Redes de Computadores II

Neylor Michel

Cuiabá-MT
2013

Presidência da República Federativa do Brasil
Ministério da Educação
Secretaria de Educação Profissional e Tecnológica
Diretoria de Integração das Redes de Educação Profissional e Tecnológica

Equipe de Revisão
Universidade Federal de Mato Grosso – UFMT

Universidade Tecnológica Federal do Paraná – PR

Coordenação Institucional
Carlos Rinaldi

Coordenação Geral e-TEC
Edilson Pontarolo

Coordenação de Produção de Material Didático Impresso
Pedro Roberto Piloni

Coordenação de Tecnologia na Educação
Henrique Oliveira da Silva

Coordenação de Curso
Eliane Maria de Bortoli Fávero

Designer Educacional
Alceu Vidoti

Designer Master
Marta Magnusson Solyszko

Diagramação
Tatiane Hirata

Revisão de Língua Portuguesa
Ewerton Viegas Romeo Miranda

Revisão Científica
Eder Reverdito

Revisão Final
Marta Magnusson Solyszko

Projeto Gráfico
Rede e-Tec Brasil / UFMT

Dados Internacionais de Catalogação na Publicação

M582 Michel, Neylor

Redes de computadores II / Neylor Michel. – Curitiba: Ed. UTFPR, 2013.
189 p. : il.

Inclui bibliografia
e-ISBN: 978-85-7014-117-0

1. Redes de computadores. 2. Roteadores (Rede de computador). 3. Redes locais de computadores.
4. Rede de computador – Protoco-los. I. Título.

CDD (22. ed.) 004.6

Bibliotecário: Adriano Lopes CRB 9/1429

Apresentação Rede e-Tec Brasil

Prezado(a) estudante,

Bem-vindo(a) à Rede e-Tec Brasil!

Você faz parte de uma rede nacional de ensino que, por sua vez, constitui uma das ações do Pronatec - Programa Nacional de Acesso ao Ensino Técnico e Emprego. O Pronatec, instituído pela Lei nº 12.513/2011, tem como objetivo principal expandir, interiorizar e democratizar a oferta de cursos de Educação Profissional e Tecnológica (EPT) para a população brasileira propiciando caminho de acesso mais rápido ao emprego.

É neste âmbito que as ações da Rede e-Tec Brasil promovem a parceria entre a Secretaria de Educação Profissional e Tecnológica (Setec) e as instâncias promotoras de ensino técnico, como os institutos federais, as secretarias de educação dos estados, as universidades, as escolas e colégios tecnológicos e o Sistema S.

A educação a distância no nosso país, de dimensões continentais e grande diversidade regional e cultural, longe de distanciar, aproxima as pessoas ao garantir acesso à educação de qualidade e ao promover o fortalecimento da formação de jovens moradores de regiões distantes, geograficamente ou economicamente, dos grandes centros.

A Rede e-Tec Brasil leva diversos cursos técnicos a todas as regiões do país, incentivando os estudantes a concluir o ensino médio e a realizar uma formação e atualização contínuas. Os cursos são ofertados pelas instituições de educação profissional e o atendimento ao estudante é realizado tanto nas sedes das instituições quanto em suas unidades remotas, os polos.

Os parceiros da Rede e-Tec Brasil acreditam em uma educação profissional qualificada – integradora do ensino médio e da educação técnica – capaz de promover o cidadão com capacidades para produzir, mas também com autonomia diante das diferentes dimensões da realidade: cultural, social, familiar, esportiva, política e ética.

Nós acreditamos em você!
Desejamos sucesso na sua formação profissional!

Ministério da Educação
Novembro de 2013

Nosso contato
etecbrasil@mec.gov.br

Indicação de ícones

Os ícones são elementos gráficos utilizados para ampliar as formas de linguagem e facilitar a organização e a leitura hipertextual.

Atenção: indica pontos de maior relevância no texto.

Saiba mais: oferece novas informações que enriquecem o assunto ou "curiosidades" e notícias recentes relacionadas ao tema estudado.

Glossário: indica a definição de um termo, palavra ou expressão utilizada no texto.

Mídias integradas: remete o tema para outras fontes: livros, filmes, músicas, *sites*, programas de TV.

Atividades de aprendizagem: apresenta atividades em diferentes níveis de aprendizagem para que o estudante possa realizá-las e conferir o seu domínio do tema estudado.

Reflita: momento de uma pausa na leitura para refletir/escrever sobre pontos importantes e/ou questionamentos.

Palavra do Professor-autor

Caro(a) estudante,

Bem-vindo(a) à disciplina Redes de Computadores II.

O material desta disciplina abrange ampla variedade de tecnologias que facilitam o trabalho, a vida e o aprendizado, através da comunicação por voz, vídeo etc. Rede e Internet afetam as pessoas de maneira distinta em partes diferentes do mundo.

Uma meta importante é enriquecer o seu conhecimento, ampliando o que já sabe e o que pode fazer. No entanto, é importante perceber que este material e o professor podem apenas facilitar o processo. Você deve se comprometer em estudar as novas habilidades. Aqui estão algumas sugestões para ajudá-lo(a) a aprender e a crescer.

1. Faça anotações. Profissionais do campo de rede normalmente mantêm diários nos quais anotam as coisas que observam e aprendem. As anotações são importantes para ajudar a compreender o crescimento, com o passar do tempo.

2. Pense nisso. A disciplina fornece informações para transformar o seu entendimento teórico e prático. À medida que completar o percurso, pergunte-se o que faz sentido e o que não faz. Pare e faça perguntas quando estiver confuso(a). Procure saber mais sobre os tópicos nos quais tem interesse.

3. Pratique. Aprender novas habilidades exige prática. Acreditamos que isso é tão importante para o e-learning (aprendizado eletrônico).

4. Ensine. Ensinar um(a) amigo(a) ou um(a) colega costuma ser uma boa forma de reforçar sua própria aprendizagem. Para ser bom(a) profissional, é necessário examinar os detalhes que podem não ter sido percebidos em sua primeira leitura. Conversas sobre o material do curso com alunos(as), colegas e com o professor podem ajudar a solidificar sua compreensão dos conceitos de networking.

Apresentação da Disciplina

Esta disciplina exige conhecimentos do modelo de referência OSI, bem como meios de comunicação de dados, que podem ser adquiridos em Redes de Computadores I.

A disciplina de Redes de Computadores II se desenvolve em seis aulas. Cada aula está organizada da seguinte forma:

I – Os objetivos;

II – Apresentação do tema da unidade e sua importância na formação profissional;

III – O tema e a respectiva seção;

IV – O conteúdo e o objetivo atrelado a ele;

V – O desenvolvimento conceitual dos temas;

VI – Ao final de cada seção, breve síntese do tema trabalhado;

VII – Uma ou duas atividades para fortalecimento da aprendizagem.

Desejamos que você tire o maior proveito possível desta disciplina e do curso em seu todo, e que saiba que pode contar conosco sempre que julgar necessário. Sobretudo, caro(a) estudante, estimule em si próprio(a) o hábito de leitura e a disciplina no estudo.

Bom curso e sucesso!

Sumário

Aula 1. Roteadores

Objetivos:

- identificar um roteador como um computador usando um S.O. e um hardware para o processo de roteamento;

- reconhecer a estrutura de uma tabela de roteamento, bem como o seu processo e comutação.

Caro(a) estudante,

Esta aula tratará de roteadores. Acreditamos na importância deste conteúdo na sua qualificação profissional. Leia com atenção os textos e não deixe de realizar as atividades de aprendizagem.

As redes atuais têm um impacto significativo em nossas vidas – alterando a forma como nós vivemos, trabalhamos e nos divertimos. As redes de computadores, e em um contexto mais amplo a Internet, permitem às pessoas se comunicar, colaborar e interagir da maneira como elas jamais viram. Nós usamos a rede de várias formas, para uso de aplicativos Web, telefonia IP, videoconferência, jogos interativos, comércio eletrônico, educação e muito mais.

No centro da rede está o roteador. Resumidamente, um roteador conecta uma rede IP à outra. Por isso, o roteador é responsável pela troca de pacotes e redes diferentes. O destino do pacote IP pode ser um servidor Web em outro país ou um servidor de e-mail na rede local. É responsabilidade dos roteadores entregar esses pacotes em tempo hábil. A efetividade da comunicação de redes interconectadas depende, amplamente, da capacidade dos roteadores de encaminhar pacotes da maneira mais eficaz possível.

Agora os roteadores estão sendo adicionados a satélites no espaço. Esses roteadores terão a capacidade de rotear tráfego IP entre satélites no espaço de maneira muito semelhante à forma como esses pacotes são movidos na Terra, o que reduz atrasos e oferece maior flexibilidade de networking.

Além do encaminhamento de pacotes, um roteador também presta outros serviços. Para atender às demandas das redes atuais, os roteadores acolhem outros usos: asseguram uma disponibilidade 24x7 (24 horas por dia, 7 dias por semana). Para ajudar a garantir o alcance da rede, os roteadores usam caminhos alternativos, caso haja falha no caminho primário.

Os roteadores fornecem serviços integrados de dados, vídeo e voz em redes com e sem fio. Eles usam a priorização de Qualidade de Serviço (QoS, Quality of Service) dos pacotes IP para assegurar que o tráfego em tempo real, como voz, vídeo e dados críticos não sejam descartados ou atrasados. Atenuam o impacto de worms, vírus e outros ataques na rede, permitindo ou negando o encaminhamento de pacotes.

Todos esses serviços são criados de acordo com o roteador e com sua responsabilidade primária de encaminhar pacotes de uma rede para a próxima. Isso acontece, pois o roteador tem a capacidade de rotear pacotes entre redes nas quais os dispositivos em redes diferentes podem se comunicar. Esta aula irá apresentar o roteador, sua função nas redes, seus principais componentes de hardware e de software, além do próprio processo de roteamento.

1.1 Roteadores são computadores?

A **ARPANET** foi desenvolvida pela ARPA (Advanced Research Projects Agency) do Departamento de Defesa dos Estados Unidos. A ARPANET foi a primeira rede de comutação de pacotes operacional do mundo e a antecessora da Internet atual.

Um roteador é um computador, assim como qualquer outro, inclusive um PC. O primeiro roteador, usado na **ARPANET** (Advanced Research Projects Agency Network), foi o Processador de Mensagem da Interface (IMP, Interface Message Processor). O IMP era um minicomputador Honeywell 316; esse computador deu vida à ARPANET no dia 30 de agosto de 1969.

Os roteadores têm muitos componentes de hardware e de software iguais, encontrados em outros computadores, inclusive:

- CPU;
- RAM;
- ROM;
- Sistema operacional;
- Roteadores estão no centro da rede.

Os usuários típicos talvez desconheçam a presença de vários roteadores em sua própria rede ou na Internet. Os usuários esperam ser capazes de acessar páginas da Web, enviar e-mails e baixar músicas – independentemente de o servidor acessado estar em sua própria rede ou em outra rede no mundo. No entanto, os profissionais de networking sabem que o roteador é responsável por encaminhar pacotes de rede a rede, ou seja, da origem ao destino.

Um roteador conecta várias redes. Isso significa que ele tem várias interfaces, cada uma pertencente a uma rede IP diferente. Quando um roteador recebe um pacote IP em uma interface, ele determina qual outra interface usar para encaminhar o pacote para seu destino. A interface que o roteador usa para encaminhar o pacote pode ser a rede do destino final do pacote (a rede com o endereço IP de destino desse pacote) ou pode ser uma rede conectada a outro roteador usado para alcançar a rede de destino.

Cada rede a que um roteador se conecta costuma exigir uma interface separada. Essas interfaces são usadas para conectar uma combinação de redes locais (LANs, Local Area Networks) e redes remotas (WAN, Wide Area Networks). As redes locais costumam ser redes Ethernet que contêm dispositivos como PCs, impressoras e servidores. As WANs são usadas para conectar redes em uma área geográfica extensa. Por exemplo, uma conexão WAN costuma ser usada para conectar uma rede local à rede do Provedor de Internet (ISP, Internet Service Provider).

Na figura 01, vemos que os roteadores R1 e R2 são responsáveis por receber o pacote em uma rede e encaminhar o pacote por outra rede para a rede de destino.

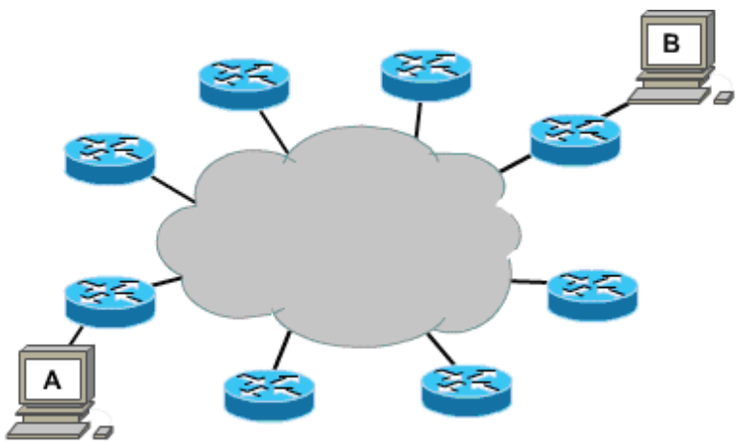


Figura 01 - Roteadores permitindo a comunicação entre os hosts A e B.
Fonte: autor

1.2 Roteadores determinam o melhor caminho

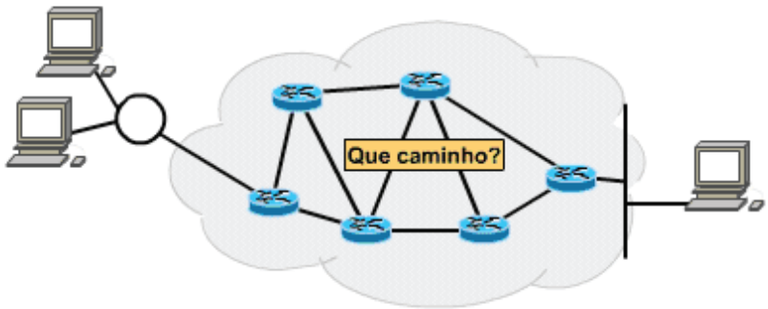


Figura 02 - Camada de Rede - Determinação de Caminho.
Fonte: http://www.gta.ufrj.br/grad/03_1/rip/RIP_Consort/Script/introducao.htm

A responsabilidade primária de um roteador é direcionar pacotes com destino para redes locais e remotas:

- Determinando o melhor caminho para enviar pacotes;
- Encaminhando pacotes para o destino.

O roteador usa sua tabela de roteamento para determinar o melhor caminho para encaminhar o pacote. Quando o roteador recebe um pacote, ele examina seu endereço IP de destino e procura a melhor correspondência com um endereço de rede em sua tabela de roteamento. A tabela de roteamento também inclui a interface a ser usada para encaminhar o pacote. Quando uma correspondência é localizada, o roteador encapsula o pacote IP no quadro de enlace da interface de saída, e o pacote é encaminhado para seu destino.

É muito provável que um roteador receba um pacote encapsulado em um tipo de quadro de enlace, como um quadro Ethernet, e, ao encaminhar o pacote, o encapsule em um tipo diferente de quadro de enlace, como o Protocolo Ponto a Ponto (PPP, Point-to-Point Protocol). O encapsulamento do quadro de enlace depende do tipo de interface do roteador e do tipo de meio a que ele se conecta. Entre as tecnologias de enlace de dados diferentes a que um roteador pode se conectar estão tecnologias de rede local, como Ethernet e conexões WAN seriais, como a conexão T1 que usa PPP, Frame Relay e Modo de Transferência Assíncrona (ATM, Asynchronous Transfer Mode).

Na figura 03, podemos acompanhar um pacote do PC de origem até o PC de destino. Observe que é de responsabilidade do roteador localizar a rede de destino em sua tabela de roteamento e encaminhar o pacote para seu destino. Neste exemplo, o Roteador R1 recebe o pacote encapsulado em um quadro Ethernet. Depois do desencapsulamento do pacote, R1 usa o endereço IP de destino do pacote para pesquisar sua tabela de roteamento em busca de um endereço de rede correspondente. Depois que um endereço de rede de destino é localizado na tabela de roteamento, R1 encapsula o pacote em um quadro PPP e o encaminha para R2. Um processo semelhante é executado por R2.

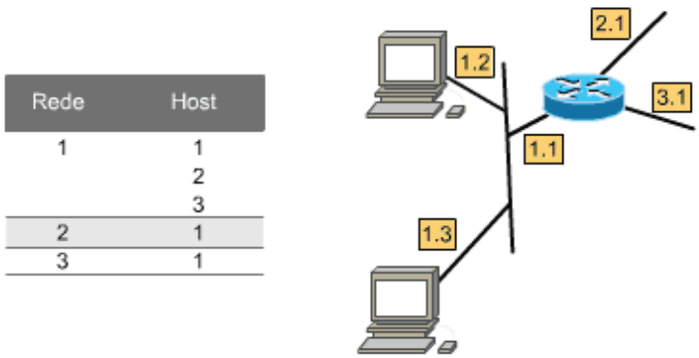


Figura 03 - Endereçamento Rede e Host.
Fonte: http://aulavirtual.tecnologicocomfenalcovirtual.edu.co/aulavirtual/mod/page/view.php?id=48664

As rotas estáticas e os protocolos de roteamento dinâmico são usados por roteadores para aprender redes remotas e criar suas tabelas de roteamento. Essas rotas e protocolos são o foco primário do curso, sendo abordados em detalhes nos capítulos posteriores, além do processo que os roteadores usam ao pesquisar suas tabelas de roteamento e ao encaminhar os pacotes.

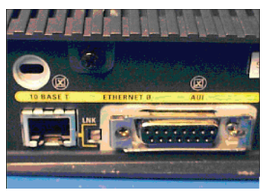


Figura 04 - Roteador e suas conexões.
Fonte: http://www.adrformacion.com/cursos/wserver082/leccion1/tutorial6.html

1.3 CPU do roteador e memória

Assim como um PC, um roteador também inclui:

- Unidade de Processamento Central (CPU, Central Processing Unit);
- Memória de Acesso Aleatório (RAM);
- Memória somente leitura (ROM).

Observe a seguir as funções de cada um desses elementos.

1.3.1 CPU

A CPU executa instruções do sistema operacional, como inicialização de sistema, funções de roteamento e de comutação.

1.3.2 RAM

A RAM armazena as instruções e os dados que precisam ser executados pela CPU. A RAM é usada para armazenar estes componentes:

- **Sistema operacional:** O IOS (Internetwork Operating System, Sistema Operacional de Internet) Cisco é copiado para a RAM durante a inicialização;
- **Running-config:** Esse é o arquivo de configuração que armazena os comandos de configuração que o IOS do roteador está usando atualmente. Com poucas exceções, todos os comandos configurados no roteador são armazenados neste arquivo;
- **Tabela de roteamento IP:** Esse arquivo armazena informações sobre redes conectadas diretamente e remotas. Ele é usado para determinar o melhor caminho para encaminhar o pacote;
- **Cache ARP:** Esse cache contém o endereço IPv4 para mapeamentos de endereço MAC, semelhante ao cache ARP em um PC. O cache ARP é usado em roteadores com interfaces de rede local, como interfaces Ethernet;
- **Buffer de pacotes:** Os pacotes são armazenados temporariamente em um buffer quando recebidos em uma interface, ou antes de saírem por uma interface.

RAM é uma memória volátil e perde seu conteúdo quando o roteador é desligado ou reiniciado. No entanto, o roteador também contém áreas de armazenamento permanentes, como ROM, memória flash e NVRAM.

1.3.3 ROM

ROM é uma forma de armazenamento permanente. Os dispositivos da Cisco usam a ROM para armazenar:

- As instruções de bootstrap;
- Software de diagnóstico básico;
- Versão redimensionada do IOS.

A ROM usa firmware, que é o software incorporado no circuito integrado. O firmware inclui o software que normalmente não precisa ser modificado ou atualizado, como as instruções de inicialização. Muitos desses recursos, inclusive o software monitor ROM, serão abordados em um curso posterior. A ROM não perde seu conteúdo quando o roteador é desligado ou reiniciado.

1.3.4 Memória flash

Flash é uma memória de computador não volátil que pode ser apagada e armazenada eletricamente. A memória flash é usada como armazenamento permanente para o sistema operacional, o Cisco IOS. Na maioria dos modelos de roteadores Cisco, o IOS é armazenado permanentemente na memória flash e copiado para a RAM durante o processo de inicialização, quando é executado pela CPU. Alguns modelos mais antigos de roteadores Cisco executam o IOS diretamente na memória flash. A memória flash consiste em placas SIMMs ou PCMCIA, que podem ser atualizadas para aumentar a quantidade da memória flash.

A memória flash não perde seu conteúdo quando o roteador é desligado ou reiniciado.

NVRAM

A RAM Não Volátil (NVRAM, Nonvolatile RAM) não perde suas informações quando a energia é desligada. Isso é o oposto ao que acontece na maioria das formas comuns de RAM, como DRAM, que exige energia ininterrupta para manter suas informações. A NVRAM é usada pelo Cisco IOS como

armazenamento permanente para o arquivo de configuração de inicialização (startup-config). Todas as alterações feitas na configuração são armazenadas no arquivo running-config na RAM e, com poucas exceções, são implementadas imediatamente pelo IOS. Para salvar essas alterações, caso o roteador seja reiniciado ou desligado, o running-config deve ser copiado para a NVRAM, onde é armazenada como o arquivo startup-config. A NVRAM manterá seu conteúdo, mesmo quando o roteador for recarregado ou desligado.

ROM, RAM, NVRAM e memória flash são abordadas na seção a seguir, que apresenta o IOS e o processo de inicialização. Elas também são tratadas mais detalhadamente em um curso posterior, referente ao gerenciamento do IOS.

É mais importante para um(a) profissional de networking compreender a função dos componentes internos principais de um roteador do que o local exato desses componentes dentro de um roteador específico. A arquitetura física interna irá variar de modelo para modelo.

1.4 Sistema operacional de Internet

O software de sistema operacional usado em roteadores Cisco é conhecido como Sistema Operacional de Internet Cisco (IOS, Internetwork Operating System). Assim como qualquer sistema operacional em qualquer computador, o Cisco IOS gerencia os recursos de hardware e de software do roteador, inclusive a alocação de memória, os processos, a segurança e os sistemas de arquivos. O Cisco IOS é um sistema operacional multitarefa, integrado a funções de roteamento, de comutação, de inter-rede e de telecomunicação.

Embora o Cisco IOS possa ser aparentemente o mesmo em muitos roteadores, há muitas imagens diferentes do IOS. Uma imagem do IOS é um arquivo que contém todo o IOS do roteador. A Cisco cria muitos tipos diferentes de imagens do IOS, dependendo do modelo do roteador e dos recursos no IOS. Normalmente, quanto mais recursos no IOS, maior será a imagem do IOS e, logo, mais memória flash e RAM são exigidas para armazenar e carregar o IOS. Por exemplo, entre alguns recursos estão a capacidade de executar IPv6 ou a capacidade do roteador de executar a Tradução de Endereços de Rede (NAT, Network Address Translation).

Assim como ocorre com outros sistemas operacionais, o Cisco IOS tem sua própria interface do usuário. Embora alguns roteadores forneçam uma Inter-

face Gráfica do Usuário (GUI, Graphical User Interface), a Interface de Linha de Comando (CLI, Command Line Interface) é um método muito mais comum de configurar roteadores Cisco. A CLI é usada ao longo deste currículo.

Durante a inicialização, o arquivo startup-config na NVRAM é copiado para a RAM e armazenado como o arquivo running-config. O IOS executa os comandos de configuração no running-config. Qualquer alteração feita pelo administrador de rede é armazenada no running-config, sendo implementada imediatamente pelo IOS. Neste capítulo, nós revisaremos alguns dos comandos básicos do IOS usados para configurar um roteador Cisco. Em capítulos posteriores, aprenderemos os comandos usados para configurar, verificar e solucionar problemas de roteamento estático e de vários protocolos de roteamento, como RIP, EIGRP e OSPF.

1.5 Interfaces do roteador

Os roteadores têm conectores físicos usados para gerenciar o roteador. Esses conectores são conhecidos como portas de gerenciamento. Diferentemente das interfaces Ethernet e seriais, as portas de gerenciamento não são usadas no encaminhamento de pacotes. A porta de gerenciamento mais comum é a porta console. A porta console é usada para conectar um terminal, ou mais frequentemente um PC que executa software emulador de terminal, para configurar o roteador sem a necessidade de acesso à rede para o roteador. A porta console deve ser usada durante a configuração inicial do roteador.

Outra porta de gerenciamento é a porta auxiliar. Nem todos os roteadores têm portas auxiliares. Às vezes, a porta auxiliar pode ser usada de maneira semelhante a uma porta console. Ela também pode ser usada no acoplamento a um modem. As portas auxiliares não serão usadas neste currículo.

A figura 05 mostra as portas de console e AUX do roteador.

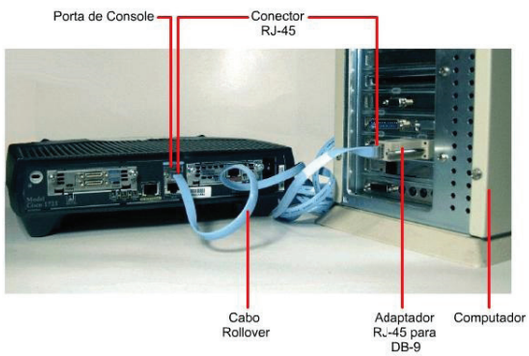


Figura 05 - Roteador com porta auxiliar a esquerda e console a direita.
Fonte: tkjbforever.blogspot.com

O termo "interface" em roteadores Cisco se refere a um conector físico no roteador cujo propósito principal é receber e encaminhar pacotes. Os roteadores têm várias interfaces usadas na conexão com várias redes. Normalmente, as interfaces se conectam a vários tipos de redes, o que significa que são necessários tipos diferentes de meio e de conectores. Um roteador, geralmente, precisará ter tipos diferentes de interfaces. Por exemplo, ele normalmente tem interfaces FastEthernet para conexões com redes locais diferentes e vários tipos de interfaces WAN para conectar vários enlaces seriais, inclusive T1, DSL e ISDN.

A figura 06 mostra as interfaces FastEthernet e seriais no roteador. Assim como as interfaces em um PC, as portas e as interfaces em um roteador estão localizadas fora do roteador. Sua localização externa possibilita um acoplamento prático aos cabos de rede e aos conectores apropriados.

Uma única interface em um roteador pode ser usada na conexão com várias redes; no entanto, isso está além do escopo deste curso, merecendo ser abordado em um curso posterior.

Assim como a maioria dos dispositivos de networking, os roteadores Cisco usam indicadores LED para fornecer informações de status. Um LED de interface indica a atividade da interface correspondente. Se um LED estiver desligado quando a interface estiver ativa, e a interface estiver conectada corretamente, isso talvez seja um indício de que existe um problema nessa interface. Se uma interface estiver muito ocupada, seu LED estará sempre ligado. As interfaces pertencem a redes diferentes

Como mostrado na figura 06, toda interface no roteador é membro ou host em uma rede IP diferente. Cada interface deve ser configurada com um endereço IP e uma máscara de sub-rede de uma rede diferente. O Cisco IOS não irá permitir que duas interfaces ativas no mesmo roteador pertençam à mesma rede.

Figura 06 - Roteador Cisco com os conectores Ethernet e WAN.
Fonte: http://www.ciscomanual.net/cisco-1841/

As interfaces de roteador podem ser divididas em dois grupos principais:

- Interfaces de rede local – como Ethernet e FastEthernet;
- Interfaces WAN – como serial, ISDN e Frame Relay.

1.6 Interfaces de rede local

Como o próprio nome diz, as interfaces de rede local são usadas para conectar o roteador à rede local, semelhantemente à forma como uma placa de rede Ethernet do PC é usada para conectar o PC à rede local Ethernet. Assim como uma placa de rede Ethernet de PC, uma interface Ethernet de roteador também tem um endereço MAC de Camada 2 e participa da rede local Ethernet da mesma forma que qualquer outro host na rede local. Por exemplo, uma interface Ethernet de roteador participa do processo ARP da rede local. O roteador mantém um cache ARP para a interface, envia solicitações ARP quando necessário e responde com respostas ARP quando solicitado.

Uma interface Ethernet de roteador normalmente usa um conector RJ-45 que oferece suporte ao cabeamento Par Trançado Não Blindado (UTP, Unshielded Twisted-Pair). Quando um roteador é conectado a um switch, um cabo straight-through é usado. Quando dois roteadores são conectados diretamente pelas interfaces Ethernet, ou quando uma placa de rede de PC é conectada diretamente a uma interface Ethernet de roteador, é usado um cabo crossover.

Use a atividade de Packet Tracer posteriormente, nesta seção, para testar suas habilidades de cabeamento.

Os endereços MAC são usados em interfaces de rede local, como Ethernet, não sendo usados em interfaces WAN. No entanto, as interfaces WAN usam seus próprios endereços de Camada 2, dependendo da tecnologia. Os tipos de encapsulamento WAN da Camada 2 e os endereços serão abordados em uma disciplina posterior.
O roteador na figura tem quatro interfaces. Cada interface tem um endereço IP de Camada 3 e uma máscara de sub-rede que a configura para uma rede diferente. As interfaces Ethernet também têm endereços MAC Ethernet de Camada 2 .

1.7 Interfaces WAN

As interfaces WAN são usadas para conectar roteadores a redes externas, normalmente a uma grande distância geográfica. O encapsulamento de Camada 2 pode ser de tipos diferentes, como PPP, Frame Relay e Controle de Enlace de Alto Nível (HDLC, High-Level Data Link Control). Semelhantemente a interfaces de rede local, cada interface WAN tem seu próprio endereço IP e máscara de sub-rede, o que a identifica como um membro de uma rede específica.

As interfaces WAN estão usando encapsulamentos de Camada 2 diferentes. Serial 0/0/0 está usando HDLC e Serial 0/0/1 está usando PPP. Esses dois protocolos ponto a ponto seriais usam um endereço de broadcast para o endereço de destino da Camada 2 ao encapsular o pacote IP em um quadro de enlace.

No ambiente de laboratório, você está restrito a uma quantidade de interfaces de rede local e WAN para configurar laboratórios práticos. No entanto, com o Packet Tracer, você tem a flexibilidade de criar designs de rede mais complexos.

1.8 Roteadores e camadas de rede

O propósito principal de um roteador é conectar várias redes e encaminhar pacotes com destino para suas próprias redes ou outras. Um roteador é considerado um dispositivo de Camada 3 porque sua decisão primária de encaminhamento se baseia nas informações no pacote IP da Camada 3, mais especificamente o endereço IP de destino. Esse processo é conhecido como roteamento.

Quando um roteador recebe um pacote, ele examina seu endereço IP de destino. Se o endereço IP de destino não pertencer a nenhuma das redes conectadas diretamente do roteador, este deve encaminhar esse pacote para outro. Na figura 07, R1 examina o endereço IP de destino do pacote. Depois de pesquisar a tabela de roteamento, R1 encaminha o pacote em R2. Quando R2 recebe o pacote, ele também examina o endereço IP de destino do pacote. Depois de pesquisar sua tabela de roteamento, R2 encaminha o pacote por sua rede Ethernet conectada diretamente para PC2.

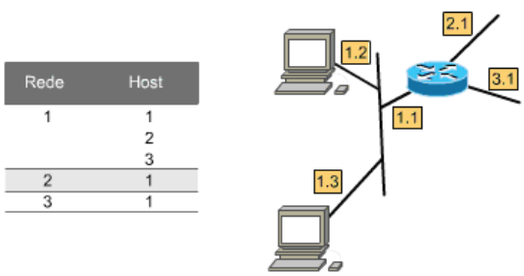


Figura 07 - Encaminhamento do pacote para a mesma rede.
Fonte: http://aulavirtual.tecnologicocomfenalcovirtual.edu.co/aulavirtual/mod/page/view.php?id=48664

Quando cada roteador recebe um pacote, ele procura em sua tabela de roteamento até encontrar a melhor correspondência entre o endereço IP de destino do pacote e um dos endereços de rede na tabela de roteamento. Quando uma correspondência é localizada, o pacote é encapsulado no quadro de enlace da Camada 2 dessa interface de saída. O tipo de encapsulamento do enlace de dados depende do tipo de interface, como Ethernet ou HDLC.

O pacote acaba alcançando um roteador que faz parte de uma rede que corresponde ao endereço IP de destino do pacote. Nesse exemplo, o Roteador R2 recebe o pacote de R1. R2 encaminha o pacote por sua interface Ethernet, que pertence à mesma rede do dispositivo de destino, PC2.

- Roteadores funcionam nas camadas 1, 2 e 3

Um roteador toma sua decisão primária de encaminhamento na Camada 3, mas como vimos em outro passo, ele também participa dos processos das camadas 1 e 2. Depois que um roteador examina o endereço IP de destino de um pacote e consulta sua tabela de roteamento para tomar sua decisão de encaminhamento, ele pode encaminhar esse pacote pela interface apropriada na direção do seu destino. O roteador encapsula o pacote IP da Camada 3 na porção de dados de um quadro de enlace de dados da Camada 2 apropriado à interface de saída. O tipo de quadro pode ser um encapsulamento Ethernet, HDLC ou algum outro de Camada 2 – independentemente do encapsulamento usado na interface em questão. O quadro de Camada 2 é codificado em sinais físicos da Camada 1, usados para representar bits no enlace físico.

Para compreender melhor esse processo, consulte a figura 08. Observe que PC1 funciona em todas as sete camadas, encapsulando os dados e enviando o quadro como um fluxo de bits codificados para R1, seu gateway padrão.

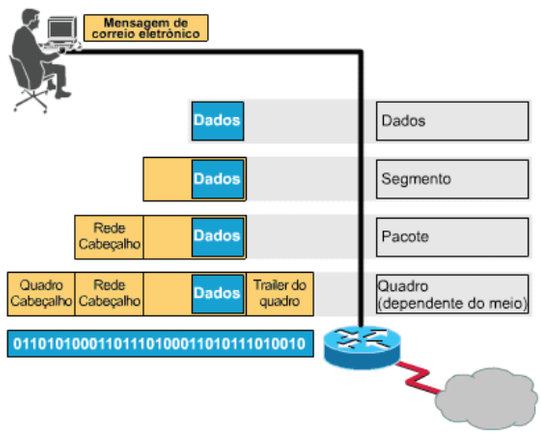


Figura 08 - Exemplo de encapsulamento.
Fonte: http://www.marcaube.com/inf3803/cours/INF3803-semaine5-h2004.htm

R1 recebe o fluxo de bits codificados em sua interface. Os bits são decodificados e passados para a Camada 2, onde R1 desencapsula o quadro. O roteador examina o endereço de destino do quadro de enlace de dados para determinar se ele corresponde à interface de recebimento, incluindo um endereço de broadcast ou multicast. Se houver uma correspondência em relação à porção de dados do quadro, o pacote IP será passado para a Camada 3, onde R1 toma sua decisão de roteamento. Em seguida, R1 reencapsula o pacote em novo quadro de enlace de dados da Camada 2 e o encaminha pela interface de saída como um fluxo de bits codificados.

R2 recebe o fluxo de bits e o processo se repete. R2 desencapsula o quadro e passa a porção de dados do quadro, o pacote IP, para a Camada 3, onde R2 toma sua decisão de roteamento. Em seguida, R2 reencapsula o pacote em novo quadro de dados da Camada 2 e o encaminha pela interface de saída como um fluxo de bits codificados.

Esse processo é repetido mais uma vez pelo Roteador R3, que encaminha o pacote IP encapsulado em um quadro de enlace de dados e codificado como bits, para PC2.

Cada roteador no caminho da origem até o destino executa esse mesmo processo de desencapsulamento, pesquisando a tabela de roteamento e reencapsulando. Esse processo é importante para sua compreensão de como roteadores participam de redes. Portanto, nós veremos novamente essa discussão com mais profundidade, em seção posterior.

1.9 Configuração básica do roteador

Durante a configuração de um roteador, são executadas determinadas tarefas básicas, como:

- Nomeação do roteador;
- Definição de senhas;
- Configuração de interfaces;
- Configuração de um banner;
- Salvando as alterações em um roteador;

- Verificação da configuração básica e das operações do roteador.

Você já deve estar familiarizado com estes comandos de configuração. No entanto, faremos uma breve revisão. Começamos nossa revisão pressupondo que o roteador não tenha um arquivo startup-config atual.

O primeiro prompt é exibido no modo de usuário. O modo de usuário permite exibir o estado do roteador, mas não modificar sua configuração. Não confunda o termo "usuário", como usado no modo de usuário, com usuários da rede. O modo de usuário se destina aos técnicos de rede, operadores e engenheiros que têm a responsabilidade de configurar dispositivos de rede.

Router>

O comando enable é usado para acessar o modo EXEC privilegiado. Esse modo permite ao usuário fazer alterações na configuração do roteador. O prompt do roteador irá passar de ">" para "#" nesse modo.

```
Router>enable

Router#
```

Nomes de host e senhas

Observe a seguir a sintaxe de comando de configuração básica do roteador usada para configurar R1 no exemplo a seguir.

Primeiro, acesse o modo de configuração global.

```
Router#config t
```

Em seguida, aplique um nome de host exclusivo ao roteador.

```
Router(config)#hostname R1

R1(config)#
```

Agora, configure uma senha a ser usada para acessar o modo EXEC privilegiado. Em nosso ambiente de laboratório, usaremos a senha class. No entanto, em ambientes de produção, os roteadores devem ter senhas fortes.

Consulte os links ao término desta seção para obter mais informações sobre como criar e usar senhas fortes.

```
Router(config)#enable secret class
```

Em seguida, configure as linhas de console e Telnet usando a senha cisco. Mais uma vez, a senha cisco é usada exclusivamente em nosso ambiente de laboratório. O comando login habilita a verificação da senha na linha. Se você não inserir o comando login na linha de console, o usuário terá acesso à linha sem inserir uma senha.

```
R1(config)#line console 0

R1(config-line)#password cisco

R1(config-line)#login

R1(config-line)#exit

R1(config)#line vty 0 4

R1(config-line)#password cisco

R1(config-line)#login

R1(config-line)#exit
```

Configurando um banner

No modo de configuração global, configure o banner message-of-the-day (motd). Um caractere de delimitação, como "#", é usado no início e no fim da mensagem. O delimitador permite configurar um banner em várias linhas, como mostrado aqui.

```
R1(config)#banner motd #

Digite a mensagem TEXT. Fim com o caractere '#'. **********
**************************

AVISO!! Acesso não autorizado. Proibido!!
```

```
**************************************
#
```

Configurar um banner apropriado faz parte de um bom plano de segurança. Um banner deve, pelo menos, advertir contra o acesso não autorizado. Jamais configure um banner com "boas-vindas" para um usuário não autorizado.

Configuração da interface do roteador

Agora você irá configurar as interfaces de roteador individuais com endereços IP e outras informações. Primeiro, acesse o modo de configuração da interface, especificando o tipo de interface e o número. Em seguida, configure o endereço IP e a máscara de sub-rede:

```
R1(config)#interface Serial0/0/0

R1(config-if)#ip address 192.168.2.1 255.255.255.0
```

É uma prática recomendada configurar uma descrição em cada interface para ajudar a documentar as informações de rede. O texto da descrição está limitado a 240 caracteres. Em redes de produção, uma descrição pode ser útil na solução de problemas, fornecendo informações sobre o tipo de rede a que a interface está conectada e se há qualquer outro roteador nessa rede.

Se a interface se conectar a um ISP ou a uma operadora de serviço, será útil inserir a conexão de terceiros e informações de contato; por exemplo:

```
Router(config-if)#description Ciruit#VBN32696-123 (help desk:1-800-555-1234)
```

Em ambientes de laboratório, insira uma descrição simples que irá ajudar a solucionar problemas em situações; por exemplo:

```
R1(config-if)#description Link to R2
```

Depois de configurar o endereço IP e a descrição, a interface deve ser ativada com o comando no shutdown. Isso é semelhante a ligar a interface. A interface também deve ser conectada a outro dispositivo (um hub, um switch,

outro roteador etc.) para que a camada física permaneça ativa.

```
Router(config-if)#no shutdown
```

Durante o cabeamento de um enlace serial ponto a ponto em nosso ambiente de laboratório, uma extremidade do cabo é marcada como DTE, e a outra como DCE. O roteador com a extremidade DCE do cabo conectado à sua interface serial precisará do comando adicional clock rate configurado nessa interface serial. Essa etapa só é necessária em um ambiente de laboratório, sendo explicada com mais detalhes no Capítulo 2, "Roteamento estático".

```
R1(config-if)#clock rate 1000000
```

Repita os comandos de configuração da interface em todas as demais interfaces a serem configuradas. Em nosso exemplo de topologia, a interface FastEthernet precisa ser configurada.

```
R1(config)#interface FastEthernet 0/0

R1(config-if)#ip address 192.168.1.1 255.255.255.0

R1(config-if)#description R1 LAN

R1(config-if)#no shutdown
```

Cada interface pertence a uma rede diferente

Neste momento, observe que cada interface deve pertencer a uma rede diferente. Embora o IOS permita configurar um endereço IP da mesma rede em duas interfaces diferentes, o roteador não irá ativar a segunda interface.

E se, por exemplo, você tentar configurar a interface FastEthernet 0/1 em R1 com um endereço IP na rede 192.168.1.0/24 e a interface FastEthernet 0/0 já recebeu um endereço nessa mesma rede? Você irá obter a seguinte mensagem:

```
R1(config)#interface FastEthernet0/1

R1(config-if)#ip address 192.168.1.2 255.255.255.0
```

192.168.1.0 overlaps with FastEthernet0/0

Se houver uma tentativa de habilitar a interface com o comando no shutdown, a seguinte mensagem será exibida:

R1(config-if)#no shutdown

192.168.1.0 overlaps with FastEthernet0/0

FastEthernet0/1: incorrect IP address assignment

Observe que a saída de comando show ip interface brief mostra que a segunda interface configurada para a rede 192.168.1.0/24, FastEthernet 0/1, ainda está desativada.

R1#show ip interface brief

Verificando a configuração básica do roteador

No exemplo atual, todos os comandos de configuração básica do roteador anteriores foram inseridos e armazenados imediatamente no arquivo de configuração em execução de R1. O arquivo running-config é armazenado na RAM, sendo o arquivo de configuração usado pelo IOS. A próxima etapa é verificar os comandos inseridos, exibindo a configuração em execução com o seguinte comando:

R1#show running-config

Agora que os comandos de configuração básica foram inseridos, é importante salvar o running-config na memória não volátil, a NVRAM do roteador. Dessa forma, no caso de uma queda de energia ou de uma recarga acidental, o roteador poderá ser inicializado com a configuração atual. Depois que a configuração do roteador foi concluída e testada, é importante salvar o running-config no startup-config como o arquivo de configuração permanente.

R1#copy running-config startup-config

Depois de aplicar e salvar a configuração básica, você poderá usar vários comandos para verificar se configurou corretamente o roteador. Todos esses

comandos são abordados com mais detalhes em capítulos posteriores. Por ora, comece a se familiarizar com a saída.

```
R1#show running-config
```

Esse comando exibe a configuração em execução atual armazenada na RAM. Com algumas exceções, todos os comandos de configuração usados serão inseridos no running-config e implementados imediatamente pelo IOS.

```
R1#show startup-config
```

Esse comando exibe o arquivo de configuração de inicialização armazenado na NVRAM. Essa é a configuração que o roteador irá usar na próxima reinicialização. Essa configuração não é alterada, a menos que a configuração em execução atual seja salva na NVRAM com o comando copy running-config startup-config.

Resumo

Essa aula teve como objetivo apresentar o roteador. Roteadores são computadores e incluem muitos dos mesmos componentes de hardware e de software encontrados em um PC típico, como CPU, RAM, ROM e um sistema operacional.

A principal finalidade de um roteador é conectar várias redes e encaminhar pacotes de uma rede para a próxima. Isso significa que um roteador normalmente tem várias interfaces. Cada interface é um membro ou host em uma rede IP diferente.

O roteador tem uma tabela de roteamento, que é uma lista de redes conhecida pelo roteador. A tabela de roteamento inclui endereços de rede de suas próprias interfaces, que são as redes conectadas diretamente, bem como endereços de rede para redes remotas. Uma rede remota é uma rede que só pode ser alcançada encaminhando-se o pacote para outro roteador.

Os roteadores tomam sua decisão primária de encaminhamento na Camada 3, a camada de rede. No entanto, as interfaces de roteador participam das camadas 1, 2 e 3. Os pacotes IP de Camada 3 são encapsulados em um quadro de enlace de dados de Camada 2 e codificados em bits na Camada 1. As interfaces de roteador participam de processos de Camada 2 associada ao seu encapsulamento. Por exemplo, uma interface Ethernet de um roteador participa do processo ARP, assim como os demais hosts na rede local.

Atividades de aprendizagem

Responda às questões abaixo:

1. Quais afirmativas descrevem corretamente os componentes de um roteador? (Escolha duas.)

a) A RAM armazena permanentemente o arquivo de configuração usado durante a sequência de inicialização.

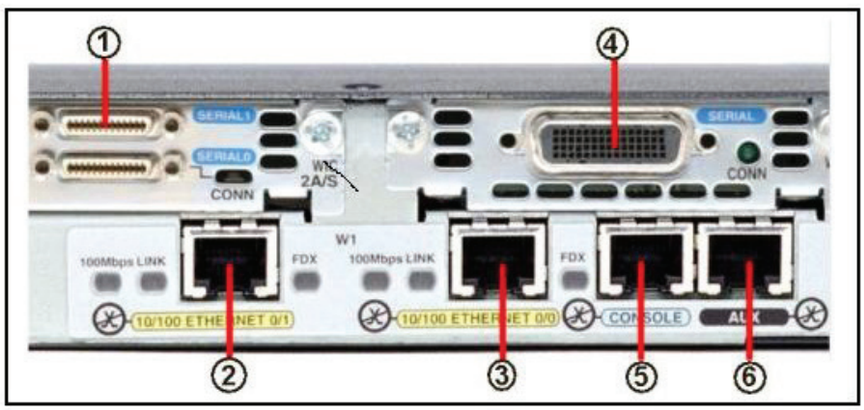
b) A ROM contém diagnósticos executados nos módulos de hardware.

c) A NVRAM armazena uma cópia de backup do IOS usado durante a sequência de inicialização.

d) A memória flash não perde seu conteúdo durante uma reinicialização.

e) A ROM contém a versão mais atual e mais completa do IOS.

f) A memória flash contém comandos do sistema de inicialização para identificar o local do IOS.



Fonte: http://www.networksheaven.com/exrercise-1-accessing-router-from-a-pc-using-hyperterminal-securecrt

2. Que interfaces na exibição acima poderiam ser usadas em uma conexão WAN (Wide Area Network, Rede remota) de linha alugada? (Escolha duas.)

a) 1

b) 2

c) 3

d) 4

e) 5

f) 6

3. Se um roteador não pode encontrar um arquivo válido de configuração durante a sequência de inicialização, o que acontece? Escolha uma das alternativas abaixo.

a) A sequência de inicialização é redefinida.

b) O roteador solicita uma resposta do usuário para entrar no modo setup.

c) A sequência startup é bloqueada até que seja adquirido um arquivo válido de configuração.

d) O roteador gera uma configuração padrão baseada na última configuração válida.

e) O roteador monitora o tráfego local para determinar os requisitos de configuração do protocolo de roteamento.

4. Qual das opções a seguir é o fluxo correto de rotinas para a inicialização de um roteador? Assinale a correta.

a) carregar bootstrap, carregar IOS, aplicar configuração

b) carregar bootstrap, aplicar configuração, carregar IOS

c) carregar IOS, carregar bootstrap, aplicar configuração, verificar hardware

d) verificar hardware, aplicar configuração, carregar bootstrap, carregar IOS

5. Quais são as funções de um roteador? (Escolha três.)

a) comutação de pacotes

b) extensão dos segmentos de rede

c) segmentação dos domínios de difusão

d) seleção de melhor caminho com base no endereçamento lógico

e) seleção de melhor caminho com base no endereçamento físico

Prezado(a) estudante,

Ainda há muito para aprender. Na próxima aula, examinaremos a configuração de rotas estáticas e apresentaremos a tabela de roteamento IP. Não desista!

Aula 2. Roteamento estático

Objetivos:

- definir a função geral que um roteador desempenha em redes;
- relacionar as redes conectadas diretamente e as diferentes interfaces de roteador;
- examinar redes conectadas diretamente na tabela de roteamento e usar o protocolo CDP;
- descrever rotas estáticas com interfaces de saída; e
- identificar e solucionar problemas de rotas estáticas.

Caro(a) estudante,

O roteamento está no centro de todas as redes de dados, movendo informações em redes interconectadas da origem para o destino. Os roteadores são os dispositivos responsáveis pela transferência de pacotes de uma rede para a próxima.

Como nós vimos na aula anterior, os roteadores aprendem as redes remotas dinamicamente, usando protocolos de roteamento, ou manualmente, usando rotas estáticas. Em muitos casos, os roteadores usam uma combinação de protocolos de roteamento dinâmico e rotas estáticas. Esta aula se concentra no roteamento estático.

As rotas estáticas são muito comuns e não exigem a mesma quantidade de processamento e sobrecarga, como veremos com os protocolos de roteamento dinâmico.

Nesta aula, acompanharemos um exemplo de topologia ao configurarmos rotas estáticas e você poderá aprender técnicas para identificação e solução

de problemas. No processo, examinaremos vários comandos essenciais do IOS e os resultados que eles exibem. Também apresentaremos a tabela de roteamento que usa redes diretamente conectadas e rotas estáticas. Não deixe de reservar uma parte do seu tempo para leitura atenciosa do conteúdo e realização das atividades de aprendizagem.

2.1 Função do roteador

O roteador é um computador com uma finalidade especial, desempenhando um papel fundamental no funcionamento de qualquer rede de dados. Os roteadores são os principais responsáveis por interconectar redes:

- Determinando o melhor caminho para enviar pacotes;
- Encaminhando pacotes para o destino.

Os roteadores executam o encaminhamento de pacotes, aprendendo as redes remotas e mantendo informações de roteamento. O roteador é a junção ou a interseção que conecta várias redes IP. A decisão primária de encaminhamento dos roteadores se baseia nas informações de Camada 3, o endereço IP de destino.

A tabela de roteamento do roteador é usada para localizar a melhor correspondência entre o IP de destino de um pacote e um endereço de rede na tabela de roteamento. A tabela de roteamento acabará determinando a interface de saída que deve encaminhar o pacote, e o roteador encapsulará esse pacote no quadro de enlace de dados apropriado a essa interface de saída.

A figura 08 mostra a topologia usada neste capítulo. A topologia consiste em três roteadores, rotulados R1, R2 e R3. Os roteadores R1 e R2 são conectados por um link WAN, e os roteadores R2 e R3, por outro link WAN. Cada roteador é conectado a uma rede local Ethernet diferente, representada por um switch e um PC.

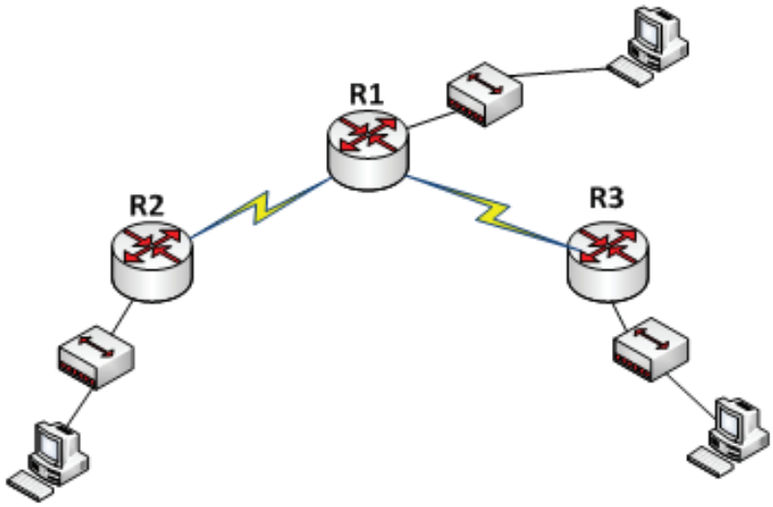


Figura 08 - Topologia de estudo.
Fonte: autor

Todos os roteadores desse exemplo são Cisco 1841. Um roteador Cisco 1841 tem as seguintes interfaces:

- Duas interfaces FastEthernet: FastEthernet 0/0 e FastEthernet 0/1;
- Duas interfaces seriais: Serial 0/0/0 e Serial0/0/1.

As interfaces em seus roteadores podem variar em relação as do 1841, mas você deve ser capaz de acompanhar os comandos nesta aula – com algumas modificações mínimas – e de concluir nos laboratórios práticos. Além disso, como as atividades do Packet Tracer estão disponíveis ao longo da discussão do roteamento estático, você pode testar suas habilidades à medida que elas forem apresentadas. O laboratório mostrará que a "Configuração básica de rota estática" reflete a topologia, as configurações e os comandos abordados nesta aula.

2.2 Examinando interfaces de roteador

Como você pôde verificar na aula anterior, o comando show ip route é usado para exibir a tabela de roteamento. Inicialmente, a tabela de roteamento permanecerá vazia se não houver nenhuma interface configurada.

Na tabela de roteamento de R1 apresentada logo após o comando, nenhuma interface foi configurada com um endereço IP e uma máscara de sub-rede, como você pôde observar.

As rotas estáticas e dinâmicas não serão adicionadas à tabela de roteamento até que as interfaces locais apropriadas, também conhecidas como as interfaces de saída, sejam configuradas no roteador. Esse procedimento será examinado mais atentamente nas próximas aulas.

2.2.1 Interfaces e seu status

O status de cada interface pode ser examinado usando vários comandos.

O comando show interfaces mostra o status e dá uma descrição detalhada de todas as interfaces no roteador. Como você pode notar, a saída do comando pode ser bem longa. Para exibir as mesmas informações, mas para uma interface específica, como FastEthernet 0/0, use o comando show interfaces com um parâmetro que especifique a interface. Por exemplo:

```
R1#show interfaces fastethernet 0/0

FastEthernet0/0 is administratively down, line protocol is down
```

Observe que a interface está administratively down e o line protocol is down. "Administratively down" (desativada administrativamente) significa que a interface está no modo desligado, ou desligada. "Line protocol is down" (Protocolo de linha está inativo) significa, nesse caso, que a interface não está recebendo um sinal de operadora de um switch ou do hub. Essa condição também pode existir devido ao fato de a interface estar no modo desligado (shutdown).

Você observará que o comando show interfaces não mostra nenhum endereço IP nas interfaces de R1. A razão disso é que nós ainda não configuramos endereços IP em nenhuma das interfaces.

2.2.2 Comandos adicionais para examinar o status da interface

O comando show ip interface brief pode ser usado para ver uma porção das informações de interface em um formato resumido.

O comando show running-config exibe o arquivo de configuração atual usado pelo roteador. Os comandos de configuração são armazenados temporariamente no arquivo de configuração em execução e implementados imediatamente pelo roteador. Usar esse comando é outra forma de verificar o status de uma interface, como FastEthernet 0/0.

R1#show running-config

<parte da saída do comando omitida>

interface FastEthernet0/0

no ip address

shutdown

<parte da saída do comando omitida>

No entanto, usar show running-config não é necessariamente a melhor forma de verificar as configurações de interface. Use o comando show ip interface brief para verificar rapidamente se as interfaces estão up (ativas) e up (administrativamente up e o protocolo de linha estão up).

2.2.3 Configurando uma interface Ethernet

Como mostrado, R1 ainda não tem nenhuma rota. Adicionemos uma rota, configurando uma interface e exploremos o que ocorre exatamente quando essa interface é ativada. Por padrão, todas as interfaces do roteador são desligadas (shutdown) ou desativadas. Para habilitar essa interface, use o comando no shutdown, que altera a interface de "administratively down" para "up".

R1(config)#interface fastethernet 0/0

R1(config-if)#ip address 172.16.3.1 255.255.255.0

R1(config-if)#no shutdown

A seguinte mensagem retorna do IOS:

*Mar 1 01:16:08.212: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up

*Mar 1 01:16:09.214: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Ambas as mensagens são importantes. A primeira mensagem changed state to up indica que, fisicamente, a conexão está boa. Se você não obtiver essa primeira mensagem, certifique-se de que a interface esteja adequadamente conectada a um switch ou um hub.

Embora habilitada no shutdown, uma interface Ethernet não permanecerá em funcionamento, ou ativa, a menos que esteja recebendo um sinal de operadora de outro dispositivo (switch, hub, PC ou outro roteador).

A segunda mensagem "changed state to up" indica que a camada de enlace de dados está em funcionamento. Em interfaces de rede local, normalmente não alteramos os parâmetros da camada de enlace de dados. No entanto, as interfaces WAN em um ambiente de laboratório exigem a sincronização em um lado do link, como abordado no Laboratório 1.5.1, "Cabeamento de rede e configuração de roteador básica", bem como posteriormente na seção "Configurando uma Interface Serial". Se você não definir corretamente o clock rate, o protocolo de linha (a camada de enlace de dados) não será alterado para ativado.

2.2.4 Mensagens não solicitadas do IOS

O IOS costuma enviar mensagens não solicitadas semelhantes às mensagens changed state to up recém-abordadas. Como você pode ver na figura, às vezes, essas mensagens ocorrerão quando você estiver digitando um comando, como ao configurar uma descrição para a interface. A mensagem do IOS não afeta o comando, mas pode fazer com que você perca a localização na linha onde você estava digitando.

Para manter a saída não solicitada separada da sua entrada, acesse o modo de configuração de linha da porta de console e adicione o comando logging synchronous, como mostrado. Você verá que as mensagens retornadas pelo IOS não interferem mais na sua digitação.

Agora observe a tabela de roteamento mostrada. Observe que R1 tem uma interface FastEthernet 0/0 "diretamente conectada" a uma nova rede. A interface foi configurada com o endereço IP 172.16.3.1/24, que faz dele um membro da rede 172.16.3.0/24.

Examine a seguinte linha de saída da tabela:

C 172.16.3.0 is directly connected, FastEthernet0/0

O C no início de cada rota indica que se trata de uma rede conectada diretamente. Em outras palavras, R1 tem uma interface que pertence a essa rede. O significado de C é definido na lista de códigos na parte superior da tabela de roteamento.

A máscara de sub-rede /24 dessa rota é exibida na linha acima da rota real.

172.16.0.0/24 is subnetted, 1 subnets

C 172.16.3.0 is directly connected, FastEthernet0/0

Roteadores normalmente armazenam endereços de rede

Com raríssimas exceções, as tabelas de roteamento têm rotas para endereços de rede, e não endereços de host individuais. A rota 172.16.3.0/24 na tabela de roteamento significa que essa rota corresponde a todos os pacotes com um endereço de destino pertencente a essa rede. Ter uma única rota representando uma rede inteira de endereços IP de host diminui a tabela de roteamento, com menos rotas, o que resulta em pesquisas mais rápidas na tabela de roteamento. A tabela de roteamento pode conter todos os 254 endereços IP de host individuais para a rede 172.16.3.0/24, mas essa é uma forma ineficaz de armazenar endereços.

Uma agenda telefônica é uma boa analogia para a estrutura de uma tabela de roteamento. Uma agenda telefônica é uma lista de nomes e números de telefone, classificados em ordem alfabética pelo sobrenome. Ao procurar um número, podemos supor que, quanto menos nomes houver na lista, mais rápida será a localização de um determinado nome. Em uma agenda com 20 páginas e talvez 2.000 entradas será muito mais fácil de pesquisar do que em uma com 200 páginas e 20.000 entradas.

A agenda só contém uma listagem para cada número de telefone. Por exemplo, a família Stanford pode ser listada como:

Stanford, Harold, 742 Evergreen Terrace, 555-1234

Essa é a única entrada para todos os que moram nesse endereço e têm o mesmo número de telefone. A agenda telefônica pode conter uma listagem para cada pessoa, mas isso aumentaria o tamanho da lista. Por exemplo, poderia haver uma listagem separada para Harold Stanford, Margaret Stanford, Brad Stanford, Leslie Stanford e Maggie Stanford – todos com o mesmo endereço e número de telefone. Se isso fosse feito com todas as famílias, a agenda telefônica seria muito maior e demoraria mais para pesquisá-la.

As tabelas de roteamento funcionam da mesma forma: uma entrada na tabela representa uma "família" de dispositivos em que todos compartilham a mesma rede ou espaço de endereço (a diferença entre uma rede e um espaço de endereço será esclarecida à medida que você avançar no curso). Quanto menos entradas houver na tabela de roteamento, mais rápido será o processo de pesquisa. Para manter as tabelas de roteamento menores, são listados endereços de rede com máscaras de sub-rede, e não endereços IP de host individuais.

Às vezes, uma "rota de host" é inserida na tabela de roteamento, o que representa um endereço IP de host individual. Ela é listada com o endereço IP de host do dispositivo e uma máscara de sub-rede /32 (255.255.255.255). O tópico das rotas de host é abordado em outro curso

2.3 Conectando uma interface WAN fisicamente

A camada física WAN descreve a interface entre o Equipamento de Terminal de Dados (DTE, Data Terminal Equipment) e o Equipamento de Comunicação de Dados (DCE, Data Circuit-terminating Equipment). Normalmente, DCE é a operadora, e DTE o dispositivo conectado. Nesse modelo, os serviços oferecidos ao DTE são disponibilizados por um modem ou uma CSU/DSU.

Normalmente, o roteador é o dispositivo DTE, estando conectado a uma CSU/DSU, que é o dispositivo DCE. A CSU/DSU (dispositivo DCE) é usada para converter os dados do roteador (dispositivo DTE) em uma forma aceitável para a operadora WAN. A CSU/DSU (dispositivo DCE) também é responsável por converter os dados da operadora WAN em uma forma aceitável pelo roteador (dispositivo DTE). O roteador costuma ser conectado à CSU/DSU usando um cabo serial DTE, conforme mostrado.

As interfaces seriais exigem um sinal de clock para controlar o timing da comunicação. Na maioria dos ambientes, a operadora (um dispositivo DCE, como uma CSU/DSU) fornecerá o clock. Por padrão, roteadores Cisco são dispositivos DTE. No entanto, em um ambiente de laboratório, não usamos nenhuma CSU/DSU e, obviamente, não temos uma operadora WAN.

2.3.1 Configurando links seriais em um ambiente de laboratório.

Em links seriais interconectados diretamente, como em um ambiente de laboratório, um lado de uma conexão deve ser considerado um DCE e fornecer um sinal de clock. Embora as interfaces seriais Cisco sejam dispositivos DTE por padrão, elas podem ser configuradas como dispositivos DCE.

Para configurar um roteador como dispositivo DCE:

1. Conecte a extremidade DCE do cabo à interface serial.

2. Configure o sinal de clock na interface serial usando o comando clock rate.

Os cabos seriais usados no laboratório costumam ser de dois tipos.

- Um cabo crossover DTE/DCE, no qual uma extremidade é DTE, e a outra DCE.

- Um cabo DTE conectado a um cabo DCE

Em nossa topologia de laboratório, a interface Serial 0/0/0 em R1 é conectada à extremidade DCE do cabo, e a interface serial 0/0/0 em R2 é conectada à extremidade DTE do cabo. O cabo deve ser rotulado como DTE ou DCE.

Você também pode diferenciar DTE de DCE, observando o conector entre os dois cabos. O cabo DTE tem um conector macho, e o cabo DCE um conector fêmea.

Se um cabo for conectado entre os dois roteadores, você poderá usar o comando show controllers para determinar qual extremidade do cabo está acoplada a essa interface. Na saída do comando, observe que R1 tem o cabo DCE conectado à sua interface serial 0/0 e que não há nenhum clock rate definido.

R1#show controllers serial 0/0/0

Interface Serial0/0/0

Hardware is PowerQUICC MPC860

DCE V.35, no clock

<saída de comando omitida>

Quando o cabo for conectado, o clock poderá ser definido com o comando clock rate. Os clock rates disponíveis, em bits por segundo, são 1200, 2400, 9600, 19200, 38400, 56000, 64000, 72000, 125000, 148000, 500000, 800000, 1000000, 1300000, 2000000 e 4000000. Algumas taxas de bit talvez não estejam disponíveis em determinadas interfaces seriais. Como a interface serial 0/0/0 em R1 tem o cabo DCE acoplado, configuraremos a interface com um clock rate.

R1(config)#interface serial 0/0/0

R1(config-if)#clock rate 64000

01:10:28: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

2.4 Conceitos da tabela de roteamento

Revisemos a finalidade de uma tabela de roteamento. Uma tabela de roteamento é uma estrutura de dados usada para armazenar informações de roteamento adquiridas de origens diferentes. A principal finalidade de uma tabela de roteamento é fornecer ao roteador caminhos para redes de destino diferentes.

A tabela de roteamento consiste em uma lista de endereços de rede "conhecidos" – ou seja, os endereços conectados diretamente, configurados estaticamente e apreendidos dinamicamente. R1 e R2 só têm rotas para redes diretamente conectadas.

Resumo

Nessa aula, você pôde verificar como as rotas estáticas podem ser usadas para alcançar redes remotas. Redes remotas são redes que só podem ser alcançadas encaminhando-se o pacote para outro roteador. As rotas estáticas são facilmente configuradas. No entanto, em grandes redes, essa operação manual pode ser bastante incômoda. Como nós veremos em aulas posteriores, as rotas estáticas ainda são usadas – mesmo quando um protocolo de roteamento dinâmico é implementado.

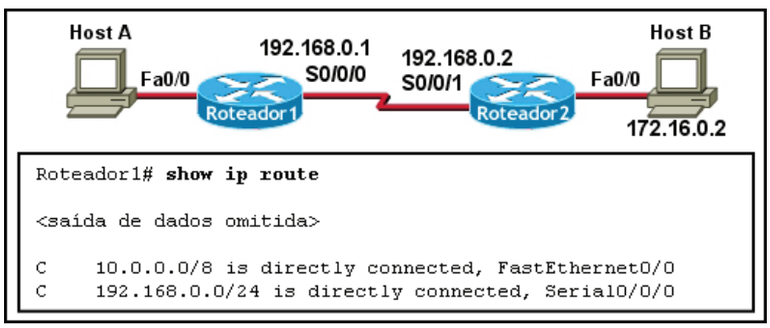
As rotas estáticas podem ser configuradas com um endereço IP do próximo salto, que normalmente é o endereço IP do roteador do próximo salto. Quando um endereço IP do próximo salto é usado, o processo da tabela de roteamento deve resolver esse endereço para uma interface de saída. Em links seriais ponto a ponto, costuma ser mais eficaz configurar a rota estática com uma interface de saída. Em redes multiacesso, como Ethernet, tanto um endereço IP do próximo salto quanto uma interface de saída pode ser configurado na rota estática.

As rotas estáticas têm uma distância administrativa padrão de "1". Essa distância administrativa também se aplica a rotas estáticas configuradas com um endereço do próximo salto, bem como uma interface de saída.

Uma rota estática só será inserida na tabela de roteamento se o endereço IP do próximo salto puder ser resolvido por meio de uma interface de saída. Mesmo que a rota estática seja configurada com um endereço IP do próximo salto ou uma interface de saída, se a interface de saída usada para encaminhar esse pacote não estiver na tabela de roteamento, a rota estática não será incluída nessa tabela.

Atividades de aprendizagem

1. Uma rota estática que aponta para o IP de próximo salto terá qual distância administrativa e métrica na tabela de roteamento?



Fonte: http://www.ccna4u.org/2011/06/ccna-2-chapter-2-2011-v4-0-answers-100.html

a) distância administrativa e métrica iguais a 0

b) distância administrativa 0 e métrica igual a 0

c) distância administrativa 1 e métrica igual a 0

d) distância administrativa e métrica iguais a 1

2. Consulte a exibição acima. Que rota estática deve ser configurada no Roteador 1 para que o host A seja capaz de alcançar o host B na rede 172.16.0.0?

a) ip route 192.168.0.0 172.16.0.0 255.255.0.0

b) ip route 172.16.0.0 255.255.0.0 192.168.0.1

c) ip route 172.16.0.0 255.255.0.0 S0/0/1

d) ip route 172.16.0.0 255.255.0.0 S0/0/0

3. A saída do comando Router# show interfaces serial 0/1 exibe o seguinte:

Serial0/1 está ativado, e o protocolo de linha está desativado.

Qual é a causa mais provável da inatividade do protocolo de linha?

a) Serial0/1 está desativado.

b) Não há nenhum cabo conectando os roteadores.

c) O roteador remoto está usando serial 0/0.

d) Nenhum clock rate foi definido.

4. Por que é aconselhável inserir um endereço IP de próximo salto ao criar uma rota estática cuja interface de saída é uma rede Ethernet?

a) Adicionar o endereço de próximo salto elimina a necessidade de o roteador fazer alguma pesquisa na tabela de roteamento antes de encaminhar um pacote.

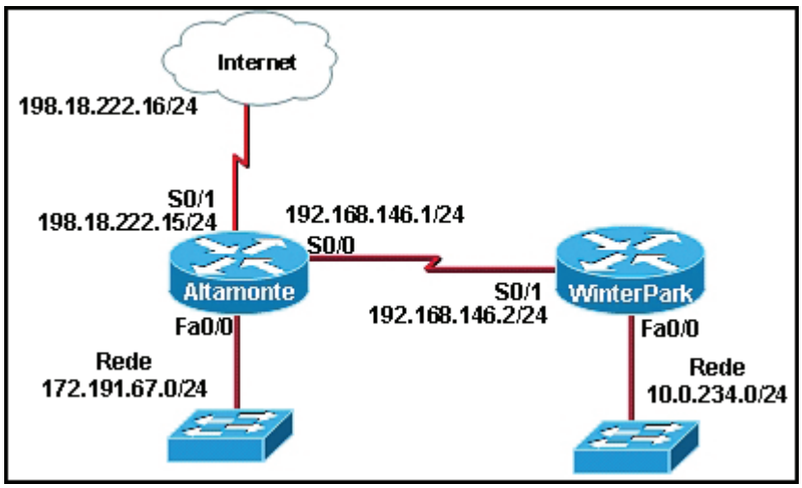
b) Em uma rede com vários acessos, o roteador não pode determinar o

endereço MAC de próximo salto do quadro Ethernet sem um endereço de próximo salto.

c) Usar um endereço de próximo salto em uma rota estática fornece uma rota com uma métrica inferior.

d) Em redes com vários acessos, usar um endereço de próximo salto em uma rota estática torna essa rota uma rota candidata padrão.

5. Consulte a exibição. Qual conjunto de comandos irá configurar rotas estáticas e permitir aos roteadores WinterPark e Altamonte entregar pacotes em cada LAN (Local Area Network, Rede local) e direcionar todos os demais tráfegos para a Internet?



Fonte: http://www.ccna4u.org/2011/06/ccna-2-chapter-2-2011-v4-0-answers-100.html

a) WinterPark(config)# ip route 0.0.0.0 0.0.0.0 192.168.146.1

b) Altamonte(config)# ip route 10.0.234.0 255.255.255.0 192.168.146.2

c) Altamonte(config)# ip route 0.0.0.0 0.0.0.0 s0/1

d) WinterPark(config)# ip route 0.0.0.0 0.0.0.0 192.168.146.1

e) Altamonte(config)# ip route 10.0.234.0 255.255.255.0 192.168.146.2

f) Altamonte(config)# ip route 198.18.222.0 255.255.255.255 s0/1

g) WinterPark(config)# ip route 172.191.67.0 255.255.255.0

192.168.146.1

h) WinterPark(config)# ip route 0.0.0.0 0.0.0.0 192.168.146.1

i) Altamonte(config)# ip route 10.0.234.0 255.255.255.0 192.168.146.2

j) WinterPark(config)# ip route 172.191.67.0 255.255.255.0 192.168.146.1

k) Altamonte(config)# ip route 10.0.234.0 255.255.255.0 192.168.146.2

l) Altamonte(config)# ip route 0.0.0.0 0.0.0.0 s0/0

Prezado(a) estudante,

Finalizamos esta aula, na qual você deu mais um passo em seu processo de aprendizagem.Nosso próximo tema será protocolos de roteamento dinâmico, conteúdo também relevante,dentro da disciplina Rede de Computadores. Continue atento(a) ao que virá.

Aula 3. Protocolos de roteamento dinâmico

Objetivos:

- descrever a função do protocolo de roteamento dinâmico;
- identificar os modos de classificar protocolos de roteamento; e
- distinguir diversos elementos na tabela de roteamento.

Caro(a) estudante,

Nas aulas anteriores, você teve oportunidade de verificar como os roteadores são usados para encaminhar pacotes e também que eles aprendem sobre as redes remotas usando rotas estáticas e roteamento dinâmico. Você pôde constatar também como as rotas para redes remotas podem ser configuradas manualmente através de rotas estáticas.

As redes de dados que usamos no cotidiano para aprendizado, diversão e trabalho variam de pequenas redes locais a grandes redes globais interconectadas. Em casa, você pode ter um roteador e dois ou mais computadores. No trabalho, sua organização pode ter vários roteadores e switches para atender às necessidades de comunicação de dados de centenas ou até mesmo milhares de PCs.

Esta aula introduz os protocolos de roteamento dinâmico, incluindo suas diferenças de classificação, qual é a métrica que eles usam para determinar o melhor caminho e os benefícios obtidos ao usar um protocolo de roteamento dinâmico. Prepare-se para o novo conteúdo com disposição para estudar e aprender.

Geralmente, os protocolos de roteamento dinâmico são usados em redes maiores para aliviar a sobrecarga administrativa e operacional causada pelo uso de rotas estáticas. Uma rede normalmente usa a combinação de um protocolo de roteamento dinâmico e rotas estáticas. Na maioria das redes, um único protocolo de roteamento dinâmico é usado. No entanto, há casos

em que partes diferentes da rede podem usar protocolos de roteamento diferentes.

Desde o início dos anos 1980, surgiram vários protocolos de roteamento dinâmico diferentes. Nesta aula, começaremos a tratar de algumas de suas características e diferenças. No entanto, elas ficarão mais evidentes nas aulas posteriores, quando apresentaremos vários desses protocolos de roteamento em detalhes.

Embora muitas redes usem um único protocolo de roteamento dinâmico ou usem somente rotas estáticas, é importante que o(a) profissional de rede entenda os conceitos e as operações de todos os protocolos de roteamento. Um(a) profissional de rede deve ser capaz de tomar uma decisão fundamentada sobre quando usar um protocolo de roteamento dinâmico e qual, entre eles, é a melhor escolha para um ambiente específico.

3.1 A evolução dos protocolos de roteamento dinâmico

Os protocolos de roteamento dinâmico são usados em redes desde o início dos anos 1980. A primeira versão do RIP foi lançada em 1982, mas alguns dos algoritmos básicos do protocolo foram usados na ARPANET já em 1969.

À medida que as redes evoluíam e se tornavam mais complexas, surgiam novos protocolos de roteamento.

Um dos primeiros protocolos de roteamento foi o Protocolo de Informações de Roteamento (RIP, Routing Information Protocol). O RIP evoluiu para uma versão mais nova: o RIPv2. No entanto, a versão mais recente do RIP ainda não pode ter sua escala alterada para implementações de rede maiores. Para atender às necessidades dessas redes, foram desenvolvidos dois protocolos de roteamento avançado:

- Abrir caminho mais curto primeiro (OSPF, Open Shortest Path First) e;
- Sistema intermediário para sistema intermediário (IS-IS, Intermediate System-to-Intermediate System).

A Cisco desenvolveu o Protocolo de Roteamento de Gateway Interior (IGRP, Interior Gateway Routing Protocol) e o EIGRP, cujas escalas também são boas

em implementação de rede maiores.

Além disso, havia a necessidade de interconectar várias redes interconectadas e possibilitar o roteamento entre elas. O Protocolo de Roteamento de Gateway de Borda (BGP, Border Gateway Protocol) agora é usado entre os ISPs e também entre ISPs e seus maiores clientes particulares para trocar informações de roteamento.

Com o advento de numerosos dispositivos consumidores que usam o IP, o espaço de endereçamento IPv4 está quase esgotado. Assim surgiu o IPv6. Para oferecer suporte à comunicação com base no IPv6, foram desenvolvidas versões mais recentes dos protocolos de roteamento IP (consulte a linha IPv6 da tabela).

3.1.1 A função do protocolo de roteamento dinâmico

O que são exatamente os protocolos de roteamento dinâmico? Os protocolos de roteamento são usados para facilitar a troca de informações de roteamento entre roteadores. Eles permitem que os roteadores compartilhem informações dinamicamente sobre redes remotas e adicionam essas informações automaticamente às suas próprias tabelas de roteamento (isso é mostrado na animação).

Os protocolos de roteamento determinam o melhor caminho para cada rede adicionada à tabela de roteamento. Um dos principais benefícios do uso de um protocolo de roteamento dinâmico é que os roteadores trocam informações de roteamento sempre que há uma alteração de topologia. Essa troca permite que os roteadores apreendam novas redes automaticamente e também localizem caminhos alternativos quando houver uma falha do link atual para uma rede.

Comparados ao roteamento estático, os protocolos de roteamento dinâmico requerem uma sobrecarga administrativa menor. Entretanto, para usar os protocolos de roteamento dinâmico, é necessário dedicar parte dos recursos de um roteador à operação de protocolos, incluindo tempo de CPU e largura de banda de link de rede. Apesar dos benefícios do roteamento dinâmico, o roteamento estático ainda é usado. Há situações em que o roteamento estático é mais apropriado, e outras em que o roteamento dinâmico é a melhor escolha. Frequentemente, você encontrará uma combinação de ambos os tipos de roteamento em qualquer rede que tenha um nível moderado de

complexidade. Apresentaremos as vantagens e as desvantagens dos roteamentos estático e dinâmico posteriormente, nesta aula.

3.1.2 A finalidade dos protocolos de roteamento dinâmico

Um protocolo de roteamento é um conjunto de processos, algoritmos e mensagens, usado para trocar informações de roteamento e tornar popular a tabela de roteamento com os melhores caminhos escolhidos por esse protocolo. Entre as finalidades de um protocolo de roteamento estão:

- a detecção de redes remotas;
- a manutenção de informações de roteamento atualizadas;
- a escolha do melhor caminho para as redes de destino;
- a capacidade de localizar um novo melhor caminho, se o caminho atual não estiver mais disponível.

3.1.3 Quais os componentes de um protocolo de roteamento?

- **Estruturas de dados** - Alguns protocolos de roteamento usam tabelas e/ou bancos de dados para suas operações. Essas informações são mantidas na RAM.
- **Algoritmo** - Um algoritmo é uma lista finita de etapas usadas na realização de uma tarefa. Os protocolos de roteamento usam algoritmos para facilitar as informações de roteamento e para determinar o melhor caminho.
- **Mensagens do protocolo de roteamento** - Os protocolos de roteamento usam vários tipos de mensagens para descobrir roteadores vizinhos, trocar informações de roteamento e outras tarefas para aprender e manter informações precisas sobre a rede.

3.1.4 Operação do protocolo de roteamento dinâmico

Todos os protocolos de roteamento têm a mesma finalidade: aprender redes remotas e adaptar-se rapidamente sempre que houver uma alteração na topologia. O método usado pelo protocolo de roteamento para isso depende

do algoritmo que ele usa e das características operacionais desse protocolo. As operações de um protocolo de roteamento dinâmico variam de acordo com o tipo de protocolo. Em geral, as operações de um protocolo de roteamento dinâmico podem ser descritas da seguinte forma:

- O roteador envia e recebe mensagens de roteamento em suas interfaces;
- O roteador compartilha mensagens e informações de roteamento com outros roteadores que estão usando o mesmo protocolo de roteamento;
- Os roteadores trocam informações de roteamento para aprender redes remotas;
- Quando um roteador detecta uma alteração de topologia, o protocolo de roteamento pode anunciar essa alteração a outros roteadores.

3.2 Uso do roteamento estático

Antes de identificar os benefícios dos protocolos de roteamento dinâmico, precisamos considerar os motivos pelos quais nós usaríamos o roteamento estático. O roteamento dinâmico tem várias vantagens sobre o roteamento estático. No entanto, o roteamento estático ainda é usado em redes. De fato, as redes geralmente usam uma combinação de roteamento estático e dinâmico.

O roteamento estático tem vários usos principais, incluindo:

- Facilidade de manutenção da tabela de roteamento em redes menores que não possuem crescimento significativo esperado;
- Roteamento de e para redes stub (consulte a aula 2);
- Uso de uma única rota padrão, usada para representar um caminho para qualquer rede;
- A não correspondência mais específica com outra rota na tabela de roteamento.

3.2.1 Vantagens e desvantagens do roteamento estático

Os recursos de roteamento dinâmico e estático são comparados diretamente. Dessa comparação, podemos listar as vantagens de cada método de roteamento. As vantagens de um método são as desvantagens do outro.

a) Vantagens do roteamento estático:

- processamento mínimo da CPU.
- maior facilidade para o administrador entender.
- facilidade de configuração.

b) Desvantagens do roteamento estático:

- configuração e manutenção demoradas.
- configuração propensa a erros, principalmente em redes grandes.
- necessidade de intervenção do administrador para manter as informações da rota alterada.
- mau dimensionamento com redes em desenvolvimento; a manutenção fica muito complicada.
- requer conhecimento completo da rede inteira para implementação adequada.

3.2.2 Vantagens e desvantagens do roteamento dinâmico

a) Vantagens do roteamento dinâmico:

- o administrador tem menos trabalho para manter a configuração ao adicionar ou excluir redes.
- os protocolos reagem automaticamente às alterações de topologia.
- a configuração é menos propensa a erros.

- mais escalável, o desenvolvimento da rede não costuma ser um problema.

b) Desvantagens do roteamento dinâmico:

- são usados recursos de roteador (ciclos de CPU, memória e largura de banda de link).

- são necessários mais conhecimentos de administrador para configuração, verificação e solução de problemas.

3.3 Classificação dos protocolos de roteamento dinâmico

Os protocolos de roteamento podem ser classificados em grupos diferentes de acordo com suas características. Os protocolos de roteamento mais usados são:

- **RIP** - Uma distância vetor do protocolo de roteamento interior;

- **IGRP** - O vetor de distância de roteamento interior desenvolvido pela Cisco (substituído de 12.2 IOS e posterior);

- **OSPF** - Um protocolo de roteamento interior de link-state;

- **IS-IS** - Um protocolo de roteamento interior de link-state;

- **EIGRP** - O protocolo de roteamento interior de vetor de distância avançado desenvolvido pela Cisco;

- **BGP** - Um protocolo de roteamento exterior de vetor de caminho.

Um sistema autônomo (AS, Autonomous System) – também conhecido como um domínio de roteamento - é um conjunto de roteadores sob a mesma administração. Alguns exemplos típicos são a rede interna de uma empresa e a rede de um provedor de Internet. Como a Internet é baseada no conceito de sistema autônomo, são necessários dois tipos de protocolos de roteamento, ou seja, protocolos de roteamento interno e externo. Esses protocolos são:

- Protocolos de gateway interior (IGP, Interior Gateway Protocol), usados para roteamento de sistema intra-autônomo - roteamento dentro de um sistema autônomo;

- Protocolos EGP, usados para roteamento de sistema interautônomo, ou seja, roteamento entre sistemas autônomos.

3.4 Características dos protocolos de roteamento IGP e EGP

Os IGPs são usados para roteamento dentro de um domínio de roteamento; redes sob controle de uma única organização. Geralmente, um sistema autônomo é formado por muitas redes individuais que pertencem a empresas, escolas e outras instituições. Um IGP é usado para fazer o roteamento no sistema autônomo e também nas próprias redes individuais. Por exemplo, o CENIC opera um sistema autônomo formado por escolas, faculdades e universidades da Califórnia. O CENIC usa um IGP para rotear dentro de seu sistema autônomo com a finalidade de interconectar todas essas instituições. Cada instituição educacional também usa um IGP próprio para rotear dentro de sua própria rede individual. O IGP usado pelas entidades fornece a determinação do melhor caminho em seus próprios domínios de roteamento, da mesma maneira que o IGP usado pelo CENIC fornece as melhores rotas no próprio sistema autônomo. Os IGPs para IP incluem RIP, IGRP, EIGRP, OSPF e IS-IS.

Os protocolos de roteamento, e mais especificamente o algoritmo usado por esse protocolo de roteamento, usam uma métrica para determinar o melhor caminho para uma rede. A métrica usada pelo protocolo de roteamento RIP é a contagem de saltos, que é o número de roteadores que um pacote deve percorrer ao alcançar outra rede. O OSPF usa a largura de banda para determinar o caminho mais curto.

Por outro lado, os EGPs foram projetados para o uso entre sistemas autônomos diferentes que estejam sob o controle de administrações diferentes. O BGP é o único EGP atualmente viável, somado ao fato de ser o protocolo de roteamento usado pela Internet. O BGP é um protocolo de vetor de caminho que pode usar muitos atributos diferentes para medir rotas. No nível do ISP, geralmente há mais questões importantes do que a simples escolha do caminho mais rápido. Normalmente, o BGP é usado entre ISPs. Às vezes, ele é usado entre uma empresa e um ISP.

Resumo

Nesta aula mostramos que os protocolos de roteamento dinâmico são usados pelos roteadores para aprender automaticamente redes remotas de outros roteadores. Apresentamos ainda os vários protocolos de roteamento dinâmico diferentes.

Demonstramos também que os protocolos de roteamento podem ser classificados como classful ou classless, link-state, de vetor de distância ou de vetor de caminho, e se um protocolo de roteamento é um protocolo IGP ou um EGP. As diferenças entre essas classificações serão mais bem compreendidas nas aulas posteriores, nas quais traremos mais informações sobre esses protocolos e conceitos de roteamento.

Os protocolos de roteamento detectam redes remotas e também têm um procedimento para manter informações de rede precisas. Quando há uma mudança na topologia, é função do protocolo de roteamento informar aos outros roteadores sobre essa mudança.

Quando houver uma mudança na topologia de rede, alguns protocolos de roteamento podem propagar essa informação por todo o domínio de roteamento com mais rapidez do que outros protocolos de roteamento. O processo que faz com que todas as tabelas de roteamento fiquem consistentes é chamado de convergência. A convergência ocorre quando todos os roteadores no mesmo domínio de roteamento ou área têm informações completas e precisas sobre a rede.

Atividades de aprendizagem

1. Quais são as duas afirmativas que descrevem corretamente os conceitos de distância administrativa e métrica? (Escolha duas.)

a) A distância administrativa se refere à confiabilidade de uma determinada rota.

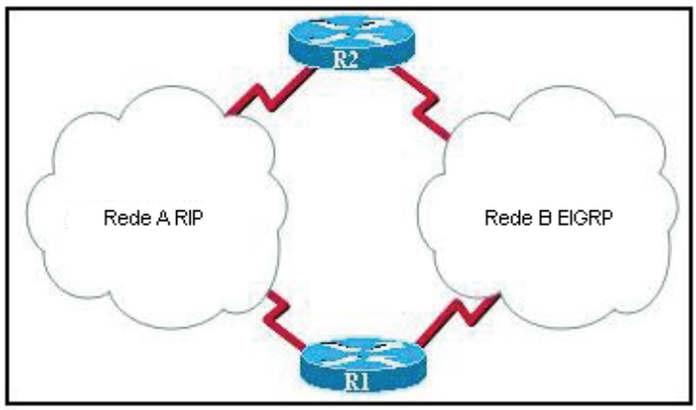
b) Um roteador instala primeiramente as rotas com as maiores distâncias administrativas.

c) O valor da distância administrativa não pode ser alterado pelo administrador de rede.

d) As rotas com a menor métrica para um destino indicam o melhor caminho.

e) A métrica é sempre determinada com base na contagem de saltos.

f) A métrica varia de acordo com o protocolo da Camada 3 que está sendo roteada, como IP ou IPX (Internetwork packet exchange, Troca de pacotes em redes interconectadas).



Fonte: http://www.blogtj.ro/refer-to-the-exhibit-which-statement-correctly-describes-how-r1-will-determine-the-best-path-to-r2/

2. Consulte a exibição. Que afirmativa descreve corretamente como R1 irá determinar o melhor caminho para R2?

a) R1 irá instalar uma rota do protocolo RIP usando a rede A em sua tabela de roteamento porque a distância administrativa do protocolo RIP é maior que o protocolo EIGRP.

b) R1 irá instalar uma rota do protocolo RIP usando a rede A em sua tabela de roteamento porque o custo do caminho do protocolo RIP é menor que o protocolo EIGRP.

c) R1 irá instalar uma rota do protocolo EIGRP usando a rede B em sua tabela de roteamento porque a distância administrativa do protocolo EIGRP é menor que o protocolo RIP.

d) R1 irá instalar uma rota do protocolo EIGRP usando a rede B em sua tabela de roteamento porque o custo do caminho do protocolo EIGRP é menor que o protocolo RIP.

e) R1 irá instalar uma rota do protocolo EIGRP e uma rota do protocolo RIP em sua tabela de roteamento e fará o balanceamento de carga entre eles.

3. Qual é a finalidade de um protocolo de roteamento?

a) É usado para criar e manter tabelas ARP.

b) Proporciona um método para a segmentação e remontagem de pacotes de dados.

c) Permite que um administrador elabore um esquema de endereçamento para a rede.

d) Permite que um roteador compartilhe informações sobre redes conhecidas com outros roteadores.

e) Proporciona um procedimento para a codificação e decodificação dos dados em bits para o encaminhamento de pacotes.

4. Qual das seguintes alternativas melhor descreve a operação dos protocolos de roteamento vetor de distância?

a) Utilizam a contagem de saltos como sua única métrica.

b) Enviam atualização apenas quando uma nova rede é adicionada.

c) Enviam suas tabelas de roteamento aos vizinhos diretamente conectados.

d) Inundam toda a rede com atualizações de roteamento.

5. Quando vários protocolos de roteamento têm uma rota para a mesma rede de destino, o que determina qual rota é instalada na tabela de roteamento?

a) melhor métrica

b) menor contagem de saltos

c) maior largura de banda disponível

d) menor distância administrativa

e) menor custo

Prezado(a) estudante,

Finalizamos esta aula, que tratou de protocolos de roteamento dinâmico. Mas para a sua qualificação profissional na área que escolheu, é preciso continuar estudando. A próxima aula será sobre desempenho da Rede (Switching). Prepare-se para este novo conteúdo.

Aula 4. Desempenho da Rede (Switching)

Objetivos:

- identificar as funções que permitem a um switch encaminhar quadros Ethernet em uma rede local;
- reconhecer a função de VLANs em uma rede e a função do entroncamento de VLANs em uma rede; e
- configurar VLANs nos switches em uma topologia de rede.

Caro(a) estudante,

Vamos apresentar mais um conteúdo que faz parte da disciplina Rede de Computadores. Nesta aula esperamos que você aprenda como configurar, gerenciar e solucionar problemas de VLANS e troncos.Você já deve ter percebido que há um encadeamento entre os temas tratados. Assim, se tiver alguma dúvida, volte às aulas anteriores antes de prosseguir, retome o que já estudou e releia com atenção o que já foi exposto.

O desempenho da rede pode ser um fator na produtividade de uma organização e em sua reputação em cumprir o que promete. Uma das tecnologias que contribuem com a excelência do desempenho da rede é a separação dos grandes domínios de broadcast em domínios menores com VLANs (Virtual Local Área Networks). Domínios de broadcast menores limitam o número de dispositivos que participam de broadcasts e permitem separar dispositivos em agrupamentos funcionais, como serviços de banco de dados para um departamento de contabilidade e de transferência de dados em alta velocidade para um departamento de engenharia.

4.1 Apresentando as VLANs

Para observar por que as VLANs estão sendo amplamente usadas atualmente, considere uma pequena universidade comunitária com os alojamentos de

aluno e as salas dos funcionários em um só edifício. Vamos imaginar que em uma rede de uma universidade os computadores dos alunos estão em uma rede local e os computadores dos funcionários em outra. Isso funciona bem porque, como cada departamento está fisicamente ligado, é fácil fornecer recursos de rede a eles.

Um ano depois, a universidade cresceu e agora tem três edifícios. A rede original é igual, mas os computadores dos alunos e dos funcionários estão espalhados em três edifícios. Os alojamentos dos alunos continuam no quinto andar e as salas dos funcionários continuam no terceiro andar. No entanto, agora o departamento de TI deseja assegurar que todos os computadores dos alunos compartilhem os mesmos recursos de segurança, com os controles da largura de banda. Como a rede pode acomodar as necessidades compartilhadas dos departamentos separados geograficamente? Você cria uma rede local grande e conecta todos os departamentos? Qual seria a facilidade para fazer alterações nessa rede? Seria ótimo agrupar as pessoas com os recursos que elas usam, independentemente da sua localização geográfica, e isso facilitaria o gerenciamento de suas necessidades específicas de segurança e largura de banda. Na figura 09 vemos um exemplo de utilização de Vlans.

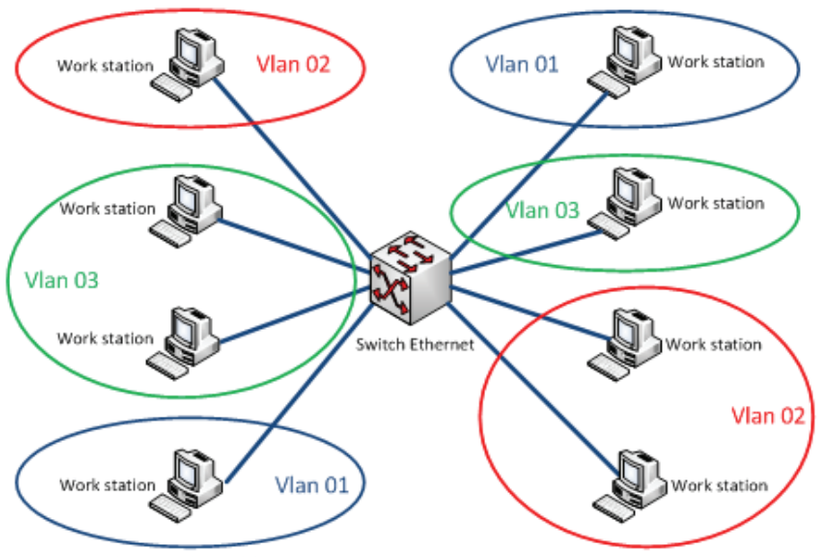


Figura 09 - Vlans estabelecidas em um único Switch.
Fonte: autor

A solução para a universidade comunitária é usar uma tecnologia chamada rede LAN virtual (VLAN). Uma VLAN permite a um administrador de rede criar grupos de dispositivos logicamente em rede que funcionam como se eles

estivessem em sua própria rede independente, mesmo se compartilharem uma mesma infraestrutura com outras VLANs. Quando você configura uma VLAN, é possível nomeá-la para descrever a função primária dos usuários dessa VLAN. Como outro exemplo, todos os computadores dos alunos de uma escola podem ser configurados na VLAN "Aluno".

Usando VLANs, é possível segmentar redes comutadas logicamente com base em funções, departamentos ou equipes de projeto. Também é possível usar uma VLAN para estruturar geograficamente sua rede e suportar a crescente dependência das empresas de funcionários que trabalham em casa. Na figura, uma VLAN é criada para alunos, e outra para os funcionários. Essas

VLANs permitem ao administrador de rede implementar políticas de acesso e de segurança a grupos específicos de usuários.

4.1.1 Benefícios de uma VLAN

A produtividade do usuário e a capacidade de adaptação da rede são os principais responsáveis pelo crescimento e o sucesso dos negócios. Implementar a tecnologia VLAN permite a uma rede suportar metas comerciais com mais flexibilidade. Os benefícios primários de usar VLANs são os seguintes:

a) Segurança – Grupos que têm dados confidenciais são separados do restante da rede, o que diminui as chances de violação das informações confidenciais. Os computadores dos funcionários estão na VLAN 10, estando totalmente separados do tráfego de dados dos alunos e dos convidados.

b) Redução de custo – Economia de custos é resultante da menor necessidade das atualizações de rede caras e do uso mais eficiente da largura de banda e dos uplinks existentes.

c) Desempenho mais alto – Dividir as redes da Camada 2 simplesmente em vários grupos de trabalho lógicos (domínios de broadcast) reduz um tráfego desnecessário na rede e aumenta o desempenho.

d) Atenuação da tempestade de broadcast – Dividir uma rede em VLANs reduz o número de dispositivos que podem participar de uma situação de descontrole por excesso de broadcast. Conforme abordado em "Configurar um Switch", a segmentação de rede local impede uma situação de descontrole em uma rede devido a excesso de broadcast.

Maior eficiência do pessoal de TI – VLANs simplificam o gerenciamento da rede porque os usuários com requisitos de rede semelhantes compartilham a mesma VLAN. Quando você provisiona um novo switch, todas as políticas e procedimentos já configurados para a VLAN específica são implementados quando as portas são atribuídas. Também é fácil para o pessoal de TI identificar a função de uma VLAN, dando a ela um nome apropriado. Tendo em vista uma identificação mais simples, a VLAN 20 pode ser nomeada como "Aluno", a VLAN 10 nomeada como "Funcionários", e a VLAN 30 "Convidado".

Projeto mais simples ou gerenciamento de aplicativo – VLANs agregam usuários e dispositivos de rede para suportar requisitos de negócios ou geográficos. Ter funções separadas simplifica o gerenciamento de um projeto ou o trabalho com um aplicativo especializado, por exemplo, uma plataforma de desenvolvimento de e-learning para os funcionários. Também é mais fácil determinar o escopo dos efeitos de atualizar os serviços de rede.

4.1.2 Intervalos de ID de VLAN

As VLANs de acesso são divididas em um intervalo normal ou estendido.

a) VLANs de intervalo normal

- Usadas em redes corporativas de pequeno e médio portes.
- Identificadas por uma ID VLAN entre 1 e 1005.
- As IDs 1002 até 1005 são reservadas para VLANs Token Ring e FDDI.
- As IDs 1 e 1002 a 1005 são criadas automaticamente, não podendo ser removidas (você obterá mais informações sobre VLAN posteriormente, nesta aula).
- As configurações são armazenadas em um arquivo do banco de dados de VLAN, chamado vlan.dat. O arquivo vlan.dat é localizado na memória flash do switch.
- O protocolo de entroncamento VLAN (VTP), que ajuda a gerenciar configurações de VLAN entre switches, só pode aprender VLANs de intervalo normal e as armazenar no arquivo de banco de dados da VLAN.

b) VLANs de intervalo estendido

- Permite a operadoras estender sua infraestrutura para um número maior de clientes. Algumas empresas globais podem ser grandes o bastante para precisar de IDs de VLAN de intervalo estendido.
- Elas são identificadas por uma ID VLAN entre 1006 e 4094.
- Elas suportam menos recursos VLAN que as VLANs de intervalo normal.
- Elas são salvas no arquivo de configuração de execução.
- VTP não aprende VLANs de intervalo estendido.

4.2 VLANs configuráveis

Um switch Cisco Catalyst 2960 pode suportar até 255 VLANs de intervalos normal e estendido, embora o número configurado afete o desempenho do hardware de switch. Como uma rede corporativa pode precisar de um switch com muitas portas, a Cisco desenvolveu switches de nível corporativo que podem ser agrupados ou empilhados para criar uma única unidade de comutação, consistindo em nove switches separados. Cada switch separado pode ter 48 portas, o que totaliza 432 portas em uma única unidade de comutação. Nesse caso, o limite de 255 VLANs por um único switch pode ser uma restrição para alguns clientes corporativos.

4.2.1 VLAN de dados

Uma VLAN de dados é uma VLAN configurada para transportar apenas o tráfego gerado pelo usuário. Uma VLAN pode transportar o tráfego baseado em voz ou o tráfego usado para gerenciar o switch, mas esse tráfego não faria parte de uma VLAN de dados. É uma prática comum para separar o tráfego de voz e de gerenciamento do tráfego de dados. A importância de separar dados de usuário dos dados de controle de gerenciamento do switch e do tráfego de voz é realçada pelo uso de um termo especial para identificar VLANs que só transportam dados de usuário – uma "VLAN de dados". Às vezes, uma VLAN de dados é conhecida como VLAN de usuário.

4.2.2 VLAN padrão

Todas as portas de switch se tornam um membro da VLAN padrão após a inicialização do switch. Ter todas as portas de switch participando da VLAN

padrão torna essas portas parte do mesmo domínio de broadcast. Isso permite a um dispositivo conectado a qualquer porta de switch se comunicar com outros dispositivos em outras portas. A VLAN padrão de switches Cisco é VLAN 1. A VLAN 1 tem todos os recursos de qualquer VLAN, exceto por não ser possível renomeá-la e excluí-la. Por padrão, o tráfego de controle da Camada 2, como CDP e o tráfego de protocolo spanning tree, é associado à VLAN 1.

O tráfego da VLAN pode ser encaminhado pelos troncos VLAN que conectam os switches S1, S2 e S3. Trata-se de prática recomendada de segurança alterar a VLAN padrão para uma VLAN diferente da VLAN 1; isso significa configurar todas as portas no switch a serem associadas a uma VLAN padrão diferente da VLAN 1. Os troncos VLAN suportam a transmissão do tráfego de mais de uma VLAN. Embora os troncos VLAN sejam mencionados ao longo desta seção, eles são explicados na próxima seção sobre o entroncamento VLAN.

Alguns administradores de rede usam a expressão "VLAN padrão" para se referir a uma VLAN, diferente da VLAN 1, definida pelo administrador de rede como a VLAN a que todas as portas são atribuídas quando não estão em uso. Nesse caso, a única função que a VLAN 1 desempenha é a de tratar o tráfego de controle da Camada 2 da rede.

4.2.3 VLAN nativa

Uma VLAN nativa é atribuída a uma porta de tronco 802.1Q. Uma porta de tronco 802.1Q oferece suporte ao tráfego de muitas VLANs (tráfego marcado), bem como ao tráfego que não vem de uma VLAN (tráfego sem marcação). A porta de tronco 802.1Q posiciona o tráfego sem marcação na VLAN nativa. A VLAN nativa é a VLAN 99. O tráfego sem marcação é gerado por um computador conectado a uma porta de switch configurada com a VLAN nativa.

As VLANs nativas são definidas na especificação IEEE 802.1Q para manter a compatibilidade com versões anteriores com tráfego sem marcação comum a cenários de rede local antigos. Tendo em vista nossas finalidades, uma VLAN nativa serve como identificador comum em extremidades opostas de um link de tronco. É prática recomendada usar uma VLAN diferente da VLAN 1 como a VLAN nativa.

4.2.4 Portas de switch

As portas de switch são interfaces apenas da Camada 2 associadas a uma porta física. As portas de switch são usadas para gerenciar a interface física e os protocolos associados da Camada 2. Elas não tratam de roteamento ou bridging. As portas de switch pertencem a uma ou mais VLANs.

- Modos de porta de switch VLAN

Ao configurar uma VLAN, você deve atribuir a ela uma ID numérica, podendo também dar-lhe um nome. A finalidade das implementações VLAN é associar criteriosamente portas com VLANs específicas. Você configura a porta para encaminhar um quadro para uma VLAN específica. Conforme mencionado em outra passagem, é possível configurar uma VLAN no modo de voz para suportar o tráfego de voz e de dados provenientes de um telefone IP Cisco. É possível configurar uma porta para pertencer a uma VLAN atribuindo um modo de associação que especifica o tipo de tráfego transportado pela porta e as VLANs asquais ela pode pertencer. Uma porta pode ser configurada para suportar estes tipos de VLAN:

a) VLAN estática – As portas em um switch são atribuídas manualmente a uma VLAN. As VLANs estáticas são configuradas usando a CLI Cisco. Isso também pode ser realizado com aplicativos de gerenciamento de interface gráfica do usuário, como o Cisco Network Assistant. No entanto, um recurso prático da CLI é que, se você atribuir uma interface a uma VLAN que não existe, a nova VLAN será criada para você. Essa configuração não será examinada em detalhes agora. Você verá essa configuração posteriormente.

b) VLAN dinâmica – Esse modo não é amplamente usado em redes de produção, não sendo explorado neste curso. No entanto, é útil saber o que é uma VLAN dinâmica. Uma associação VLAN de porta dinâmica é configurada usando um servidor especial chamado VLAN Membership Policy Server (VMPS). Com o VMPS, você atribui portas de switch a VLANs dinamicamente, com base no endereço MAC de origem do dispositivo conectado à porta. O benefício vem quando você move um host entre portas e switches na rede; o switch atribui dinamicamente a nova porta à VLAN correta para esse host.

c) VLAN de voz – Uma porta é configurada para estar no modo de voz para que seja capaz de suportar um telefone IP acoplado. Antes de configurar uma VLAN de voz na porta, você primeiro precisa configurar uma VLAN para voz e uma VLAN para dados. A VLAN 150 é a VLAN de voz, e a VLAN 20 é a

VLAN de dados. Supõe-se que a rede tenha sido configurada para assegurar que o tráfego de voz pudesse ser transmitido com um status de prioridade sobre outros. Quando um telefone é conectado pela primeira vez a uma porta de switch que está no modo de voz, a porta de switch envia mensagens para o telefone, fornecendo a ele a ID da VLAN de voz e a configuração apropriada. O telefone IP marca as estruturas de voz com a ID da VLAN de voz e encaminha todo o tráfego por essa VLAN específica.

O comando de configuração mls qos trust cos assegura que o tráfego de voz seja identificado como tráfego de prioridade. Lembre-se de que toda a rede deve ser configurada para priorizar o tráfego de voz. Não é possível configurar a porta apenas com esse comando.

O comando switchport voice vlan 150 identifica a VLAN 150 como a VLAN de voz. É possível observar isso na captura na parte inferior da tela: Voice VLAN: 150 (VLAN0150).

O comando switchport access vlan 20 configura a VLAN 20 como a VLAN do modo de acesso (dados). É possível observar isso na captura na parte inferior da tela: Access Mode VLAN: 20 (VLAN0020).

4.3 Redes sem VLANs

Em operação normal, quando um switch recebe um quadro de broadcast em uma das portas, ele encaminha o quadro por todas as demais portas no switch. Na figura 10, toda a rede está configurada na mesma sub-rede, 172.17.40.0/24. Dessa forma, quando o computador dos funcionários, PC1, envia um quadro de broadcast, o switch S1 envia esse quadro por todas as suas portas. Toda a rede acaba recebendo-o; a rede é um domínio de broadcast.

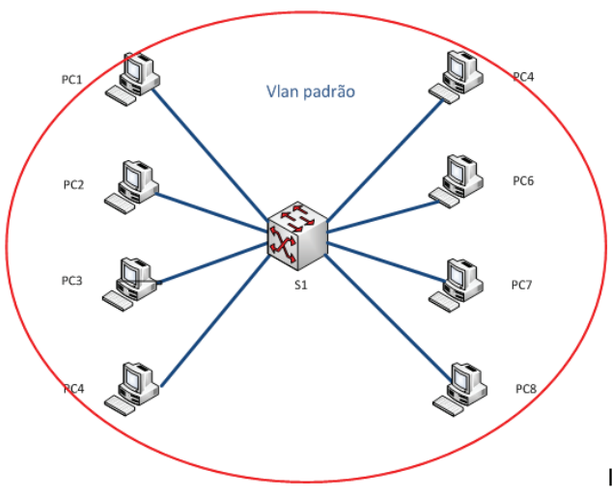


Figura 10 - Vlan padrão.
Fonte: autor

4.4 Rede com Vlans

Na figura 11, a rede foi segmentada em seis VLANs: quando o quadro de broadcast é enviado do computador dos funcionários, PC1, para o switch S1, o switch só encaminha esse quadro de broadcast para essas portas de switch configuradas para suportar VLAN 02.

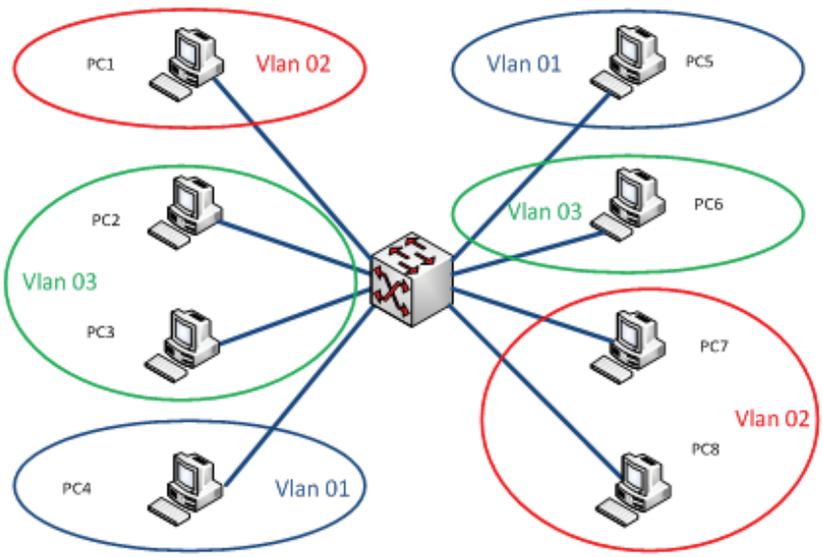


Figura 11 - Switch com Vlans.
Fonte: autor

Quando as VLANs são implementadas em um switch, a transmissão de tráfego unicast, multicast e broadcast de um host em uma VLAN específica é restringida aos dispositivos que estão na VLAN.

Observe como adicionar, configurar e excluir VLANS:

a) Adicionar uma VLAN

Neste tópico, você poderá aprender como criar uma VLAN estática em um switch Cisco Catalyst, que usa o modo de configuração global de VLAN. Há dois modos diferentes de configurar VLANs em um switch Cisco Catalyst: modo de configuração de banco de dados e modo de configuração global. Embora a documentação Cisco mencione o modo de configuração de banco de dados, ele está sendo substituído pelo modo de configuração global de VLAN.

Você configurará VLANs com IDs no intervalo normal. Lembre-se de que há dois intervalos de IDs de VLAN. O intervalo normal inclui IDs de 1 a 1001 e

o intervalo estendido consiste em IDs de 1006 a 4094. A VLAN 1 e de 1002 a 1005 são números de ID reservados. Quando você configura VLANs de intervalo normal, os detalhes da configuração são armazenados automaticamente na memória flash no switch em um arquivo chamado vlan.dat. Como você sempre configura outros aspectos de um switch Cisco ao mesmo tempo, trata-se de prática recomendada salvar alterações feitas na configuração corrente para a NVRAM.

Depois de criar uma VLAN, atribua uma ou mais portas à VLAN. Quando você atribui manualmente uma porta de switch a uma VLAN, isso é conhecido como uma porta de acesso estático. Essa porta pode pertencer a apenas uma VLAN por vez.

b) Verificar VLANs e associações de porta

Depois de configurar a VLAN, é possível validar as configurações de VLAN usando os comandos-show do Cisco IOS.

A sintaxe de vários comandos-show do Cisco IOS deve ser bem conhecida. Você já usou o comando-show vlan brief.

É possível ver que o comando-show vlan name student não produz uma saída de dados muito legível. A preferência aqui é usar o comando-show vlan brief. O comando-show vlan summary exibe a contagem de todas as VLANs configuradas. A saída de dados mostra seis VLANs: 1, 1002-1005 e a VLAN do aluno, VLAN 20.

Esse comando exibe muitos detalhes que estão além da finalidade desta aula. As principais informações são exibidas na segunda linha da captura de tela, indicando que a VLAN 20 está ativa.

Esse comando exibe informações que são úteis para você. É possível determinar que a porta F0/18 está atribuída à VLAN 20, e que a VLAN nativa é VLAN 1. Você usou esse comando para revisar a configuração de uma VLAN de voz.

c) Excluir VLANs

Como alternativa, todo o arquivo vlan.dat pode ser excluído usando-se o comando delete flash:vlan.dat no modo EXEC privilegiado. Depois que o

switch for recarregado, as VLANs configuradas anteriormente já não estarão mais presentes. Isso coloca o switch efetivamente no "padrão de fábrica" em relação a configurações de VLAN.

Resumo

Nesta aula, apresentamos as VLANs. As VLANs são usadas para segmentar domínios de broadcast em uma rede local comutada. Isso melhora o desempenho e a gerenciabilidade das redes locais. As VLANs dão aos administradores de rede um controle flexível sobre o tráfego associado aos dispositivos na rede local.

Há vários tipos de VLANs: padrão, de gerenciamento, nativas, de usuário/dados e de voz.

Atividades de aprendizagem

Responda as questões abaixo:

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4
2	VLAN2	active	Fa0/5, Fa0/6, Fa0/7
3	VLAN3	active	Fa0/8, Fa0/9
4	VLAN4	active	Fa0/10, Fa0/11, Fa0/12
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

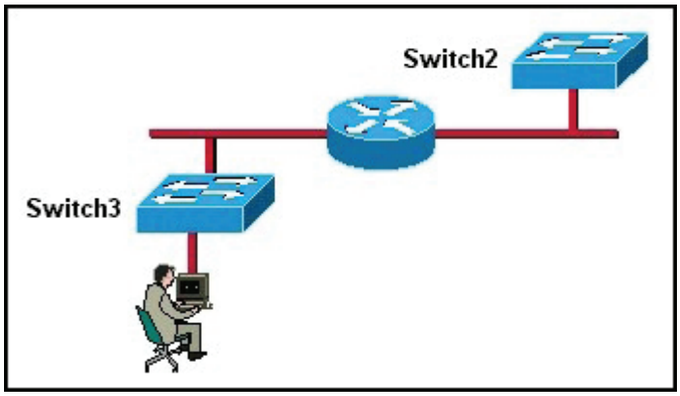
1. Quais comandos são utilizados para obter as informações apresentadas na figura acima?

a) show vlan ifindex

b) show vlan id

c) show vlan

d) show running-config



Fonte: http://www.frameip.com/examen-cisco/ccna-v3.1-semestre-3-module-6.php

2. O administrador de redes, como mostra a figura, está conectado ao Switch 3 por meio de uma conexão LAN/Ethernet. Ele precisa verificar as configurações no novo Switch 2 instalado. Quais ações devem ser tomadas para que o acesso ao Switch 2 possa ser executado com um navegador da Web? (Escolha três respostas.)

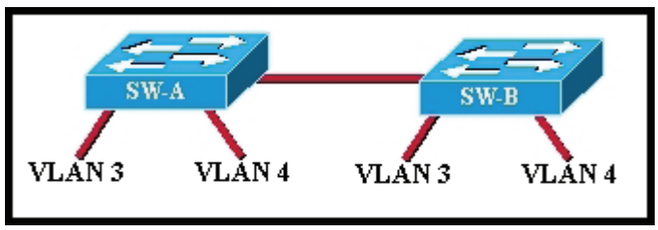
a) Configurar o nome de host no Switch 2.

b) Ativar o serviço HTTP no Switch 2.

c) Definir a senha de gerenciamento da VLAN.

d) Configurar os parâmetros de endereçamento IP no Switch 2.

e) Estabelecer a conectividade do host para o Switch 2.



Fonte: http://www.frameip.com/examen-cisco/ccna-v3.1-semestre-3-final.php

3. Observe a figura acima. Dois switches Catalyst estão conectados. Os dois switches têm portas configuradas para as VLANs 3 e 4. Os hosts conectados à VLAN 3 em SW-A precisam estabelecer comunicação com os hosts na VLAN 3 em SW-B. Por outro lado, os hosts conectados à VLAN 4 em SW-A precisam estabelecer comunicação com os hosts na VLAN 4 em SW-B. Qual

das seguintes alternativas é usada em um switch Catalyst da Cisco para fornecer esse recurso através de um link único?

a) IEEE 802.1Q

b) STP

c) CDP

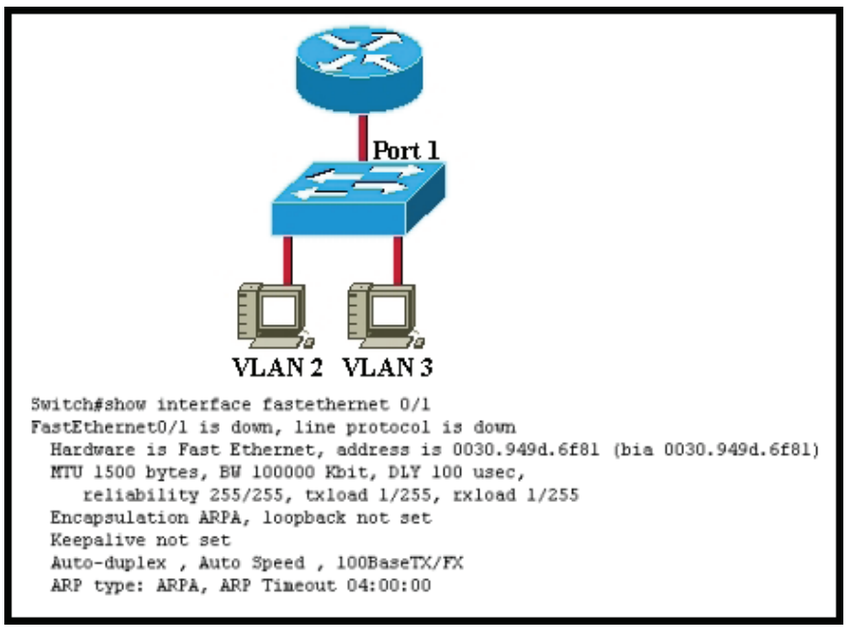
d) VTP

4. Qual é a primeira etapa no processo spanning tree?

a) Escolher um switch designado

b) Usar um roteador para localizar um gateway padrão

c) Escolher um root bridge



Fonte: http://blog.ccna.com.br/2008/05/07/ccna-desafio-da-semana-1-maio-de-2008/

d) Determinar o custo do caminho de cada porta ativa no switch

5. Observe a figura acima. O host na VLAN 2 não consegue comunicar-se com o host na VLAN 3. Qual das seguintes alternativas pode ser a causa do problema, com base no resultado do comando show interface fastethernet

0/1 do switch?

a) A porta 1 do switch não está definida para o modo de acesso.

b) A interface do roteador conectada à porta 1 do switch está desativada.

c) O roteador não está configurado para o tronco.

d) A porta do switch não está configurada para full duplex ou a uma velocidade de 100 Mbps.

Caro(a) estudante,

Finalizamos a quarta aula, que tratou de VLANS, mas o conteúdo preparado pra esta disciplina ainda tem informações relevantes que certamente vão auxiliá-lo(a) futuramente em suas atividades profissionais. Na próxima aula o tema será rede local sem fio. Continue atento(a) e não deixe de realizar as atividades de aprendizagem.

Aula 5. Rede local sem fio

Objetivos:

- distinguir os componentes e a operação básica de redes locais sem fio;
- identificar os componentes e as operações de segurança básica de WLAN;
- configurar o acesso à rede local sem fio básica; e
- reconhecer o acesso à rede local sem fio.

Prezado(a) estudante,

Nesta aula, você terá oportunidade de estudar como uma rede local sem fio (WLANs) oferece às empresas um ambiente de rede flexível. Neste conteúdo, você poderá reconhecer os diferentes padrões sem fio disponíveis atualmente e as características de cada um. Demonstraremos quais componentes de hardware são normalmente necessários em uma infraestrutura sem fio, como as WLANs operam e como protegê-las. Traremos também informações sobre a configuração de um ponto de acesso sem fio e de um cliente para rede sem fio.

5.1 Por que redes locais sem fio se tornaram tão populares?

Atualmente, redes de negócios estão evoluindo para oferecer suporte às pessoas na correria do dia a dia. Funcionários e empregadores, alunos e corpo docente, agentes do governo e seus superiores, fãs de esporte e consumidores, todos têm aparelhos móveis, e muitos deles estão "conectados" uns aos outros. Talvez você transfere mensagens instantâneas para um telefone celular quando está longe do computador. Esta é a visão de mobilidade: um ambiente em que as pessoas podem se locomover para onde quiserem sem

perder a conexão com a rede.

Há muitas infraestruturas diferentes (rede local cabeada, redes de provedores de serviços) que possibilitam essa mobilidade, mas em um ambiente de negócios, a mais importante é a WLAN.

A produtividade já não é restringida a um local de trabalho fixo ou um período de tempo determinado. Agora, o que as pessoas querem é permanecer conectadas, a qualquer hora e em qualquer lugar, do escritório para o aeroporto ou até mesmo em casa. Antes, funcionários que estivessem viajando ficavam limitados a telefones públicos para verificar mensagens e retornar chamadas entre um voo e outro. Agora eles podem verificar e-mail, correio de voz e o status de produtos em assistentes digitais pessoais (PDAs) enquanto vão de um lugar para outro.

Em casa, muitas pessoas mudaram o modo de viver e de aprender. A Internet se tornou um serviço padrão em muitas casas, juntamente com a TV e o telefone. Até mesmo o modo de acessar a Internet mudou rapidamente de serviço temporário de discagem com modem para DSL dedicado ou serviço de cabo. Usuários domésticos estão buscando muitas das mesmas soluções sem fio flexíveis que funcionários em um escritório já possuem. Pela primeira vez, em 2005, foram comprados mais laptops móveis habilitados com Wi-Fi do que desktops fixos.

Além da flexibilidade que as WLANs oferecem, outro benefício importante é o custo reduzido. Por exemplo, com uma infraestrutura sem fio já em operação, a economia é percebida quando uma pessoa muda de local em um prédio, quando um laboratório é reorganizado, ou quando a equipe muda para locais temporários. Em média, o custo de TI para mover um funcionário para um novo local dentro de um prédio é de US$375.

Outro exemplo é a mudança de uma empresa para um novo prédio que não tem nenhuma infraestrutura cabeada. Nesse caso, a economia resultante do uso de WLANs pode ser ainda mais notável porque evita o custo de passar cabos por paredes, teto e chão.

Embora seja mais difícil provar com números, as WLANs podem resultar em produtividade melhor e funcionários menos tensos, trazendo melhores resultados para clientes e maiores lucros.

5.1.1 Redes locais sem fio

Nas aulas anteriores, você pôde aprender sobre tecnologias de switch e funções. A maioria das redes de negócio atuais faz uso de redes locais baseadas em switch para operações cotidianas dentro do escritório. Porém, trabalhadores estão utilizando mais tecnologia móvel e desejam manter acesso aos seus recursos comerciais de rede local a partir de locais que não sejam a escrivaninha ou suas mesas. Os funcionários no escritório desejam levar os laptops para reuniões ou para o escritório de um colega de trabalho. Ao usar um laptop em outro local, não é conveniente confiar em uma conexão cabeada. Neste tópico, você aprenderá sobre redes locais sem fio (WLANs) e como elas beneficiam um negócio. Você também explorará as questões de segurança associadas a WLANs.

A comunicação portátil se tornou uma expectativa em muitos países em todo o mundo. Existe portabilidade e mobilidade em tudo, desde teclados e fones de ouvido sem fio a telefones via satélite e sistemas de posicionamento global (GPS). A mistura de tecnologias sem fio em tipos diferentes de redes permite a mobilidade dos funcionários.

Você pode ver que a WLAN é uma extensão da rede local Ethernet. A função da rede local agora é móvel. Você vai conhecer a tecnologia WLAN e os padrões por trás da mobilidade que permitem que pessoas continuem uma reunião enquanto caminham, andam de táxi ou estão no aeroporto.

Antes de tratarmos das redes sem fio, precisamos comparar uma WLAN com uma rede local. Observe.

Redes locais sem fio compartilham uma origem semelhante com redes locais Ethernet. O IEEE adotou o portfólio de rede local 802/MAN de padrões de arquitetura de rede de computadores. Os dois grupos 802 dominantes em funcionamento são Ethernet 802.3 e rede local sem fio IEEE 802.11. No entanto, há diferenças importantes entre os dois.

WLANs usam frequências de rádio (RF) em vez de cabos na camada física e na subcamada MAC da camada de enlace de dados. Em comparação com cabo, RF tem as seguintes características:

- RF não tem limites, como os limites de uma cerca em volta de um quintal. A ausência de tais limites permite que estruturas de dados viajem pelas mídias de RF para estarem disponíveis a qualquer um que possa receber

o sinal de RF.

- RF não é isolada de sinais externos, embora o cabo fique isolado. Rádios que operam independentemente na mesma área geográfica, mas usando a mesma RF ou uma RF semelhante, podem interferir entre si.

- A transmissão de RF está sujeita aos mesmos desafios inerentes a qualquer tecnologia baseada em onda, como rádio de casa. Por exemplo, conforme você se afasta da origem, pode ouvir estações tocando e se sobrepondo, ou pode ouvir estática na transmissão. Consequentemente, você pode perder todo o sinal. Redes locais cabeadas têm cabos de comprimento apropriado para manter a intensidade do sinal.

- Faixas de RF são regulamentadas de maneira diferente em vários países. O uso de WLANs é sujeito a regulamentos e conjuntos de padrões adicionais que não se aplicam a redes locais cabeadas.

Assim como nas redes locais, as VLANS permitem:

- conectar clientes à rede por um ponto de acesso sem fio (AP) em vez de um switch Ethernet;

- conectar dispositivos móveis que frequentemente funcionam com bateria, ao contrário de dispositivos de rede local que funcionam conectados à tomada. Placas de interface de rede sem fio tendem a reduzir a vida útil da bateria de um dispositivo móvel;

- suportar hosts que disputam acesso nas mídias de RF (faixas de frequência). Redes 802.11 determinam prevenção contra colisão em vez de detecção de colisão para o acesso de mídia evitar colisões preventivamente na mídia;

- usar um formato de quadro diferente do formato usado pelas redes locais Ethernet cabeadas. WLANs exigem informações adicionais no cabeçalho do quadro da Camada 2.

As WLANs ainda aumentam os problemas de privacidade porque as frequências de rádio podem ir além das instalações.

Apresentando as redes locais sem fio

Redes locais sem fio 802.11 estendem as infraestruturas de rede local Ethernet 802.3 para fornecer opções de conectividade adicionais. Entretanto, são usados componentes e protocolos adicionais para concluir as conexões sem fio.

Em uma rede local Ethernet 802.3, cada cliente tem um cabo que conecta a placa de rede de cliente a um switch. O switch é o ponto em que o cliente ganha acesso à rede.

Em uma rede local sem fio, cada cliente usa um adaptador sem fio para ganhar acesso à rede por um dispositivo sem fio, como um roteador ou ponto de acesso sem fio.

O adaptador sem fio no cliente se comunica com o roteador ou ponto de acesso sem fio que usa sinais de RF. Uma vez conectados à rede, clientes da rede sem fio podem acessar recursos de rede como se estivessem conectados a ela por cabos.

Padrões de redes locais sem fio:

Rede local sem fio 802.11 é um padrão de IEEE que define como a frequência de rádio (RF), nas faixas de frequência industriais, científicas e médicas (ISM) sem licença, é usada para a camada física e para a subcamada MAC de links sem fio.

Na primeira vez em que o 802.11 foi lançado, ele determinava taxas de dados de 1 a 2 Mb/s na faixa de 2,4 GHz. Naquela época, redes locais cabeadas operavam a 10 Mb/s, então a nova tecnologia sem fio não foi adotada com entusiasmo. Desde então, os padrões de redes locais sem fio melhoraram continuamente com o lançamento do IEEE 802.11a, do IEEE 802.11b, do IEEE 802.11g e do 802.11n, em fase de testes.

Normalmente, a escolha do padrão WLAN a ser usado é baseada em taxas de dados. Por exemplo, os 802.11a e g podem suportar até 54 Mb/s, enquanto o 802.11b suporta no máximo 11 Mb/s, sendo este o padrão "lento", fazendo os 802.11 a e g os mais preferidos. Um quarto padrão de WLAN em fase de testes, o 802.11n, excede as taxas de dados disponíveis atualmente. O IEEE 802.11n foi aprovado em 2009.

As taxas de dados de padrões de redes locais sem fio diferentes são afetadas por algo chamado de técnica de modulação. As duas técnicas de modulação que serão abordadas nesta disciplina são Espectro Distribuído de Sequência Direta (DSSS, Direct Sequence Spread Spectrum) e Multiplexação da Divisão de Frequência Ortogonal (OFDM, Orthogonal Frequency Division Multiplexing). Você não precisa saber como essas técnicas funcionam, mas deve saber que, quando um padrão usa a técnica OFDM, ele tem taxas de dados mais rápidas. Entretanto, a DSSS é mais simples que a OFDM, portanto a implementação dela é menos dispendiosa.

802.11a

O IEEE 802.11a adota a técnica de modulação OFDM e usa a faixa de 5 GHz.

Dispositivos 802.11a que operam na faixa de 5 GHz apresentam menos problemas de interferência do que dispositivos que operam na faixa de 2,4 GHz porque há menos dispositivos consumidores usando a faixa de 5 GHz. Além disso, frequências mais altas permitem o uso de antenas menores.

Há algumas desvantagens relevantes quanto ao uso da faixa de 5 GHz. A primeira é que ondas de rádio de frequência mais altas são absorvidas mais facilmente por obstáculos, como paredes, tornando o 802.11a suscetível a baixo desempenho devido a bloqueios. A segunda é que essa faixa de frequência mais alta tem alcance ligeiramente mais limitado que o 802.11b ou g. Além disso, alguns países, como a Rússia, não permitem o uso da faixa de 5 GHz, o que pode continuar restringindo sua implantação.

802.11b e 802.11g

O 802.11b especifica taxas de dados de 1, 2, 5.5 e 11 Mb/s na faixa de ISM de 2,4 GHz usando DSSS. O 802.11g obtém taxas de dados mais altas nessa faixa usando a técnica de modulação OFDM. O IEEE 802.11g também especifica o uso de DSSS para compatibilidade com sistemas do IEEE 802.11b. São suportadas taxas de dados DSSS de 1, 2, 5.5 e 11 Mb/s, assim como taxas de dados OFDM de 6, 9, 12, 18, 24, 48 e 54 Mb/s.

Há vantagens quanto ao uso da faixa de 2,4 GHz. Dispositivos na faixa de 2,4 GHz têm alcance melhor que os da faixa de 5 GHz. Além disso, as transmissões nesta faixa não são bloqueadas tão facilmente quanto o 802.11a.

Há uma desvantagem relevante quanto ao uso da faixa de 2,4 GHz. Muitos dispositivos consumidores também usam a faixa de 2,4 GHz e tornam os dispositivos 802.11b e g propensos a interferência.

802.11n

O objetivo do padrão IEEE 802.11n é melhorar as taxas de dados WLAN e o intervalo sem exigir alimentação ou alocação de faixas de RF adicionais. O 802.11n usa rádios e antenas múltiplos em extremidades, cada um transmitindo na mesma frequência para estabelecer fluxos múltiplos. A tecnologia de entradas múltiplas/saídas múltiplas (MIMO) divide um fluxo de taxa de dados alta em múltiplos fluxos de taxa menores e os transmite simultaneamente através de rádios e antenas disponíveis. Isso possibilita uma taxa de dados máxima teórica de 248 Mb/s usando dois fluxos.

Importante: faixas RF são alocadas pelo setor de comunicação de rádio da International Telecommunication Union (ITU-R). O ITU-R designa as faixas de frequência de 900 MHz, 2,4 GHz e 5 GHz como não licenciadas para comunidades ISM. Mesmo que as faixas ISM sejam não licenciadas no mundo todo, elas estão sujeitas a regulamentações locais. O uso dessas faixas é administrado pela FCC (Federal Communications Commission, Comissão Federal de Comunicações) nos Estados Unidos e pelo ETSI (European Telecommunications Standards Institute, Instituto Europeu de Normas de Telecomunicações) na Europa. Esses problemas afetarão a seleção de componentes sem fio em uma implementação sem fio.

Certificação Wi-Fi

A certificação Wi-Fi é fornecida pela Wi-Fi Alliance (http://www.wi-fi.org), uma associação global de comércio industrial sem fins financeiros dedicada a elevar o crescimento e a aceitação de WLANs. Você entenderá melhor a importância da certificação Wi-Fi se considerar a função da Wi-Fi Alliance no contexto de padrões de WLAN.

Os padrões garantem a interoperabilidade entre dispositivos feitos por fabricantes diferentes. Internacionalmente, as três principais organizações que influenciam os padrões de WLAN são:

- ITU-R;
- IEEE;
- Wi-Fi Alliance.

O ITU-R regulamenta a alocação do espectro de RF e das órbitas de satélite. Eles são descritos como recursos naturais finitos que estão em demanda de consumidores como redes fixas sem fio, redes móveis sem fio e sistemas de posicionamento global.

O IEEE desenvolveu e mantém os padrões para redes locais e de áreas metropolitanas com a família de padrões IEEE 802 LAN/MAN. O IEEE 802 é gerenciado pelo Comitê de Padrões IEEE 802 LAN/MAN (LMSC), que administra grupos de trabalho múltiplos. Os padrões dominantes na família IEEE 802 são Ethernet 802.3, 802.5 Token Ring e Rede local sem fio 802.11.

Embora o IEEE tenha especificado padrões para dispositivos de modulação RF, ele não especificou padrões de fabricação, fazendo interpretações dos padrões 802.11 por fornecedores diferentes causarem problemas de interoperabilidade entre os dispositivos.

A Wi-Fi Alliance é uma associação de fornecedores cujo objetivo é melhorar a interoperabilidade de produtos baseados no padrão 802.11, certificando fornecedores para estarem em conformidade com as normas da indústria e aderirem aos padrões. A certificação inclui as três tecnologias RF IEEE 802.11, bem como a adoção prévia de padrões IEEE em fase de teste, como o 802.11n, e os padrões de segurança WPA e WPA2 baseados no IEEE 802.11i.

As funções dessas três organizações podem ser resumidas da seguinte forma:

- O ITU-R regulamenta a alocação de faixas de RF.
- O IEEE especifica como o RF é modulado para transmitir informações.
- A Wi-Fi assegura que fornecedores façam dispositivos interoperáveis.

5.2 Placas de rede sem fio

Talvez você já use uma rede sem fio em casa, em uma lan house ou em sua escola. Já imaginou que componentes de hardware estão envolvidos para permitir o acesso sem fio à rede local ou à Internet? Neste tópico, você poderá verificar quais componentes estão disponíveis para implementar WLANs e como cada um é usado na infraestrutura sem fio.

Revendo: os componentes básicos de uma WLAN são estações cliente que se conectam a pontos de acesso que, por sua vez, se conectam à infraestrutura de rede. O dispositivo que permite que uma estação cliente possa enviar e receber sinais de RF é a placa de rede sem fio.

Como uma placa de rede Ethernet mostrada na figura 12, a placa de rede sem fio mostrada na figura 13, usando a técnica de modulação à qual está configurada para usar, codifica um fluxo de dados sobre um sinal de RF. Placas de rede sem fio são frequentemente associadas a dispositivos móveis, como laptops. Nos anos 90, placas de rede sem fio para laptops eram placas que deslizavam para dentro do slot PCMCIA. Placas de rede sem fio PCMCIA ainda são comuns, mas muitos fabricantes começaram a fazer a placa de rede sem fio já dentro do laptop. Ao contrário das interfaces 802.3 Ethernet feitas em PCs, a placa de rede sem fio não é visível porque não há nenhuma necessidade de conectar um cabo ao PC.

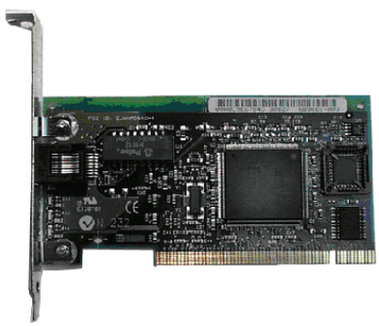


Figura 12 - Placa de rede com fio - Wirede.
Fonte: http://alumnosistema.galeon.com/IS-1Y2/TEMA_II/TEMA_2_1_3.htm

Figura 13 - Placa de rede sem fio - Wireless.
Fonte: http://www.dlink.com.br/produtos-detalhes/items/dwa-547.html

Outras opções surgiram ao longo dos anos. Desktops localizados em instalações não cabeadas podem ter uma placa PCI sem fio. Há também várias opções USB disponíveis para configurar rapidamente um PC, um dispositivo móvel ou um desktop com uma placa de rede sem fio.

Além disso, temos uma variedade de possibilidades de acesso, como:

- Pontos de acesso sem fio

Um ponto de acesso conecta clientes para rede sem fio (ou estações) à rede local cabeada. Dispositivos de cliente normalmente não se comunicam diretamente entre si; eles se comunicam com o AP, figura 14. Essencialmente, um ponto de acesso converte os pacotes de dados TCP/IP de seu formato de encapsulamento de quadro 802.11 no ar para o formato de quadro 802.3 Ethernet na rede Ethernet cabeada.

Figura 14 - Ponto de acesso sem fio.
Fonte: http://www.worldstart.com/wireless-router-tips/

Em uma rede de infraestrutura, clientes devem associar-se a um ponto de acesso para obter serviços de rede. Associação é o processo pelo qual um cliente se une a uma rede 802.11. É semelhante a conectar-se a uma rede local cabeada. A associação é discutida em tópicos posteriores.

Um ponto de acesso é um dispositivo de Camada 2 que funciona como um hub 802.3 Ethernet. RF é um meio compartilhado, e pontos de acesso escutam todo o tráfego de rádio. Da mesma maneira que com o 802.3 Ethernet, os dispositivos que desejam usar o meio disputam por ele. Apesar disso, diferentemente das placas de rede Ethernet, é caro fazer placas de rede sem fio que possam transmitir e receber ao mesmo tempo; assim, dispositivos de rádio não detectam colisões. Em vez disso, dispositivos de WLAN são criados

para evitá-las.

CSMA/CA

Pontos de acesso supervisionam uma função de coordenação distribuída (DCF) chamada Acesso Múltiplo com Verificação de Portadora (Carrier Sense Multiple Access with Collision Avoidance, CSMA) com Anulação de Colisão (CSMA/CA). Isso simplesmente significa que dispositivos em uma WLAN devem sentir o meio para verificar alimentação (estímulo de RF acima de um certo limite) e esperar até que o meio esteja livre antes de transmitir. Como todos os dispositivos precisam fazer isso, a função de coordenação do acesso ao meio é distribuída. Se um ponto de acesso recebe dados de uma estação cliente, ele envia ao cliente uma confirmação do recebimento dos dados. Essa confirmação impede que o cliente suponha que houve uma colisão e que ele transmita os dados novamente.

Sinais de RF se atenuam. Isso significa que eles perdem energia conforme se afastam do ponto de origem. É como uma estação de rádio saindo de sintonia. Essa atenuação de sinal pode ser um problema em uma WLAN na qual estações disputam pelo meio.

Imagine duas estações cliente conectadas ao mesmo ponto de acesso, mas em lados opostos. Se eles estiverem ao intervalo máximo para alcançar o ponto de acesso, não poderão alcançar um ao outro. Assim, nenhuma dessas estações sente a outra no meio, e eles podem acabar transmitindo simultaneamente. Isso é conhecido como o problema de nó oculto (ou estação oculta).

Uma maneira de solucionar o problema de nó oculto é um recurso do CSMA/CA chamado Solicitar para enviar/Limpar para enviar (RTS/CTS). O RTS/CTS foi desenvolvido para permitir uma negociação entre um cliente e um ponto de acesso. Quando ele está habilitado em uma rede, pontos de acesso alocam o meio à estação solicitante pelo tempo necessário para concluir a transmissão. Quando a transmissão termina, outras estações podem solicitar o canal de maneira semelhante. Caso contrário, a função de prevenção contra colisão normal continua.

5.2.1 Parâmetros configuráveis para pontos de extremidade sem fio

A figura 15 mostra a tela inicial da configuração sem fio em um roteador

para rede sem fio Linksys. Vários processos podem ser seguidos para estabelecer uma conexão entre cliente e ponto de acesso. É necessário configurar parâmetros no ponto de acesso - e subsequentemente no dispositivo de cliente para habilitar a negociação desses processos.

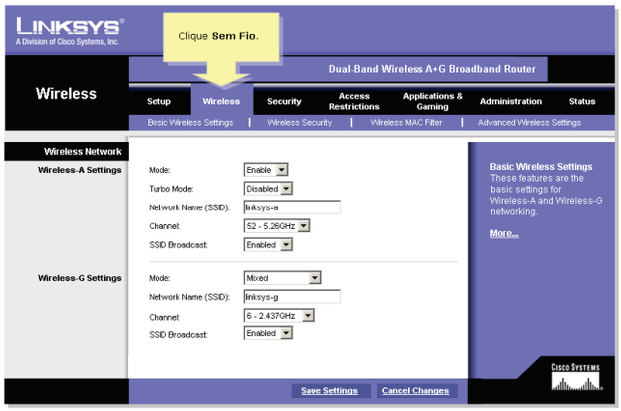


Figura 15 - Tela de configuração do ponto de acesso sem fio.
Fonte: http://kb.linksys.com/Linksys

O modo de rede sem fio se refere aos protocolos de WLAN: 802.11a, b, g, ou n. Como o 802.11g é compatível com o antecessor 802.11b, pontos de acesso suportam os dois. Lembre-se: se todos os clientes se conectarem a um ponto de acesso com o 802.11g, todos eles terão as melhores taxas de dados à sua disposição. Quando clientes do 802.11b se associam ao ponto de acesso, todos os clientes mais rápidos que estejam competindo pelo canal devem esperar, antes de transmitir, que os clientes do 802.11b liberem o canal. Quando um ponto de acesso Linksys está configurado para aceitar tanto clientes do 802.11b quanto do 802.11g, ele está operando em modo misto.

Um Identificador do Conjunto de Serviços Compartilhado (SSID) é um identificador exclusivo usado por dispositivos cliente para distinguir entre redes sem fio múltiplas na mesma área. Um SSID pode ser compartilhado entre vários pontos de acesso em uma rede.

O padrão IEEE 802.11 estabelece o esquema de canalização para o uso das faixas de RF ISM não licenciadas em WLANs. A faixa de 2.4 GHz é interrompida em 11 canais na América do Norte e 13 canais na Europa. Esses canais têm uma separação de frequência de centro de apenas 5 MHz e uma largura de banda de canal geral (ou ocupação de frequência) de 22 MHz. A largura de banda de canal de 22 MHz, combinada com a separação de 5 MHz entre de frequências de centro, significa que há uma sobreposição de canais su-

cessivos. Práticas recomendadas para WLANs que exigem múltiplos pontos de acesso são definidas para o uso de canais não sobrepostos. Se houver três pontos de acesso adjacentes, use os canais 1, 6 e 11. Se houver apenas dois, selecione quaisquer dois que estejam separados por cinco canais, como os canais 5 e 10. Muitos pontos de acesso podem selecionar um canal automaticamente, baseando-se no uso de canal adjacente. Alguns produtos monitoram o espaço de rádio continuamente para ajustar as configurações de canal de maneira dinâmica de acordo com alterações no ambiente.

a) Topologias 802.11

Redes locais sem fio podem acomodar várias topologias de rede. Ao descrever essas topologias, o componente básico da arquitetura de WLAN do IEEE 802.11 é o conjunto de serviços básico (BSS). O padrão define um BSS como um grupo de estações que se comunicam entre si.

b) Redes ad hoc

Redes sem fio podem operar sem pontos de acesso; isso é chamado de topologia ad hoc. Estações clientes configuradas para operar em modo ad hoc configuram os parâmetros sem fio entre si. O padrão IEEE 802.11 se refere a uma rede ad hoc como um BSS independente (IBSS).

c) Conjunto de serviços básico

Pontos de acesso fornecem uma infraestrutura que adiciona serviços e melhora o intervalo para clientes. Um único ponto de acesso em modo de infraestrutura gerencia os parâmetros sem fio, e a topologia é simplesmente um BSS. A área de cobertura para um IBSS e um BSS é a Área de Serviço Básica (BSA).

d) Conjunto de serviços estendidos

Quando um único BSS fornece cobertura de RF insuficiente, um ou mais BSS podem ser unidos por um sistema de distribuição comum em um Conjunto Estendido de Serviços (ESS). Em um ESS, um BSS é diferenciado de outro pelo identificador de BSS (BSSID), que é o endereço MAC do ponto de acesso que serve o BSS. A área de cobertura é a Área de Serviço Estendida (ESA).

e) Sistema de distribuição comum

O sistema de distribuição comum permite que múltiplos pontos de acesso em um ESS pareçam ser um único BSS. Um ESS geralmente inclui um SSID comum para permitir que um usuário migre entre pontos de acesso.

Células representam a área de cobertura fornecida por um único canal. Um ESS deve ter de 10 a 15% de sobreposição entre células em uma área de serviço estendida. Com uma sobreposição de 15% entre células, um SSID e canais não sobrepostos (uma célula no canal 1 e outra no canal 6), pode ser criado o recurso de roaming.

f) Associação entre cliente e ponto de acesso

Um dos pontos principais do processo 802.11 é descobrir uma WLAN e subsequentemente conectar-se a ela. Os componentes principais desse processo são:

- **Beacons** - Quadros usados pela rede de WLAN para anunciar sua presença.
- **Investigações** - Quadros usados por clientes WLAN para localizar suas redes.
- **Autenticação** - Um processo que é um artefato do padrão 802.11 original, mas ainda assim exigido pelo padrão.
- **Associação** - O processo para estabelecer o enlace entre um ponto de acesso e um cliente WLAN.

O propósito principal da beacon é permitir que clientes WLAN saibam quais redes e pontos de acesso estão disponíveis em uma determinada área e escolham qual rede e ponto de acesso usar. Pontos de acesso podem transmitir beacons periodicamente.

Embora os beacons possam ser regularmente transmitidos por um ponto de acesso, os quadros de investigação, autenticação e associação são usados apenas durante o processo de associação (ou reassociação).

5.3 O processo de união 802.11 (Associação)

Antes de um cliente 802.11 poder enviar dados por uma rede de WLAN, ele passa pelo processo de três estágios a seguir:

a) Estágio 1 – investigação 802.11

Clientes procuram uma rede específica enviando uma solicitação de investigação em canais múltiplos. A solicitação de investigação especifica o nome da rede (SSID) e as taxas de bits. Um cliente WLAN típico é configurado com um SSID desejado. Assim, solicitações de investigação do cliente WLAN contêm o SSID da rede de WLAN desejada.

Se o cliente WLAN está simplesmente tentando descobrir redes de WLAN disponíveis, ele pode enviar uma solicitação de investigação sem SSID, e respondem todos os pontos de acesso configurados para responder a esse tipo de consulta. WLANs com o recurso de broadcast de SSID desabilitado não respondem.

b) Estágio 2 – autenticação 802.11

O 802.11 foi originalmente desenvolvido com dois mecanismos de autenticação. O primeiro, chamado autenticação aberta, é essencialmente uma autenticação NULA, em que o cliente diz "autentique-me" e o ponto de acesso responde com "sim". Esse é o mecanismo usado em quase todas as implantações 802.11.

Um segundo mecanismo de autenticação é chamado de autenticação de chave compartilhada. Essa técnica se baseia em uma chave de Wired Equivalency Protection (WEP) compartilhada entre o cliente e o ponto de acesso. Nessa técnica, o cliente envia uma solicitação de autenticação ao ponto de acesso. Em seguida, o ponto de acesso envia um texto de desafio ao cliente, que, por sua vez, criptografa a mensagem usando sua chave compartilhada e devolve o texto criptografado ao ponto de acesso. Então, o ponto de acesso descriptografa o texto usando sua chave e, se o texto descriptografado corresponde ao texto de desafio, o cliente e o ponto de acesso compartilham a mesma chave, e o ponto de acesso autentica a estação. Se as mensagens não correspondem, o cliente não é autenticado.

Embora a autenticação de chave compartilhada deva ser incluída nas implementações do cliente e do ponto de acesso para conformidade de padrões

gerais, ela não é usada ou recomendada. O problema é que a chave WEP é normalmente usada para criptografar dados durante o processo de transmissão. O uso da mesma chave WEP no processo de autenticação proporciona um invasor com a capacidade de extrair a chave, detectando e comparando o texto de desafio não criptografado e, em seguida, a mensagem de retorno criptografada. Quando a chave WEP é extraída, qualquer informação criptografada transmitida pelo link pode ser facilmente descriptografada.

c) Estágio 3 – associação 802.11

Este estágio finaliza as opções de segurança e taxa de bits, e estabelece o enlace entre o cliente WLAN e o ponto de acesso. Como parte deste estágio, o cliente aprende sobre o BSSID, que é o endereço MAC do ponto de acesso, e o ponto de acesso mapeia uma porta lógica conhecida como o identificador de associação (AID) para o cliente WLAN. A AID é equivalente a uma porta em um switch. O processo de associação permite que o switch de infraestrutura mantenha um controle dos quadros destinados ao cliente WLAN de forma que eles possam ser encaminhados.

Uma vez que um cliente WLAN está associado a um ponto de acesso, o tráfego pode ir de um lado para outro entre os dois dispositivos.

5.4 Planejamento da rede local sem fio

A implementação de uma WLAN que explora ao máximo os recursos e fornece o melhor serviço pode exigir planejamento cuidadoso. WLANs podem variar de instalações relativamente simples a designs bem mais complexos e detalhados. É preciso haver um plano bem documentado antes que uma rede sem fio possa ser implementada. Neste tópico, apresentaremos o que deve ser considerado no design e no planejamento de uma rede local sem fio.

O número de usuários que uma WLAN pode suportar não é um cálculo simples. O número dos usuários depende do layout geográfico de suas instalações (quantos corpos e dispositivos cabem em um espaço), das taxas de dados esperadas pelos usuários (porque o RF é um meio compartilhado, e quanto mais usuários houver, maior será a contenção para RF), do uso de canais não sobrepostos por diversos pontos de acesso em um ESS e das configurações de capacidade de transmissão (que são limitados por um regulamento local). Você terá suporte sem fio suficiente para seus clientes se você planejar sua rede para cobertura apropriada de RF em um ESS. Os detalhes

sobre o planejamento de números específicos de usuários estão além do conteúdo que esta disciplina abrange.

Ao planejar o local de pontos de acesso, talvez você não possa simplesmente desenhar círculos de área de cobertura e jogá-los em um mapa. A área de cobertura circular aproximada é importante, mas há algumas recomendações adicionais.

Se os pontos de acesso vão usar cabeamento existente, ou se há locais em que pontos de acesso não podem ser colocados, indique esses locais no mapa.

- Posicione os pontos de acesso acima de obstruções.

- Posicione os pontos de acesso verticalmente perto do teto no centro de cada área de cobertura, se possível.

- Posicione os pontos de acesso em locais em que se espera que os usuários estejam. Por exemplo, salas de conferência são normalmente um local melhor para pontos de acesso do que um corredor.

Quando os pontos tiverem sido endereçados, estime a área de cobertura esperada de um ponto de acesso. Esse valor varia, dependendo do padrão ou da mescla de padrões de WLAN que você está implantando, da natureza das instalações, da capacidade de transmissão para a qual o ponto de acesso está configurado, e assim por diante. Consulte sempre as especificações para o ponto de acesso ao planejar áreas de cobertura.

Com base em seu plano, coloque os pontos de acesso na planta baixa, de forma que os círculos de cobertura se sobreponham, como mostra o exemplo a seguir.

5.4.1 Cálculo de exemplo

Os requisitos de rede especificam que deve haver uma produtividade de 802.11b de 6 Mb/s, no mínimo, em cada BSA, porque há uma implementação de voz sobre WLAN sem fio sobreposta nesta rede. Com pontos de acesso, 6 Mbps podem ser obtidos em áreas abertas como as do mapa, com uma área de cobertura de 464 m2 (5,000 ft2) em muitos ambientes.

Observação: a área de cobertura de 464 m2 é para um quadrado. O BSA leva seu raio na diagonal a partir do centro desse quadrado.

5.4.2 Determinando a colocação dos pontos de acesso

As instalações têm 1.800 m2. Logo, a divisão de 1.800 m2 por uma área de cobertura de 464 m2 por ponto de acesso resulta em pelo menos quatro pontos de acesso necessários para o auditório. Em seguida, determine a dimensão das áreas de cobertura e as organize na planta baixa.

- Já que a área de cobertura é um quadrado de lateral "Z", o círculo que é tangente a seus quatro cantos tem um raio de 15,24 m (50 ft), como mostram os cálculos.

- Quando as dimensões da área de cobertura tiverem sido determinadas, você as organizará de maneira semelhante.

5.5 Visão geral dos protocolos de rede sem fio

Neste tópico, mostraremos as características dos protocolos sem fio comuns e o nível de segurança proporcionado por cada um.

Dois tipos de autenticação foram introduzidos com o padrão 802.11 original: autenticação de chave WEP aberta e compartilhada. Enquanto a autenticação aberta realmente não é "nenhuma autenticação" (um cliente solicita autenticação e o ponto de acesso o concede), a autenticação WEP foi criada para proporcionar privacidade a um link, fazendo-o ser como um cabo que conecta um PC a uma tomada Ethernet. Como já foi mencionado, as chaves WEP compartilhadas apresentaram falhas, e algo melhor era necessário. A primeira coisa feita pelas empresas para combater a fragilidade das chaves WEP compartilhadas foi tentar técnicas como disfarçar SSIDs e filtrar endereços MAC. Essas técnicas também eram muito frágeis. Mais adiante, você saberá mais sobre isso.

As falhas com a criptografia das chaves WEP compartilhadas foram duas. Primeiro, o algoritmo usado para criptografar os dados era descoberto facilmente. Segundo, a escalabilidade era um problema. As chaves WEP de 32 bits foram gerenciadas manualmente, sendo acessadas manualmente pelos usuários, de maneira frequentemente incorreta, criando chamadas aos serviços de suporte técnico.

Após as falhas na segurança baseada em WEP, houve um período intermediário de medidas de segurança. Fornecedores como a Cisco, desejando atender à demanda por maior segurança, desenvolveram seus próprios sistemas ao mesmo tempo em que ajudavam a aprimorar o padrão 802.11i. Enquanto isso, o algoritmo de criptografia TKIP foi criado e vinculado ao método de segurança Wi-Fi Alliance WiFi Protected Access (WPA).

Atualmente, o padrão que deve ser seguido na maioria das redes empresariais é o 802.11i. Ele é como o padrão Wi-Fi Alliance WPA2. Para empresas, o WPA2 inclui uma conexão com um banco de dados Remote Authentication Dial In User Service (RADIUS). RADIUS será descrito mais adiante.

5.5.1 Autenticação à rede local sem fio

Em uma rede aberta, como uma rede doméstica, a associação pode ser o necessário para conceder a um cliente acesso a dispositivos e serviços na WLAN. Em redes com requisitos de segurança mais rígidos, uma autenticação adicional ou um login é exigido para conceder tal acesso a clientes. O processo de login é gerenciado pelo Extensible Authentication Protocol (EAP). O EAP é uma estrutura para autenticar o acesso de rede. O IEEE desenvolveu o padrão 802.11i para autenticação de WLAN e autorização para usar o IEEE 802.1x.

O processo de autenticação de WLAN empresarial está resumido a seguir:

- O processo de associação 802.11 cria uma porta virtual para cada cliente de WLAN no ponto de acesso;
- O ponto de acesso bloqueia todas as estruturas de dados, com exceção do tráfego baseado em 802.1x;
- Os quadros 802.1x levam os pacotes de autenticação EAP pelo ponto de acesso para um servidor que mantém credenciais de autenticação. Trata-se de servidor de autenticação, autorização e contabilidade (AAA) que executa um protocolo RADIUS;
- Se a autenticação EAP obtém êxito, o servidor de AAA envia uma mensagem EAP de êxito ao ponto de acesso, que então permite que o tráfego de dados do cliente de WLAN passe pela porta virtual;

- Antes de abrir a porta virtual, é estabelecida uma criptografia de enlace entre o cliente de WLAN e o ponto de acesso para assegurar que nenhum outro cliente de WLAN possa acessar a porta estabelecida para determinado cliente autenticado.

Antes de o 802.11i (WPA2) ou mesmo o WPA serem utilizados, algumas empresas tentavam proteger suas WLANs através da filtragem de endereços MAC e da não transmissão de SSIDs. Nos dias atuais, é fácil usar um software para modificar endereços MAC anexados a adaptadores para enganar facilmente a filtragem de endereços MAC. Não quer dizer que você não deva fazer isso, mas se você estiver usando esse método, será melhor utilizar segurança adicional, como o WPA2.

Mesmo que um SSID não seja transmitido por um ponto de acesso, o tráfego que passa de um lado para outro entre o cliente e o ponto de acesso acaba revelando o SSID. Se um invasor está monitorando a faixa de RF passivamente, o SSID pode ser detectado em uma dessas transações porque é enviado em texto não criptografado. A facilidade para descobrir SSIDs levou algumas pessoas a deixar a transmissão de SSIDs ativada. Nesse caso, isso provavelmente deve ser uma decisão organizacional registrada na política de segurança.

A ideia de que você pode proteger sua WLAN apenas com a filtragem de MAC e desativação das transmissões de SSIDs pode tornar uma WLAN completamente desprotegida. A melhor maneira de certificar-se de que os usuários finais supostamente estejam na WLAN é usar um método de segurança que incorpore controle de acesso à rede baseado em porta, como o WPA2.

5.6 Criptografia

Dois mecanismos de criptografia de nível empresarial especificados pelo 802.11i são certificados como WPA e WPA2 pela Wi-Fi Alliance: o Temporal Key Integrity Protocol (TKIP) e a criptografia (AES).

TKIP é o método de criptografia certificado como WPA. Ele dá suporte para equipamentos de WLAN herdados, direcionando-se às falhas originais associadas com o método de criptografia 802.11 WEP. Usa o algoritmo de criptografia original usado pelo WEP.

O TKIP tem duas funções principais:

a) criptografa o payload da Camada 2;

b) executa uma verificação de integridade da mensagem (MIC) no pacote criptografado. Isso ajuda a impedir a adulteração de uma mensagem.

Embora o TKIP lide com todas as falhas de WEP conhecidas, a criptografia AES de WPA2 é o método preferido, porque alinha os padrões de criptografia de WLAN com práticas recomendadas e padrões mais amplos da indústria de TI, notavelmente o IEEE 802.11i.

O AES tem as mesmas funções do TKIP, mas usa dados adicionais do cabeçalho de MAC que permitem que hosts de destino verifiquem se os bits não criptografados foram adulterados. Além disso, ele adiciona um número de sequência ao cabeçalho dos dados criptografados.

Quando você configura pontos de acesso Linksys ou roteadores sem fio, como o WRT300N, talvez você não veja WPA ou WPA2. Em vez disso, talvez você veja referências a algo chamado chave pré-compartilhada (PSK). Veja a seguir alguns tipos de PSK:

- PSK ou PSK2 com TKIP é o mesmo que WPA
- PSK ou PSK2 com AES é o mesmo que WPA2
- PSK2, sem um método de criptografia especificado, é o mesmo que WPA2

5.7 Controle de acesso à rede local sem fio

O conceito de profundidade significa ter várias soluções disponíveis. É como ter um sistema de segurança em casa bloqueando todas as portas e janelas, e ainda pedir aos vizinhos para tomar conta dela para você. Os métodos de segurança apresentados, principalmente o WPA2, são como um sistema de segurança. Se você deseja segurança adicional para o acesso à sua WLAN, você pode adicionar profundidade.

a) disfarce de SSID - Desabilite transmissões de SSID de pontos de acesso;

b) filtragem de endereços MAC - Tabelas são construídas manualmente no ponto de acesso para permitir ou não clientes baseados em seu endereço de hardware físico;

c) implementação de segurança de WLAN - WPA ou WPA2.

Uma consideração adicional para um administrador de rede cuidadoso é configurar pontos de acesso localizados próximos a paredes externas de edifícios para transmitir em uma opção de alimentação mais baixa que outros pontos de acesso mais próximos ao centro do edifício. Isso é simplesmente reduzir a assinatura de RF no lado de fora do prédio, onde qualquer pessoa executando uma aplicação como Netstumbler (http://www.netstumbler.com), Wireshark ou até mesmo o Windows XP pode mapear WLANs.

Nem o disfarce de SSID nem a filtragem de endereços MAC são considerados meios válidos para proteger uma WLAN pelas seguintes razões:

- endereços MAC são facilmente driblados.
- SSIDs são facilmente descobertos mesmo que os pontos de acesso não os transmitam.

5.7.1 Configuração de segurança

Essas configurações definem a segurança de sua rede sem fio. Há sete modos de segurança sem fio suportados pelo WRT300N. Eles foram listados aqui, na ordem em que você os vê na interface gráfica do usuário, do mais fraco para o mais forte, com exceção da última opção, que é desabilitada:

- WEP;
- PSK-Personal ou WPA-Personal em firmware v0.93.9 ou mais recente;
- PSK2-Personal ou WPA2-Personal em firmware v0.93.9 ou mais recente;
- PSK-Enterprise, ou WPA-Enterprise em firmware v0.93.9 ou mais recente;
- PSK2-Enterprise, ou WPA2-Enterprise em firmware v0.93.9 ou mais recente;
- RADIUS;

- Disabled.

Quando você vê "Personal" em um modo de segurança, nenhum servidor de AAA está sendo usado. "Enterprise" no nome de modo de segurança indica que um servidor de AAA e uma autenticação de EAP estão sendo usados.

Acreditamos que você já aprendeu que WEP é um modo de segurança com falhas. PSK2, que é o mesmo que o WPA2 ou o IEEE 802.11i, é a opção favorita para a maior segurança. Se o WPA2 é o melhor, você deve estar se perguntando por que há tantas outras opções. A resposta é que muitas redes locais sem fio suportam dispositivos sem fio antigos. Como todos os dispositivos de cliente que se associam a um ponto de acesso devem executar o mesmo modo de segurança que o ponto de acesso executa, o ponto de acesso precisa ser definido para suportar o dispositivo que executa o modo de segurança mais fraco. Todos os dispositivos de rede local sem fio fabricados após março de 2006 devem poder suportar o WPA2, ou no caso de roteadores Linksys, PSK2, conforme os dispositivos são atualizados, você pode comutar seu modo de segurança de rede para PSK2.

A opção RADIUS disponível para um roteador para rede sem fio Linksys permite que você use um servidor RADIUS em combinação com o WEP.

Para configurar a segurança, faça o seguinte:

- Security Mode (Modo de Segurança) - Selecione o modo desejado: PSK Personal, PSK2 Personal, PSK Enterprise, PSK2 Enterprise, RADIUS, ou WEP.

- Mode Parameters (Parâmetros de Modo) - Cada um dos modos PSK e PSK2 tem parâmetros que podem ser configurados. Se você selecionar a versão de segurança PSK2 Enterprise, você deverá ter um servidor RADIUS anexado a seu ponto de acesso. Se você tiver essa configuração, precisará configurar o ponto de acesso para apontar ao servidor de RADIUS.

- RADIUS Server IP Address (Endereço IP do servidor RADIUS) - Digite o endereço IP do servidor RADIUS.

- RADIUS Server Port (Porta de servidor RADIUS) - Digite o número da por-

ta usada pelo servidor RADIUS. O padrão é 1812.

- Encryption (Criptografia) - Selecione o algoritmo desejado, AES ou TKIP. (O AES é um método de criptografia mais forte que o TKIP.)

- Pre-shared Key (Chave pré-compartilhada) - Digite a chave compartilhada pelo roteador e pelos outros dispositivos de rede. Ela deve ter de 8 a 63 caracteres.

- Key Renewal (Renovação da chave) - Digite o período de renovação da chave, que indica de quanto em quanto tempo o roteador deve alterar as chaves de criptografia.

5.7.2 Busca por SSIDs

Quando o ponto de acesso tiver sido configurado, você precisará configurar a placa de rede sem fio em um dispositivo de cliente para que o ponto de acesso possa se conectar à rede sem fio. Você também deverá verificar se o cliente para rede sem fio se conectou com êxito à rede sem fio correta, especialmente porque pode haver muitas WLANs disponíveis às quais se conectar. Apresentaremos também alguns passos básicos de identificação e solução de problemas para reconhecer problemas comuns relacionados com a conectividade de WLAN.

Se seu PC for equipado com uma placa de rede sem fio, você estará pronto para fazer uma busca por redes sem fio. PCs que executam o Microsoft Windows XP têm um monitor de redes sem fio interno e um utilitário de cliente. Você pode ter um utilitário diferente instalado e selecionado como preferência à versão nativa do Microsoft Windows XP.

A etapa abaixo é para o uso do recurso de exibição de redes sem fio no Microsoft Windows XP:

- Na bandeja do sistema na barra de ferramentas do Microsoft Windows XP, localize o ícone de conexão de rede. Clique duas vezes no ícone para abrir a caixa de diálogo Conexões de rede.

Se você tiver uma WLAN que não esteja aparecendo na lista de redes, talvez o broadcast de SSID esteja desabilitado no ponto de acesso. Se esse for o caso, você deverá digitar o SSID manualmente.

Resumo

Nesta aula, tratamos da evolução dos padrões de redes locais sem fio, incluindo o IEEE 802.11a, b, g e, agora, n, em fase de teste. Padrões mais novos levam em conta a necessidade de suportar voz e vídeo e a qualidade de serviço requerida.

Mostramos que um único ponto de acesso conectado à rede local cabeada fornece um conjunto de serviços básicos a estações de cliente associadas a ela. Vários pontos de acesso que compartilham um identificador de conjunto de serviços se combinam para formar um conjunto de serviços estendidos. Redes locais sem fio podem ser detectadas por qualquer dispositivo de cliente habilitado por rádio e podem, portanto, habilitar acesso por invasores que não têm acesso a uma rede apenas cabeada.

Atividades de aprendizagem

1. Em quais camadas do modelo OSI os Access point funcionam?

a) física

b) enlace de dados

c) rede

d) aplicação

2. Para ajudar a garantir uma rede sem fio segura, qual padrão IEEE deve ser seguido pela maioria das redes corporativas?

a) 802.11a

b) 802.11b

c) 802.11c

d) 802.11i

3. Quais das combinações de canais 802.11b permitem que dois APs wireless funcionem simultaneamente na mesma sala sem sobreposição de canais? (escolha duas)

a) canais 10 e 6

b) canais 9 e 6

c) canais 8 e 5

d) canais 7 e 2

e) canais 6 e 2

f) canais 6 e 11

Prezado(a) estudante,

Finalizamos a penúltima aula desta disciplina. A próxima aula, na qual trataremos de tecnologias com IP, representa a finalização de uma etapa em seu processo de aprendizagem, o que significa que você deve continuar estudando para se manter atualizado(a) nessa área, em que descobertas e inovações surgem a cada dia. Caso tenha alguma dúvida, antes de prosseguir com a próxima aula, volte ao conteúdo anterior, estudando-o atentamente.

Aula 6. Tecnologias relacionadas com IP

Objetivos:

- identificar os endereços IP disponíveis; e
- reconhecer o novo esquema de endereçamento IP.

Caro(a) estudante,

Faça uma pausa e reflita na quantidade de informações a que você teve acesso desde que iniciou esta disciplina. Acreditamos que valeram a pena seu esforço e dedicação ao estudo.

Nesta última aula, na qual o tema é tecnologia relacionadas ao IP, continue disciplinado(a), separando sempre uma parte do seu tempo para ler o conteúdo exposto e realizar as atividades de aprendizagem.

A Internet e as tecnologias relacionadas com IP passaram por um rápido crescimento. Uma razão para o crescimento se deve, em parte, à flexibilidade do design original. Entretanto, esse design não previu a popularidade da Internet e a demanda resultante por endereços IP. Por exemplo, cada host e cada dispositivo na Internet exige um endereço do exclusivo IP versão 4 (IPv4). Por essa razão, em meados dos anos 90, o IETF solicitou propostas para um novo esquema de endereçamento IP. O grupo de trabalho IP Next Generation (IPng, Última Geração de IP) reagiu. Por volta do ano de 1996, o IETF começou a liberar diversas RFCs definindo o IPv6.

O principal recurso do IPv6 sendo adotado hoje em dia é o maior espaço de endereço: os endereços no IPv6 possuem um tamanho de 128 bits contra os 32 bits do IPv4.

6.1 O IPv6

Por que precisamos de mais espaço de endereço?

Para compreender os problemas de endereçamento IP que atingem os administradores de rede, considere que o espaço de endereço do IPv4 fornece, aproximadamente, 4.294.967.296 endereços exclusivos. Desses, apenas 3,7 bilhões de endereços podem ser atribuídos porque o sistema de endereçamento do IPv4 separa os endereços em classes e reserva os endereços para multicast, teste e outros usos específicos.

Com base nos números de janeiro de 2007, aproximadamente 2,4 bilhões dos endereços de IPv4 disponíveis já foram atribuídos a usuários finais ou ISPs. Isso deixa aproximadamente 1,3 bilhão de endereços ainda disponíveis do espaço de endereços do IPv4. Apesar desse número aparentemente grande, o espaço de endereços do IPv4 está acabando.

Na última década, a comunidade da Internet analisou o esgotamento dos endereço do IPv4 e publicou pilhas de relatórios. Alguns relatórios preveem que o esgotamento dos endereços de IPv4 não acontecerá até 2013.

O crescimento da Internet, aliado ao aumento do poder da computação, aumentou o alcance dos aplicativos baseados em IP.

O conjunto de números está sendo reduzido pelos seguintes motivos:

- Crescimento da população - A população da Internet está crescendo. Em novembro de 2005, a Cisco estimou que havia 973 milhões de usuários aproximadamente. Esse número dobrou desde então. Além disso, os usuários ficam online por mais tempo, reservando os endereços IP por períodos mais longos e entrando em contato com cada vez mais pontos diariamente;

- Usuários móveis - A indústria produziu mais de um bilhão de telefones celulares. Foram produzidos mais de 20 milhões de dispositivos móveis habilitados para IP, inclusive assistentes digitais pessoais (PDAs, Personal Digital Assistants), canetas digitais, blocos de notas e leitores de códigos de barra. Cada vez mais dispositivos móveis habilitados para IP ficam online todos os dias. Os telefones celulares antigos não precisavam de endereços IP, os novos precisam;

- Transporte – As empresas aéreas já fornecem a conectividade da Internet em seus voos. Mais operadoras, incluindo os navios, também fornecem serviços semelhantes;

- Equipamentos eletrônicos - Os dispositivos mais novos permitem a monitoração remota usando a tecnologia IP. São exemplos os gravadores de vídeo digital (DVRs, Digital Video Recorder), que fazem o download de guias de programas e os atualizam pela Internet. As redes locais podem conectar esses dispositivos.

6.2 Motivos para usar o IPv6

O movimento para mudar do IPv4 para o IPv6 já começou, especialmente na Europa, Japão e na região da Ásia-Pacífico. Essas áreas estão esgotando seus endereços IPv4 distribuídos, o que torna o IPv6 ainda mais atraente e necessário. O movimento foi oficialmente iniciado no Japão no ano 2000, quando o governo japonês determinou a incorporação do IPv6 e definiu o prazo final para 2005 para que se atualizassem os sistemas existentes em todos os negócios e no setor público. A Coreia, China e Malásia tiveram iniciativas semelhantes.

Em 2002, a IPv6 Task Force da Comunidade Europeia formou uma aliança estratégica para encorajar a adoção do IPv6 em todo o mundo. A IPv6 Task Force norte-americana começou a exigir que os mercados norte-americanos adotassem o IPv6. Os primeiros avanços significativos nos Estados Unidos são provenientes do Departamento de Defesa Norte-Americano (DoD, U.S Department of Defense). Prevendo o futuro e conhecendo as vantagens de dispositivos habilitados para IP, o DoD designou, já em 2003, que todos os novos equipamentos comprados, além de serem habilitados para IP, fossem habilitados para o IPv6. Em setembro de 2010, o chefe do gabinete de tecnologia da informação emitiu memorando recomendando que os órgãos governamentais implementassem o IPv6 até setembro de 2014.

Foi criado também um sistema para monitorar a evolução desta implementação. Dentro desse programa, os *sites* governamentais tiveram até setembro de 2012 para implantar o IPv6, já realizando para esta etapa a troca de equipamentos na borda da rede que não tivessem suporte IPv6. Disponível em :< **http://ipv6.br/o-papel-dos-governos-na-implantacao-do-ipv6/**)> Acesso em: 11 out.2013

A capacidade de dimensionar as redes para as demandas futuras requer um fornecimento ilimitado de endereços IP e uma mobilidade aprimorada que o DHCP e a NAT, sozinhos, não conseguem atingir. O IPv6 satisfaz os requisitos cada vez mais complexos do endereçamento hierárquico que o IPv4 não fornece.

Devido à enorme base instalada do IPv4 no mundo, não é difícil avaliar que a transição das implantações do IPv4 para o IPv6 seja um desafio. Entretanto, existe uma variedade de técnicas, inclusive uma opção de configuração automática, para fazer a transição de modo mais fácil. O mecanismo de transição usado por você dependerá das necessidades de sua rede.

Então, o que aconteceu com o IPv5? O IPv5 foi usado para definir um protocolo experimental de streaming em tempo real. Para evitar qualquer confusão, foi decidido não usar o IPv5 e nomear o novo protocolo IP como IPv6.

O IPv6 não existiria não fosse o esgotamento reconhecido de endereços IPv4 disponíveis. Porém, além do maior espaço de endereços IP, o desenvolvimento do IPv6 apresentou oportunidades para aplicar as lições aprendidas a partir das limitações do IPv4 para criar um protocolo com recursos novos e aprimorados.

Uma arquitetura de cabeçalho e uma operação de protocolo simplificados se traduzem em gastos operacionais reduzidos. Os recursos de segurança integrados significam práticas de segurança mais fáceis, extremamente ausentes em muitas redes atuais. Entretanto, talvez a melhoria mais significativa oferecida pelo IPv6 sejam os recursos de autoconfiguração que ele possui.

A Internet está evoluindo rapidamente de uma coleção de dispositivos fixos para uma rede fluida de dispositivos móveis. O IPv6 permite que os dispositivos móveis adquiram e façam a transição rapidamente entre endereços conforme eles se movem entre redes externas, sem que haja necessidade de um agente externo. (Um agente externo é um roteador que pode funcionar como o ponto de anexo para um dispositivo móvel quando for de sua rede local para uma rede externa.)

A autoconfiguração de endereço também significa uma conectividade de rede plug and play mais sólida. A autoconfiguração suporta clientes que tenham qualquer combinação de computadores, impressoras, câmeras digitais, rádios digitais, telefones IP, dispositivos domésticos habilitados para a Internet e brinquedos eletrônicos conectados às suas redes locais. Muitos fabricantes já integram o IPv6 em seus produtos.

Muitos dos aprimoramentos oferecidos pelo IPv6 são explicados a seguir, incluindo:

- Endereçamento IP aprimorado;
- Cabeçalho simplificado;
- Mobilidade e segurança;
- Riqueza de transição.

6.3 Endereçamento IP aprimorado

Um espaço maior de endereço oferece vários aprimoramentos, incluindo:

- Melhor acessibilidade e flexibilidade globais;
- Melhor agregação de prefixos de IP anunciados nas tabelas de roteamento;
- Hosts multihome. Multihoming é uma técnica para aumentar a confiabilidade da conexão da Internet de uma rede IP. Com o IPv6, um host pode ter vários endereços IP sobre um link upstream físico. Por exemplo, um host pode conectar-se a vários ISPs;
- A autoconfiguração, que pode incluir endereços de camada de enlace de dados no espaço de endereço;
- Mais opções de plug and play para mais dispositivos;
- Reendereçamento público para privado e fim a fim sem tradução de endereços. Ele torna a rede ponto a ponto (P2P) mais funcional e mais fácil de ser implantada;
- Mecanismos simplificados para renumeração e modificação do endereço.
- O cabeçalho de IPv4 possui 20 octetos e 12 campos de cabeçalho básicos, seguidos por um campo de opções e uma porção de dados (normalmente o segmento de camada de transporte). O cabeçalho de IPv6 possui 40 octetos, 3campos de cabeçalho básicos de IPv4 e 5 campos de cabeçalho adicionais.

O cabeçalho simplificado de IPv6 oferece várias vantagens com relação ao IPv4:

- melhor eficiência de roteamento para desempenho e escalabilidade de taxa de encaminhamento;
- ausência de broadcasts e, desse modo, ausência de ameaças de broadcast storms;
- sem necessidade de processar checksums;
- mecanismos de cabeçalho de extensão simplificados e mais eficientes;
- rótulos de fluxo para processamento por fluxo sem a necessidade de abrir o pacote interno de transporte para identificar os diversos fluxos de tráfego.

6.4 Mobilidade e segurança aprimoradas

A mobilidade e a segurança ajudam a garantir a conformidade com a funcionalidade dos padrões de IP móveis e Segurança IP (IPsec). A mobilidade permite que as pessoas com dispositivos de rede móveis, muitas com conectividade sem fio, movam-se entre as redes.

O padrão de IP móvel da IETF está disponível para o IPv4 e o IPv6. Ele permite que os dispositivos móveis se movam em conexões de rede estabelecidas sem interrupções. Os dispositivos móveis usam um endereço secundário para obter essa mobilidade. Com o IPv4, esses endereços são configurados manualmente. Com o IPv6, as configurações são dinâmicas, dando uma mobilidade integrada aos dispositivos habilitados para Ipv6.

O IPsec está disponível para IPv4 e IPv6. Embora as funcionalidades sejam essencialmente idênticas em ambos os ambientes, o IPsec é obrigatório no IPv6, tornando a Internet do IPv6 mais segura.

O IPv4 não desaparecerá do dia para a noite. Ao contrário, ele coexistirá com o IPv6 e será gradualmente substituído por ele. Por essa razão, o IPv6 foi criado com técnicas de migração para abranger todos os casos concebíveis de atualização do IPv4. Porém, no final das contas, muitas foram rejeitadas pela comunidade tecnológica.

Existem atualmente três abordagens principais:

- Pilha dupla;
- Tunelamento 6to4;
- NAT-PT, tunelamento ISATAP e tunelamento Teredo (métodos de último caso).

Algumas dessas abordagens serão discutidas com mais detalhes posteriormente nesta aula.

O conselho atual para fazer a transição para o IPv6 é "Pilha dupla onde puder, túnel onde precisar".

Observe a seguir as possíveis estruturas de endereços.

a) Representação de endereço IPv6

Você conhece o endereço IPv4 de 32 bits como uma série de quatro campos de 8 bits, separada por pontos. Porém, endereços IPv6 maiores, de 128 bits, precisam de uma representação diferente por causa de seu tamanho. Os endereços IPv6 usam dois-pontos para separar as entradas em uma série de hexadecimal de 16 bits.

O endereço 2031:0000:130F:0000:0000:09C0:876A:130B. O IPv6 não requer uma notação de cadeia de endereços explícita.

Os zeros à esquerda em um campo são opcionais. Por exemplo, o campo 09C0 é igual ao 9C0 e o campo 0000 é igual a 0. Assim 2031:0000:130F:0000:0000:09C0:876A:130B podem ser escritos como 2031:0:130F:0000:0000:9C0: 876A:130B.

Os campos sucessivos de zeros podem ser representados como dois sinais de dois-pontos "::". Entretanto, este método de taquigrafia só pode ser usado uma vez em cada endereço. Por exemplo, 2031:0:130F:0000:0000:9C0:876A:130B pode ser escrito como 2031:0:130F::9C0:876A:130B.

Um endereço especificado é escrito como "::" porque contém somente zeros.

Usando o "::", a notação reduz bastante o tamanho da maioria dos endereços, como mostrado. Um analista de endereços identifica o número de zeros faltantes separando duas partes quaisquer de um endereço e digitando 0s até que os 128 bits estejam completos.

b) Endereço de unicast global do IPv6

O IPv6 possui um formato de endereço que permite eventualmente uma maior agregação para o ISP. Endereços de unicast globais consistem geralmente de um prefixo de roteamento global de 48 bits e uma ID de sub-rede de 16 bits. As organizações individuais podem usar um campo de sub-rede de 16 bits para criar sua própria hierarquia de endereçamento local. Esse campo permite que uma organização use até 65.535 sub-redes individuais.

A hierarquia adicional é acrescentada ao prefixo de roteamento global de 48 bits com o prefixo de registro, prefixo de ISP e prefixo do site.

O endereço de unicast global atual que é atribuído pelo IANA usa o intervalo de endereços iniciado com o valor binário 001 (2000::/3), que é 1/8 do espaço total do endereço IPv6 e que é o maior bloco de endereços atribuídos. O IANA está alocando o espaço de endereços IPv6 nos intervalos de 2001::/16 para os cinco registros RIR (ARIN, RIPE NCC, APNIC, LACNIC e AfriNIC).

Para obter mais informações, consulte a RFC 3587, formato de endereços de unicast de IPv6, que substitui a RFC 2374.

c) Endereços reservados

O IETF reserva uma porção do espaço de endereços IPv6 para vários usos, presentes e futuros. Os endereços reservados representam 1/256 do espaço de endereço IPv6 total. Alguns dos outros tipos de endereços IPv6 são originados deste bloco.

d) Endereços privados

Um bloco de endereços IPv6 é reservado para endereços privados, assim como é feito no IPv4. Esses endereços privados são locais somente para um link ou local específico e, portanto, nunca são roteados para fora de uma rede corporativa específica. Os endereços privados possuem um valor de primeiro octeto de "FE" em notação hexadecimal, com o próximo dígito

hexadecimal sendo um valor de 8 para F.

Esses endereços são divididos ainda em dois tipos, com base no escopo.

- Endereços locais de site são endereços semelhantes à alocação de endereços para Internet privada no IPv4 da RFC 1918 de hoje. O escopo desses endereços é um site ou organização inteiros. Entretanto, o uso dos endereços locais é problemático e está sendo substituído desde 2003 pela RFC 3879. Em hexadecimais, os endereços locais começam com "FE" e então de "C" até "F" para o terceiro dígito hexadecimal.

- Endereços de enlace locais são novos para o conceito de endereçamento com IP na camada de rede. Esses endereços têm um escopo menor do que os endereços locais de site. Eles se referem somente a um link físico específico (rede física). Os roteadores não encaminham datagramas utilizando endereços de enlace locais, nem mesmo dentro da organização. Eles servem somente para comunicação local em um segmento de rede físico específico. Eles são usados para comunicações de link como a configuração de endereço automática, detecção de vizinho e detecção de roteador. Muitos protocolos de roteamento do IPv6 também usam endereços de enlace locais. Os endereços de enlace locais começam com "FE" e, assim, possuem um valor de "8" para "B" para o terceiro dígito hexadecimal.

e) Endereço de loopback

Assim como ocorre no IPv4, foi fornecido um endereço IPv6 de loopback especial para testes. Os datagramas enviados para esse endereço retornam para o dispositivo de origem. Entretanto, existe apenas um endereço no IPv6 para essa função, e não um bloco inteiro. O endereço de loopback é 0:0:0:0:0:0:0:1, normalmente expresso com o uso da compressão do zero com o ":: 1."

f) Endereço não especificado

No IPv4, um endereço IP somente com zeros tem um significado especial. Ele se refere ao próprio host e é usado quando um dispositivo não souber seu próprio endereço. No IPv6, esse conceito foi formalizado, e o endereço somente com zeros (0:0:0:0:0:0:0:0) recebe o nome de endereço "não especificado." Ele é usado normalmente no campo de origem de um datagrama,

o qual é enviado por um dispositivo que busca ter seu endereço IP configurado. É possível aplicar a compressão de endereços a esse endereço. Como somente contém zeros, ele se tornará simplesmente "::".

g) Gerenciamento de endereços IPv6

Os endereços do IPv6 usam identificadores de interface para identificar as interfaces em um link. Considere-os como a "porção de host" de um endereço IPv6. Os identificadores de interface devem ser exclusivos em um link específico. Os identificadores de interface são sempre de 64 bits e são derivados dinamicamente de um endereço de Camada 2 (endereço MAC).

Você pode atribuir uma ID de endereço IPv6 estática ou dinamicamente:

- Atribuição estática usando uma ID de interface manual;
- Atribuição estática usando uma ID de interface EUI-64;
- Configuração automática sem estado;
- DHCP para IPv6 (DHCPv6).

6.4.1 Atribuição de ID de interface manual

Uma maneira de atribuir um endereço IPv6 estaticamente a um dispositivo é atribuir o prefixo (rede) e a porção da ID de interface (host) do endereço IPv6. Para configurar um endereço IPv6 em uma interface do roteador Cisco, use o comando ipv6 address ipv6-address/prefix-length no modo de configuração de interface. O exemplo seguinte mostra a atribuição de um endereço IPv6 à interface de um roteador Cisco:

```
RouterX(config-if)#ipv6 address 2001:DB8:2222:7272::72/64
```

Atribuição de ID de interface EUI-64

Outra maneira de atribuir um endereço IPv6 é configurar a porção do prefixo (rede) do endereço IPv6 e derivar a porção da ID de interface (host) do endereço MAC de camada 2 do dispositivo, conhecido como a ID de interface EUI-64.

O padrão EUI-64 explica como expandir os endereços MAC do IEEE 802 de 48 para 64 bits inserindo o 0xFFFE de 16 bits no meio do 24º bit do endereço MAC, a fim de criar um identificador de interface de 64 bits exclusivo.

Para configurar um endereço IPv6 em uma interface do roteador Cisco e habilitar o processamento de IPv6 usando o EUI-64 nessa interface, use o comando ipv6 address ipv6-prefix/prefix-length eui-64 no modo de configuração de interface. O exemplo seguinte mostra a atribuição de um endereço EUI-64 à interface de um roteador Cisco:

```
RouterX(config-if)#ipv6 address 2001:DB8:2222:7272::/64 eui-64
```

Configuração automática sem estado

A configuração automática configura automaticamente o endereço IPv6. No IPv6, presume-se que os dispositivos que não sejam do PC, bem como os terminais de computador, serão conectados à rede. O mecanismo de configuração automática foi introduzido para permitir que a rede plug-and-play desses dispositivos ajude a reduzir a sobrecarga de administração.

DHCPv6 (sem estado)

O DHCPv6 permite que os servidores DHCP transmitam os parâmetros de configuração, como os endereços de rede IPv6, para os nós do IPv6. Ele oferece o recurso de alocação automática de endereços de rede reutilizáveis e uma flexibilidade de configuração adicional. Esse protocolo é um correspondente sem estado da configuração automática de endereços sem estado do IPv6 (RFC 2462) e pode ser usado separado da configuração automática de endereços sem estado do IPv6, ou simultaneamente a ela, para obter os parâmetros de configuração.

Estratégias de transição do IPv6

A transição do IPv4 não exige melhorias concomitantes em todos os nós. Muitos mecanismos de transição permitem uma integração tranquila do IPv4 e IPv6. Outros mecanismos que permitem que os nós de IPv4 se comuniquem com os nós de IPv6 estão disponíveis. Situações diferentes exigem estratégias diferentes.

Lembre-se do conselho: "Pilha dupla onde puder, túnel onde precisar". Esses dois métodos são as técnicas mais comuns para fazer a transição de IPv4 para IPv6.

Empilhamento duplo

O empilhamento duplo é um método de integração no qual um nó possui implementação e conectividade a uma rede IPv4 e a uma rede IPv6. Essa é a opção recomendada e envolve a execução de IPv4 e IPv6 ao mesmo tempo. Os roteadores e os switches são configurados para suportar ambos os protocolos, sendo que o IPv6 é o protocolo preferido.

Tunelamento

Outra técnica de transição importante é o tunelamento. Existem várias técnicas de tunelamento disponíveis, incluindo:

- Tunelamento manual de IPv6 sobre IPv4 - Um pacote de IPv6 é encapsulado dentro do protocolo IPv4. Esse método exige roteadores de pilha dupla.

- Tunelamento dinâmico 6to4 – Estabelece a conexão das ilhas de IPv6 automaticamente através de uma rede IPv4, normalmente a Internet. Ele aplica automaticamente um prefixo de IPv6 válido e exclusivo a cada ilha de IPv6, permitindo a rápida implantação do IPv6 em uma rede corporativa sem que ocorra a recuperação de endereço dos ISPs ou dos registros.

Outras técnicas de tunelamento menos populares, que estão além do proposto para este curso, incluem:

- Protocolo de endereçamento automático de túnel intra-site (ISATAP - Intra-Site Automatic Tunnel Addressing Protocol) – Mecanismo de tunelamento de sobreposição automática que usa a rede de IPv4 subjacente como uma camada de enlace para o IPv6. Os túneis do ISATAP permitem que os hosts de pilha dupla individuais de IPv4 ou IPv6 dentro de um local se comuniquem com outros hosts em um link virtual, criando uma rede de IPv6 que utiliza a infraestrutura de IPv4.

- Tunelamento Teredo - Uma tecnologia de transição de IPv6 que fornece o tunelamento automático de host para host em vez de um tunelamento

de gateway. Essa abordagem transmite o tráfego unicast de IPv6 quando os hosts de pilha dupla (hosts que executam tanto o IPv6 quanto o IPv4) estão localizados atrás de um ou de vários NATs de IPv4.

6.5 Tradução do protocolo NAT (NAT-PT)

As rotas do IPv6 usam os mesmos protocolos e técnicas que o IPv4. Embora os endereços sejam mais longos, os protocolos usados no roteamento de IPv6 são simplesmente extensões lógicas dos protocolos usados no IPv4.

A RFC 2080 define a última geração do Protocolo de informações de roteamento (RIPng, Routing Information Protocol next generation) como um protocolo de roteamento simples baseado em RIP. O RIPng não é nem mais potente nem menos potente do que o RIP, porém fornece uma maneira simples de ativar uma rede de IPv6 sem a necessidade de criar outro protocolo de roteamento.

O RIPng é um protocolo de roteamento do vetor de distância com um limite de 15 saltos que usa o split horizon e as atualizações de poison reverse para evitar os loops de roteamento. Sua simplicidade vem do fato de ele não exigir nenhum conhecimento global da rede. Somente os roteadores vizinhos trocam mensagens locais.

O RIPng inclui as seguintes características:

- Baseia-se no RIP versão 2 (RIPv2) do IPv4 e é semelhante ao RIPv2.
- Utiliza o IPv6 para o transporte.
- Inclui o prefixo de IPv6 e o endereço IPv6 do próximo salto.
- Utiliza o grupo multicast FF02::9 como o endereço de destino para atualizações de RIP (semelhante à função de broadcast executada pelo RIP no IPv4).
- Envia atualizações na porta UDP 521.
- É suportado pelo IOS Cisco Release 12.2 (2) T e mais recentes.

Em implantações que sofreram empilhamento dual, são necessários o RIP e o RIPng.

Existem duas etapas básicas para ativar o IPv6 em um roteador. Primeiro, você deve ativar o encaminhamento de tráfego IPv6 no roteador e, em seguida, deve configurar cada interface que exija o IPv6.

Por padrão, o encaminhamento de tráfego do IPv6 está desabilitado em um roteador Cisco. Para ativá-lo entre as interfaces, é necessário configurar o comando global ipv6 unicast-routing.

O comando IPv6 address pode configurar um endereço IPv6 global. O endereço de enlace local será configurado automaticamente quando um endereço for atribuído à interface. Você deve especificar o endereço IPv6 de 128 bits inteiro ou deve especificar o uso do prefixo de 64 bits usando a opção eui-64.

Você pode especificar completamente o endereço IPv6 ou pode computar o identificador de host (64 bits mais à direta) do identificador de EUI-64 da interface. No exemplo, o endereço IPv6 da interface é configurado usando o formato EUI-64.

Como alternativa, você pode especificar completamente o endereço IPv6 inteiro para atribuir um endereço a uma interface do roteador usando o comando ipv6 addressipv6-address/prefix-length no modo de configuração de interface.

A configuração de um endereço IPv6 em uma interface configura automaticamente o endereço de enlace local para essa interface.

Configurar o RIPng com IPv6

Ao configurar os protocolos de roteamento suportados no IPv6, é necessário criar o processo de roteamento, habilitar o processo de roteamento nas interfaces e personalizar o protocolo de roteamento para sua rede privada.

Antes de configurar o roteador para que ele execute o RIP de IPv6, faça a habilitação global usando o comando de configuração global IPv6 unicast-routing e habilite o IPv6 nas interfaces em que o RIP de IPv6 deverá ser habilitado.

Para habilitar o roteamento RIPng no roteador, use o comando de configuração global IPv6 router rip name. O parâmetro name (nome) identifica o processo RIP. Esse nome de processo é usado posteriormente ao configurar o RIPng nas interfaces participantes.

Para o RIPng, em vez de usar o comando network para identificar quais interfaces devem executar o RIPng, você usa o comando ipv6 rip name enable no modo de configuração de interface para habilitar o RIPng em uma interface. O parâmetro name (nome) deve corresponder ao parâmetro de nome no comando IPv6 router rip.

A habilitação do RIP em uma interface cria dinamicamente um processo de "router rip", se necessário.

Exemplo: RIPng para configuração de IPv6

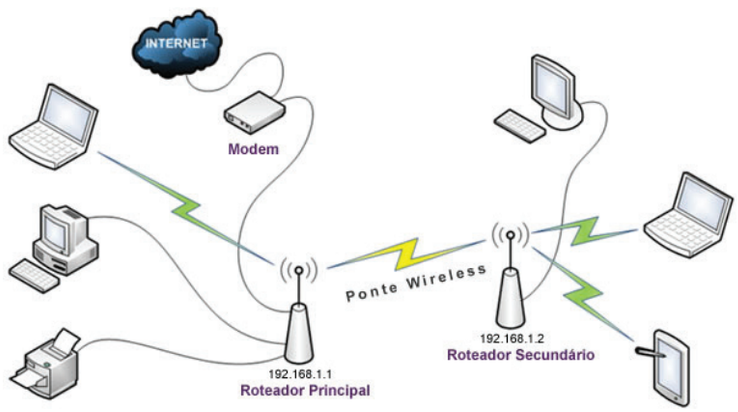


Figura 16
Fonte: http://infohelp.org/thales-laray/repetindo-o-sinal-com-o-linksys-wrt54g/

O exemplo mostra uma rede de dois roteadores. O roteador R1 está conectado à rede padrão. Nos roteadores R2 e R1, o nome RT0 identifica o processo de RIPng. O RIPng é habilitado na primeira interface Ethernet do roteador R1 usando o comando IPv6 rip RT0 enable. O roteador R2 mostra que o RIPng está habilitado nas interfaces Ethernet usando o comando IPv6 rip RT0 enable.

Essa configuração permite que as interfaces Ethernet 1 no roteador R2 e Ethernet 0 de ambos os roteadores troquem informações de roteamento de RIPng.

Resumo

Nesta aula você pôde verificar que o aparecimento do IPv6 não lida somente com o esgotamento dos endereços IPv4 e deficiências de NAT, ele fornece novos e melhores recursos. Na breve introdução ao IPv6 no conteúdo exposto mostramos como os endereços IPv6 são estruturados, como eles irão aprimorar a segurança e a mobilidade da rede e como o mundo do IPv4 fará a transição para o IPv6.

Atividades de Aprendizagem

1. Quais são as duas afirmações que descrevem precisamente o protocolo de roteamento RIPng. (escolha duas)

a) RIPng tem um limite de 15 saltos

b) RIPng é um protocolo de roteamento Link State

c) RIPng usa a porta UDP 238 para atualizações

d) RIPng usa poison reverse

e) RIPng encaminha broadcast de IPv6

2. Quais são os dois métodos automáticos para atribuir um endereço IPv6 a uma interface que podem ser usados em conjunto. (escolha duas)

a) DHCPv6

b) Configuração automática sem estado

c) EUI-64

d) atribuição estática

e) DNS

Prezado(a) estudante,

Chegamos ao fim da última aula da disciplina rede de Computadores II. Esperamos que o conteúdo das aulas sirvam de auxílio quando você estiver atuando na área para a qual está se capacitando. Reafirmamos que seus

estudos não devem parar por aqui, pois sempre há muito para conhecer e aprender.

Palavras finais

Chegamos ao final de nosso estudo da disciplina Redes de Computadores II. As ferramentas estudadas o(a) ajudarão a desenvolver um melhor entendimento do funcionamento das redes.

O que foi apresentado poderá auxiliá-lo(a) no desenvolvimento das habilidades necessárias para planejar e implementar redes através de uma série de aplicações.

Encerramos esta disciplina esperando ter contribuído com informações relevantes relacionadas a uma vasta gama de tecnologias que facilitam a maneira como as pessoas trabalham, vivem, jogam e aprendem se comunicando com voz, vídeo e outros tipos de dados.

No entanto, é preciso continuar estudando, pesquisando e se qualificando, pois o competitivo mercado de trabalho atual absorve, cada vez mais, profissionais capacitados(as) e atualizados(as) com as novas tecnologias.

A tecnologia pode nos ajudar a viver melhor! Não desista de estudar.

Guia de Soluções

Atividades - Aula 1

1. b,d

2. a,d

3. b

4. a

5. a,c,d

Atividades - Aula 2

1. c

2. d

3. d

4. b

5. a

Atividades - Aula 3

1. a,d

2. c

3. d

4. c

5. d

Atividades - Aula 4

1. c

2. b,d,e

3. a

4. c

5. b

Atividades - Aula 5

1. b

2. d

3. d,f

Atividades - Aula 6

1. a, d

2. a, b

Referências

CEPTRO.BR, Centro de estudos e Pesquisas em Tecnologia de Redes e Operações. **O Papel dos governos na implantação do IPv6**. Disponível em: < http://ipv6.br/o-papel-dos-governos-na-implantacao-do-ipv6/> Acesso em: 11 out. 2013.

COMER, Douglas E; STEVENS, David L. **Interligação em rede com TCP/IP**. Rio de Janeiro: Campus, 1998-1999. 2 v. ISBN 85-352-0270-6 (v. 1).

OLIVEIRA, Gorki Starlin da Costa. **TCP/IP: internet - intranet - extranet**. 5. ed. Rio de Janeiro: Book Express, 2001. 352 p. ISBN 8588281023.

WEBB, Karen. **Construindo redes Cisco usando comutação multicamadas**. São Paulo, SP: Pearson Education do Brasil, 2003. xxi, 408 p. ISBN 8534615012.

PROJETO de interconexão de redes: **Cisco internetwork design** - CID. São Paulo, SP: Pearson Education, 2003. xxxvi, 597 p. ISBN 8534614997.

HELD, Gilbert. **Comunicação de dados**. Rio de Janeiro: Campus, 1999. 708 p. ISBN 85-352-0465-2.

ALVES, Luiz. **Comunicação de dados**. 2.ed., rev. e ampl. São Paulo: Makron, 1994. 323 p. ISBN 85-346-0239-5.

SILVEIRA, Jorge Luis da. **Comunicação de dados e sistemas de teleprocessamento**. São Paulo: Makron, 1991.

SILVA JÚNIOR, Denizard Nunes da; TABINI, Ricardo. **Fibras ópticas**. 3. ed. São Paulo: Érica, 1990 127 p. ISBN 85-7194-054-1.

SOUSA, Lindeberg Barros de. **Redes de computadores: dados, voz e imagem**. 5. ed. São Paulo: Érica, 2002

Currículo do Professor-autor

Neylor Michel

Professor e pesquisador da Universidade Tecnológica Federal do Paraná - UTFPR. Doutor em Engenharia pela Universidade Federal de Campina Grande, mestre em Ciências da Computação pela Universidade Federal de Santa Catarina.

Tem experiência na área de Ciência da Computação, atuando principalmente nos seguintes temas: Protocolos de Roteamento, IPv6.

Autor do Livro Redes de Computadores I.