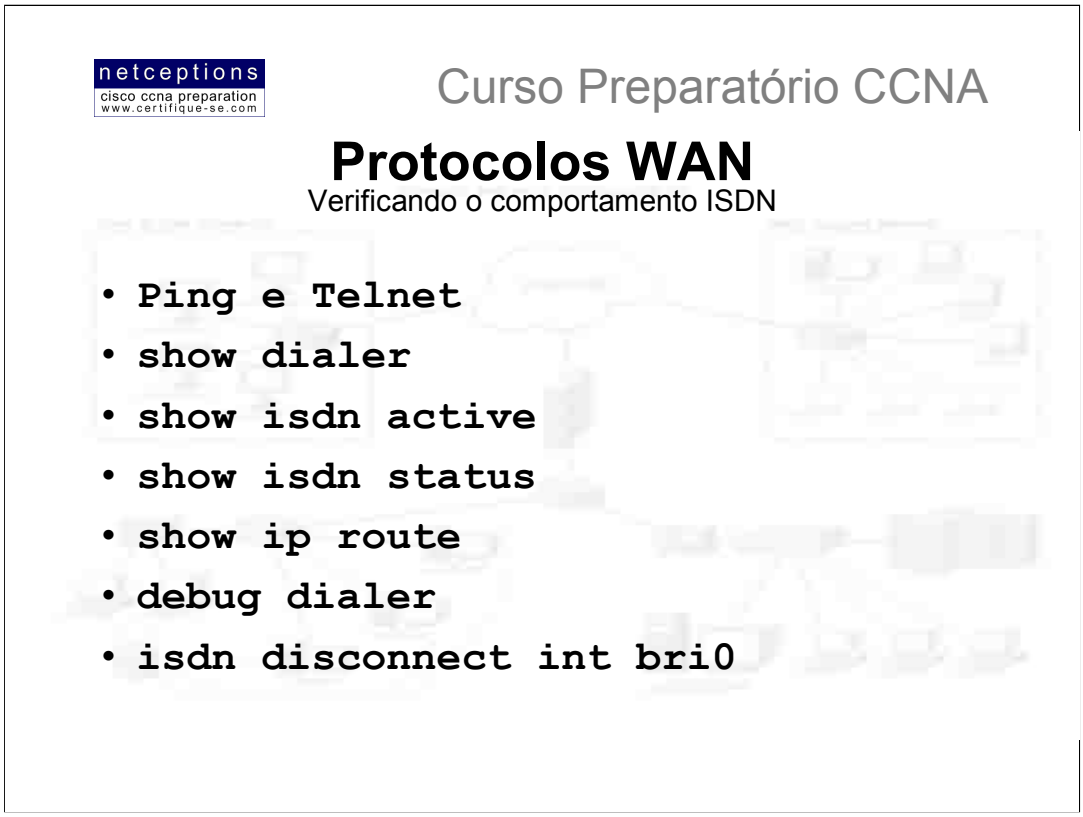
O valor de 125 no primeiro caso informa a interface BRI para ativa o segundo canal se a carga do tráfego entrante ou sainte no primeiro canal chegar a 50%



Listas de acesso podem ser utilizadas para especificar o que é tráfego interessante. Em um exemplo anterior, nós configuramos o dialer para que qualquer tráfego IP ativasse a linha ISDN. Isso é interessante se você está efetuando testes, mas acaba como propósito de se utilizar DDR. Listas de acesso estendidas podem ser utilizadas para definição de restrições específicas. Por exemplo, definir como tráfego interessante apenas pacotes gerados pelas aplicações e-mail e Telnet.

Acima exemplificamos como definir o dialer list para utilizar uma lista de acesso.

No exemplo acima, o comando **`dialer-list`** foi configurado para acessar uma lista de acesso. Isso não está restrito ao IP. Pode ser qualquer protocolo. Crie uma lista de acesso **(a)** e aplique-a à sua interface BRI através do comando **`dialer-group`** **(b)**.



• **Ping e Telnet**

Ferramentas IP úteis em qualquer tipo de rede. Entretanto, lembre-se que, para Ping e Telnet funcionarem como ferramentas de testes em sua rede ISDN, eles devem estar especificados como tráfego interessante para ativar um link.

• **show dialer**

Apresenta informações úteis sobre informações de diagnóstico do dialer e apresenta o número de vezes que um dialer string foi usado, os valores de timeout de cada canal B, a duração de cada chamada e o nome do router à qual q interface encontra-se conectada.

• **show isdn active**

Apresenta o número chamado e se existe alguma ligação em progresso.

• **show isdn status**

Bom comando para se usar antes da discagem. Informa se o SPID é válido e se você encontra-se conectado e comunicando-se com as camadas 1 à 3 do switch ISDN do provedor.

• **show ip route**

Apresenta todas as rotas IP conhecidas pelo router.

• **debug dialer**

Apresenta atividade inerentes à ativação e desativação das linhas.

• **isdn disconnect int bri0**

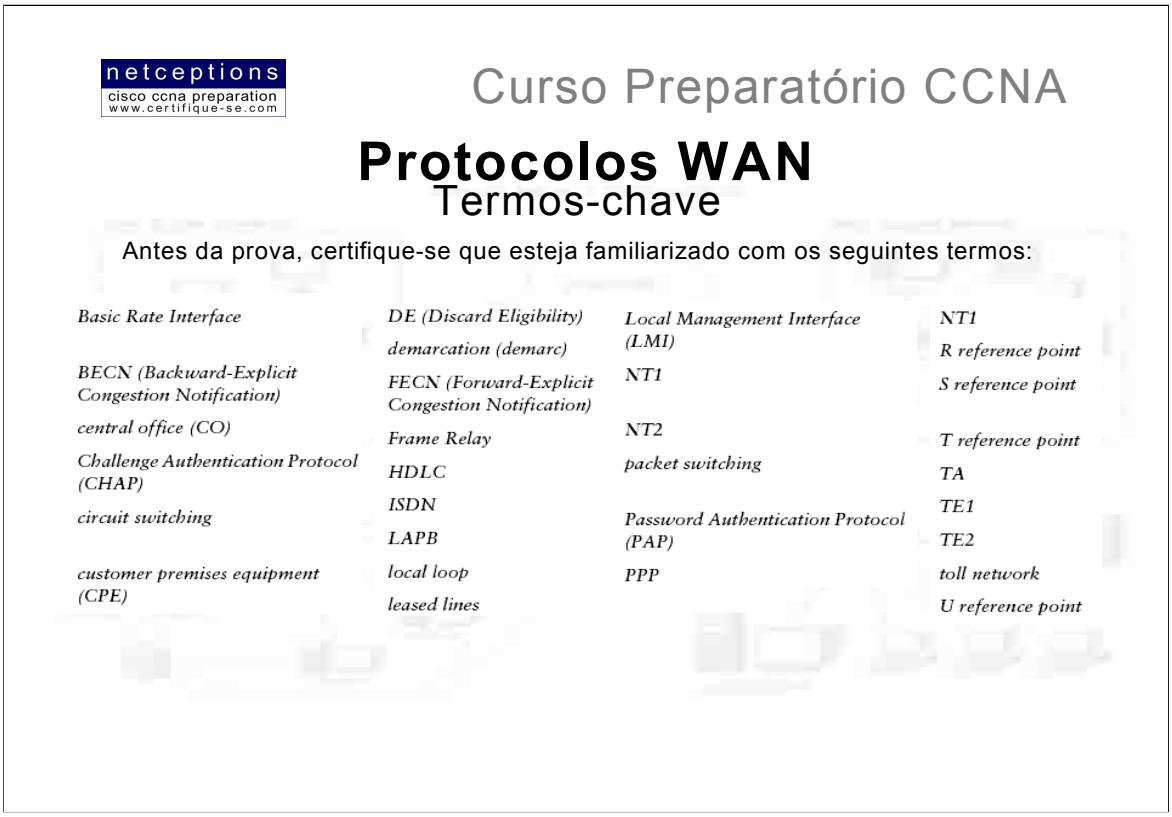
Limpa a interface e efetua a desconexão. Efetuar um comando **shutdown** na interface provê o mesmo resultado..

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Relação dos comandos analisados:

Comando	Descrição
debug dialer	Apresenta as atividades inerentes ao estabelecimento e encerramento de ligações
debug frame-relay lmi	Apresenta o fluxo lmi entre um router e um switch Frame Relay
debug isdn q921	Apresenta processos de camada 2
debug isdn q931	Apresenta processos de camada 3
dialer idle-timeout {valor}	Informa a linha BRI para efetuar a desconexão caso tráfego interessante deixe de fluir
dialer list	Especifica tráfego interessante para um link DDR
dialer load-threshold	Define parâmetros para ativar a segunda linha BRI
dialer map	Utilizado no lugar do comando dialer-string para prover mais segurança
dialer-string	Define o número à ser chamado por uma interface ISDN
encapsulation frame-relay	Muda o encapsulamento para Frame-Relay em uma interface serial
encapsulation frame-relay ietf	Muda o encapsulamento para ietf, permitindo a interconexão entre routers Cisco e de outros fabricantes
encapsulation hdlc	Reestabelece o encapsulamento default (HDLC) em um link serial
encapsulation ppp	Altera o encapsulamento em um link serial para PPP
frame-relay interface-dlci	Configura o endereço PVC em uma interface ou subinterface serial
frame-relay lmi-type	Configura o tipo do LMI em um link serial
frame-relay map	Cria mapas PVC-para-IP estáticos
interface s0.16 multipoint	Cria uma interface multiponto em um link serial
interface s0.16 point-to-point	Cria uma interface ponto-à-ponto em um link serial
isdn spid1	Define o número que identifica o primeiro canal ao switch ISDN
isdn spid2	Define o número que identifica o segundo canal ao switch ISDN
isdn switch-type	Define o tipo de switch ISDN com o qual o router irá se comunicar
no inverse-arp	Desativa o recurso IARP para a configuração estática de mapas Frame Relay
ppp authentication chap	Informa PPP para usar o método de autenticação CHAP
ppp authentication pap	Informa PPP para usar o método de autenticação PAP
show dialer	Apresenta o número de vezes que um dialer string foi usado, os valores timeout de cada canal B, a duração da chamada e o nome do router à qual a interface se encontra conectada.
show frame-relay lmi	Define o tipo do LMI em uma interface serial
show frame-relay map	Apresenta o mapeamento IP/IPX-para-PVC estático e dinâmico
show frame-relay pvc	Apresenta os PVCs configurados e respectivos DLCIs
show ip route	Apresenta a tabela de roteamento IP
show isdn active	Apresenta o número chamado e o status da chamada
show isdn status	Efetua a checagem do SPID e a comunicação router-switch ISDN
username {nome} password {pwd}	Cria usernames e senhas para autenticação em um router Cisco



Resumo da aula 7-b:

Neste módulo, cobrimos os seguintes tópicos:

• A diferença entre os diversos serviços WAN (LAPB, Frame Relay, ISDN, SDLC, HDLC e PPP)
• Termos e conceitos Frame Relay e X.25
• Configuração de Frame Relay LMIs, mapas e subinterfaces
• Monitoramento Frame Relay em um router
• Identificação de operações PPP
• ISDN Networking
• Protocolos, grupos funcionais, pontos de referência e canais ISDN
• Implementação ISDN BRI de acordo com a Cisco

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

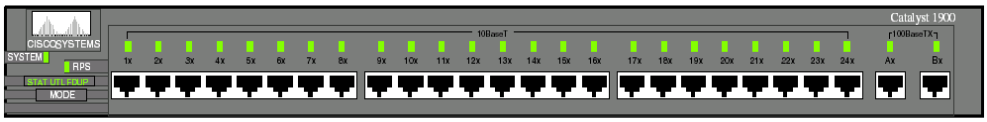
FIM AULA 07

Apostila Aula 8

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Aula 8 / Configurando o Switch Catalyst 1900



O switch Cisco Catalyst 1900

O switch Catalyst 1900 é um modelo básico dentro da família Catalyst da Cisco. Existem 2 modelos dentro dessa linha: 1912 e 1924. O modelo 1912 possui 12 portas 10BaseT, enquanto que o 1924 possui 24. Ambos apresentam 2 portas uplink de 100Mbps, para tanto cabos UTP quanto para fibra.

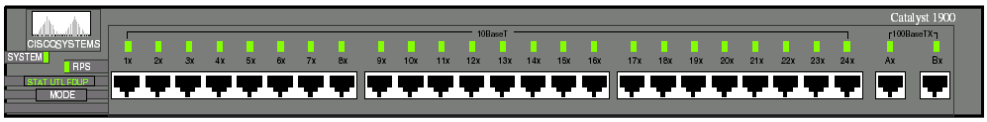
Nem todos os switches Cisco rodam o sistema IOS. Nesta aula, analisaremos como inicializar e configurar um switch Catalyst 1900 via linhas de comando (CLI). Começaremos com a conexão do cabo console, e com o que acontece assim que um switch é inicializado. Após o aprendizado dos comandos básicos, ilustraremos como configurar VLANs, roteamento ISL e VTP em um switch. Os comandos que cobriremos incluem os seguintes:

- Definição de senhas
- Configuração do hostname
- Configuração de endereços IP e máscaras de rede
- Identificação de interfaces
- Configuração uma descrição para as interfaces
- Definição da porta duplex
- Verificação da configuração
- Gerenciamento da tabela de endereçamento MAC
- Definição de endereços MAC permanentes e estáticos
- Configuração de segurança em portas
- Descrição do comando show version
- Alterando o tipo de LAN switch
- Configuração de VLANs
- Adição de VLAN memberships às portas do switch
- Criação de um domínio VTP
- Configuração de trunking
- Configuração de pruning

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Configurando o Switch Catalyst 1900



O switch Cisco Catalyst 1900

Recursos do switch 1900

A linha 1900 permite a configuração via CLI, até então a configuração do mesmo era feita apenas através de um sistema de menus. Existem 2 tipos de sistemas operacionais que podem rodar em switches Cisco:

IOS-Based: Nesse caso, o processo de configuração do switch é muito similar ao do router. Switches Catalyst 1900, 2820 e 2900 podem ser configurados tanto via IOS quanto via menus.

Set-based: Esse sistema usa uma série de comnado CLI mais antigos. Os switches que são configurados via CLI set-based são: 2926, 1948G, linhas 4000, 5000 e 6000.

Estaremos nos concentrando na linha 1900, pois o Catalyst 1900 é o switch que é abrangido nas questões do exame CCNA 2.0.

A linha Catalyst adota uma interface de configuração muito similar ao IOS, que já vimos. A diferença é que ele pode ser configurado via Web, utilizando um recurso chamado VSM (Visual Switch Manager). Para configurar o switch através do VSM, basta digitar o endereço IP da switch no web-browser de sua preferência. Configuração via sistema de menus também é possível. Para configuração do switch via Telnet ou web, o mesmo precisa ter um enedereço IP configurado.

Conexão à porta console

A linha 1900 possui uma porta console em sua parte traseira, semelhante aos routers da linha 2500. Trata-se de uma porta RJ-45 para conexão ao terminal. Uma vez conectado o cabo ao switch e ao terminal, é necessário inicializar um programa emulador de terminal, como o Hyper-Term, do Windows. Eis as configurações para esse programa:

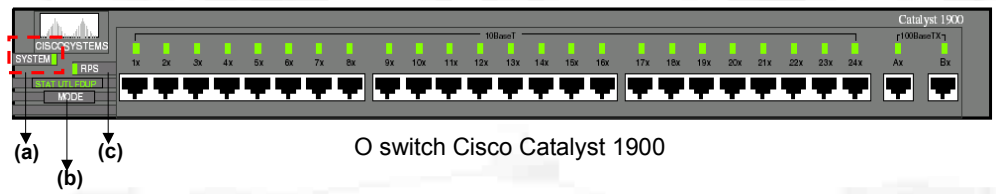
- 9600bps
- 8 Data Bits
- Parity None
- Stop Bits 1
- Flow Control None

***NUNCA** conecte um cabo ethernet, ISDN ou telefônico à porta console de um switch. Isso pode danificá-lo.*

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Configurando o Switch Catalyst 1900



O switch Cisco Catalyst 1900

Inicialização do switch

Antes de inicializar um switch, certifique-se do seguinte:

- Todos os cabos de rede encontram-se firmemente conectados
- O terminal encontra-se conectado à porta console
- O software emulador do terminal encontra-se corretamente configurado

Uma vez que tudo esteja OK, ligue o switch e observe a sequência dos leds.

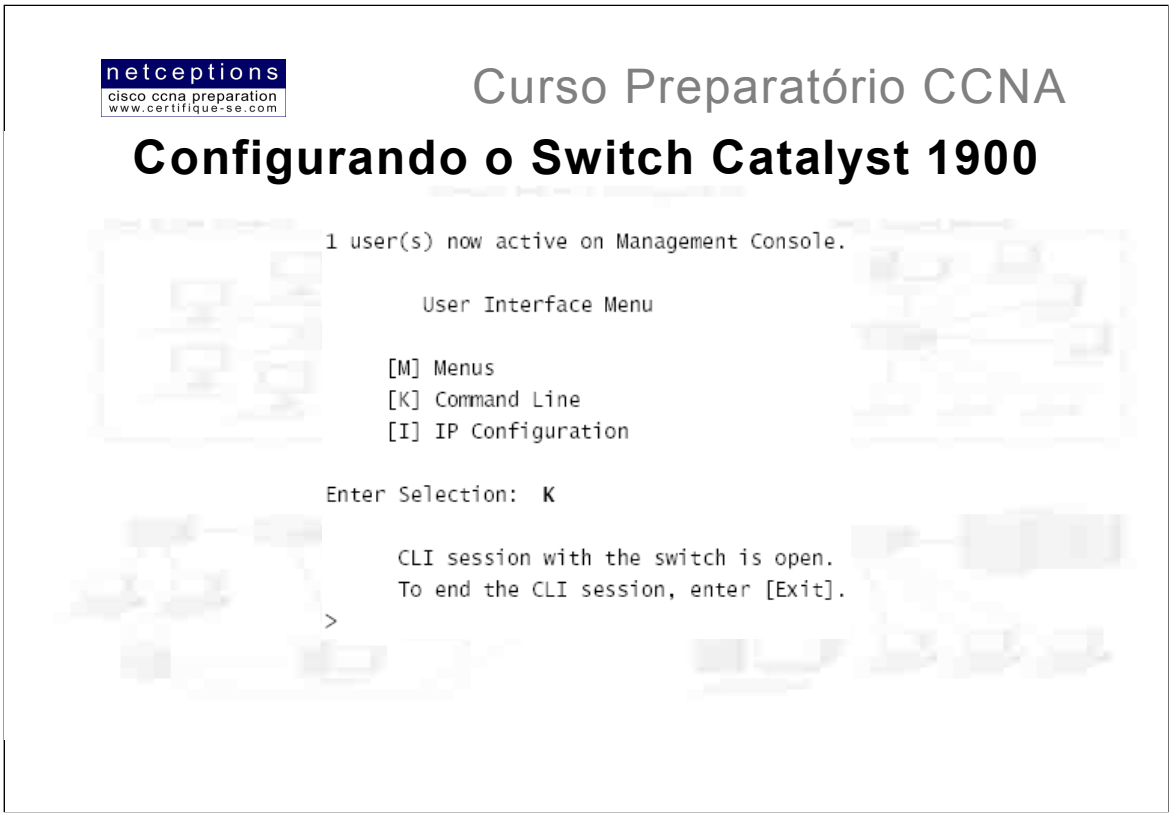
Uma luz verde aparece ao lado da palavra SYSTEM **(a)** assim que o sistema encontrar-se operacional. Caso um problema ocorra, a cor será âmbar (alaranjado). O LED RPS **(c)** apenas encontrar-se-à ativo na existência de uma fonte de alimentação redundante (chamada RPS - Redundant Power Supply). O único botão existente é o botão MODE **(b)**. Ao pressioná-lo você pode ver os 3 diferentes status dos LEDs do switch:

Stat: Indica o status das portas. Verde = dispositivo conectado ao switch / Verde Piscante = atividade na porta / âmbar = falha de comunicação na porta.

UTL: Indica a largura de banda do switch. Em um switch 1912, por exemplo, ao se pressionar o botão mode e os LEDs das portas 1 à 4 se ativam, isso significa que uma largura de banda entre 0.1 e 1.5Mbps está sendo consumida. Caso os LEDS das portas 5 à 8 se ativem, uma utilização de banda entre 1.5 e 20Mbps está ocorrendo. LEDS das portas 9 à 12: 20 à 120Mbps de utilização.

FDUP: Apresenta as portas do switch configuradas em full duplex.

Assim que um switch é inicializado, ele entra em modo de teste (POST). No início, todos os LEDs encontram-se verdes. Esses LEDs são apagados após o final do modo POST. Caso uma porta seja identificada como falha durante o POST, ambos os LEDs SYSTEM e da porta em questão mudam a cor para âmber. Caso nenhuma falha seja identificada, todos os LEDS piscam e, em seguida, se apagam.



Após o POST, caso você tenha um terminal conectado ao switch, o menu acima é apresentado. Selecionando “K” disponibiliza a interface de linha de comando (CLI). Optando por “M” você pode configurar o switch através do sistema de menus. “I” permite que um IP seja designado ao switch. Entretanto, isso também pode ser feito através das 2 opções anteriores.

A linha 1900 possui portas do tipo fixas, ou seja, não há como alterar suas características através de módulos. A linha 1900 disponibiliza portas 10BaseT para conexão à workstations e 2 portas 100BaseT ou FX para uplinks (conexão com outros switches). Para conectar 2 switches através das portas uplink, um cabo crossover deve ser utilizado. Para conexão de um switch com routers, workstations, servidores, impressoras, etc, utilize um cabo straight-through.

Assim que um dispositivo é conectado à uma porta do switch, o LED correspondente se ativa, e assim permanece. Caso o LED não se ative, pode haver um problema com a outra ponta, ou com o cabo utilizado. Caso o LED se ative e desative, pode haver um problema de auto-speed e duplex. Alaremos disso mais adiante.

O conhecimento desta lista é muito importante para o exame CCNA. Sem os conhecimentos acima, será muito difícil avançarmos para configurações mais complexas.

Definindo senhas de modo usuário e privilegiado

Senhas em um switch são configuradas de modo diferente do que em um router. Você utiliza o comando enable password, o mesmo para um router, porém, você pode definir diferentes níveis de acesso. O mesmo comando é utilizado para definir senhas de modo usuário e privilegiado. Porém, os diferentes níveis designados determinam o tipo de acesso.

Eis um exemplo de como se configurar ambas as senhas em um switch:

```
(config)#enable password level 1 todd      (a)
(config)#enable password level 15 todd1    (b)
(config)#exit
```

Para configurar uma senha de modo usuário, utilize o nível 1 **(a)**. Para modo privilegiado, nível 15 **(b)**. As senhas devem ter uma extensão entre 4 e 8 caracteres.

NOTA: Senhas de switches devem ser lembradas, e muito bem guardadas pois, ao contrário de routers, não há como recuperá-las uma vez perdidas.

Para configurar a senha **enable secret**, proceda do mesmo modo que em um router:

```
(config)#enable secret todd2
```

A senha **enable secret** é mais segura e supersede a senha **enable**, ou seja, caso a senha **enable secret** esteja configurada, não se preocupe em configurar a senha **enable**.

Outro detalhe: senhas em switches não são “case-sensitive”, ou seja, não importa se você as digita como maiúsculas ou minúsculas.

Configuração do hostname

A configuração do hostname é feita exatamente da mesma maneira que em um router:

```
#config t
Enter configuration commands, one per line. End with
CNTL/Z
(config)#hostname Todd1900EN
Todd1900EN(config)#
```

Configuração do endereço IP

Não é obrigatória a configuração de um endereço IP para o switch, porém, se você deseja dispor do recurso de configurá-lo remotamente através de um web browser ou via Telnet, um IP precisa ser configurado. Outra razão para configuração de um endereço IP em um switch seria se voc6e desejasse configurá-lo com diferentes VLANs e outras funcionalidades de rede. Abaixo a configuração default de um switch Catalyst 1900:

```
IP address and default gateway: 0.0.0.0
CDP: Enabled
Switching Mode: FragmentFree
100BaseT ports: Auto-negotiate duplex mode
10BaseT ports: Half duplex
Spanning Tree: Enabled
Console password: Not set
```

Para configurar o endereço IP e default gateway em um switch, utilize os comandos abaixo ilustrados:

```
Todd1900EN#config t
Enter configuration commands, one per line. End with
CNTL/Z
Todd1900EN(config)#ip address 172.16.10.16 255.255.255.0
Todd1900EN(config)#ip default-gateway 172.16.10.1
Todd1900EN(config)#
```

Configuração de interfaces

É importante saber como acessar as portas de um switch. O switch 1900 usa a sintaxe {tipo} {slot}/{porta}, ou seja, Ethernet 0/3 referencia a porta 3 - 10BaseT. Outro exemplo seria FastEthernet 0/26, referenciando a primeira das 2 portas fastethernet (uplinks) disponíveis em um switch. O switch 1900 possui apenas um slot (0).

No caso do modelo 1912, apenas as portas de 1 à 12 existem (e as portas 26 e 27, os uplinks). Porém, existe uma porta 25 na parte traseira deste switch. Essa porta, chamada de AUI (Attachment Unit Interface) é usada para conectar um switch à outro, ou mesmo para conectá-lo à uma rede coax Ethernet.

Para configurar uma interface em um switch 1900, basta ir ao modo de configuração global e utilizar o comando **`interface`**. Descrevemos o processo abaixo:

```
Todd1900EN(config)#int ethernet 0/?
<1-25> IEEE 802.3
Todd1900EN(config)#int ethernet 0/1
```

No exemplo acima, o comando help (?) nos mostra 25 portas disponíveis (1-25). Essa mensagem seria a mesma para um switch 1912, que possui apenas 12 portas (1-12), a porta 25 na parte traseira e as portas 26 e 27 (uplinks). Um pequeno "deslize" da Cisco...! As portas 26 e 27 não aparecem listadas como uma opção por se tratarem de portas FastEthernet. No caso, nossa opção foi Ethernet, apenas.

Uma vez que você se encontre no modo de configuração de interface (**`config-if`**), você pode utilizar o comando help (?) para verificar uma lista dos comandos disponíveis. Dentre elas, temos: **`cdp`**, **`description`**, **`duplex`**, **`exit`**, **`help`**, **`port`**, **`shutdown`**, **`spantree`** e **`vlan-membership`**.

Configuração FastEthernet

Para configurar as portas 26 e 27, utilize o comando **int**, porém, informando agora interface FastEthernet:

```
Todd1900EN(config)#int fastEthernet 0/?
<26-27> FastEthernet IEEE 802.3
Todd1900EN(config)#int fastEthernet 0/26
```

Configuração de descrições nas interfaces

Mais uma vez, o modo de efetuar esse procedimento copia o modo como o mesmo é feito em routers:

```
Todd1900EN(config)#int e0/1
Todd1900EN(config-if)#description Finance_VLAN
Todd1900EN(config-if)#int f0/26
Todd1900EN(config-if)#description trunk_to_Building_4
Todd1900EN(config-if)#
```

Espaços não são permitidos nas strings de descrição. Use “underscore”, no lugar, como no exemplo acima.

Para visualizar as descrições, utilize o comando **sh int** (ex: **sh int e0/1**)

Configuração de porta duplex

O comando duplex pode ser aplicado somente em switches 1900, pois todas as portas do mesmo possuem velocidade fixa. A seguir, ilustramos como proceder:

```
Todd1900EN(config)#int f0/26
Todd1900EN(config-if)#duplex ?
auto Enable auto duplex configuration
full Force full duplex operation
full-flow-control Force full duplex with flow control
half Force half duplex operation
Todd1900EN(config-if)#duplex full
```

A tabela abaixo apresenta as diferentes opções duplex disponíveis em switches 1900. As portas FastEthernet são auto-duplex, por default, o que significa que tentarão detectar o tipo de duplex configurado na outra ponta. Isso pode ou não funcionar. Uma boa regra é configurar as portas FastEthernet como half-duplex.

Parâmetro	Definição
Auto	Aplica à porta o modo de auto-configuração. Default para toda as portas 100BaseTX
Full	Força as portas 10 ou 100Mbps para modo full-duplex
Full-flow-control	Funciona apenas em portas 100BaseTX. Usa controle de fluxo para que não haja sobrecarga nos buffers
Half	Default para portas 10BaseT. Força as portas para funcionarem em modo half-duplex.

Uma vez que o modo duplex esteja definido, você pode usar o comando show int para verificar sua configuração:

```
Todd1900EN#sh int f0/26
FastEthernet 0/26 is Suspended-no-linkbeat
Hardware is Built-in 100Base-TX
Address is 0030.80CC.7D1A
MTU 1500 bytes, BW 100000 Kbits
802.1d STP State: Blocking Forward Transitions: 0
Port monitoring: Disabled
Unknown unicast flooding: Enabled
Unregistered multicast flooding: Enabled
Description: trunk_to_Building_4
Duplex setting: Full duplex
Back pressure: Disabled
```

Verificando a conectividade IP

É importante sempre testar a configuração IP de qualquer dispositivo de rede. Switches não fogem à regra. Ping e Telnet, como sempre, são 2 das melhores ferramentas para se utilizar nesse caso. Entretanto, você **NÃO PODE** efetuar um Telnet ou um comando **`traceroute`** de um switch. Você pode efetuar um Telnet ou traceroute **PARA** um switch (desde que seu IP encontre-se devidamente configurado), mas nunca **DE** um (NOTA: ISSO COSTUMA CAIR NO EXAME CCNA!). Veja o exemplo abaixo:

Todd1900EN#**ping 172.16.10.10**
Sending 5, 100-byte ICMP Echos to 172.16.10.10, time out
is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max
0/2/10/ ms
Todd1900EN#**telnet 172.16.10.10**
^
% Invalid input detected at '^' marker.

Notou o que ocorre quando tentamos usar o comando telnet de um switch?

Deletando a configuração de um switch

A configuração de um switch, assim como a de um router, encontra-se armazenada na NVRAM. Não há, entretanto, como verificar o conteúdo da NVRAM em um switch. Apenas o conteúdo da RAM (running-config). Quando você efetua alterações na running-config de um switch, ele automaticamente armazena essas alterações na NVRAM, ou seja, não há necessidade de utilizar o comando **`copy run start`** em um switch. O conteúdo da NVRAM de um switch pode ser apagado. Para deletar o conteúdo da NVRAM em um switch, utilize o comando **`delete nvram`** (**ATENÇÃO**! ISSO SEMPRE CAI NO EXAME CCNA - UMA TENTATIVA DE CONFUNDI-LO COM O COMANDO **`erase start`**, USADO EM ROUTERS!). Veja exemplo abaixo:

```
Todd1900EN#delete ?
nvram NVRAM configuration
vtp Reset VTP configuration to defaults
Todd1900EN#delete nvram
This command resets the switch with factory defaults. All
system parameters will revert to their default factory
settings. All static and dynamic addresses will be
removed.
Reset system with factory defaults, [Y]es or [N]o? Yes
```

Gerenciamento da tabela de endereços MAC

Switches fazem a filtragem da rede através dos endereços de hardware (MAC) dos dispositivos. Switches criam tabelas MAC que incluem endereços dinâmicos, permanentes e estáticos. A tabela-filtro é gerada conforme hosts enviam frames com dados sobre seus endereços de hardware. Os switches, então, armazenam esses dados em suas tabela-filtro, relacionando-os com o segmento e porta onde foram recebidos.

Os switches estão adicionando novos endereços MAC continuamente às suas tabelas-filtro. Conforme hosts são adicionados ou removidos da rede, os switches dinamicamente atualizam suas tabelas-filtro. Caso um dispositivo seja removido da rede, ou perca o contato com um switch por muito tempo, seus dados na tabela-filtro do switch irão “expirar” após um período pré-determinado de tempo. A tabela-filtro de um switch pode ser visualizada através do comando show mac-address-table, conforme ilustramos abaixo:

```
Todd1900EN#sh mac-address-table
Number of permanent addresses : 0
Number of restricted static addresses : 0
Number of dynamic addresses : 4
Address Dest Interface Type Source
Interface List
00A0.246E.0FA8 Ethernet 0/2 Dynamic All
0000.8147.4E11 Ethernet 0/5 Dynamic All
0000.8610.C16F Ethernet 0/1 Dynamic All
00A0.2448.60A5 Ethernet 0/4 Dynamic All
```

Os endereços na tabela apresentada anteriormente são de 4 dispositivos conectados ao switch. Todos foram dinâmicamente inseridos, o que significa que o switch verificou o endereço de origem do frame assim que o mesmo atravessou a interface, e o inseriu em sua tabela MAC. Caso a tabela MAC se sobrecarregue e atinja sua capacidade de armazenamento, o switch irá propagar todos os novos endereços recebidos até que um dos armazenados em sua tabela "expire".

A tabela MAC de um switch pode ser apagada completamente através do comando **clear mac-address-table:**

```
#clear mac-address-table ?
dynamic Clear 802.1d dynamic address
permanent Clear 802.1d permanent addresses
restricted Clear 802.1d restricted static address
<cr>
```

Configuração de endereços MAC estática e dinamicamente

Administradores podem configurar endereços permanentes à porta de um switch. Endereços permanentes jamais expiram. Um dos motivos para se adotar a configuração de endereços permanentes em uma determinada porta é prover segurança à mesma pois, a menos que um endereço de hardware específico seja configurado à porta, essa não funcionará. Isso evita que usuários simplesmente "pluguem" dispositivos ao switch sem o consentimento do administrador. Administradores podem também criar entradas permanentes na tabela MAC, manualmente. Essas entradas na tabela criam um caminho para um endereço hardware de origem. Como isso pode ser muito restritivo, você deve ser cuidadoso ao criar entradas estáticas pois, caso a configuração não seja bem feita, você pode estar desativando o switch.

Configuração de endereços MAC permanentes

Endereços MAC permanentes podem ser configurados em uma porta de switch através do comando **mac-address-table [endereço MAC] [interface]**. Veja o exemplo abaixo:

```
Todd1900EN#config t
Enter configuration commands, one per line. End with CNTL/Z
Todd1900EN(config)#mac-address-table ?
aging-time Aging time of dynamic addresses ---------->       (permite alterar o tempo que um
                                                             endereço MAC permanece na tabela
                                                             até que seja expurgado)

permanent Configure a permanent address ------------>       (Define um endereço permanente
                                                             para a interface. Caso o usuário
                                                             mude o cartão de rede (NIC), o
                                                             host não funcionará até que o
                                                             endereço aqui configurado seja
                                                             alterado)

restricted Configure a restricted static address --->       (Esse parâmetro é usado com o
                                                             comando para definir um caminho
                                                             para os endereços de hardware de
                                                             origem. Restringe muito para onde
                                                             o host pode enviar frames)
```

Uma vez escolhida a opção, adicione o endereço de hardware e a interface associada ao mesmo. Isso irá restringir a interface para aceitar apenas frames que originem desse endereço de hardware:

```
Todd1900EN(config)#mac-address-table permanent ?
H.H.H 48 bit hardware address
Todd1900EN(config)#mac-address-table permanent 00A0.2448.60A5 e0/4
```

Para verificar suas configurações, utilize o comando **show mac-address-table**.

Configuração de endereços MAC estáticos

Podemos levar o assunto segurança um passo adiante. Podemos informar uma interface de origem para apenas enviar frames para uma interface específica. Para isso, utilizamos o comando **`restricted static`**. O comando precisa que 2 parâmetros sejam informados: o endereço de hardware da interface destino e a interface origem que estará habilitada a se comunicar com a mesma. Veja exemplo a seguir:

```
Todd1900EN(config)#mac-address-table restricted static 00A0.246E.0FA8 e0/2 e0/5
```

No exemplo acima, determinamos que a interface 0/5 pode enviar frames apenas para a interface 0/2, utilizando o endereço de hardware 00A0.246E.0FA8. Lembre-se que entradas na tabela podem ser individualmente apagadas através do comando **`clear mac-address-table [dynamic/static/restricted] [interface destino] [interface origem]`**.

Configuração de segurança em portas

Segurança em portas (port security) é um modo de se evitar que usuários conectem um dispositivo ao switch sem que o administrador tenha conhecimento. Por default, 132 endereços de hardware podem ser permitidos em uma única interface de um switch. Isso pode ser alterado através do comando **`port secure max-mac-count`**, conforme exemplo abaixo:

```
Todd1900EN#config t
Enter configuration commands, one per line. End with CNTL/Z
Todd1900EN(config)#int e0/2
Todd1900EN(config-if)#port secure ?
max-mac-count Maximum number of addresses allowed on the port
<cr>
Todd1900EN(config-if)#port secure max-mac-count ?
<1-132> Maximum mac address count for this secure port
Todd1900EN(config-if)#port secure max-mac-count 1
```

As portas seguras criadas podem usar tanto endereços de hardware estáticos como endereços “assimilados” (sticky-learns). Sticky-learns é o processo definido pela Cisco para uma porta encontrar dinamicamente o endereço de hardware origem e, automaticamente, criar uma entrada permanente na tabela de filtragem MAC.

Utilizando o comando `show version`

O comando **`show version`** pode ser utilizado na visualização de informações básicas sobre o switch. Essas informações incluem o tempo de utilização do switch, a versão do IOS, e o endereço MAC do switch em si.

Alteração do tipo de LAN switching

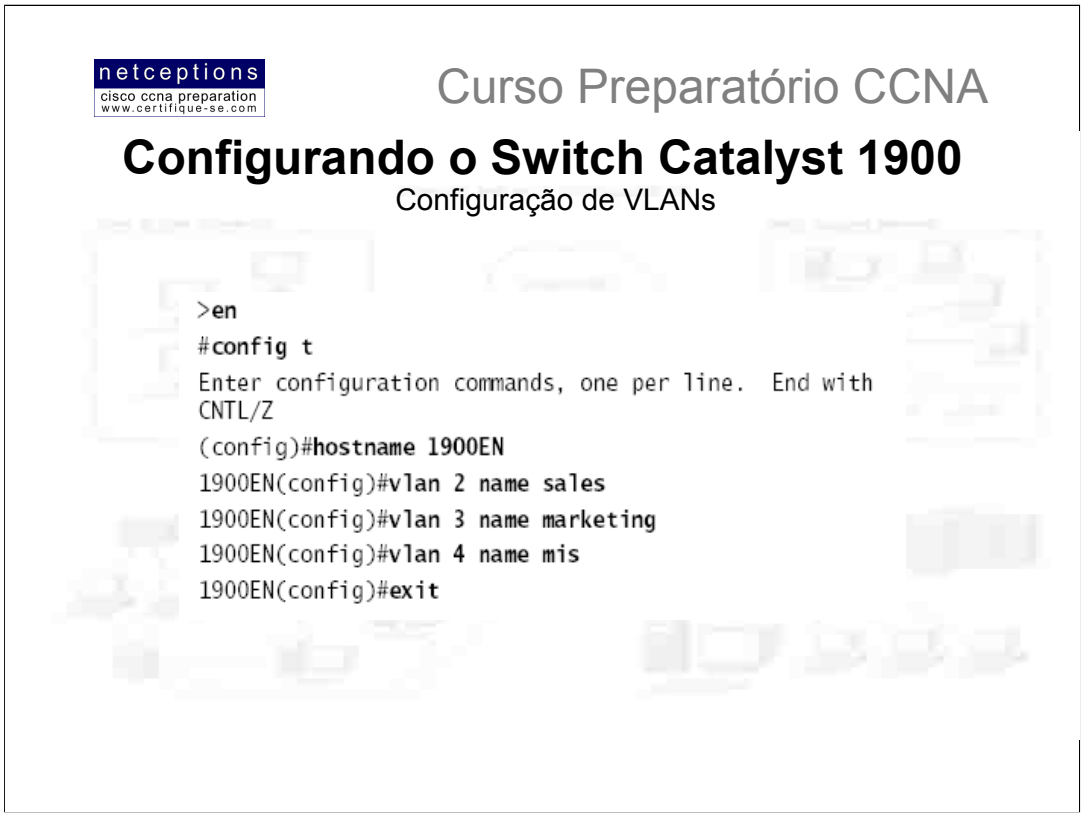
Você pode visualizar a versão de LAN switching ativa em seu switch através do comando **`show port system`**. Este pode ser alterado à partir do modo de configuração global através do comando **`switching-mode`**. Os únicos modos permitidos são FragmentFree e store-and-forward. O modo default é FragmentFree. Eis um exemplo da saída do comando **`show port system`**:

```
1900EN#sh port system
Switching mode: FragmentFree
Use of store and forward for multicast: Disabled
Network port: None
Half duplex backpressure (10 Mbps ports): Disabled
Enhanced Congestion Control (10 Mbps ports): Disabled
Default port LED display mode: Port Status
```

E um exemplo do comando **`switching-mode`**:

```
1900EN(config)#switching-mode ?
fragment-free Fragment Free mode
store-and-forward Store-and-Forward mode
```

Se você alterar o tipo de LAN switching, essa alteração afetará todas as portas ativas do switch.



A configuração de VLANs, ao contrário do que se possa imaginar, é direta e descomplicada. A parte complicada é entender quais usuários devem ser alocados em cada VLAN. Uma vez definido o número de VLANs à serem criadas e os usuários participantes em cada uma, a VLAN pode ser criada sem problemas. Em um switch da linha 1900, até 64 VLANs podem ser criadas. Uma diferente ocorrência do spanning tree pode ser configurado em cada VLAN criada.

Para configurar VLAN em um switch via IOS, utilize o comando **`vlan [número da VLAN] name [nome da VLAN]`**. Acima ilustramos um exemplo da criação de 3 VLANs para 3 diferentes departamentos (sales, marketing e mis). Uma vez criadas as VLANs desejadas, as mesmas podem ser verificadas através do comando **`show vlan`**. Por default, todas as portas do switch encontram-se configuradas para a VLAN 1. Para alterar a VLAN associada à uma porta, você deve acessar cada interface e informar de qual VLAN ela será parte.

Uma vez criadas as VLANs, você deve definir quais portas farão parte de cada uma. Você pode configurar cada porta do switch para participar de uma VLAN através do comando **`vlan-membership`**. A configuração deve ser feita porta-à-porta. Lembre-se que você pode configurar associações estáticas ou dinâmicas em uma porta. Para o exame CCNA, apenas associações estáticas são abrangidas. Abaixo ilustramos a associação da interface 2 à VLAN 2, interface 4 à VLAN 3, e interface 5 à VLAN 4:

```
1900EN#config t
Enter configuration commands, one per line. End with CNTL/Z
1900EN(config)#int e0/2
1900EN(config-if)#vlan-membership ?
dynamic Set VLAN membership type as dynamic static Set VLAN membership type as static
1900EN(config-if)#vlan-membership static ?
<1-1005> ISL VLAN index
1900EN(config-if)#vlan-membership static 2
1900EN(config-if)#int e0/4
1900EN(config-if)#vlan-membership static 3
1900EN(config-if)#int e0/5
1900EN(config-if)#vlan-membership static 4
```

Para verificar sua configuração, utilize o comando **`sh vlan`**. Outro comando que pode ser usado para verificação de VLANs é o **`sh vlan-membership`**. Esse comando apresenta cada porta do switch, de qual VLAN cada porta é membro, e o tipo de associação (estática ou dinâmica).

Configuração de portas de transporte

A linha 1900 de switches roda o método de encapsulamento DISL (Dynamic Inter-Switch Link). Para configurar uma porta FastEthernet para agir como um trunk link, utilize o comando **`trunk [parâmetro]`** na interface FE desejada. Abaixo ilustramos um exemplo de utilização deste comando:

```
1900EN#config t
Enter configuration commands, one per line. End with
CNTL/Z
1900EN(config)#int f0/26
1900EN(config-if)#trunk ?
auto Set DISL state to AUTO
desirable Set DISL state to DESIRABLE
nonegotiate Set DISL state to NONEGOTIATE
off Set DISL state to OFF
on Set DISL state to ON
1900EN(config-if)#trunk on
```

Onde:

Auto = A interface será de transporte apenas se o dispositivo conectado à mesma encontrar-se configurado como “on” ou “desirable”.

Desirable = Caso o dispositivo conectado à interface encontre-se configurado como “on”, “desirable”, ou “auto”, será negociada a conversão do link para link de transporte.

Nonegotiate = A interface tornar-se-à uma porta de transporte ISL em caráter permanente, e não negociará com nenhum dispositivo conectado.

Off = A interface será impossibilitada de agir como porta de transporte.

On = A interface tornar-se-à uma porta de transporte ISL em caráter permanente, porém, poderá negociar com o dispositivo conectado para conversão do link para link de transporte.

Todas as VLANs encontram-se na porta de transporte configurada, por default. Para permitir apenas determinadas VLANs em um link de transporte, as VLANs indesejadas devem ser manualmente deletadas (cleared) **(ATENÇÃO!!! ISSO COSTUMA CAIR NO EXAME CCNA!)**

Utilize o comando **`clear trunk`** para impedir que informações relativas à VLANs sejam transmitidas através do link de transporte (trunk link). Existem 2 razões pelas quais você gostaria de fazer isso: Você não deseja que broadcasts de uma determinada VLAN atravesse o link de transporte, ou porque você deseja evitar que informações sobre alterações na topologia sejam propagadas através de um link onde a VLAN em questão não é suportada.

Para deletar VLANs de um link de transporte em um switch 1900, utilize o comando **`no trunk-vlan [número da VLAN]`**.

No exemplo abaixo, deletamos a VLAN 5 do link de transporte:

```
1900EN(config-if)#no trunk-vlan ?
<1-1005> ISL VLAN index
1900EN(config-if)#no trunk-vlan 5
1900EN(config-if)#
```

Esse procedimento deve ser feito para cada VLAN que não deva ter suas informações transportadas através do link de transporte.

Verificação de links de transporte

Para verificar suas portas de transporte, utilize o comando show trunk. No caso de haver mais de uma porta de transporte e você deseje apenas visualizar as estatísticas de uma porta específica, utilize o parâmetro [número da porta] em conjunto com o comando. No switch 1900, a porta FastEthernet0/26 é identificada como trunk A, e a porta FastEthernet0/27 é identificada como trunk B. O exemplo abaixo ilustra as VLANs permitidas (allowed) na porta de transporte 0/26:

```
1900EN#sh trunk ?
A Trunk A
B Trunk B
1900EN#sh trunk a ?
allowed-vlans Display allowed vlans
joined-vlans Display joined vlans
joining-vlans Display joining vlans
prune-eligible Display pruning eligible vlans
<cr>
1900EN#sh trunk a allowed-vlans
1-4, 6-1004
1900EN#
```

Como excluímos a VLAN 5 anteriormente, a mesma não aparece na saída do comando acima.

Configuração de roteamento ISL

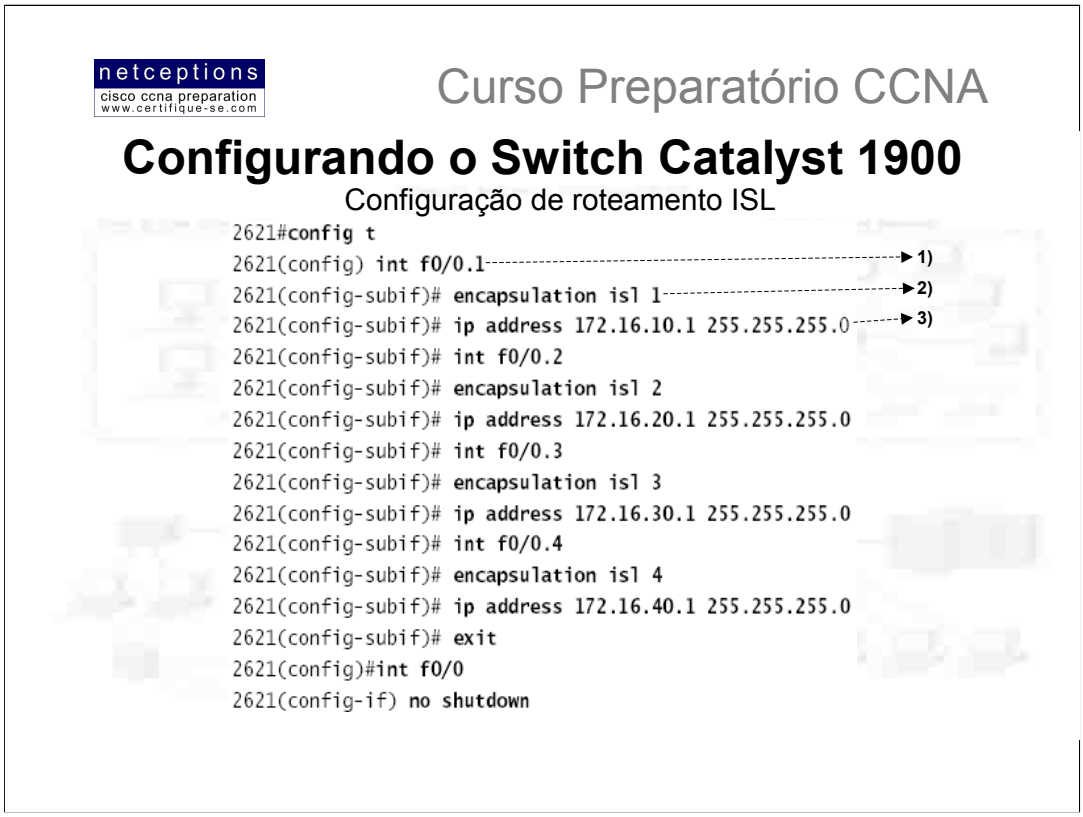
Para ser capaz de suportar roteamento ISL em uma interface FastEthernetde um router, essa interface é dividida em uma série de interfaces lógicas, uma para cada VLAN. Essas são conhecidas como subinterfaces. Como temos 4 VLANs (de nossos exemplos anteriores), precisamos de 4 subinterfaces. Cada VLAN é uma subrede diferente, portanto, eis o endereçamento que estaremos adotando:

VLAN 1	default	172.16.10.0/24
VLAN 2	sales	172.16.20.0/24
VLAN 3	marketing	172.16.30.0/24
VLAN 4	mis	172.16.40.0/24

Cada host pertencente à cada uma destas VLANs deve usar o mesmo endereçamento de sub-rede. Para configurar o router para roteamento inter-VLAN, os 3 passos à seguir devem ser completados:

1. Ative ISL trunking na porta do switch conectada ao router
2. Ative encapsulamento ISL na subinterface do router
3. Defina um endereço IP à subinterface e um outro tipo de endereçamento lógico (IPX, por exemplo), se necessário.

A criação de subinterfaces já foi discutida anteriormente, portanto, não iremos repetir o procedimento aqui. Para configurar roteamento ISL em uma subinterface, utilize o comando **`isl [número da VLAN]`**. Você pode, então, definir um endereço IP, IPX, AppleTalk, etc, à subinterface. Por se tratar de uma única sub-rede, é aconselhável que todos os hosts nessa VLAN façam parte da mesma sub-rede. Na página seguinte ilustramos como proceder na configuração do router 2621 para que o mesmo suporte roteamento ISL para as 4 VLANs que definimos.



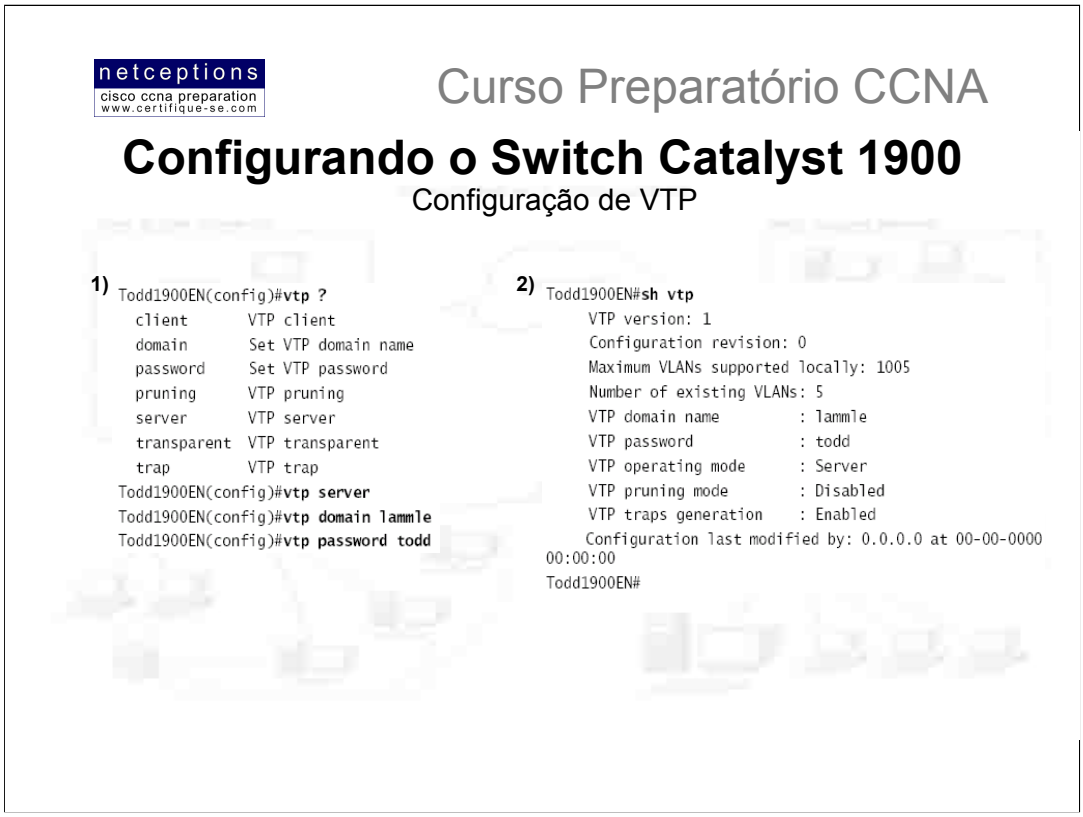
Eis o que fizemos:

1) Configuramos a subinterface com o mesmo número da VLAN que desejamos rotear. Isso possui significância local, somente, ou seja, os números das subinterfaces não importam para a rede.

2) Em seguida configuramos o método de encapsulamento (ISL)

3) E finalmente informamos o endereço IP e máscara de rede para a subinterface em questão. Note que o endereço IP definido para a subinterface deve pertencer ao intervalo válido da sub-rede em questão. No caso, a VLAN 1 possui endereço de rede 172.16.10.0, portanto, a subinterface 0/0.1 foi configurada com o endereço IP 172.16.10.1.

O mesmo é feito para as 3 VLANs restante. Note, no entanto, que cada subinterface se encontra em uma sub-rede diferente.



A linha 1900 - como todos os switches - vem configurada de fábrica para agir como um servidor VTP. Para configurar VTP, primeiro configure o nome de domínio que você deseja usar. Uma vez que a informação VTP encontre-se configurada no switch, ela deve ser verificada.

Quando se cria um domínio VTP, existe a opção de se definir um nome de domínio, senha, modo de operação e capabilidades de pruning do switch. Utilize o comando **`vtp`** em modo de configuração global para definir tais informações. No exemplo **(a)** acima, configuramos o switch como servidor VTP, o domínio VTP "lammle" e a senha VTP foi definida como "todd".

Uma vez que a configuração acima encontre-se finalizada, verifique-a através do comando **`show vtp`**, ilustrado acima **(b)**.

Adição de switches ao domínio VTP criado

A adição de switches ao domínio VTP deve ser feita com cautela. Se um switch for adicionado ao domínio com informações incorretas sobre VLAN, isso pode resultar na propagação da base de dados VTP através da rede com informações inconsistentes. A recomendação da Cisco é que se delete a base de dados VTP antes da adição de um switch ao domínio VTP. Vimos anteriormente como deletar a NVRAM de um switch. Esse procedimento, porém, NÃO deleta o banco de dados VTP. Para apagar a informação VTP configurada em um switch você deve utilizar o comando **`delete vtp`**. Abaixo exemplificamos o procedimento:

```
Todd1900EN#delete ?
nvram NVRAM configuration
vtp Reset VTP configuration to defaults
Todd1900EN#delete vtp
This command resets the switch with VTP parameters set to
factory defaults.
All other parameters will be unchanged.
Reset system with VTP parameters set to factory defaults,
[Y]es or [N]o? Yes
```

VTP Pruning

O exemplo abaixo ilustra como ativar VTP pruning em um switch 1900.Não há muito o que fazer. Lembre-se que, ativando VTP pruning em um servidor VTP, você estará ativando pruning para todo o domínio VTP.

```
Todd1900EN(config)#vtp ?
client VTP client
domain Set VTP domain name
password Set VTP password
pruning VTP pruning
server VTP server
transparent VTP transparent
trap VTP trap
Todd1900EN(config)#vtp pruning ?
disable Disable VTP pruning
enable Enable VTP pruning
Todd1900EN(config)#vtp pruning enable
Todd1900EN(config)#
```

Note que você ativa VTP pruning para o switch como um todo.

Recuperando ou atualizando o IOS em um switch Catalyst 1900

Você pode recuperar ou atualizar o IOS em um switch 1900, porém, não há um comando para efetuar o back-up da imagem do IOS do switch 1900 para um servidor TFTP. O comando para recuperar ou atualizar o IOS em um switch 1900 é:

```
1900B#copy tftp://192.168.0.120/cat1900EN_9_00.bin opcode
TFTP operation succeeded
1900B#
```

Onde **opcode** é o comando que informa ao router para transferir o arquivo para a memória FLASH do switch.

Efetuando back-up da configuração de um switch 1900

Para efetuar uma cópia de segurança do arquivo de configuração de um switch 1900 para um servidor TFTP, proceda conforme exemplo abaixo:

```
1900B#copy nvram tftp://192.168.0.120/conf-1900
Configuration upload is successfully completed
And here's an example of the output from the console of a TFTP host.
Wed June 01 14:16:10 2000: Receiving '1900en' file from
192.168.0.120 in ASCII mode
##
Wed Mar 01 14:16:11 2000: Successful.
```

Para restaurar a configuração acima, proceda conforme o exemplo abaixo:

```
1900B#copy tftp://192.168.0.120/conf-1900 nvram
TFTP successfully downloaded configuration file
```

CDP funciona com todos os dispositivos Cisco, incluindo o switch Catalyst 1900. A saída do comando show cdp em um switch 1900 é ilustrada acima **(a)**. Note que tanto o router quanto o switch possuem um CDP timer de 60 segundos, e um holdtime de 180 segundos. Isso significa que informações CDP recebidas de routers vizinhos serão mantidas por 180 segundos.

DECORE ESSES TIMERS! TANTO NOS ROUTERS QUANTO NOS SWITCHES! No exame CCNA SEMPRE há uma ou 2 questões a esse respeito.

Os timers CDP em switches podem ser alterados da mesma forma que em routers, através dos comandos **`cdp timer`** e **`cdp holdtime`**, digitados no modo de configuração global, conforme ilustração acima **(b)**.

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

Relação dos comandos analisados:

Comando	Descrição
config t	Coloca o switch em modo de configuração global
enable password level 1	Configura a senha de modo usuário
enable password level 15	Configura a senha de modo privilegiado
enable secret	Configura a senha enable secret
show run	Apresenta a configuração ativa
hostname	Define um hostname para o switch
show ip	Apresenta a configuração IP do switch
ip address	Configura um endereço IP para o switch
ip default-gateway	Define o default-gateway do switch
interface ethernet 0/1	Configura interface e0/1
interface fastethernet 0/26	Configura interface f0/26
show inter e0/1	Apresenta estatísticas da interface e0/1
show int f0/26	Apresenta estatísticas da interface f0/26
description	Configura uma descrição para uma interface
duplex	Define o modo duplex de uma interface
ping	Testa a configuração IP
delete nvram	Deleta a configuração do switch
show mac-address-table	Apresenta a tabela MAC gerada dinamicamente
clear mac-address-table	Limpa a tabela MAC gerada dinamicamente
mac-address-table permanent	Cria uma entrada em caráter permanente de um endereço na tabela MAC
mac-address-table restricted static	Define um endereço restrito na tabela MAC permitindo que apenas interfaces configuradas devidamente possam se comunicar com o endereço restrito
port secure max-mac-count	Permite apenas a um número definido de dispositivos se conectar à uma interface
show version	Fornece informação sobre o IOS, assim como tempo de atividade do switch e endereço MAC do mesmo
show vlan	Apresenta todas as VLANs configuradas
interface e0/5	Configura interface Ethernet 5
interface f0/26	Configura interface FastEthernet 26
vlan 2 name sales	Cria a VLAN 2 chamada Sales
vlan-membership static 2	Associa uma VLAN à uma porta, estaticamente
show vlan-membership	Apresenta todas as associações de portas e VLANs
trunk on	Define modo de trunking permanente à uma porta
trunk auto	Configura uma porta no modo aut-trunking
show trunk A	Apresenta o trunking status na porta f0/26
show trunk B	Apresenta o trunking status na porta f0/27
vtp domain	Define o nome do domínio VTP
vtp server	Configura o switch para agir como servidor VTP
vtp client	Configura o switch para agir como cliente VTP
vtp password	Define uma senha para o domínio VTP
show vtp	Apresenta a configuração VTP em um switch
vtp pruning enable	Ativa VTP pruning em um switch
delete vtp	Deleta configurações VTP de um switch
int f0/0.1	Cria uma subinterface
encapsulation isl 2	Define roteamento ISL para a VLAN 2

Resumo da aula 8:

Nesta aula, cobrimos os seguintes tópicos:

- Configuração de senhas enable e enable secret
- Configuração do hostname
- Configuração do endereço IP e máscara de rede
- Identificação de interfaces através do comando **`sh int`**.
- Configuração de descrições para interfaces
- Definição do modo duplex em portas do switch
- Verificação da configuração através do comando **`sh run`**
- Gerenciamento da tabela de endereços MAC
- Configuração de endereços MAC estáticos e dinâmicos
- Configuração de segurança de portas

netceptions
cisco ccna preparation
www.certifique-se.com

Curso Preparatório CCNA

FIM AULA 08

Bibliografia:

CCNA Study Guide – Lammle, Todd. Editora Sybex

Cisco.com

Boson.com

Websites e grupos de discussão diversos