

DlteC do Brasil®
www.dltec.com.br
info@dltec.com.br | 41 3045.7810



DLTEC DO
BRASIL

CURSO FUNDAMENTOS DE REDES CISCO
(TÓPICO 1.0 DO CCNA 200-301)

Curso Fundamentos de Redes Cisco
DlteC do Brasil®
Todos os direitos reservados©

Copyright © 2020.

É expressamente proibida cópia, reprodução parcial, reprografia, fotocópia ou qualquer forma de extração de informações deste sem prévia autorização da DlteC do Brasil conforme legislação vigente.

O conteúdo dessa apostila é uma adaptação da matéria online do Curso Fundamentos de Redes Cisco.

Aviso Importante!

Esse material é de propriedade da DlteC do Brasil e é protegido pela lei de direitos autorais 9610/98.

Seu uso pessoal e intransferível é somente para os alunos devidamente matriculados no curso.

A cópia e distribuição é expressamente proibida e seu descumprimento implica em processo cível de danos morais e material previstos na legislação contra quem copia e para quem distribui.

Para mais informação visite www.dltec.com.br

Seja muito bem-vindo(a) ao curso Curso Fundamentos de Redes Cisco, o qual faz parte da trilha da certificação Cisco CCNA 200-301, da Dltec!

Aqui, você terá todo o background necessário para aprender sobre os Fundamentos de Redes e ser aprovado(a) no exame **200-301 da Cisco** ao final da trilha. O exame citado anteriormente é conhecido também como exame **CCNA** ou **Cisco Certified Network Associate**.

Os assuntos encontram-se distribuídos conforme o **Blueprint** do exame – sendo assim, esteja bastante atento(a) a todo o conteúdo que aqui será apresentado. Não perca de vista o peso de cada tópico – isso é importante para você ter uma noção de quanto investirá o seu tempo em cada um.

Busque praticar o máximo de exercícios possíveis e, além disso, busque compreender cada assunto de maneira objetiva. Não esqueça o propósito principal: ser aprovado(a).

A DlteC estará com você em todos os momentos dessa jornada!

Bons estudos!

Introdução

Olá!

Como parte integrante da Trilha para a Certificação **CCNA 200-301** da Dltec do Brasil, esta apostila representa uma adaptação textual do material disponibilizado online do **Curso Fundamentos de Redes Cisco**. Por isso, recomendamos que você a utilize como um importante recurso offline. Combinando-a com o conteúdo online, você estará muito mais bem preparado(a) para realizar o exame **200-301 (CCNA: Cisco Certified Network Associate)**.

É de suma importância que você, além de participar dos fóruns, realize o máximo possível de exercícios e simulados (todos encontrados na trilha do 200-301 Online).

Para iniciar, assista aos vídeos introdutórios do capítulo 01 (disponibilizados na Trilha do 200-301), pois lá você obterá mais detalhes sobre o funcionamento geral do curso.

Esperamos que você aproveite ao máximo este material, que foi idealizado com o intuito verdadeiro de fazê-lo(a) obter êxito no exame. Estamos torcendo pelo seu sucesso!

Bons estudos!

Fundamentos de Redes Cisco

Peso no CCNA 200-301: 20%
(Tópico 1.0 Network Fundamentals)

Objetivos

Ao final desse curso você deverá ter conhecimentos sobre:

- Explicar o papel e a função dos principais dispositivos de Rede
- Descrever as características das principais arquiteturas de Rede
- Comparar as interfaces físicas e tipos de cabos utilizados em uma LAN
- Identificar os principais problemas relacionados ao cabeamento de LAN
- Comparar os protocolos TCP e UDP
- Configurar e verificar os endereçamentos IPv4 e IPv6
- Realizar a divisão em sub-redes e compreender o uso dos endereços privativos no IPv4
- Comparar os tipos de endereços IPv6
- Configurar parâmetros de Rede em clientes Windows, MAC-OS e Linux
- Descrever os princípios de funcionamento de Redes sem fio
- Explicar os fundamentos da virtualização (máquinas virtuais)
- Descrever os principais conceitos de switching

Sumário

1	Introdução	8	4.4	Switches Camada 3 (L3 ou Layer 3)	61
1.1	Introdução ao Curso	8	4.5	Roteadores (Routers)	63
1.2	Sobre a Cisco e o CCNA - Cisco Certified Network Associate	9	4.6	Firewall vesus Next-Generation Firewalls (NGFW)	65
1.3	Plano de Estudos para o CCNA	11	4.7	IPS versus Next-Generation IPS (NGIPS)	67
1.4	Como Estudar	13	4.8	Controllers (Controladoras)	68
2	Tópicos do Curso vs Blueprint do CCNA 200-310 – Peso 20%	14	4.8.1	Wireless LAN Controllers	69
3	Revisão de Modelo OSI e TCP/IP	16	4.8.2	Cisco DNA Center	71
3.1	Revisão do Modelo de Referência OSI	16	4.8.2.1	Resumo dos Recursos e benefícios do Cisco DNA Center	72
3.1.1	Função das Camadas do Modelo OSI	18	4.8.2.2	Underlay, Overlay e Fabric	73
3.2	Revisão do Protocolo TCP/IP	20	4.8.3	ACI (Application Centric Infrastructure - Datacenter)	75
3.2.1	Camada de Aplicação	21	5	Topologias de Rede	77
3.2.2	Camada de Transporte: TCP vs UDP	24	5.1	Como Podemos Conectar Dispositivos em Rede?	78
3.2.3	Camada de Internet	27	5.2	Small Office/Home Office (SOHO)	79
3.2.4	Camada de Acesso aos Meios (Data Link e Camada Física)	28	5.2.1	Home Office	80
3.2.4.1	Endereço MAC	30	5.2.2	Small Office ou Branch Office	81
3.2.5	Encapsulamento de Dados no TCP/IP	31	5.3	Two Tier	82
4	Dispositivos de Rede	33	5.4	Three Tier	84
4.1	Endpoints - Computadores e Servidores	33	5.5	WAN	85
4.1.1	Computadores	35	5.5.1	Tecnologias Ponto a Ponto e Hub-and-spoke	86
4.1.2	Servidores	36	5.5.2	MPLS - MultiProtocol Label Switching	89
4.1.3	Virtualização de Servidores	38	5.5.3	Metro Ethernet	91
4.1.3.1	Máquinas Virtuais ou VMs (Virtual Machines)	40	5.5.3.1	Topologias Metro Ethernet	93
4.1.3.2	Hypervisors	41	5.5.4	Internet como WAN	94
4.1.3.3	Tipos de Hypervisors	42	5.5.5	SD-WAN ou Software Defined WAN	96
4.1.3.4	Conectando VMs à Rede	43	5.6	Spine and Leaf	98
4.1.4	Outros Tipos de Endpoints	44	5.7	On-premises e Cloud	101
4.2	Switches Camada 2 (L2 ou Layer 2)	46	5.7.1	A Nuvem como Serviço	104
4.2.1	MAC, Frames e Ethernet	48	5.7.2	Conectando-se com a Nuvem Pública via Internet	106
4.2.2	Principais Funções de um Switch L2	50	5.7.3	Conectando-se com a Nuvem Pública via VPN ou Link Dedicado	108
4.2.2.1	Aprendizado de Endereços MAC	51	6	Conexões, Interfaces e Tipos de Cabeamento	109
4.2.2.2	Encaminhar ou filtrar quadros entre portas	52	6.1	Cabos Metálicos	109
4.2.2.3	Evitar Loops utilizando o protocolo Spanning-tree (STP):	54	6.1.1	Montagem e Testes dos Cabos de Pares Trançados	111
4.2.3	Frame Flooding	54	6.2	Fibras Ópticas	112
4.2.4	Tabela de Endereços MAC	55	6.2.1	Tipos de Fibra Óptica	113
4.3	Access Points (AP)	57	6.2.2	Fibras Ópticas Multimodo	114

6.2.3	Fibras Ópticas Monomodo	115	7.2 Protocolo TCP	157	
6.2.4	Onde Devo Utilizar os Tipos de Fibra Óptica Monomodo e Multimodo na prática?	117	7.2.1	Arquitetura Cliente/Servidor	159
6.2.5	Principais Tipos de Conectores Ópticos	117	7.2.2	Estabelecendo uma Conexão TCP	162
6.2.6	Exemplo de Link Óptico entre Dois Switches	119	7.2.3	Confirmação de Recebimento de Segmentos TCP	164
6.3 Opções de Conexões em Switches Cisco Catalyst		120	7.2.4	Retransmissão de Segmentos TCP	166
6.4 PoE – Power Over Ethernet		123	7.2.5	Controle de Congestionamento TCP	169
6.4.1	Detecção e Negociação de Potência via PoE	125	7.2.6	Reagrupamento de Segmentos TCP	170
6.4.2	PoE e Design de LANs	126	7.3 Protocolo UDP	171	
6.5 Identificando os Principais Problemas em Interfaces e Cabeamento		127	7.4 Identificando Conexões e Aplicações Com Portas TCP e UDP	173	
6.5.1	Um pouco mais sobre Comando Show Interfaces	128	8 Endereçamento IPv4, Sub-Redes e Configurações	175	
6.5.2	Problemas Comuns e Testes em Interfaces LAN	131	8.1 IP versão 4 - Formato do Pacote e Endereçamento	175	
6.5.3	Problemas com Half/Full-Duplex	132	8.2 Sistemas de Numeração	177	
6.6 Conexões Sem Fio – 802.11		134	8.2.1	Sistema Decimal	178
6.6.1	Rede Cabeada versus Wireless	135	8.2.2	Sistema Binário	178
6.6.2	Tipos de Redes Sem Fio	137	8.3 Conversão Binária	180	
6.6.3	Modos de Operação de uma WLAN – Ad-hoc e Infraestrutura	138	8.4 Hosts, Redes e Máscaras	181	
6.6.4	Arquiteturas WLAN Ad-Hoc	139	8.5 Endereçamento IP e a Internet	182	
6.6.5	Arquiteturas WLAN Infraestrutura	139	8.6 Classes de Endereços IP	184	
6.6.5.1	BSS - Basic Service Area	140	8.6.1	Endereço IP Classe A	186
6.6.5.2	ESS - Extended Service Areas	141	8.6.2	Endereço IP Classe B	187
6.6.5.3	Outros Modos de Operação dos APs	142	8.6.3	Endereço IP Classe C	189
6.6.6	Técnicas de Modulação – Enviando um Bit via RF	143	8.6.4	Endereço IP Classe D e Classe E	190
6.6.7	Funcionamento Básico do CSMA-CA	146	8.7 Tipos de Comunicação Suportada pelo Protocolo IP	190	
6.6.7.1	Descobrindo uma Rede sem Fio (Scan)	147	8.8 Endereçamento IPv4 na Prática	192	
6.6.7.2	Autenticação, Criptografia e Associação de Clientes	149	8.9 Dividindo Redes IPv4 em Sub-redes	196	
6.6.7.3	Associação	151	8.9.1	Método Tradicional de Análise de Endereços IP	198
6.6.8	Tecnologias Wireless da Família 802.11	152	8.9.2	Exemplo Prático I – Dividindo Redes Classe A, B e C em duas Sub-redes	200
6.6.8.1	Padrão 802.11b	152	8.9.3	Exemplo Prático II - Projeto de Sub-redes por Redes	202
6.6.8.2	Padrão 802.11a	152	8.9.4	Entendendo a Subnet-Zero e Broadcast-Subnet	204
6.6.8.3	Padrão 802.11g	153	8.9.5	Exemplo Prático III - Projeto de Sub-redes por Hosts	206
6.6.8.4	Padrão 802.11n	153	8.9.6	Análise de Endereços IP com a Metodologia DltcC	207
6.6.8.5	Padrão 802.11ac	154	8.9.7	Máximo de Bits de Host Emprestados	209
6.6.8.6	Padrão 802.11ax	154	8.9.8	Resumo das Máscaras de Sub-rede por Classe	210
6.6.9	Non-Overlapping Channels	155	8.9.9	Dicas Finais sobre Exercícios de Sub-rede para o CCNA	214
7 TCP versus UDP		157			
7.1 Revisão		157			

**8.10 VLSM, CIDR e Sumarização de Rotas
216****8.11 Configurando Endereços IPv4 em
Interfaces de Roteadores e Switches 220**

8.11.1	Endereços IPs Secundários	221
8.11.2	Configurando Endereços IP em Switches	222
8.11.3	Erros Comuns ao Configurar Interfaces	225
8.11.4	Apagando e Alterando Endereços Configurados	227
8.11.5	Verificando as Configurações das Interfaces	229
8.11.6	Testando as Interfaces com Ping, Traceroute e Telnet	231

**9 Endereçamento IPv6, Tipos e
Configurações 233****9.1 Tipos de Comunicação e Endereços em
IPv6 237****9.2 Escrevendo e Abreviando Endereços
IPv6 240****9.3 Tipos de Endereços IPv6 242**

9.3.1	IEEE EUI-64 ou Modified EUI 64	243
9.3.2	Link Local	244
9.3.3	Unique Local Address	245
9.3.4	Global Unicast Address ou GUA	246
9.3.5	Multicast	248
9.3.6	Outros Tipos de Endereços IPv6	250

**9.4 Configurações e Verificações de
Interfaces IPv6 251**

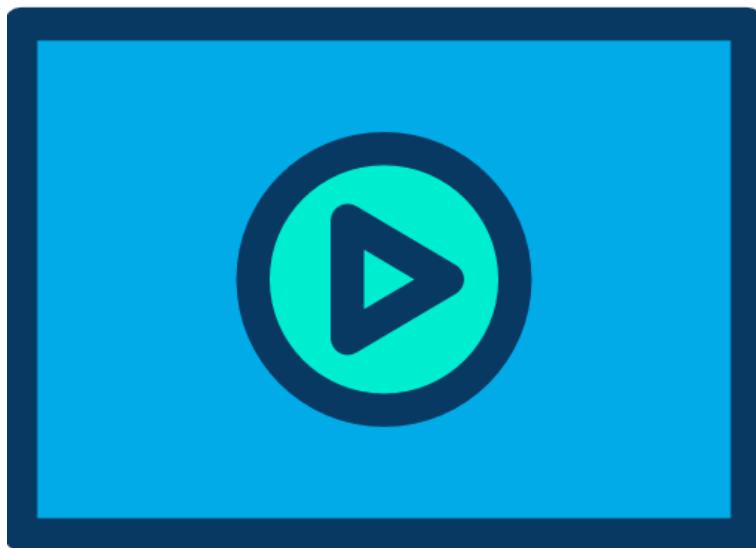
9.4.1	Configurando Interfaces IPv6 no Cisco IOS	252
9.4.2	Grupos de Multicast Padrões das Interfaces Cisco	255
9.4.3	Redes Locais e Diretamente Conectadas no IPv6	256
9.4.4	Testando a Conectividade das Interfaces IPv6	258
9.4.5	Verificando Vizinhos IPv6 – Protocolo NDP	260

**10 Clientes de Rede: MAC OS, Linux e
Windows 262****10.1 Verificando Informações da Camada-
2 262****10.2 Verificando Informações da Camada-
3 266**

10.2.1	Verificando DNS e Gateway no Linux e MAC OS	270
--------	--	-----

1 Introdução

1.1 Introdução ao Curso



Bem-vindo ao **Curso Fundamentos de Redes Cisco**, o qual também faz parte do conteúdo preparatório para a prova de certificação **CCNA 200-301**.

O **Curso Fundamentos de Redes Cisco** possui como objetivo fornecer ao aluno uma visão abrangente sobre o funcionamento de uma Rede de Computadores, seus dispositivos, cabeamento, endereçamento e protocolos básicos de comunicação.

Ao final do curso, você deverá ser capaz de:

- Explicar o papel e a função dos principais dispositivos de Rede
- Descrever as características das principais arquiteturas de Rede
- Comparar as interfaces físicas e tipos de cabos utilizados em uma LAN
- Identificar os principais problemas relacionados ao cabeamento de LAN
- Comparar os protocolos TCP e UDP
- Configurar e verificar os endereçamentos IPv4 e IPv6
- Realizar a divisão em sub-redes e compreender o uso dos endereços privativos no IPv4
- Comparar os tipos de endereços IPv6
- Configurar parâmetros de Rede em clientes Windows, MAC-OS e Linux
- Descrever os princípios de funcionamento de Redes sem fio
- Explicar os fundamentos da virtualização (máquinas virtuais)
- Descrever os principais conceitos de switching

Mesmo que você não esteja trilhando os estudos para a certificação CCNA 200-301 você pode sim fazer esse curso para aumentar seus conhecimentos no mundo de Redes e mais especificamente nos fundamentos de Rede e princípios de funcionamento de dispositivos de Rede do fabricante Cisco.

Mas se você está na trilha da certificação, saiba que esse curso aborda o **Tópico 1.0 ou "Network Fundamentals"**, o qual corresponde a **20% das questões do exame CCNA 200-301.**

Em termos de questões, como a nova prova terá entre 100 e 120 questões, podemos dizer que **devem cair de 20 a 24 questões** relacionadas ao conteúdo desse curso, dependendo da quantidade total de questões que forem sorteadas para seu exame específico.

Não esqueça que ao final do curso você poderá emitir o seu certificado!

1.2 Sobre a Cisco e o CCNA - Cisco Certified Network Associate

A Cisco é uma empresa líder mundial em TI e redes, tendo seus produtos e tecnologias utilizadas por diversas empresas dos mais variados segmentos de mercado no mundo todo.

Fundada em 1984 por Len Bosack e Sandy Lerner atua até os dias de hoje com tecnologia de ponta e inovações que auxiliam no crescimento do mercado de TI.

A Cisco atua na área de Redes (com os famosos Roteadores e Switches), Software, Internet das Coisas, Mobilidade e Comunicação sem fio, Segurança, Colaboração (Voz e Vídeo sobre IP), Data Center, Cloud, Pequenos e Médios Negócios e Provedores de Serviço.

Para garantir que os profissionais que atuam com seus produtos e tecnologias realmente tem os conhecimentos técnicos necessários para desempenhar um bom trabalho, a Cisco desenvolveu um programa de **Certificação** com **Três Níveis** no início:

- **Associate ou CCNA (Cisco Certified Network Associate)**
- Professional ou CCNP (Cisco Certified Network Professional)
- Expert ou CCIE (Cisco Certified Internetwork Expert)

Mais especificamente falando da certificação **CCNA ou Cisco Certified Network Associate** é uma das primeiras certificações lançadas pela Indústria de Redes e com certeza a mais famosa até os dias de hoje.

A primeira versão de CCNA data de 1998 chamada de 640-407, o qual foi atualizado sete vezes até a última mudança feita em 2016 com a versão 200-125 (CCNA Routing and Switching em uma prova) e as versões do 100-105 e 200-105 (Modelo em duas provas: CCENT/ICND-1 + ICND-2).

Em **julho de 2019** foi anunciada uma grande mudança em maioria das certificações Cisco e o CCNA volta ao que era no início, sendo uma certificação unificada para diversas áreas e englobando não somente assuntos de Roteamento e Switching, mas também segurança, redes sem fio e automação de Redes.

Esse curso que você está prestes a iniciar faz parte da nossa trilha para a certificação **CCNA 200-301.**

O que se espera de um CCNA no mercado de trabalho?

Um profissional certificado CCNA deve conhecer uma larga gama de tecnologias e configurações de diversos equipamentos Cisco, tais como Roteadores, Switches, Access Points e Wireless LAN Controllers.

Além disso, deve estar preparado para a nova geração da Infraestrutura de TI, a qual a automação e programabilidade será cada vez mais utilizada.

Não confunda programabilidade com a necessidade de ser um programador, pois um profissional CCNA no mercado faz a operação e manutenção da Rede, não necessariamente precisará ser um programador e sim entender como utilizar algumas ferramentas e interagir com APIs.

É o primeiro passo de uma carreira promissora e que tem muitas possibilidades de crescimento nas mais diversas áreas de tecnologia de rede.

A seguir vamos falar sobre como a preparação para o **CCNA** está dividida no **Portal da DLteC** e como você deverá utilizar nosso material para conquistar sua certificação.

1.3 Plano de Estudos para o CCNA

Nesse novo modelo de prova existe apenas um caminho para obtenção da certificação CCNA que é através do exame 200-301, ou seja, não existe mais opção em duas provas como na versão anterior.

O **plano de estudos** para você ter sucesso na **CCNA** é o seguinte:



1. Ativar a trilha do curso **CCNA 200-301** no Menu Cursos (somente se você ainda não ativou)
2. Estudar o conteúdo de cada Capítulo dentro da trilha (sequência de capítulos/cursos express a seguir)
3. Repetir os comandos e demonstrações práticas realizadas pelo Prof. Marcelo durante as vídeo aulas como laboratório
4. Fazer os simulados que estão dentro do curso "**CCNA 200-301**"
5. A qualquer momento tirar as dúvidas do conteúdo utilizando os fóruns correspondentes de cada capítulo (*)
6. Passar para o próximo capítulo
7. Realizar a prova Final para treinar e obter o certificado do curso CCNA 200-301 (média da aprovação igual ou acima a 70 pontos em um total de 100)
8. Fazer o preparatório Final com laboratórios e questionários (em inglês) específicos para a certificação
9. Agendar a prova e realizá-la

O exame CCNA 200-301 é composto por uma prova em computador que pode ter de 100 a 120 questões (depende do sorteio que é feito por candidato).

Essas questões devem ser resolvidas em 120 minutos no dia do exame.

Cada um dos capítulos do curso um **Peso** associado na prova e quanto maior o peso, maior será a quantidade de questões desse assunto no exame, sendo que seguimos as recomendações da Cisco na divisão de questões para que você treine em um ambiente o mais real possível.

Para ser aprovado(a), você deverá conseguir obter entre 800 e 850 pontos de um máximo 1000 pontos no exame.

Se você ativou esse curso com o objetivo de tirar a certificação então a partir de agora, foco total no objetivo: **OBTER A CERTIFICAÇÃO**.

Você será aprovado(a) – já coloque isso “na cabeça”.

Para isso, pratique os comandos, leia os tópicos com cautela e, de preferência, marque logo o dia do seu exame (para você já ter uma data limite).

Faça o seu cronograma, estipule as horas de estudo e, sinceramente, não tem erro.

Repita essa frase todos os dias: **Eu serei aprovado(a)**.

Se você assumir esse compromisso com sinceridade e vontade de vencer, tudo **dará certo**.

Estamos ao seu lado! Bons estudos!

(*) Os fóruns do curso são exclusivos para TIRAR AS DÚVIDAS DO CURSO, caso você tenha dúvidas do dia a dia ou que não tenham correlação com o curso utilize os grupos do Facebook ou Telegram para troca de ideias.

1.4 Como Estudar

Nesse curso você terá **vídeo aulas, material de leitura e laboratórios em simuladores** para o aprendizado do conteúdo.

Posso somente ler ou assistir aos vídeos? NÃO RECOMENDAMOS!

O ideal é você assistir aos vídeos e na sequência ler os conteúdos ou...

... se preferir leia os conteúdos e depois assista aos vídeos, tanto faz.

POR QUE LER E ASSISTIR?

Simples, porque **um conteúdo complementa o outro**. Principalmente se você está se preparando para a prova de certificação é crucial que você tanto veja os vídeos como a matéria de leitura!

Os questionários ou simulados com questões de prova estão dentro da estrutura do curso CCNA 200-301.

Siga a sequência sugerida no plano de estudos e **faça os questionários apenas depois** de ter lido, assistido aos vídeos e feito os laboratórios em simulador. Assim você terá um aproveitamento muito melhor do curso.

2 Tópicos do Curso vs Blueprint do CCNA 200-310 – Peso 20%

Na tabela abaixo seguem os itens do blueprint ou conteúdo do exame Cisco CCNA 200-301 relacionados ao conteúdo do curso. Os capítulos que não aparecem explicitamente aqui fazem parte da matéria e complementam o aprendizado. Estude TODO o conteúdo do curso.

Network Fundamentals 1.0	
Fundamentos de Redes	Capítulos do Curso
1.1 Explain the role and function of network components	4 Dispositivos de Rede
1.1.a Routers	4.5 Roteadores (Routers)
1.1.b L2 and L3 switches	4.2 Switches Camada 2 (L2 ou Layer 2) 4.4 Switches Camada 3 (L3 ou Layer 3)
1.1.c Next-generation firewalls and IPS	4.7 IPS versus Next-Generation IPS (NGIPS)
1.1.d Access points	4.2 Switches Camada 2 (L2 ou Layer 2)
1.1.e Controllers (Cisco DNA Center and WLC)	4.8 Controllers (Controladoras)
1.1.f Endpoints	4.1 Endpoints - Computadores e Servidores
1.1.g Servers	
1.2 Describe characteristics of network topology architectures	5 Topologias de Rede
1.2.a 2 tier	5.3 Two Tier
1.2.b 3 tier	5. Three Tier
1.2.c Spine-leaf	5.6 Spine-Leaf
1.2.d WAN	5.5 WAN
1.2.e Small office/home office (SOHO)	5.2 Small Office/Home Office (SOHO)
1.2.f On-premises and cloud	5.7 On-premises e Cloud
1.3 Compare physical interface and cabling types	6 Conexões, Interfaces e Tipos de Cabeamento
1.3.a Single-mode fiber, multimode fiber, copper	6.1 Cabos Metálicos
1.3.b Connections (Ethernet shared media and point-to-point)	6.2 Fibras Ópticas
1.3.c Concepts of PoE	6.4 PoE – Power Over Ethernet
1.4 Identify interface and cable issues (collisions, errors, mismatch duplex, and/or speed)	6.5 Identificando os Principais Problemas em Interfaces e Cabeamento
1.5 Compare TCP to UDP	7 TCP versus UDP

1.6 Configure and verify IPv4 addressing and subnetting	8 Endereçamento IPv4, Sub-Redes e Configurações
1.7 Describe the need for private IPv4 addressing	8.5 Endereçamento IP e a Internet 8.6 Classes de Endereços IP
1.8 Configure and verify IPv6 addressing and prefix	9.4 Configurações e Verificações de Interfaces IPv6
1.9 Compare IPv6 address types	9.3 Tipos de Endereços IPv6
1.9.a Global unicast	9.3.4 Global Unicast Address ou GUA
1.9.b Unique local	9.3.3 Unique Local Address
1.9.c Link local	9.3.2 Link Local
1.9.d Anycast	9.1 Tipos de Comunicação e Endereços em IPv6
1.9.e Multicast	9.3.5 Multicast
1.9.f Modified EUI 64	9.3.1 IEEE EUI-64 ou Modified EUI 64
1.10 Verify IP parameters for Client OS (Windows, Mac OS, Linux)	10 Clientes de Rede: MAC OS, Linux e Windows
1.11 Describe wireless principles	6.6 Conexões Sem Fio – 802.11
1.11.a Nonoverlapping Wi-Fi channels	6.6.9 Non-Overlapping Channels
1.11.b SSID	6.6.5 Arquiteturas WLAN Infraestrutura
1.11.c RF	6.6.6 Técnicas de Modulação – Enviando um Bit via RF
1.11.d Encryption	6.6.7.2 Autenticação, Criptografia e Associação de Clientes
1.12 Explain virtualization fundamentals (virtual machines)	4.1.3 Virtualização de Servidores
1.13 Describe switching concepts	4.2.2 Principais Funções de um Switch L2
1.13.a MAC learning and aging	4.2.2.1 APRENDIZADO DE ENDEREÇOS MAC
1.13.b Frame switching	4.2.2.2 ENCAMINHAR OU FILTRAR QUADROS ENTRE PORTAS
1.13.c Frame flooding	4.2.3 Frame Flooding
1.13.d MAC address table	4.2.3 Tabela de Endereços MAC

3 Revisão de Modelo OSI e TCP/IP

Porque Modelo OSI se ele foi retirado dessa versão de CCNA?

Simples, agora o CCNA é realizado em apenas uma prova (exame 200-301), a qual foi projetada pensando em um profissional que já tem UM ANO de experiência com Redes e Dispositivos Cisco.

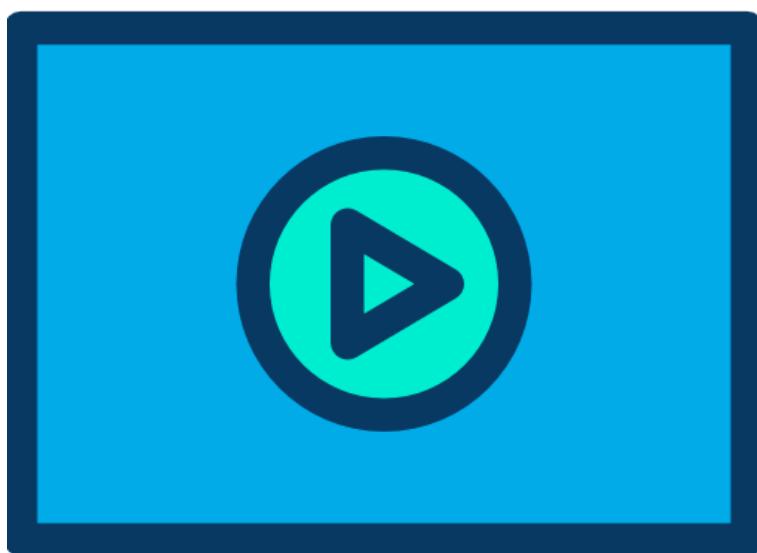
Apesar de retirado não quer dizer que você não vai precisar conhecer e saber relacionar as camadas!

O Modelo de Referência OSI é utilizado para dar o nome das regiões ou camadas que se comunicam entre os dispositivos de rede, além disso, é utilizado para classificar os dispositivos, por isso mesmo não entraremos a fundo, apenas vamos fazer uma breve revisão sobre o assunto.

Devido ao fato do Modelo OSI ser uma referência e o TCP/IP ser a pilha de protocolos realmente aplicada na prática das Redes de Computadores, sempre vai haver uma correlação e até mesmo sobreposição de nomenclatura que você deve saber.

Vamos começar revisando rapidamente o Modelo OSI.

3.1 Revisão do Modelo de Referência OSI



É de conhecimento geral que nos últimos vinte anos houve um grande aumento na quantidade e no tamanho das redes de computadores.

O problema é que esse crescimento não foi implementado de maneira ordenada pelos mais diversos fabricantes e fornecedores, ou seja, cada um implementava seu hardware e software da maneira que lhe fosse mais vantajoso.

O resultado é que essas redes de computadores eram incompatíveis umas com as outras. Isso trazia um enorme problema, tanto para os desenvolvedores de soluções quanto para os clientes (donos) dessas redes, que ficavam como que “reféns” de seus fornecedores.

Foi então que a ISO (a International Organization for Standardization) lançou em 1984 o modelo de referência OSI (Open Systems Interconnection).

Como o próprio nome diz, esse modelo serve de referência para que os desenvolvedores programem redes que podem se comunicar e trabalhar independente do fabricante. O grande segredo é **padronização e interoperabilidade**.

Já o TCP/IP é uma pilha de protocolos que realmente foi implementada na prática e utilizada até os dias de hoje, porém precisamos conhecer ambos os modelos, pois os equipamentos de rede são classificados conforme o modelo de referência OSI, apesar do TCP/IP estar funcionando na prática e o OSI não! Isso porque tudo se iniciou com o modelo OSI, portanto ele acabou sendo um modelo teórico para os desenvolvedores e estudiosos.

O modelo OSI divide as funções da rede em sete camadas (numeradas de 01 a 07). Veja as camadas e seus respectivos nomes na figura a seguir.



A camada mais próxima ao usuário final é a sete (7), chamada de camada de aplicação.

Já a camada um (1) ou física é a mais próxima do cabeamento ou da infraestrutura de redes.

Cada uma das camadas deve fornecer seus serviços exclusivamente à camada imediatamente superior, e consequentemente a função de cada camada depende dos serviços da camada imediatamente inferior.

Cada camada possui uma estrutura própria, chamada PDU (Protocol Data Unit).

3.1.1 Função das Camadas do Modelo OSI

Resumidamente a camada de aplicação (camada 7 ou layer 7) é a interface entre os programas e aplicativos e a Rede, ou seja, quando algum programa precisa acessar a rede ele faz através da camada de aplicação.

Por exemplo, quando um programa precisa acessar uma página da Web ele faria uma requisição ao serviço de HTTP ou HTTPS para a camada de aplicação.

Após essa etapa a camada de apresentação (camada 6 ou layer 6) e sessão (camada 5 ou layer 5) prepararão os dados para serem transmitidos de maneira correta. A camada de apresentação cuida da representação dos dados e a de sessão cuida do envio correto em cada sessão.

No TCP/IP essas três camadas viram apenas "Aplicação", veremos isso mais tarde.

A camada de transporte (camada 4 ou layer 4) prepara as informações recebidas da camada de sessão para serem enviadas na rede basicamente através de dois protocolos: TCP ou UDP.

Nessa camada os dados são identificados por números de porta, as quais marcam a quem pertence cada fluxo de informação dentro do computador, além de que aplicação deve tratar essa informação no destino.

Por exemplo, uma informação enviada para um servidor HTTP terá como porta de destino a porta 80 do protocolo TCP. (veremos mais sobre o funcionamento do TCP e UDP posteriormente).

Veja que até esse momento, todo o processo de sair da aplicação e chegar até a camada de transporte está dentro do computador, ainda não enviamos nada realmente na rede!

Agora que os fluxos estão identificados no computador, com a numeração de porta de origem e destino, eles devem ser realmente enviados na Rede.

Portanto a camada de transporte passa suas informações (chamadas de datagramas ou segmentos) para a camada de Rede (camada 3 ou layer 3).

A camada de rede tem a responsabilidade de endereçar globalmente os hosts de origem (o próprio computador) e destino (servidor remoto) com um endereço de camada-3.

Normalmente esse endereço é chamado de endereço IP (Internet Protocol), o qual pode ser conforme versão 4 ou 6 (IPv4 ou IPv6 respectivamente) nos dias atuais.

Dessa forma o servidor de destino poderá ser encontrado na rede e quando houver a resposta, a rede saberá para quem deve devolver as informações solicitadas ao servidor.

Além disso, a camada de Rede deve ser capaz de controlar o envio dessas informações e também saber como elas devem ser encaminhadas na rede através de protocolos de Roteamento. A informação enviada pela camada de Rede se chama pacote.

Quem receberá essas informações da camada de rede e vai preparar o envio no meio físico (seja cabo, wireless ou fibra) é a camada de Enlace (camada 2 ou layer 2).

A camada de enlace tem a responsabilidade de endereçar localmente os hosts, por exemplo, em redes ethernet através do endereço físico ou MAC (Media Access Control Address).

Além disso, a camada de enlace precisa "enquadrar" os dados em um formato mais simples para transmissão no meio físico, por isso mesmo a informação enviada entre camadas de enlace se chama "Quadro" ou "Frame".

Uma vez o pacote de camada de rede está enquadrado pela camada de enlace ele deve ser enviado através do meio físico utilizando uma interface elétrica, ótica ou sem fio.

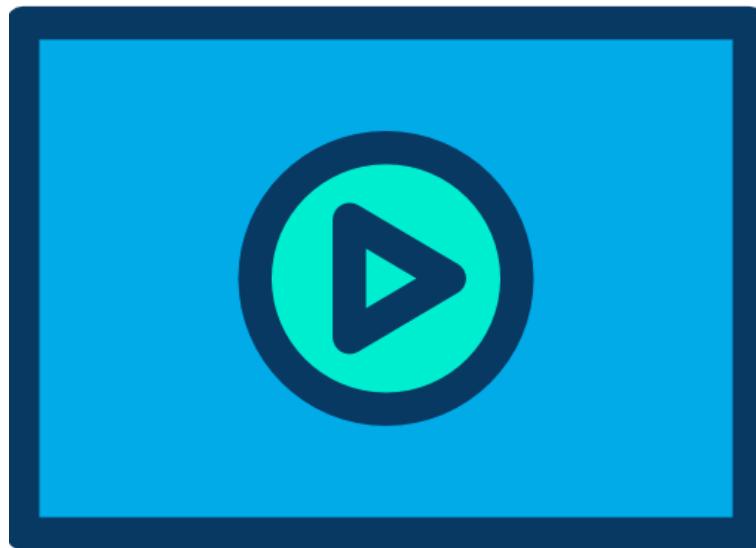
Esse envio das informações é realizado pela camada Física (camada 1 ou layer 1) através de bits e bytes.

Todo esse processo é chamado de encapsulamento de dados, que vamos estudar a seguir.

Quando o servidor ou computador remoto receber essas informações ocorrerá o desencapsulamento, para que a requisição chegue até o programa ou aplicativo de destino.

O processo de encapsulamento e desencapsulamento ocorre até o final da troca de informações entre os dois dispositivos.

3.2 Revisão do Protocolo TCP/IP

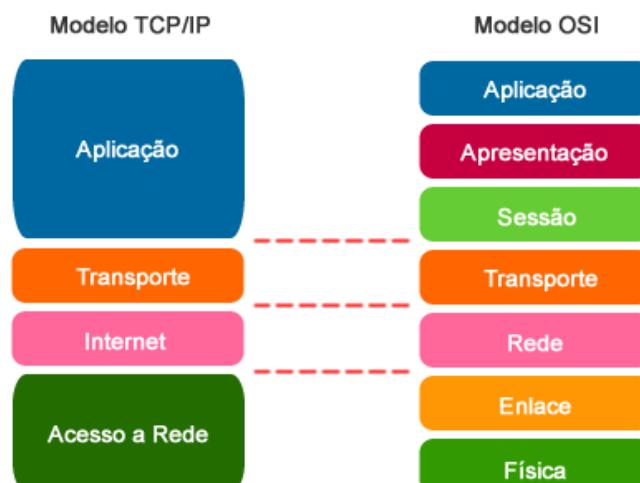


Apesar do modelo OSI ser a referência para as redes e toda sua nomenclatura, a arquitetura **TCP/IP é a que foi realmente implementada** e está em uso até os dias de hoje tanto nas redes internas (Intranets ou Redes Corporativas) como na Internet.

A arquitetura TCP/IP é composta por apenas 4 camadas (formando a pilha da estrutura do protocolo), sendo que na prática, as camadas 5, 6, e 7 do modelo OSI foram mescladas para formar a camada de **Aplicação** do TCP/IP.

Já as camadas 3 e 4 do modelo OSI são similares às camadas 2 e 3 do TCP/IP, inclusive a camada de transporte do TCP/IP tem o mesmo nome, porém a camada 3 do modelo OSI (rede) no TCP/IP é chamada de **Internet**.

Por fim, as camadas 1 e 2 do modelo OSI foram mescladas no TCP/IP para formar a camada de **acesso aos meios** ou **acesso à rede**. Veja a figura a seguir.



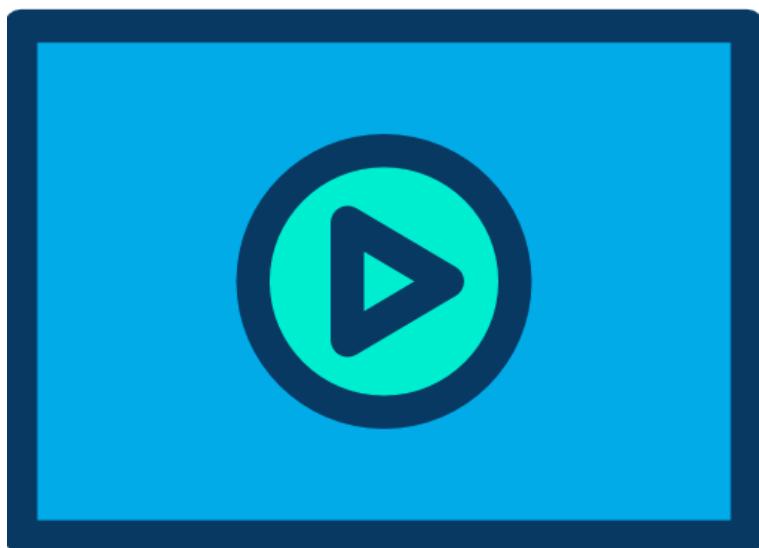
No TCP/IP não costumamos nos referir por camadas e sim pelos nomes delas, pois quando nos referimos pelo número da camada estamos falando do OSI.

Você pode encontrar bibliografias dividindo o TCP/IP em cinco camadas, tratando a camada de Acesso a Rede ou Acesso aos meios físicos como: Enlace ou Data Link e Física.

Essa divisão em 5 camadas ao invés de 4 camadas é puramente didática, pois a RFC 1122 não prevê o protocolo TCP/IP em 5 camadas.

Vamos estudar as camadas do TCP/IP e suas principais características.

3.2.1 Camada de Aplicação

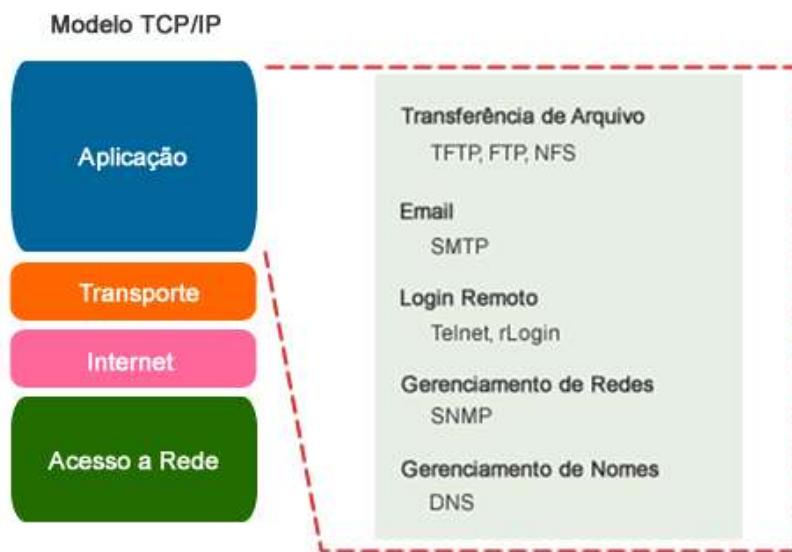


Assim como no Modelo OSI, a camada de Aplicação é a camada superior do modelo TCP/IP.

Ela é responsável por fornecer a interface entre as aplicações que utilizamos para comunicação e a rede subjacente pela qual nossas mensagens são transmitidas.

Os protocolos da camada de aplicação são utilizados para troca de dados entre programas executados nos hosts de origem e de destino.

Existem diversos protocolos da camada de Aplicação, e outros novos estão em constante desenvolvimento, veja alguns exemplos na figura a seguir.



A camada de aplicação do modelo TCP/IP trata de protocolos de alto nível, questões de representação, codificação e controle de diálogos, ou seja, o que as camadas 5, 6 e 7 do modelo OSI fazem separadamente a aplicação do TCP/IP trata como um pacote só, fazendo interface direta com a camada de transporte.

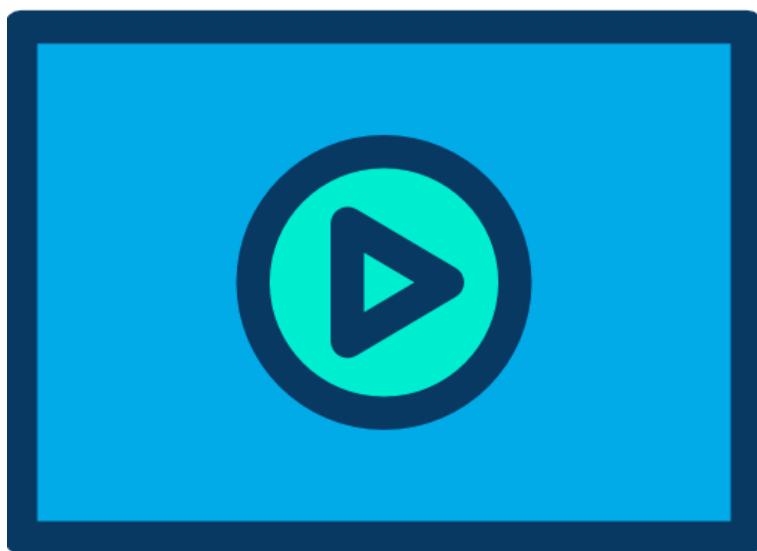
Abaixo temos mais de detalhes sobre alguns dos principais protocolos da camada de aplicação:

- **DNS (Domain Name System – Sistema de Nomes de Domínio)** – O DNS é um sistema usado na Internet para converter os nomes de domínios e seus respectivos nós de rede divulgados publicamente em endereços IP.
- **DHCP (Dynamic Host Configuration Protocol)** – Utilizado para fornecer dados de configuração das interfaces dinamicamente aos computadores e demais endpoints da rede. Os dados fornecidos são no mínimo endereço IP, máscara de rede, endereço do roteador padrão e servidor DNS. Sem ele os administradores de rede teriam um imenso trabalho braçal.
- **WWW ou HTTP (Hypertext Transfer Protocol)** – Serviço básico utilizado pelos navegadores de Internet ou browsers para acessar o conteúdo das páginas web. Sua versão segura (com criptografia) é o HTTPS.
- **FTP (File Transfer Protocol – Protocolo de Transferência de Arquivos)** – é um serviço confiável, orientado a conexões, que usa o TCP para transferir arquivos. Suporta transferências bidirecionais de arquivos binários e ASCII.
- **TFTP (Trivial File Transfer Protocol – Protocolo de Transferência de Arquivos Simples)** – serviço sem conexão que usa o UDP (User Datagram Protocol – Protocolo de Datagrama de Usuário). É usado no roteador para transferir arquivos de configuração e imagens IOS da Cisco e para transferir arquivos entre sistemas que suportam TFTP. É útil em algumas redes locais porque opera mais rápido do que o FTP em um ambiente instável.
- **SMTP (Simple Mail Transfer Protocol – Protocolo Simples de Transferência de Correio)** – Administra a transmissão de correio eletrônico através de redes de computadores. Ele não oferece suporte à transmissão de dados que não estejam em texto simples.

- **POP3 e IMAP** – São os protocolos utilizados pelos clientes para a leitura do e-mail. A diferença entre eles é que o POP3 baixa os arquivos para o micro do usuário apagando no servidor, já o IMAP é possível deixar uma cópia dos e-mails, utilizando como um espelho sem apagar as mensagens, assim o usuário pode ler seus e-mails antigos independente do micro que está utilizando.
- **Telnet (Terminal emulation – Emulação de terminal)** – Permite o acesso remoto a outro computador. Permite que um usuário efetue logon em um host da Internet e execute comandos, porém os dados são transmitidos em texto claro, podendo ser capturado e lido por um invasor no meio do caminho. Existe também uma versão segura chamada Secure Shell ou SSH, o qual possibilita a transferência de informações criptografadas pela rede.
- **NFS (Network File System – Sistema de Arquivos de Rede)** – Conjunto de protocolos de sistema de arquivos distribuído, desenvolvido pela Sun Microsystems, que permite acesso a arquivos de um dispositivo de armazenamento remoto, como um disco rígido, através da rede.
- **SNMP (Simple Network Management Protocol – Protocolo Simples de Gerenciamento de Rede)** – Oferece uma forma de monitorar e controlar dispositivos de rede e de gerenciar configurações, coleta de dados estatísticos, desempenho e segurança.

Normalmente esses protocolos são chamados também de “**Serviços de Rede**” e terão um curso específico mais aprofundado sobre os principais serviços dentro da trilha do CCNA 200-301.

3.2.2 Camada de Transporte: TCP vs UDP



A função da camada de Transporte é proporcionar a identificação dos serviços de rede, segmentação de dados e o controle necessário para reagrupar esses segmentos em fluxos de comunicação. Veja a figura abaixo.



Para tal a camada de transporte deve ser capaz de fazer as seguintes tarefas:

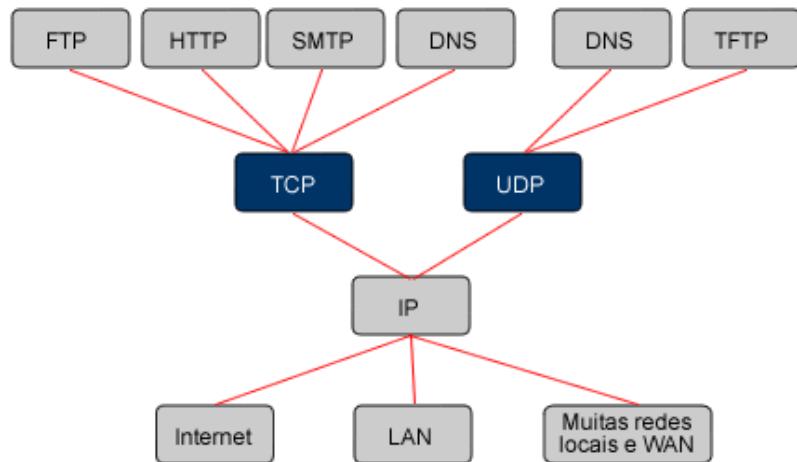
- Rastreamento de Conversações Individuais
- Segmentação de Dados
- Reagrupamento de Segmentos
- Identificação das Aplicações (número de porta TCP ou UDP)

No TCP/IP a camada de transporte pode oferecer dois caminhos ou serviços, confiável através do protocolo TCP e não confiável através do protocolo UDP.

Mas note que na teoria geral essa camada se refere às características gerais do protocolo TCP normalmente.

Ambos os protocolos gerenciam a comunicação de múltiplas aplicações que desejam acessar a rede simultaneamente.

Veja a figura a seguir para entender melhor o posicionamento da camada de transporte dentro da pilha de protocolos TCP/IP.



Perceba que as aplicações normalmente usam um ou outro protocolo como serviço de transporte ponto a ponto.

O TCP é um protocolo orientado à conexão, descrito na RFC 793. O TCP causa sobrecarga adicional na rede, pois possui funções adicionais - entrega ordenada, entrega confiável e controle de fluxo.

Cada segmento TCP tem 20 bytes de overhead no cabeçalho que encapsula o dado da camada de Aplicação, enquanto o segmento UDP tem apenas 8 bytes.

Algumas das aplicações que usam TCP são:

- Navegadores web (HTTP e HTTPS)
- E-mail (SMTP, POP e IMAP)
- FTP
- DNS – consulta entre servidores

O UDP é um protocolo simples e sem conexão, descrito na RFC 768.

Ele tem a vantagem de fornecer uma entrega de dados com baixa sobrecarga e maior velocidade, pois ele não possui os mecanismos de controle do TCP.

Sua desvantagem é que não é confiável, por isso a camada de aplicação deve tratar dessas características.

Os segmentos de comunicação em UDP são chamados datagramas.

Estes datagramas são enviados como o "**melhor esforço**" por este protocolo da camada de Transporte, ou seja, o UDP envia e não espera por confirmação nem tampouco controla fluxo.

As aplicações que usam UDP incluem:

- DNS – consulta de cliente a servidor
- Voz Sobre IP (RTP – Real time protocol)
- TFTP
- SNMP

Lembre-se, o que define o TCP é confiabilidade e o que define o UDP é velocidade!

São características comuns ao TCP e UDP:

- Segmentação de dados das aplicações das camadas superiores.
- Envio de segmentos de um dispositivo em uma ponta para um dispositivo em outra ponta.
- Multiplexação de informações da camada de aplicação (transporte de vários fluxos simultaneamente).
- Identificação das aplicações e conexões de cliente utilizando números de porta.

São características exclusivas do TCP:

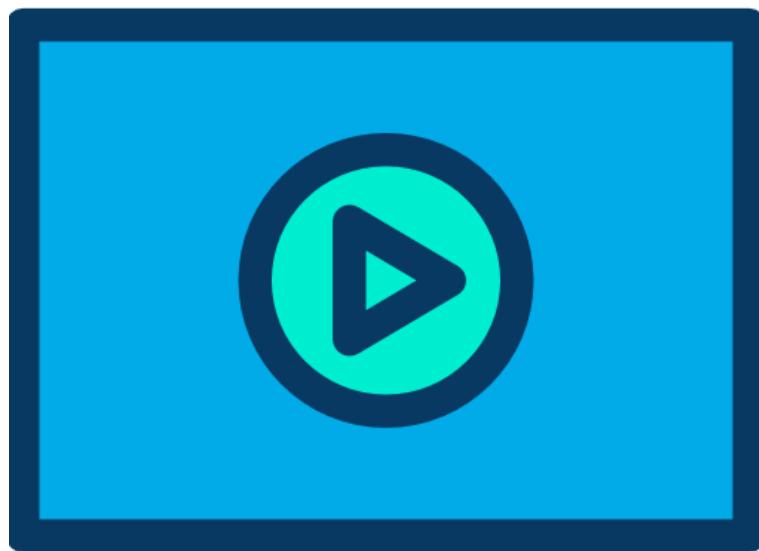
- Estabelecimento de operações ponta a ponta (hand-shake de três vias).
- Controle de fluxo proporcionado pelas janelas móveis (janelamento).
- Confiabilidade proporcionada por números de sequência e confirmações de entrega dos segmentos.
- Retransmissão de segmentos perdidos.

Podemos fazer aqui uma comparação da aplicação sendo um veículo que tem duas estradas para escolher, uma das estradas é segura e com certeza você vai chegar ao seu destino, porém ela tem tantos pontos de checagem, pedágios e outros mecanismos de controle de tráfego que acaba sendo mais lenta, esse é o TCP.

Por outro lado, temos uma pista sem controle de tráfego nenhum e por isso ela é muito mais rápida, porém para trafegar nessa pista seu carro vai precisar que você tenha um mapa preciso, GPS e muita atenção do motorista (a aplicação), pois ela não tem indicações. Esse é o UDP.

Por isso o UDP é utilizado, por exemplo, para o tráfego de Voz sobre a rede IP e implementações de VPN (redes virtuais privadas), pois a voz e o acesso VPN precisam de velocidade. Já aplicações como HTTP para leitura de páginas não precisam dessa urgência, por isso utilizam o TCP como meio de transporte.

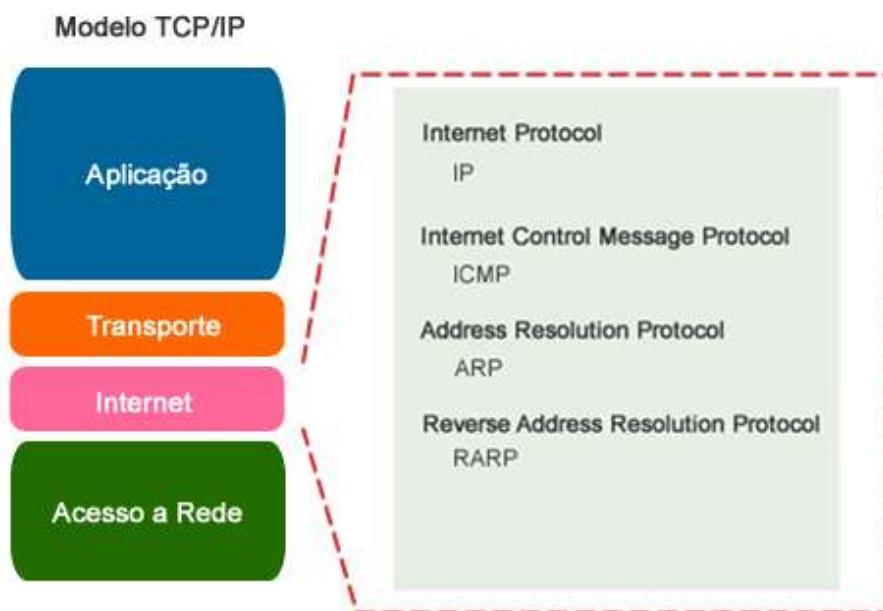
3.2.3 Camada de Internet



A finalidade da Camada de Internet é a mesma que a camada de rede do modelo OSI, ou seja, fornecer esquema de endereçamento e escolher o melhor caminho para os pacotes viajarem através da rede.

A determinação do melhor caminho e a comutação de pacotes também ocorre nesta camada.

Veja os principais protocolos da camada de Internet na figura a seguir.



Abaixo seguem as principais funções de cada um dos protocolos:

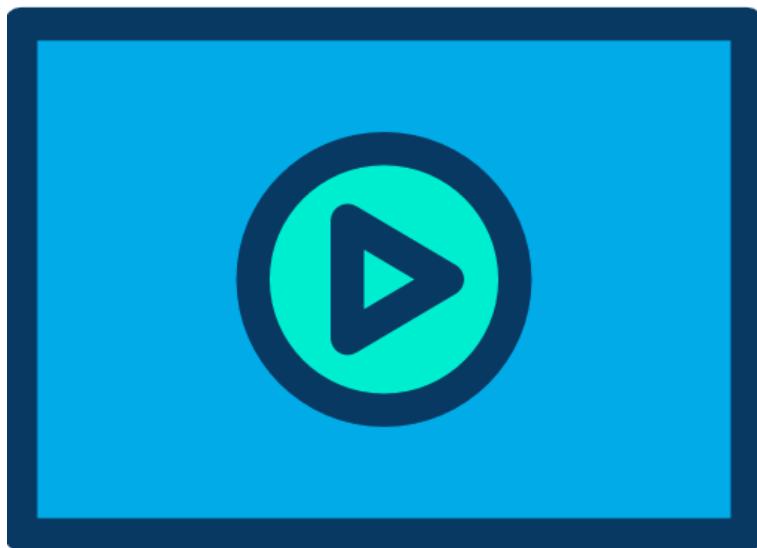
- O **IP** oferece roteamento de pacotes sem conexão, e uma entrega de melhor esforço. Ele não se preocupa com o conteúdo dos pacotes, apenas procura um caminho até o destino.
- O **ICMP** (Internet Control Message Protocol – Protocolo de Mensagens de Controle da Internet) oferece recursos de controle e de mensagens, tais como ping.
- O **ARP** (Address Resolution Protocol – Protocolo de Resolução de Endereços) determina o endereço da camada de enlace (endereço MAC) para os endereços IP conhecidos.
- O **RARP** (Reverse Address Resolution Protocol – Protocolo de Resolução Reversa de Endereços) determina os endereços IP quando o endereço MAC é conhecido.
- **Protocolos de roteamento** são responsáveis por ler o endereçamento IP configurado e trocar informações de rota para definir o melhor caminho entre as diversas redes da Internetwork.

O protocolo IP atualmente possui duas versões: **IPv4 (32 bits)** e **IPv6 (128 bits)**, ou seja, a IP versão 4 e IP versão 6.

Atualmente a maioria das redes utiliza o IPv4, porém a implementação do IPv6 vem crescendo vertiginosamente a partir do lançamento global realizado em 2012.

Ambas as versões do protocolo IP são “**best effort**”, ou seja, enviam suas informações na rede como o UDP estudado anteriormente, sem pedir confirmações.

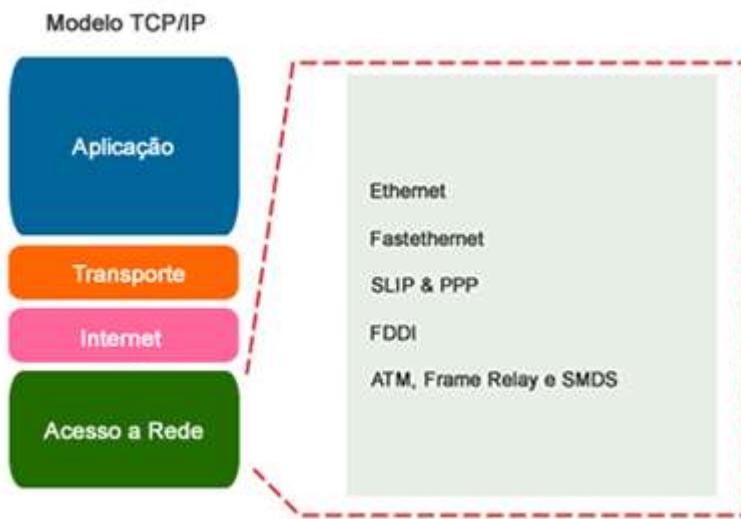
3.2.4 Camada de Acesso aos Meios (Data Link e Camada Física)



O objetivo da camada de acesso à rede (algumas fontes bibliográficas também chamam de acesso aos meios) é que o pacote IP estabeleça efetivamente um link físico com os meios físicos disponíveis da rede de maneira transparente, ou seja, não importando o meio de transmissão que esteja sendo utilizado.

Aqui **algumas bibliografias podem dividir de forma didática** a camada de acesso aos meios em duas camadas, assim como o modelo OSI: Enlace e Física, o que tornaria o TCP/IP com cinco camadas.

Essa camada inclui detalhes de tecnologia de redes locais e de WANs e todos os detalhes contidos na camada física e de enlace de dados do modelo OSI e suas funções incluem o mapeamento de endereços IP para endereços físicos de hardware e o encapsulamento de pacotes IP em quadros. Veja a figura a seguir.



É importante lembrar que durante a transmissão de dados em uma rede IP os cabeçalhos da camada de acesso à rede ou camada de enlace do modelo OSI variam de acordo com a tecnologia adotada, porém o cabeçalho do IP nunca irá variar do início ao fim da comunicação.

Os quadros ou frames são montados e remontados a cada salto de rede diferente que o IP navega, mas o IP nunca é alterado.

Além disso, a camada de acesso aos meios define um endereço físico que pode variar de formato e tamanho conforme protocolo específico.

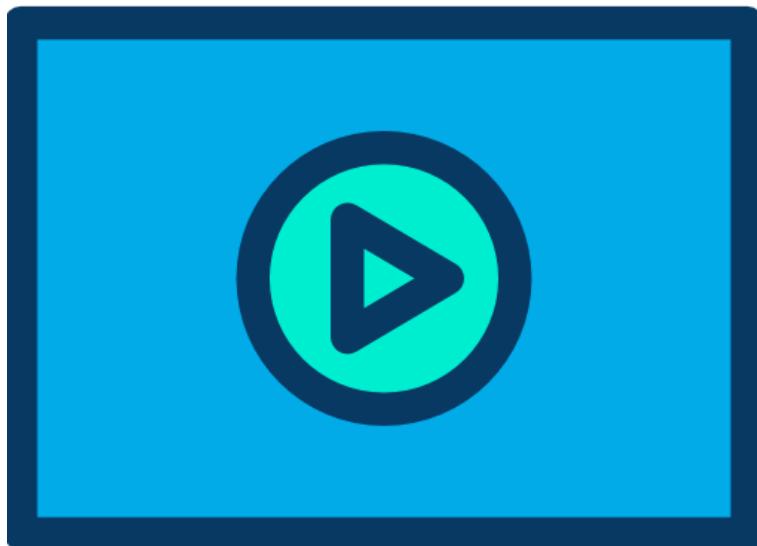
Já a parte física da camada de acesso aos meios define as especificações elétricas, mecânicas, funcionais e de procedimentos para ativar, manter e desativar o link físico entre sistemas finais.

Características como tipos de cabo (UTP ou fibra óptica), níveis de voltagem, distâncias máximas de transmissão, conectores físicos são definidos pelas especificações da camada física.

A camada física tem como função básica a adaptação do sinal ao meio de transmissão.

Nessa camada estão situados os Hubs, repetidores, transcievers, patch pannel, cabos e conectores.

Os padrões de nível físico utilizados são, por exemplo, X.21, X.21 bis, V.24, V.28, V.35, RS-232 I.430, I.431, G.703, etc...

3.2.4.1 ENDEREÇO MAC

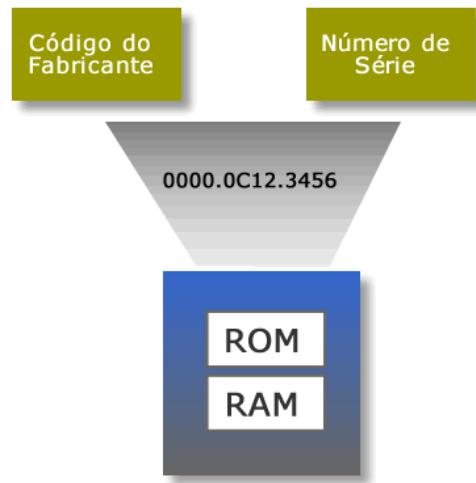
O mais importante dos endereços da camada de acesso aos meios e também da camada de enlace do Modelo OSI é o endereço MAC, por ser utilizado nas placas de rede de computadores e servidores.

O endereço MAC (Media Access Control) é o endereço físico da estação, ou melhor, da interface de rede.

É um endereço de 48 bits, representado em hexadecimal. Este endereço é o utilizado na camada 2 (Enlace) do Modelo OSI em redes Ethernet.

Os três primeiros octetos são destinados à identificação do fabricante, os 3 posteriores são números arbitrados pelo fabricante, ou seja, um serial.

É um endereço único, ou seja, não existem, em todo o mundo, duas placas com o mesmo endereço físico, pelo menos na teoria, pois na prática são relatados casos de placas de rede "clonadas" (piratas) com seriais iguais, porém isso é uma história para quando começarmos a praticar em switches.



O endereço MAC pode ser escrito de outras formas dependendo do sistema operacional do endpoint, por exemplo, em máquinas Windows ele seria escrito da seguinte maneira:

- 00-00-0C-12-34-56

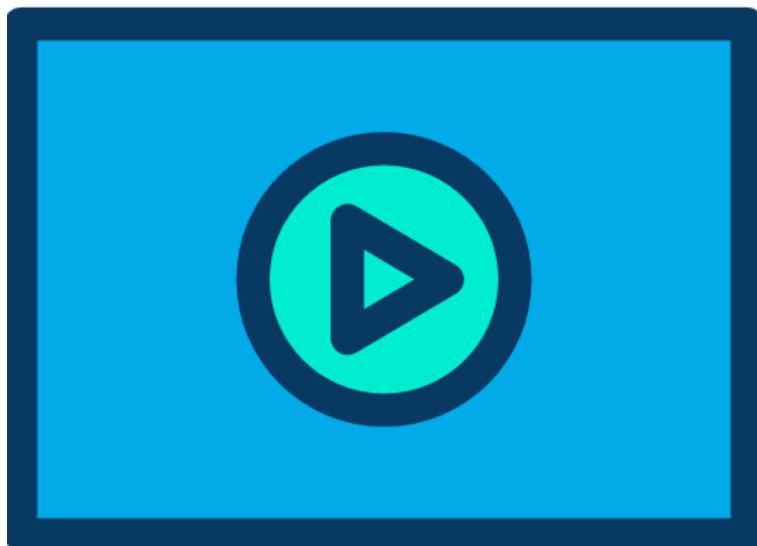
Em um computador com Linux o mesmo endereço seria visualizado como 00:00:0C:12:34:56, portanto o importante é que são 12 algarismos em Hexa, totalizando 48 bits, pois cada algarismo em Hexa possui 4 bits.

Em dispositivos Cisco ele normalmente é escrito em três conjuntos de 4 algarismos Hexadecimais, por exemplo, "afc0.dd1a.bbac".

Abaixo segue um resumo das características de um endereço MAC:

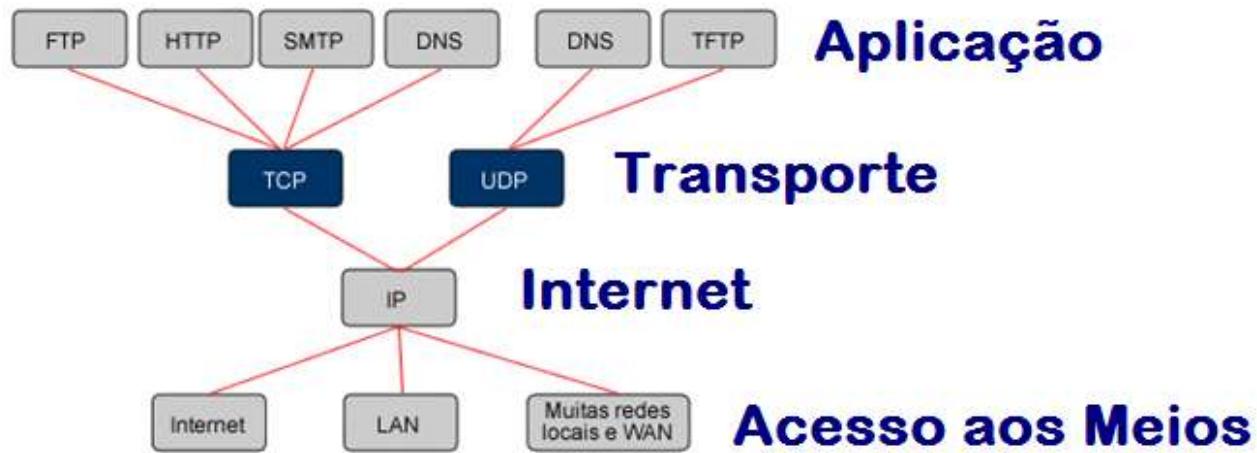
- Endereço da camada 2
- Gravado no chip da ROM em uma placa de rede Ethernet
- Número exclusivo de 48 bits que está gravado como doze números hexadecimais.
- Os primeiros 24 bits representam o fornecedor ou o fabricante (OUI)
- Os últimos 24 bits do fornecedor formam o número de série

3.2.5 Encapsulamento de Dados no TCP/IP



Portanto no TCP/IP o processo de encapsulamento é um pouco diferente, mais simples, pois a camada de Aplicação envia seus dados para a camada de Transporte.

A camada de transporte envia seus segmentos ou datagramas para a camada de Internet (não é mais Rede do TCP/IP), a qual envia seus pacotes para a camada de acesso aos meios para que as informações (bits) sejam enviadas no meio físico.



Com o TCP/IP em cinco camadas a Internet envia seus pacotes para a camada de Data Link, a qual envia seus quadros ou frames para a camada física.

Tenha sempre em mente essa nomenclatura das informações trocadas entre as camadas, tanto do modelo OSI como TCP/IP, isso é importante para a prova e para sua vida prática!

4 Dispositivos de Rede

A função de uma rede é conectar dispositivos locais ou remotos através de diversos protocolos, tais como o IPv4 ou IPv6.

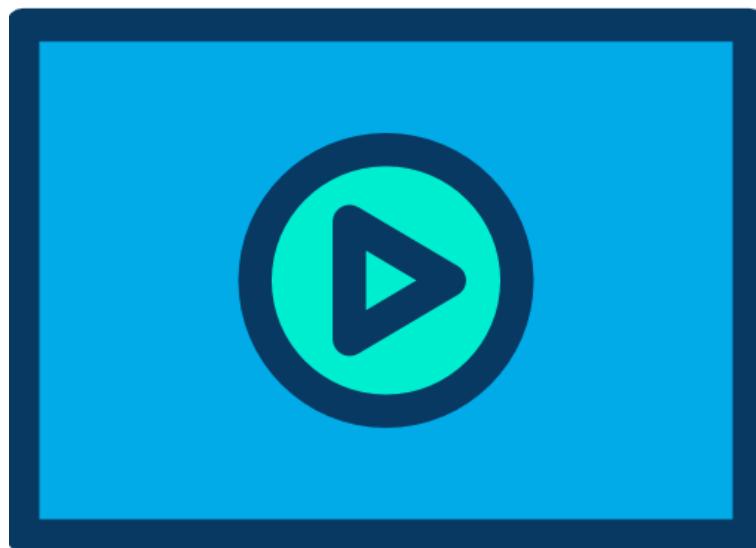
E para que isso ocorra é preciso que os quadros, pacotes e dados trafeguem por uma "Infraestrutura de Redes", a qual é composta por diversos "Dispositivos de Rede".

Dentro do escopo do CCNA 200-301 vamos estudar os seguintes dispositivos nesse capítulo:

- Endpoints (Computadores e demais dispositivos dos clientes)
- Switches Camada 2 (L2 ou Layer 2)
- Access Points
- Controladoras Wireless (Wireless LAN Controllers)
- Switches Camada 3 (L3 ou Layer 3)
- Roteadores (Routers)
- Next-Generation Firewalls (NGFW)
- IPS (Intrusion Prevention System)
- Cisco DNA Center (Automação, SDN e SD-Access - Enterprise)
- ACI (Application Centric Infrastructure - Datacenter)
- Servidores (Físicos e virtualizados)

Apenas o ACI na realidade não faz parte do tópico 1.0 do atual Blueprint do CCNA, o qual é foco desse curso, porém vamos fazer uma breve introdução para que você tenha uma visão completa dos dispositivos de Rede que serão estudados durante o CCNA.

4.1 Endpoints - Computadores e Servidores



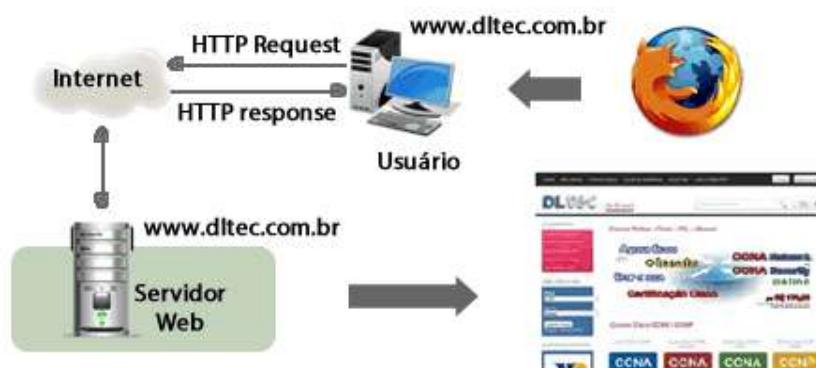
As redes de computadores têm como dispositivos finais os **hosts**, o qual é um termo genérico assim como **endpoint** (dispositivo final em inglês).

Podemos também chamá-los de clientes de rede, dispositivos que permitem aos usuários acessarem aos serviços de rede.

Como já estudamos, as redes TCP/IP utilizam uma arquitetura cliente/servidor, ou seja, temos dispositivos clientes (que desejam utilizar serviços de rede) e servidores, os quais prestam os serviços de rede.

Um exemplo que utilizamos todos os dias é o serviço de Web (WWW), em nossos micros temos programas chamados **browsers** (como o IE, Mozilla, Google Chrome, dentre outros) e digitamos um nome de site para acessar as informações na tela do nosso computador.

Essa informação está contida em um servidor web, máquina com um determinado serviço de rede instalado, nesse caso o HTTP, que provê o conteúdo da página solicitada.



Vamos estudar a seguir os principais endpoints que encontramos nas redes.

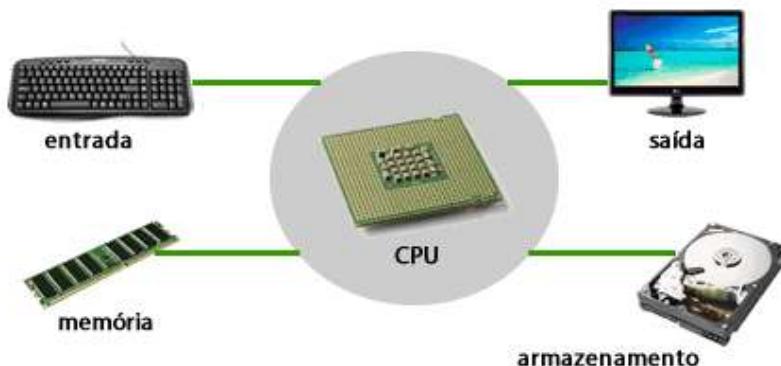
4.1.1 Computadores

Equipamentos utilizados para o processamento de dados que, na visão de rede, podem ser classificados como **estações de trabalho** (clientes ou desktops) e **servidores**, os quais estudaremos em um tópico a parte.

Mas nesse caso vamos falar mais especificamente sobre os computadores, desktops, laptops e notebooks, os micros ou PCs (Personal Computer) utilizados em casa ou nas empresas para as tarefas diárias envolvendo acesso a programas, aplicativos e à Internet e seus mais variados serviços.

Um computador é basicamente composto por **Hardware**, **Software** e **Firmware**.

O Hardware de um computador é formado pelos seguintes componentes básicos:



- **Unidade de Processamento:** Composto pelo Processador ou UCP (Unidade Central de Processamento ou CPU – Central Processing Unit - em inglês). A CPU tem papel parecido ao **cérebro** no computador.
- **Unidades de Armazenamento:** Compostas pelas memórias (RAM, ROM, etc.), unidades de disco (Unidades de Disco Rígido ou HD – Hard Disk, também conhecido como Winchester, Unidades de Disco Flexível ou Floppy Disk, Unidades de CD – Compact Disk, Unidades de DVD, etc.).
- **Dispositivos de Entrada e Saída:** Monitor, Teclado, Impressora, Mouse, Plotter, etc.
- **Interface de Rede:** Atualmente podemos ter placas de redes para cabeamento físico ou placas de rede sem fio (wireless). A interface de rede pode ser onboard, ou seja, está integrada na placa mãe ou em uma placa externa USB, PCI ou PCMCIA.

Sobre o **Software** temos basicamente o **Sistema Operacional** e os **Aplicativos**.

O **Sistema Operacional** (OS – Operational System) é um software que permite a utilização da máquina como um todo por outros programas, ativando-a e gerenciando a memória e os dispositivos de entrada e saída, por exemplo. Além disso, ele define o ambiente de trabalho do usuário no computador. É na realidade um conjunto de programas (rotinas) executado pelo processador que estabelece uma interface de contato do usuário com o computador e do computador com o usuário. Exemplos de sistemas operacionais utilizados em computadores de clientes são as diversas distribuições de Linux, Windows e MacOS.

Já o **Firmware** é o programa instalado na memória de inicialização do computador, contendo as instruções básicas para inicialização do computador (BIOS – Basic Input/Output System).

4.1.2 Servidores

Os servidores não são nada mais que computadores normalmente mais “poderosos” que os utilizados em nossas casas, tanto é que você pode instalar aplicações específicas ou ativar recursos do seu sistema operacional e transformar seu computador em um servidor também!

Então por que tratar dos servidores separadamente dos computadores?

Porque dependendo do porte da empresa ou do perfil da aplicação a ser utilizada, um computador normal não aguentaria a exigência de processamento e de memória RAM que esse serviço de rede precisaria para operar.

Por exemplo, imagine você pegar um computador comum e colocar na Internet hospedando um site famoso como o Google.

Com certeza serão milhares e até milhões de acessos simultâneos que esse site irá receber diariamente e ele, um computador, comum não aguentaria essa carga de solicitações, pois ele não foi projetado para esse fim.

Na realidade um serviço desse porte normalmente está espalhado por diversos servidores **virtualizados** em máquinas que compartilham recursos em rede para melhorar a performance do serviço como um todo.

Falando genericamente, um servidor terá um sistema operacional mais poderoso ou preparado para tal finalidade, por exemplo, no caso do Windows existe uma versão para servidor, o **Windows Server**.

Já para o Linux existem distribuições que são mais utilizadas em servidores de rede, por exemplo, o **Red Hat** e o **Debian**.

Portanto, apesar da estrutura básica de um computador e um servidor serem as mesmas, o que difere é a **capacidade**.

Normalmente o servidor terá um ou mais processadores mais poderosos, uma quantidade de memória RAM maior, capacidade de armazenamento maior ou até utilizar o armazenamento externo através de uma rede SAN utilizando Storages.

Além disso, também terá um sistema operacional mais adequado e serviços de rede ou aplicações corporativas instaladas, como por exemplo, serviço de e-mail, web, FTP, sistema de arquivos (file system), serviços corporativos como os ERPs, Bancos de Dados e CRMs, podendo estes serviços estarem em um mesmo servidor ou espalhados em diversos servidores. Essa escolha de **agregar** ou **consolidar** os serviços em apenas um servidor depende do volume de processamento exigido pelas aplicações ou pelo volume de solicitações aos serviços que os clientes irão realizar.

Em termos físicos, os servidores podem ser gabinetes como os que estamos acostumados com os desktops (chamados de **torre**), de rack ou então em blades (se pronuncia "bleide").

As soluções em torre têm problemas de espaço limitado e precisam de processamento centralizado. Este modelo é recomendado para empresas pequenas que necessitam de apenas um servidor.



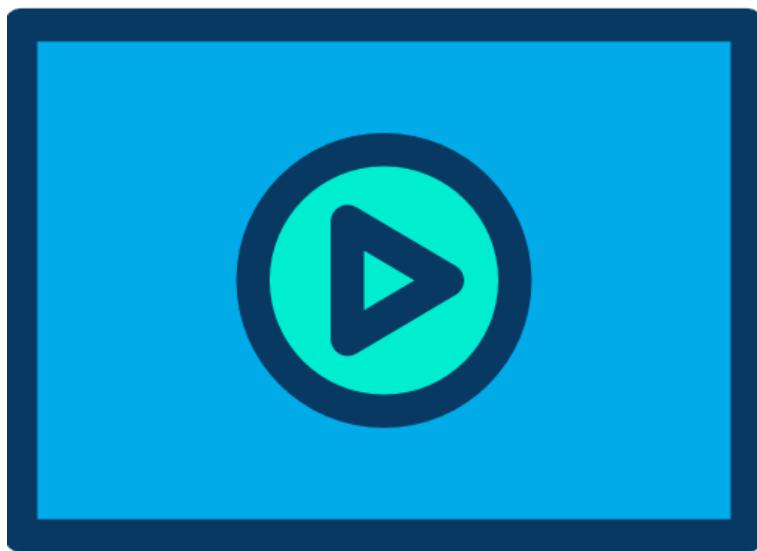
Já os servidores em rack já são recomendados para empresas que necessitam de mais de um servidor e tem problemas de espaço ou então precisam de maior capacidade de armazenamento interno.

Os servidores blade são recomendados para empresas que necessitam de uma capacidade de computação bastante elevada ou para empresas que planejam desenvolver um data center próprio.

Com esse tipo de servidor há ganho de espaço, processamento e consumo de energia, porém o custo é bem mais elevado. Acompanhe na figura abaixo que cada espaço do sub-bastidor você tem uma lâmina ou blade que é na realidade um servidor.



4.1.3 Virtualização de Servidores



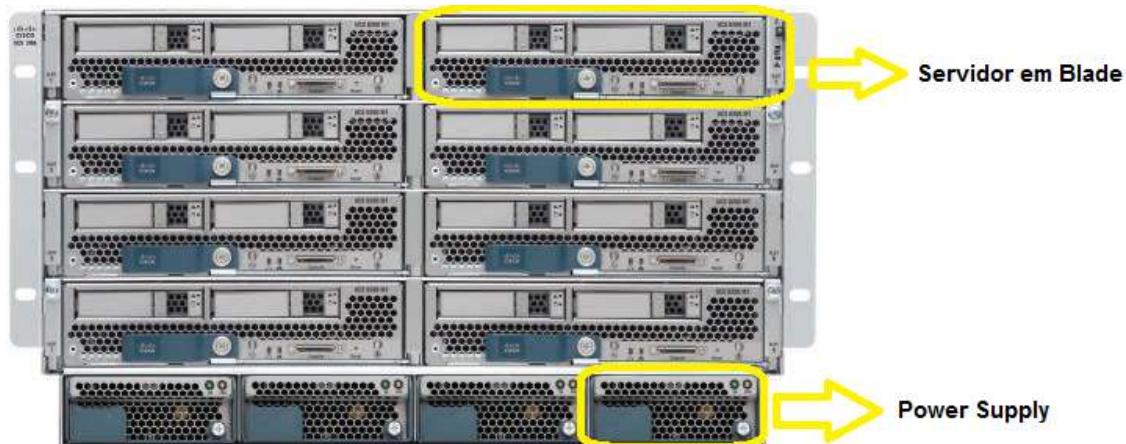
Quando você ouve a palavra servidor o que vem em sua mente?

Provavelmente é um desktop (normalmente uma torre) com muita CPU, memória RAM e HD? Ou um servidor de rack já preparado para inserir na sala de servidores ou no Data Center da sua empresa?

Ou nem isso, você já pensa em uma máquina virtual (VM – Virtual Machine) com um determinado sistema operacional rodando nela?

Além disso, muita gente pensa na Cisco apenas como uma empresa fabricante de dispositivos de rede, como roteadores e switches, porém mais ou menos em 2010 eles decidiram expandir a linha de produtos e entraram no mercado de servidores com a linha Cisco Unified Computing System ou simplesmente UCS.

Abaixo segue a foto de um UCS série B (B-Series - Blade series), o qual utiliza um chassi para montagem em rack e servidores em blade, ou seja, ao invés de desktops são como placas que encaixam no chassi.

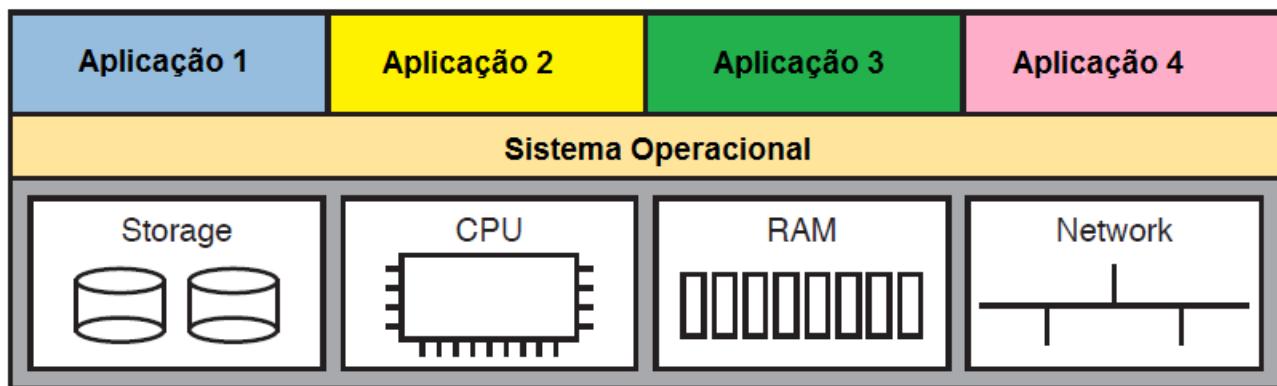


Nesse exemplo temos um modelo que suporta até 8 servidores em blade (4 em cada lado) montados horizontalmente. Além disso, embaixo ele possui quatro fontes de alimentação (power supplies).

Como você pode notar esses servidores não tem teclado, monitor e mouse (KVM - keyboard, vídeo display, mouse), pois os administradores de redes ou de aplicações acessam esses servidores remotamente através da rede.

Outro detalhe é o espaço que esses servidores ocupam, cada vez mais as empresas e provedores de serviços visam dispositivos que economizem espaço físico e energia, que sejam mais eficientes tanto na parte de tecnologia da informação como ambiental.

Durante o curso, como o foco é rede, representamos os servidores como um ícone, sem analisar sua parte interna, mas abaixo segue uma representação simples de um servidor com seus principais componentes.



Nessa representação simplificada temos o hardware (armazenamento ou storage, CPU, memória RAM e interface de rede – network), controlado por um sistema operacional como Windows Server, Linux ou Unix que por sua vez possibilitam que as aplicações rodem para fornecer serviços aos clientes, tais como páginas de Web (HTTP), serviços de arquivo como FTP, bancos de dados, sistemas de controle corporativo como ERP (Enterprise Resource Planning) e demais aplicações necessárias na empresa.

Em uma arquitetura tradicional cada aplicativo ou App (abreviação de Application) seria instalado em um servidor próprio isolado dos demais, no máximo alguns serviços como de armazenamento de arquivos e páginas de Web compartilhavam o mesmo servidor.

Mas onde entra a virtualização se estamos apenas analisando aspectos de servidores físicos até o momento? Acho que você deve estar pensando nisso nesse momento... Acertei?

Vamos estudar a seguir...

4.1.3.1 MÁQUINAS VIRTUAIS OU VMs (VIRTUAL MACHINES)

Bom, você sabe quanto em média um servidor físico com aplicações instaladas de maneira tradicional é utilizado em média (pensando em processamento/CPU e memória)?

Pesquisas apontam que entre 5% a 7%, ou seja, temos mais de 90% de tempo onde o computador está livre ou pelo menos sem nenhuma sobrecarga.

Se você fizer uma conta bem por alto, somente levando em conta essa média, podemos dizer que um servidor poderia ser quebrado em no mínimo 10 (considerando que ele tem 10% de ocupação média).

Levando em conta esse número com aquele modelo de servidores em Blade da Cisco que permitem 8 servidores em um chassi teríamos a capacidade de rodar 80 servidores virtuais.

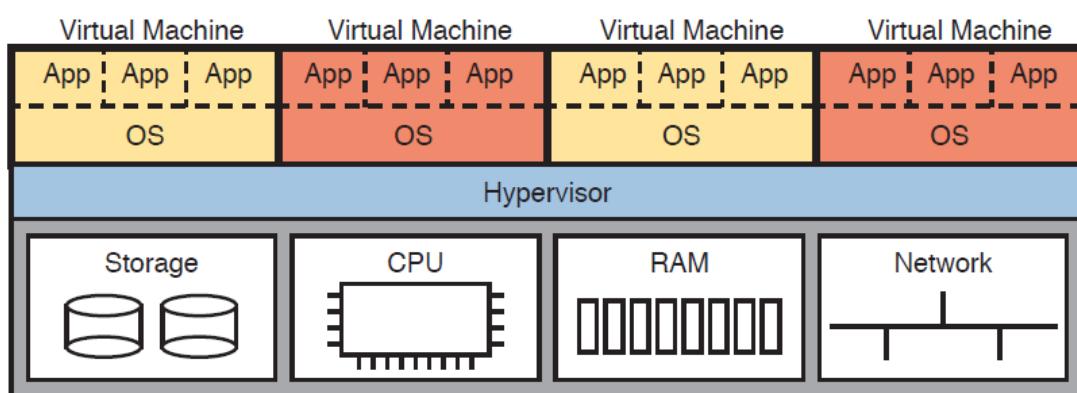
Claro que esse valor passado acima é uma estimativa, porém na prática o número de servidores que podem ser virtualizados precisa de uma quantificação que cada fabricante faz conforme suas especificações.

Uma máquina virtual ou VM (Virtual Machine) é então uma instância de sistema operacional que roda em um hardware virtual, está desacoplada do hardware físico, mas mesmo assim precisa ainda ser executada em um hardware físico.

Cada sistema operacional tem requisitos que a VM deve obedecer em sua configuração, por exemplo, deve ter um mínimo de vCPUs (CPUs virtuais), memória RAM, disco rígido (HD ou Storage) e assim por diante.

O sistema de virtualização começa em um sistema físico que tem certas capacidades de hardware, portanto essas capacidades é que serão divididas entre as máquinas virtuais para criação dessas instâncias de sistema operacional que serão as VMs rodando no servidor físico.

Então cada VM que está rodando em um servidor físico e utilizando um pedaço da sua CPU, RAM, armazenamento e placa de rede (NIC – Network Interface Card), veja o conceito na figura a seguir.



4.1.3.2 HYPERVISORS

O que você nota de diferente entre essa figura e a mostrada no tópico anterior quando comparamos com um servidor físico? Suba um pouco e compare as imagens... O que tem de diferença?

Se você respondeu “**Hypervisor**” acertou!

O hypervisor tem a função de alocar e gerenciar os recursos de hardware do servidor (CPU, RAM, etc.) para cada VM de acordo com as configurações realizadas para cada uma delas. Portanto ele está fazendo o “meio de campo” entre os sistemas operacionais das máquinas virtuais e o hardware físico.

Por exemplo, a primeira VM desse servidor está configurada com 4 CPUs e 8 GB of RAM, quem garante isso para essa máquina virtual é o hypervisor, o qual aloca corretamente as partes de CPU e memória RAM que essa VM vai realmente utilizar.

Na prática existem vários produtos que fazem o que discutimos até agora, sendo que os mais conhecidos para uso em Data Centers são VMware vCenter, Microsoft HyperV, Citrix XenServer e Red Hat KVM.

Além de comercializar simplesmente um hypervisor, essas empresas trabalham com sistemas completos de virtualização (virtualization systems).

Esses sistemas de virtualização permitem a criação dinâmica de VMs, suas inicializações, movimentação manual ou automática entre diferentes servidores, parada dessas VMs e assim por diante tudo de maneira centralizada ou distribuída.

Por exemplo, um determinado servidor precisa ser desligado para troca de um componente, o que iria acontecer se fosse um servidor físico no mundo convencional? Provavelmente seria o caos... seria necessário agendar uma janela de manutenção e o cliente ficaria sem serviço durante esse tempo!

No mundo virtual seria possível que o responsável pela manutenção movesse as VMs que estão nesse servidor para outra máquina física, muitas vezes sem nem precisar parar essas VMs, e aí sim desligar o servidor para manutenção, com muito menos downtime para o cliente, ou seja, o cliente ficaria fora do ar por muito menos tempo.

Esse é somente um exemplo de melhoria com a virtualização, que é a base para a criação do conceito de nuvem que vamos estudar ainda nesse curso.

4.1.3.3 TIPOS DE HYPERVISORS

O foco desse capítulo está nos data centers, porém os hypervisores podem classificar-se em dois tipos:

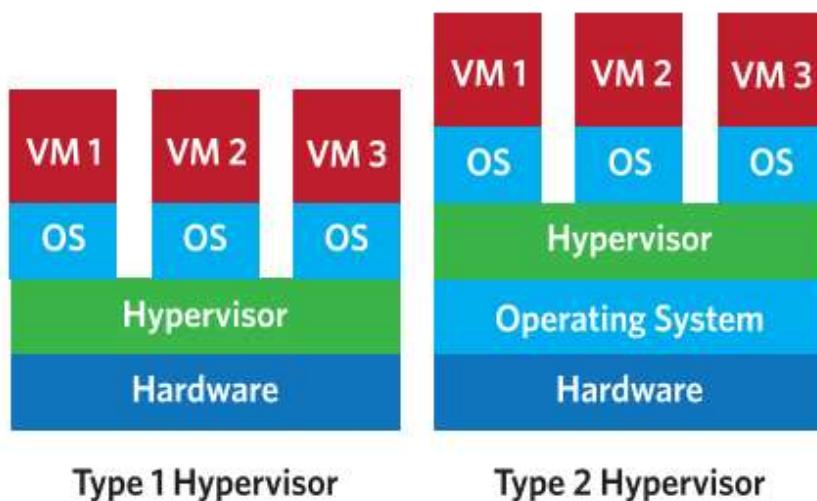
- **Hipervisor tipo 1 (type 1)**: Também denominado nativo, unhosted o bare metal (sobre o metal nu), é software que se executa diretamente sobre o hardware, para oferecer a funcionalidade descrita. Foi o exemplo utilizado na arquitetura do tópico anterior.

Alguns dos hipervisores tipo 1 mais conhecidos são os seguintes: VMware ESXi (grátis), VMware ESX (Software comercial), Xen (livre), Citrix XenServer (grátis), Microsoft Hyper-V Server (grátis).

- **Hipervisor tipo 2 (type 2)**: Também denominado hosted, é software que se executa sobre um sistema operacional para oferecer a funcionalidade descrita. Ele é um software instalado em computadores normais, você já pode ter até utilizado um dos exemplos abaixo no seu próprio computador.

Alguns dos hypervisors tipo 2 mais utilizados são os seguintes: Oracle VirtualBox (grátis), VMware Workstation (comercial), QEMU (livre), oVirt (livre), Microsoft Virtual PC, etc.

Veja na figura abaixo a comparação entre os dois tipos de virtualização. Note que OS é o sistema operacional (Operating System) e VM é a máquina virtual (Virtual Machine).

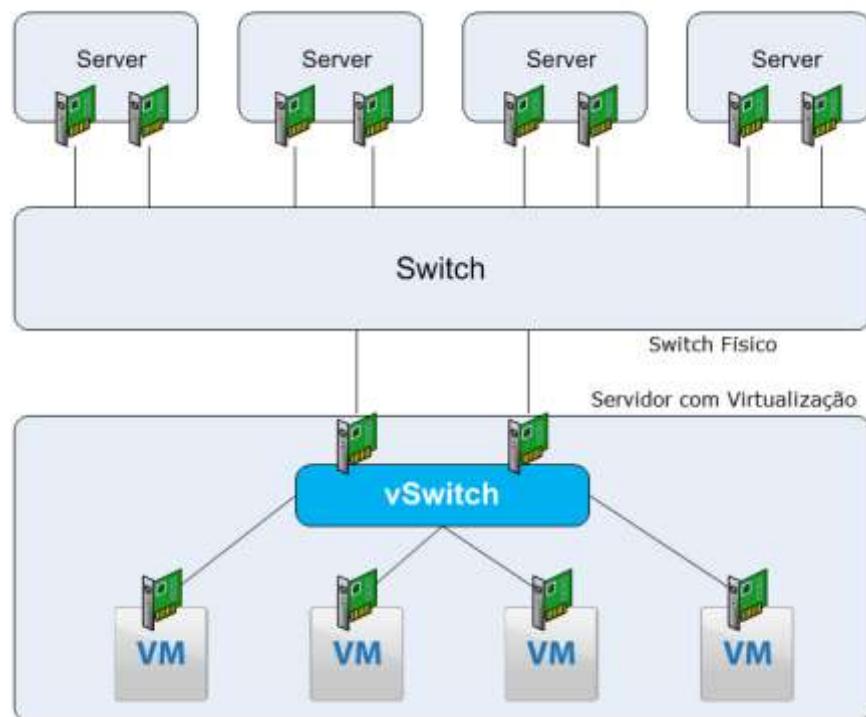


4.1.3.4 CONECTANDO VMs À REDE

Falando mais especificamente da Rede em uma máquina virtual, podemos dizer que cada VM utiliza uma placa de rede Virtual ou Virtual NIC (Network Interface Card ou vNIC), que pode se conectar à rede de várias formas diferentes.

Uma das maneiras de conexão das diversas VMs em um servidor virtualizado é através do uso de um Switch virtual (Virtual Switch ou vSwitch).

Veja a figura a seguir.



Nesse exemplo temos um servidor utilizado para virtualização com quatro VMs conectadas a um vSwitch ou Switch Virtual, o qual se conecta utilizando a placa de rede do servidor ao switch físico da Rede.

Normalmente essa conexão é um Link de trunk, seguindo padrões normais de conexão de interfaces entre switches.

A Cisco possui o switch virtual Nexus 1000VE para esse tipo de aplicação.

4.1.4 Outros Tipos de Endpoints

Além dos computadores e servidores podemos ter vários outros dispositivos que necessitam de acesso aos recursos de rede, pois até os telefones celulares, mais especificamente os smartphones, têm possibilidade de acesso à rede através de uma interface sem fio (wireless).



Portanto abaixo seguem outros dispositivos que vocês podem encontrar como endpoints em uma rede de computadores:

- **Câmeras de segurança IP:** utilizadas para monitorar e gravar o ambiente residencial ou corporativo e tanto a monitoração como o controle é realizado via rede.
- **Dispositivos de Colaboração ou Collaboration (Telefones IP, ATAs e softphones):** cada vez mais comuns são os sistemas de telefonia IP, onde agora a voz é transmitida pela rede e um PABX ou Central Telefônica IP é que faz a interface e comutação das chamadas internas e externas. Nesses tipos de sistemas temos a central instalada em um servidor ou em um dispositivo proprietário e os endpoints podem ser telefones IP, adaptadores que interligam o mundo convencional com o mundo IP (chamados de ATAs) ou então o telefone IP pode estar instalado nos computadores dos usuários através de um aplicativo, o qual recebe o nome de softphone ou telefone por software.
- **Smartphones e Tablets:** cada vez mais utilizados no mundo corporativo são os smartphones e os tablets, os quais permitem o uso pessoal ou então acesso aos recursos da empresa, tais como serviços de e-mail, banco de dados e sistemas corporativos. Aqui normalmente o acesso é realizado através da rede sem fio (wireless).
- **Thin Clients:** em português, o "cliente magro" é um computador cliente em uma rede de modelo cliente-servidor de duas camadas o qual tem pouco ou nenhum aplicativo instalado, ou seja, ele depende primariamente de um servidor central para o processamento de atividades. A palavra "thin" (magro) se refere a uma pequena imagem de boot que tais clientes tipicamente requerem - talvez não mais do que o necessário para fazer a **conexão com a rede** e **iniciar um navegador web** dedicado ou uma conexão de "**Área de Trabalho Remota**" tais como X11, Citrix ICA ou Microsoft RDP.

- **Aparelhos de Vídeo Conferência:** utilizados para comunicação de voz e áudio entre diferentes localidades de uma mesma empresa ou até entre empresas parceiras. Tanto a telefonia IP ou VoIP como a vídeo conferência necessitam de recursos e configurações especiais na rede, tanto no que se refere à largura de banda suficiente como aos requisitos de qualidade de serviços (QoS).
- **Sistemas de Catracas Eletrônicas ou Biométricas:** muitas empresas utilizam um sistema de liberação de acesso a determinadas áreas, assim como ponto eletrônico com cartões magnéticos ou até mesmo com recursos de biometria (leitura de impressão digital, por exemplo). Para isso, na maioria dos casos, essas catracas estão interligadas via rede IP com um sistema de autorização e registro de entrada e saída dos funcionários a um servidor.
- **Dispositivos IoT – Internet of Things ou Internet das Coisas:** A ideia por trás do conceito de IoT é possibilitar a conexão a diversos outros dispositivos do nosso dia a dia à Rede mundial. O que diferencia um dispositivo munido de tecnologia IoT dos demais, não é apenas a conexão à internet que ele possui, mas também a capacidade de trocar informações relevantes acerca de suas tarefas com os demais aparelhos. O principal ponto de um dispositivo de IoT é, então, a comunicação que permite a troca de dados para que a melhoria de performance do aparelho e de outros periféricos seja possível.

Para você entender o conceito de IoT vamos usar o mais popular de todos que são as Casas Inteligentes. Segundo o Google, as casas inteligentes são a aplicação IOT mais amplamente pesquisada na rede.

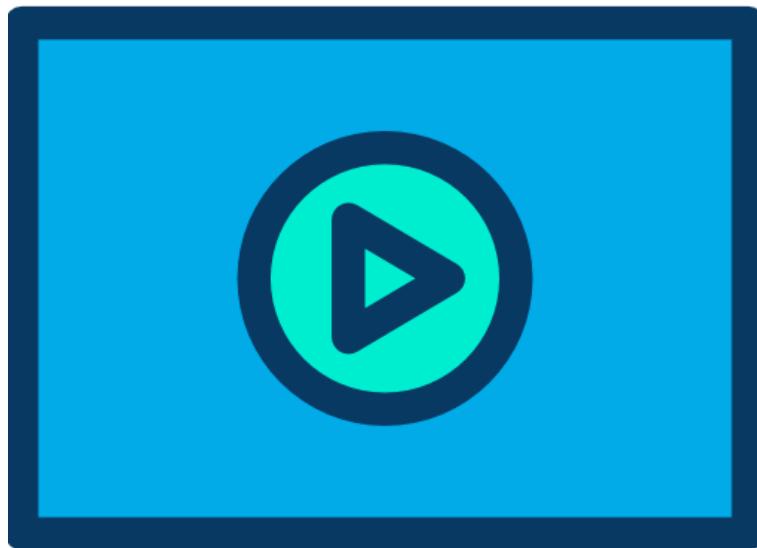
Agora imagine, você pode monitorar a segurança de sua casa durante as férias.

Não será ótimo se você puder ligar o ar-condicionado 10 minutos antes de chegar a sua casa do escritório ou desligá-lo para evitar desperdício de eletricidade quando ninguém estiver em casa? O enorme potencial nessa área já levou US\$3 bilhões em financiamento para essa linha de negócios.

Citamos aqui os exemplos de outros tipos de endpoints mais relevantes, porém com o avanço tecnológico mais e mais dispositivos surgem, os quais com necessidades específicas de acesso à rede e seus serviços.

Esse é o maior desafio de uma rede, o de manter-se atualizada e suportar os diferentes requisitos de cada sistema, aplicação ou dispositivo de forma segura e escalável!

4.2 Switches Camada 2 (L2 ou Layer 2)



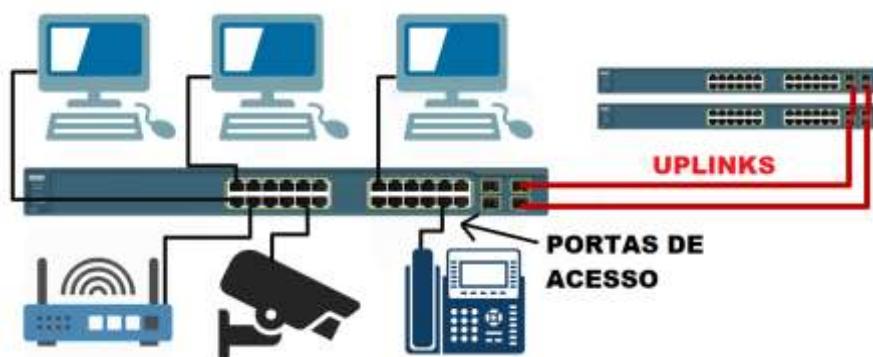
Os switches (comutadores) operam por padrão na camada 2 (Enlace) do modelo OSI e tem a função de conectar endpoints, como computadores e servidores, à rede.

Os switches possuem diversos modelos com um número variado de portas, podendo ir de 12 a 48 portas em configurações fixas (não modulares) ou até mais de 100 portas quando trabalhamos com switches Modulares.

Normalmente as portas dos switches são divididas entre portas de acesso ou “access ports” e portas trunk, as quais podemos chamar também de Uplinks.

Uma porta de acesso conecta os endpoints, já os uplinks conectam a outros switches ou até mesmo em roteadores.

Veja A imagem a seguir.



Além disso, os switches podem operar em outras camadas do modelo OSI além da camada 2, por exemplo, existem switches layer 3 que atuam ao mesmo tempo como roteador e switch, fazendo além da comutação dos quadros de camada 2 também o roteamento dos pacotes IP através da rede, mas isso veremos mais para frente.

Abaixo segue ilustração de diferentes switches Cisco Catalyst.

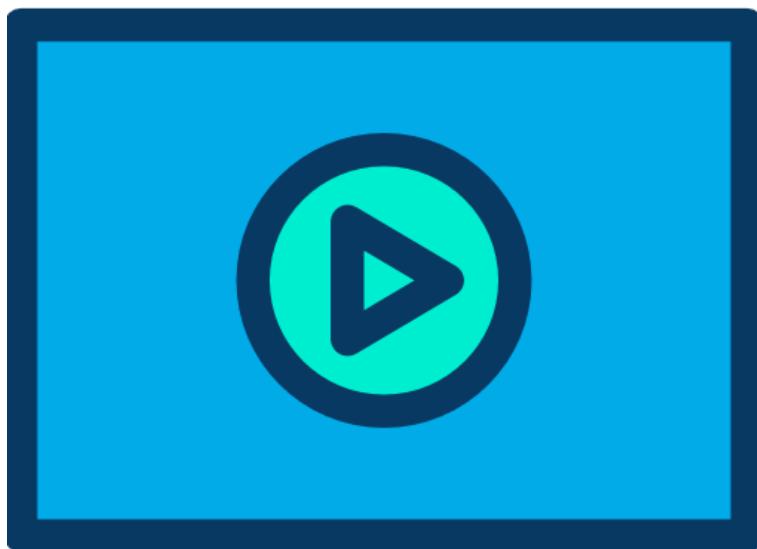


Porque um switch é considerado um dispositivo camada ou layer 2 (L2)?

Lembra do endereço MAC que estudamos anteriormente? Um switch encaminha os quadros de camada-2 na rede utilizando esse endereço, o qual está na camada-2 do modelo OSI ou na camada de acesso aos meios do TCP/IP.

Por ele tomar sua “decisão” de encaminhamento com um endereço de camada-2 ele é classificado nessa camada do modelo OSI.

4.2.1 MAC, Frames e Ethernet



Antes de iniciar o capítulo vamos rever alguns conceitos sobre o processo de encapsulamento do TCP/IP:

- A Camada de Aplicação fornece a interface para o usuário.
- A Camada de Transporte é responsável pela divisão e gerenciamento das comunicações entre os processos que são executados nos dois sistemas finais.
- Os protocolos da Camada de Rede, como o IP, organizam os dados de comunicação de modo que eles possam viajar através da conexão de rede a partir do host de origem até o host de destino.

Para que os pacotes da Camada de Rede sejam transportados do host de origem ao host de destino, eles devem atravessar diferentes redes físicas, por diferentes meios físicos de transmissão, por exemplo, podem pegar uma fibra óptica, rádios digitais e até satélites.

Essas redes físicas podem ser diferentes e devem ser transparentes para a Camada de Rede, ou seja, para os pacotes IP.

Os pacotes da Camada de Rede não têm um caminho para acessar diretamente estes diferentes meios, portanto a Camada de Acesso aos Meios é quem deve desempenhar esse papel.

Portanto, o papel da Camada de Acesso aos Meios, mais especificamente a de Enlace do modelo OSI, é preparar os pacotes da Camada de Rede para transmissão no meio físico.

Em uma rede LAN veremos protocolos da família **Ethernet** (Fastethernet, Gigabit Ethernet ou 10 Gigabit Ethernet), cujo endereço MAC tem papel fundamental, pois redes Ethernet são primordialmente meios **compartilhados**, ou seja, são utilizados por vários elementos (computadores ou servidores) que desejam se comunicar ao mesmo tempo utilizando o mesmo meio físico.

Portanto, o endereço MAC vai identificar o tipo de comunicação que a camada-3 quer realizar e com quem dentro da mesma rede, pois estamos tratando de redes Locais (LAN).

Veja na figura abaixo o formato do quadro Ethernet da camada-2 e a seguir o que significa cada campo.

Protocolo Ethernet						
	Quadro					
Nome do campo	Preâmbulo	Endereço de Destino	Endereço de Origem	Tipo	Dados	Seqüência de Verificação do Quadro
Comprimento	8 bytes	6 bytes	6 bytes	2 bytes	46 - 1500 bytes	4 bytes

- **Preâmbulo (preamble)** - utilizado para sincronização. Também contém um delimitador para marcar o final da informação cronometrada.
- **Endereço MAC de Destino (destination address)** - Endereço MAC de 48 bits do computador ou endpoint de destino (quem vai receber).
- **Endereço MAC de Origem (source address)** - Endereço MAC de 48 bits do computador ou endpoint de origem (quem está enviando).
- **Tipo (type)** - valor para indicar que protocolo de camada superior receberá os dados depois que o processo Ethernet for concluído.
- **Dados (data ou payload)** - esta é a PDU, normalmente um pacote IPv4 ou Ipv6, que deve ser transportado pelos meios físicos.
- **Sequência de Verificação de Quadro (FCS – frame check sequence)** - um valor utilizado para verificar quadros danificados através de uma conta chamada CRC ou Check de Redundância Cíclica.

Mas porque eu preciso saber esse quadro de camada 2?

Na realidade é necessário entender o quadro e saber que ele possui dois identificadores que mostram a origem e destino da comunicação, ou seja, quando um computador quer enviar informações a outro em uma LAN ele deve montar um quadro e colocar seu endereço MAC como origem e como destino deve colocar o endereço MAC do computador remoto, o qual ele deseja se comunicar.

Note que antes de enviar ele também faz uma conta com os bits que serão enviados e coloca o resultado no campo FCS, chamada Check de Redundância Cíclica.

Essa conta permite que o receptor saiba se houve erros na transmissão. A família Ethernet não prevê recuperação de erros, ou seja, o receptor recebe um quadro, recalcula o campo FCS, compara com o valor que foi calculado no campo FCS pelo transmissor e aceita ou rejeita o quadro.

A recuperação de erros é função das camadas superiores.

Outra informação importante do quadro ethernet é que ele aceita no máximo 1500 bytes de informação, o que é chamado de **MTU** ou tamanho máximo para transmissão (**Maximum Transmission Unit**).

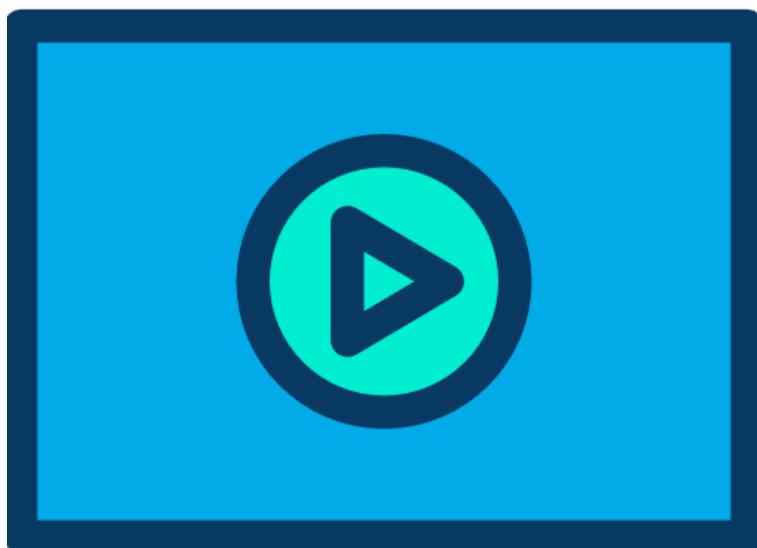
Se vierem mais que 1500 bytes o receptor irá descartar aquele quadro e incrementar um erro em sua interface.

Para finalizar o estudo do quadro ethernet veja agora o campo **Tipo** ou **Type**, ele traz a informação do protocolo de camada superior que será transportado pelo quadro, por exemplo, o protocolo IP é representado pelo valor 0x0800 e o IPv6 é representado pelo valor 0x86DD.

O símbolo “0x” indica que os algarismos estão escritos em Hexadecimal.

Portanto, a troca de quadros é realizada dentro de uma mesma rede LAN, com finalidade de formar um link local entre dois dispositivos!

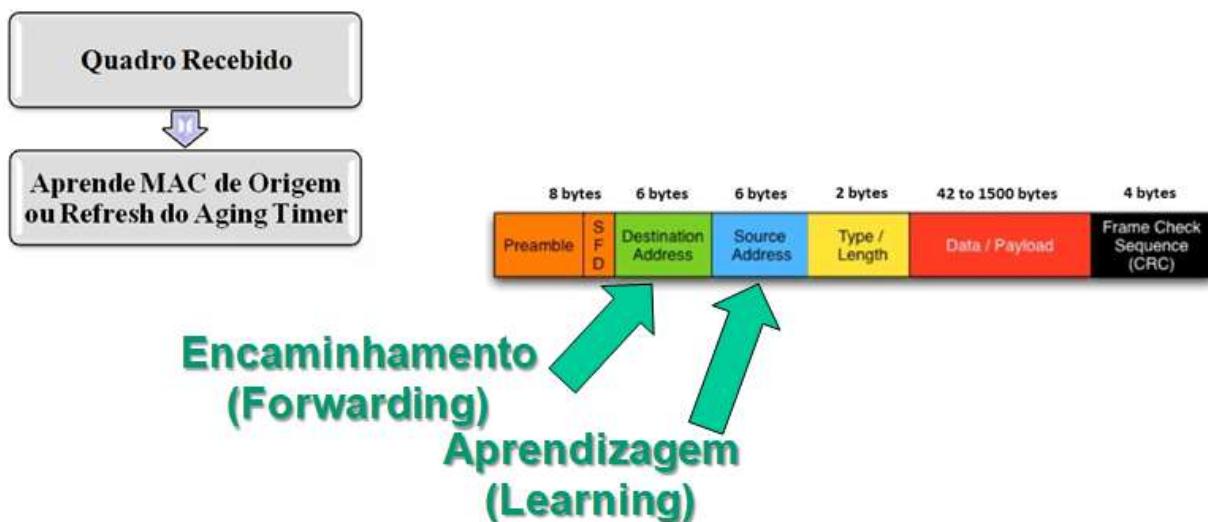
4.2.2 Principais Funções de um Switch L2



As principais funções de switch são aprendizado, encaminhamento e filtragem de MACs, além disso, um switch precisa evitar loops de camada-2, porém esse último assunto não é foco desse curso.

4.2.2.1 APRENDIZADO DE ENDEREÇOS MAC

O **aprendizado** dos MACs é realizado através do **endereço MAC de origem (Source Address)** contidos nos quadros Ethernet.



Abaixo segue um resumo do processo de aprendizagem de quadros em portas de switches.

- Ao ligar o switch ele não conhece os hosts conectados às portas.
- À medida que os quadros são encaminhados na rede os switches **aprendem os MAC's de origem** (de quem está enviando um quadro) e criam uma tabela relacionando os endereços de camada-2 às portas do switch.
- Essa tabela é chamada de MAC Address Table ou CAM (Content Addressable Memory) Table ou Tabela de Endereços MAC.
- Quando um endereço MAC é adicionado à tabela de endereços MAC, um indicador de "tempo", temporizador ou "**time stamp**" é inserido juntamente na tabela.
- Se um MAC conhecido, que já estava na tabela de endereços é recebido, o switch atualiza o "**time stamp**" da tabela.

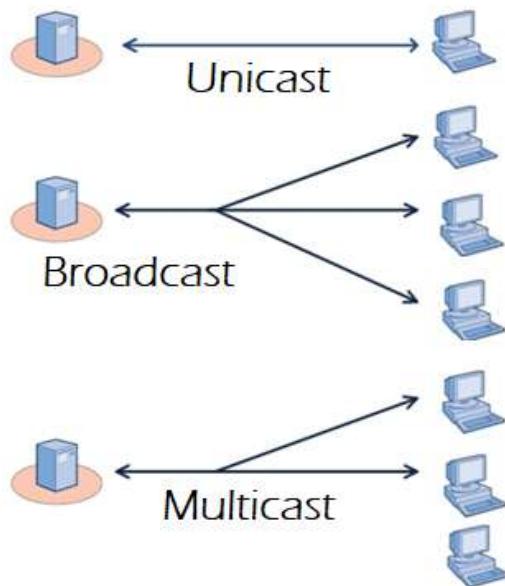
Esse tempo é chamado de "**aging timer**" e serve para medir o período de inatividade de um computador. O padrão são 5 minutos ou 300 segundos.

Portanto se um computador ficar "quieto" por 5 minutos, o switch removerá aquele endereço MAC da tabela, pois pode significar que o endpoint foi removido ou mudou de localização.

4.2.2.2 ENCAMINHAR OU FILTRAR QUADROS ENTRE PORTAS

Existem três tipos de comunicação básicas em uma rede IPv4 que são:

- **Unicast**: um para um
- **Broadcast**: um para todos
- **Multicast**: um para um grupo



Quando dois computadores se comunicam usam **Unicast**, portanto utilizam como endereços de origem e destino seus próprios endereços MAC gravados na placa de rede.

No **Broadcast** utilizam seu MAC de origem e como destino utilizam tudo 1 no MAC ou ffff.ffff.ffff, conhecido como endereço MAC de broadcast.

No **Multicast** temos uma comunicação de em grupo, onde todos os hosts usam o mesmo endereço de camada-3 e como MAC se for IPv4 inicia com 01:00:5e e se for um multicast IPv6 o MAC inicia sempre com 33:33:33.

Portanto, o processo de encaminhamento de quadros de um switch ocorre conforme endereço MAC de destino que ele receber no quadro que chega em sua Porta para ser encaminhado.

As opções de encaminhamento são:

- Após a tabela de endereços MAC estar completa, os switches **encaminham o quadro ou filtram baseado no endereço de destino**.
- Endereços MAC de **Unicast conhecidos** são encaminhados conforme tabela de endereços MAC, ou seja, para a porta de destino que o switch encontrar nessa tabela.
- Endereços MAC de **Unicast não conhecidos (Unknown Unicast Addresses)** sofrem o processo de **flooding**, ou seja, são encaminhados para todas as portas menos a porta de origem que recebeu o quadro.
- Quadros com endereço de destino contendo um endereço de **broadcast** (ffff.ffff.ffff) ou **multicast** (inicia com **01:00:5e** para IPv4 ou **33:33:33** para o IPv6) são encaminhados para todas as portas menos a porta de origem (**processo de flooding**).

Veja a seguir a imagem com o fluxo de decisão de encaminhamento dos quadros que um switch L2 utiliza.



Veja que o encaminhamento do multicast está considerando o comportamento padrão do switch, pois ele pode mudar conforme configuração.

Já o Broadcast não, ele sempre passará pelo processo de flooding.

Dica: **flooding** é uma inundação ou cópia do quadro em todas as portas menos para a porta de origem e é um processo realizado em camada-2 (vamos estudar mais detalhes do flooding a seguir).

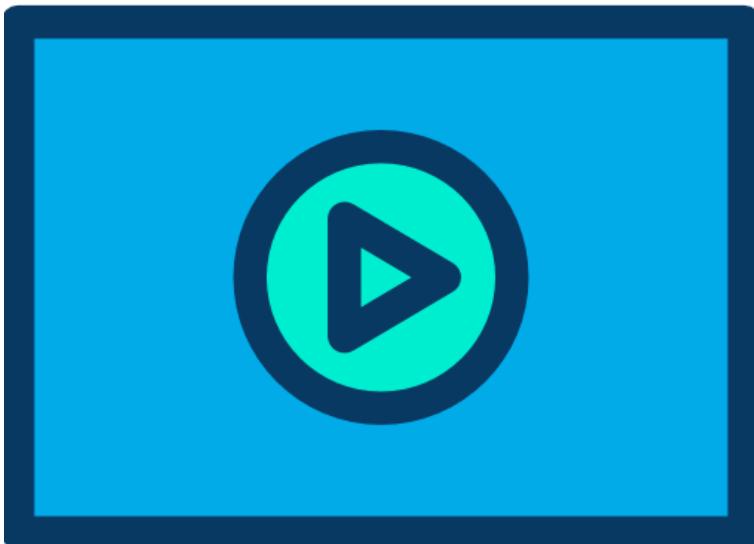
Muitos alunos ficam se perguntando “Porque um switch filtraria um quadro?”.

A resposta é simples, é só colocar um HUB em uma das portas que pode haver a necessidade de filtragem se dois computadores conectados ao mesmo HUB tentarem se comunicar.

4.2.2.3 EVITAR LOOPS UTILIZANDO O PROTOCOLO SPANNING-TREE (STP):

Caminhos redundantes são necessários, porém trazem problemas de loop de camada-2 e o spanning-tree é um protocolo que aprende os caminhos redundantes e evita loops.

Essa função de evitar loops e o protocolo STP não será abordada nesse curso por não ser foco dessa parte do blueprint, teremos cursos específicos sobre o assunto.

4.2.3 Frame Flooding

Muitos alunos confundem o processo de broadcast com o flooding, mas você não vai confundir mais isso!

O flooding é um processo realizado em camada-2 para encaminhar quadros que tenham endereços de Unicast desconhecidos, Broadcasts e Multicasts com configuração padrão.

Ele apenas garante que o receptor vai receber aquele quadro, pois ele não sabe "quem é o dono" ou em que porta do switch está o dono desses endereços citados acima.

No caso do endereço de destino do quadro de camada-2 ser um broadcast, o switch nunca saberá o dono e sempre fará um flooding, pois é isso que um broadcast pede.

Pense em um sistema de broadcast de televisão, simplesmente TODOS os usuários com televisão ligada tem que receber aquele sinal, simples assim!

Com um quadro de broadcast a regra é a mesma, TODOS os endpoints naquele domínio de broadcast precisam receber a informação e ponto final!

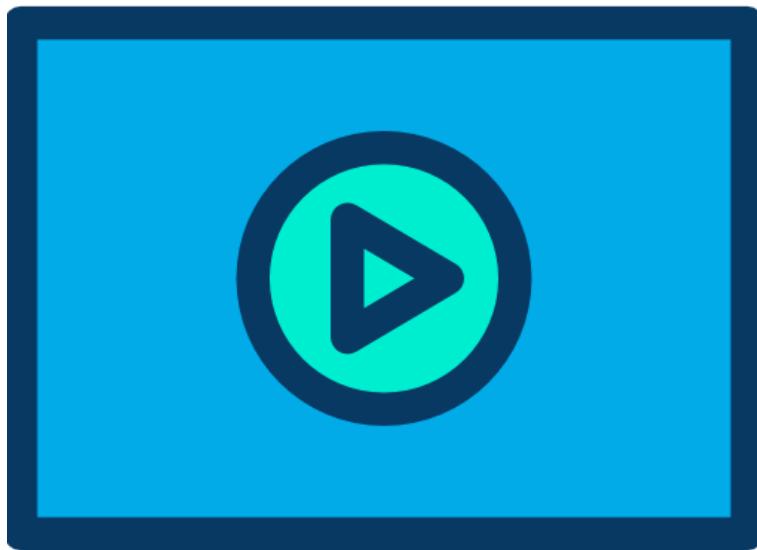
Mas porque o broadcast não é igual a um flooding? Se todos tem que receber a mensagem?

Porque um broadcast é gerado pelo endpoint, seja ele um computador ou servidor, o switch não pode "gerar um broadcast" em nome de um cliente, pois ele deve ser transparente para as camadas superiores.

Um switch pode gerar um broadcast?

Pode, quando ele está agindo como um host e solicitando informações de um servidor ou serviço que seja em broadcast. Mas é uma ação DELE MESMO e não em nome de um cliente.

4.2.4 Tabela de Endereços MAC



Na realidade, os switches Cisco Catalyst e da família Nexus inserem mais uma informação em sua MAC Address Table, que é o VLAN-ID ou número da VLAN a qual a porta está vinculada.

Uma VLAN ou LAN Virtual é um agrupamento de portas camada-2 em um domínio isolado de broadcast, ou seja, é como se a gente quebrasse o switch em vários switches menores de acordo com as portas alocadas em cada VLAN.

Veja o formato da tabela de endereços MAC em switches Cisco abaixo:

Vlan	Mac Address	Type	Ports
---	-----	-----	-----
All	0100.0ccc.cccc	STATIC	CPU
...	saídas omitidas		
All	0180.c200.000e	STATIC	CPU
All	0180.c200.000f	STATIC	CPU
All	0180.c200.0010	STATIC	CPU
All	ffff.ffff.ffff	STATIC	CPU
50	44d3.ca05.7490	DYNAMIC	Gi0/2
50	f068.65e6.0840	DYNAMIC	Fa0/23
60	04fe.8de2.4226	DYNAMIC	Fa0/24
1	180d.2c6a.813a	DYNAMIC	Fa0/22
1	44d3.ca05.7491	DYNAMIC	Gi0/1
10	1ce6.c772.6484	DYNAMIC	Fa0/2
10	1ce6.c772.6c09	DYNAMIC	Fa0/7
10	1ce6.c773.351c	DYNAMIC	Fa0/4
10	44d3.ca05.7491	DYNAMIC	Gi0/1
10	641c.677d.1e1b	DYNAMIC	Fa0/2
10	70fd.4664.f0d2	DYNAMIC	Fa0/22
10	9883.89f0.582f	DYNAMIC	Fa0/7
10	9883.89f0.5a59	DYNAMIC	Fa0/4
10	d050.99a0.f129	DYNAMIC	Fa0/8

```

10    d077.146f.dea0      DYNAMIC   Fa0/22
10    ecc8.82b0.43e1      DYNAMIC   Fa0/8
10    f430.b96d.91d2      DYNAMIC   Fa0/22
30    1ce6.c772.6484      DYNAMIC   Fa0/2
30    1ce6.c772.6c09      DYNAMIC   Fa0/7
30    1ce6.c773.351c      DYNAMIC   Fa0/4
30    44d3.ca05.7491      DYNAMIC   Gi0/1
30    ecc8.82b0.43e1      DYNAMIC   Fa0/8
Total Mac Addresses for this criterion: 42

```

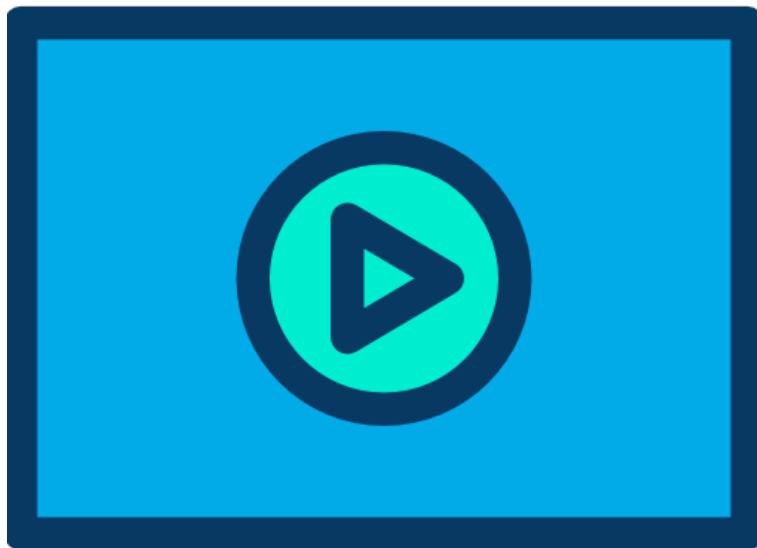
O comando que utilizamos para ver a tabela MAC em switches Cisco é o "show mac address-table" e note que ele traz as informações sobre:

- **Vlan**: a que LAN virtual a porta pertence.
- **Mac Address**: endereço MAC de origem ao dispositivo de rede ou endpoint conectado à porta.
- **Type**: tipo de endereço MAC, ou seja, como ele foi aprendido. Normalmente o endereço pode ser estático (MACs internos ou configurados via comando) ou dinâmico (aprendidos dinamicamente).
- **Ports**: porta onde o MAC está conectado, ou seja, o "dono" do MAC de origem que enviou um quadro naquela porta específica.
- **Total Mac Addresses for this criterion**: contagem dos MACs encontrados no comando.

Veja que temos uma linha grifada na tabela de endereços MAC, vamos analisá-la:

- **"10 1ce6.c772.6484 DYNAMIC Fa0/2"**: veja que essa linha significa que o endereço MAC do endpoint que está conectado na interface FastEthernet 0/2 (Fa0/2 – segunda porta do switch) foi aprendido dinamicamente (dynamic) e tem o valor "1ce6.c772.6484". Além disso, esse endpoint está vinculado à VLAN 10 do switch.

4.3 Access Points (AP)



Um Access Point ou ponto de acesso é um dispositivo que permite interligar duas redes sem fio entre si ou uma rede a vários dispositivos em um mesmo ambiente.

Em geral, o access point se conecta a uma rede cabeada e fornece acesso sem fio a esta rede para dispositivos móveis no raio de alcance do sinal de rádio.

Portanto, o AP se conecta à rede cabeada e serve de interface entre os dispositivos com placa de rede sem fio até os demais dispositivos de rede.

Existem vários padrões de rede sem fio, chamadas também de wifi, que são baseadas nas recomendações do 802.11.

Temos atualmente o 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac e 802.11ax sendo que cada uma dessas tecnologias tem uma característica de velocidade, alcance e tecnologia.

Em redes de pequeno porte os APs são autônomos, ou seja, cada dispositivo precisa ser configurado manualmente um a um e trabalham de forma independente.

Veja a figura a seguir onde temos um roteador sem fio e um repetidor fornecendo acesso wireless aos computadores de um pequeno escritório.



Portanto, os APs autônomos são configurados como os APs residenciais, ou seja, um a um de maneira individual.

Agora imagine em uma grande empresa que possui 1000 Aps... será que seria simples administrar um a um desses equipamentos?

Com certeza não e para isso você pode utilizar uma rede integrada, a qual utiliza controladoras para gerenciar diversos APs.

Uma controladora de redes sem fio ou “**Wireless LAN controller**” (**WLC**) tem a função de controlar e gerenciar as funções de TODOS os APs (Access Points) na rede, por exemplo, roaming, que redes sem fio e SSIDs os APs utilizarão WLANs, autenticação e muito mais.

Na Cisco os Access Points podem ser configurados como **APs autônomos** e **LAPs (Lightweight Access Points)** ou APs controlados por **WLCs - Wireless LAN Controllers** na LAN ou Campus.

No modo LAP os Access points são controlados pelas controladoras sem fio ou WLCs, as quais passam a controlar todos os aspectos da comunicação sem fio, inclusive todas as configurações dos LAPs.

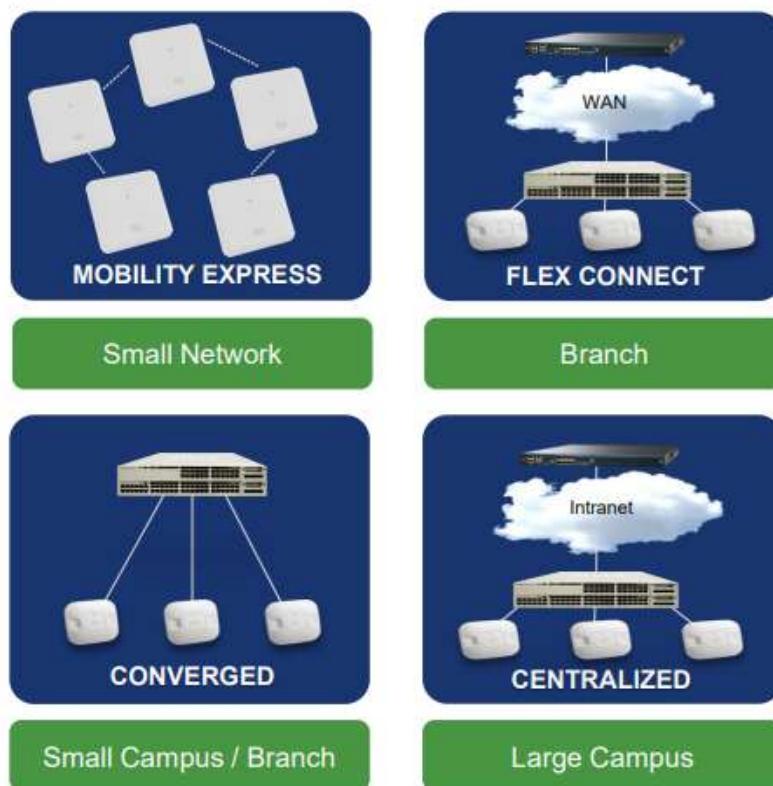
Portanto APs em modo LAP são projetados para serem configurados pela WLC, conhecido como **“zero touch deployment”**, ou seja, não precisa fazer nada nos LAPs, eles inicializam e pegam todas as configurações da sua controladora de redes sem fio (WLC - Wireless LAN Controller).



Falando mais especificamente de soluções Cisco podemos ter várias opções dependendo do tamanho da rede e tipo de conexão entre os dispositivos, por exemplo:

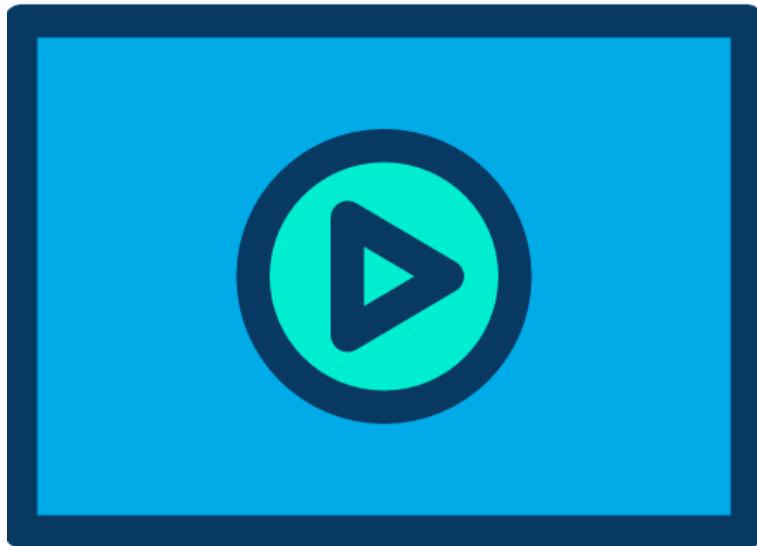
- **Mobility Express:** utilizado em redes de pequeno (small networks) porte sem o uso de WLCs, onde um dos access points pode assumir a função de controladora da rede utilizando o Mobility Express.
- **Flex Connect:** para soluções em branch offices ou escritórios remotos conectados ao ponto central via WAN. Nesse caso se a WAN ficar indisponível deve haver um suporte local para autenticar e encaminhar os dados dos clientes.
- **Convergida ou Converged:** onde o switch de acesso ou distribuição tem uma controladora como parte do seu sistema operacional, possibilitando que ele mesmo controle um número limitado de LAPs da LAN. Essa solução é utilizada em ambientes pequenos (small networks) e branch offices (unidades remotas)
- **Centralizada ou Centralized:** utiliza uma WLC normalmente em um ponto central da rede ou no datacenter para controlar os LAPs da empresa. Utilizada em grandes ambientes (large networks ou large campus).

Veja a imagem a seguir com exemplos de cada uma das soluções explicadas anteriormente.



Vamos falar mais sobre os WLCs posteriormente.

4.4 Switches Camada 3 (L3 ou Layer 3)



A diferença de um switch camada-3 para um switch camada-2 é que ele faz tudo o que o switch L2 faz, mas também faz “muita coisa” que um Roteador faria!

Um switch camada-2 não consegue “entender” ou “ler” os pacotes IP, por isso mesmo ele faz o encaminhamento através dos endereços MAC, os quais estão nos quadros ou frames de camada-2.

Por isso mesmo, a parte de roteamento entre diferentes redes os switches L2 precisam de um “roteador” ou dispositivo de camada-3 para realizar essa tarefa.

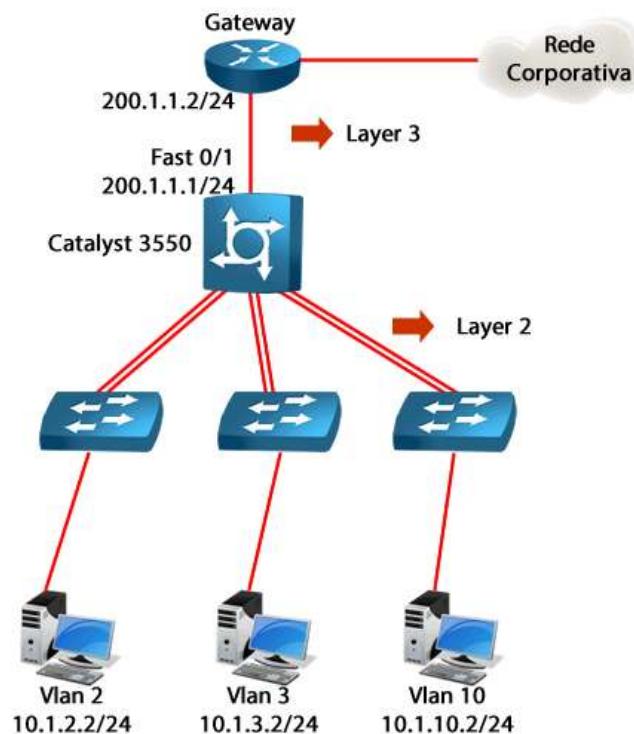
Portanto um switch de camada-3 ou switch L3, além de montar a tabela de endereços MAC, monta uma tabela de roteamento IP, a qual possibilita que ele encaminhe também pacotes IP.

A diferença de um switch L3 e um roteador é que o switch L3 pode realizar roteamento de pacotes de maneira semelhante ao encaminhamento dos quadros, ou seja, através de hardware ao invés de software como nos roteadores, isso torna os switches camada 3 até mais rápidos que os roteadores para o encaminhamento dos pacotes.

Os switches Layer 3 da Cisco que rodam o sistema operacional Cisco IOS são na realidade switches layer 2 por padrão e para terem a facilidade de roteamento IP (Layer 3) você deve utilizar um IOS mais avançado, que suporte o protocolo IP, e também habilitar o protocolo IP com o comando “**ip routing**” em modo de configuração global.

Note que o mesmo comando que já vem habilitado por padrão nos roteadores.

Vamos mostrar um exemplo de configuração de roteamento entre VLANs em um switch layer 3 modelo Catalyst 3550 e como configurar uma interface para layer 3 e conexão com um roteador, veja a topologia na figura abaixo.

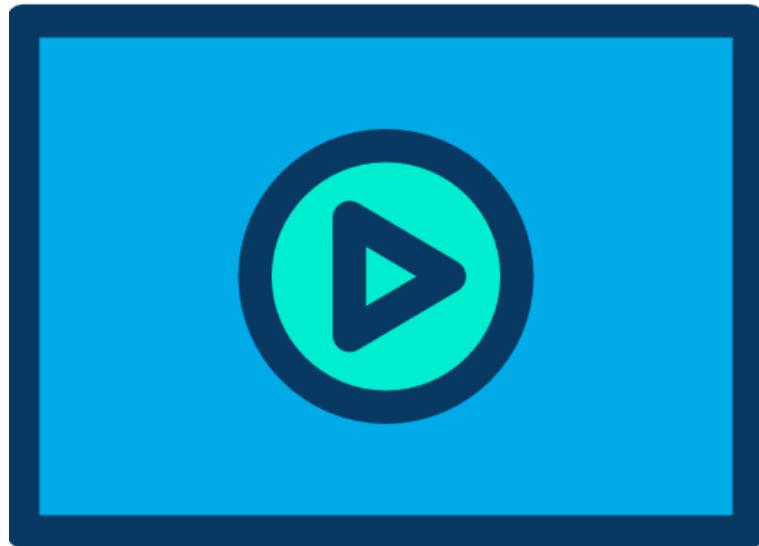


Vamos partir do pressuposto que as configurações básicas do switch 3550 foram realizadas e os switches de acesso também, portanto vamos apenas nos preocupar com ativar o roteamento IP no 3550, configurar o roteamento entre VLANs e ativar o recurso de layer 3 na interface Fast 0/1 para configurar um endereço IP nela.

Também teremos que configurar o roteamento no switch 3550, para que ele possa encaminhar pacotes de redes não conhecidas em direção à rede corporativa, faremos isso com uma rota estática padrão apontando para o roteador, o qual é seu gateway padrão.

Sem um switch L3 você precisaria de um roteador local para fazer o roteamento entre VLANs.

4.5 Roteadores (Routers)



O Roteador ou Router é um equipamento que opera na camada 3 (Rede) do modelo OSI e permite a conexão entre diferentes redes locais (LAN) ou entre duas ou mais redes locais que estão distantesumas das outras através de uma rede de longa distância (WAN).

Suas principais funções são:

- Filtrar e encaminhar os pacotes IP
- Determinar as melhores rotas para redes de destino
- Servir como interface entre diferentes tipos de redes, atuando como um gateway



Quanto a sua forma de operação, as rotas são determinadas a partir do endereço de rede do computador de destino através da consulta de uma **tabela de roteamento**.

Essas tabelas são atualizadas utilizando-se informações de roteamento e por meio de algoritmos de roteamento (protocolos de roteamento dinâmicos) ou mantidas através de rotas criadas pelos próprios administradores de redes, chamadas rotas estáticas.

Essa é a função principal de um roteador, ou seja, **rotear** ou **encaminhar os pacotes** através da rede.

Estamos acostumados em nossas casas com os roteadores ADSL ou roteadores sem fio, os quais são dispositivos de pequeno porte e que apenas servem para conectar a nossa LAN à Internet.

Já em ambientes corporativos os roteadores podem assumir outros papéis, atuando como gateways e servindo como ponto de conexão de diferentes tipos de interfaces e tecnologias.

Por exemplo, uma empresa que utiliza telefonia IP normalmente precisa, além dos canais de voz que trafega via rede, de uma conexão com a rede pública de telefonia convencional (POTS).

Isso pode ser realizado por um roteador, que nesse caso recebe o nome de gateway de voz.

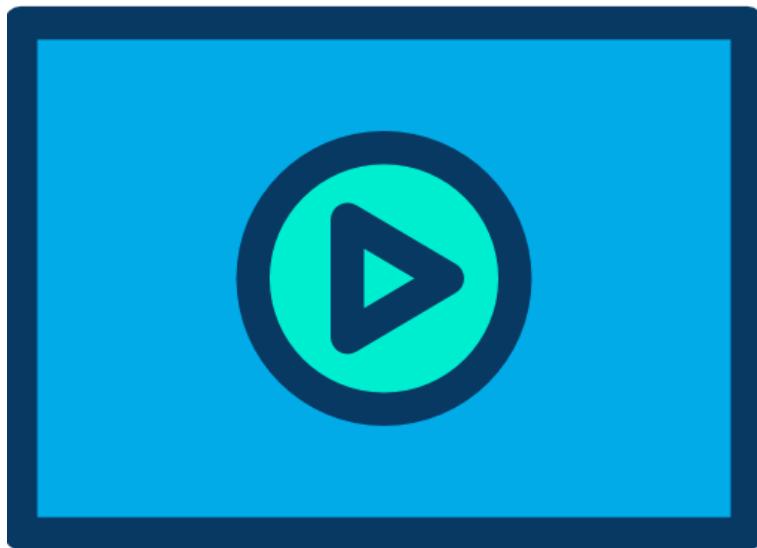
Nesse mesmo roteador iremos conectar a LAN, a WAN e a rede de telefonia pública através de diferentes interfaces!



Os roteadores desse tipo são chamados também de “**multisserviço**”, pois além de rotear podem fornecer outros tipos de serviço de rede, tais como Voz, Vídeo, atuar como um AP através de uma interface sem fio, ter possibilidade de conexão de placas para servidores virtualizados, correio de voz e muito mais, tudo isso em apenas um equipamento.

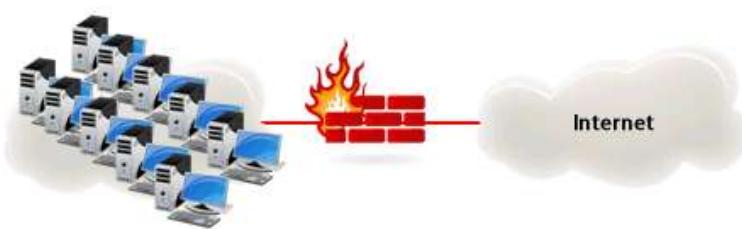
Dica: Outra opção de menor porte utilizada em ambientes virtualizados e de nuvem é o roteador virtualizado ou vRouter chamado CSR 1000-V, versão virtualizada do roteador físico ASR 1000. Esse roteador virtual é compatível com VMware ESXi, Red Hat KVM, Citrix Xen, Microsoft Hyper-V and Azure e Amazon Web Services.

4.6 Firewall versus Next-Generation Firewalls (NGFW)



Um “Firewall” tradicional é o nome dado ao dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto de controle da rede.

Sua função consiste em regular o tráfego de dados entre redes distintas e impedir a transmissão e/ou recepção de acessos nocivos ou não autorizados de uma rede para outra.



Normalmente os firewalls convencionais fazem a segurança do perímetro utilizando filtragem de pacotes IP (ACL ou Lista de Controle de Acesso), filtragem de segmentos TCP e UDP através de números de portas, stateful inspection (verificando o estado da conexão), Deep Packet Inspection (DPI), NAT ou Network Address Translation e VPNs (redes virtuais privadas).

Tudo isso configurado por um administrador de Redes ou de Segurança.

Resumindo, um firewall convencional filtra com base em endereços e portas, as quais identificam as aplicações em uma rede, apenas bloqueando ou deixando passar o tráfego.

Como muitos já devem ter visto uma lista de controle de acesso ou Access Control List, é “permit” ou “deny”, permitir ou negar o tráfego.

Um NGFW faz tudo o que um firewall tradicional faz, porém ele tem um IPS integrado (Intrusion Prevention System), pode controlar melhor as aplicações que estão sendo utilizadas na rede, ter maior visibilidade e controle.

Além disso, são capazes de utilizar inteligência externa para buscar informações sobre como proteger a rede.

As novas tecnologias de firewall podem filtrar com base nas aplicações ou tipos de tráfego que estão passando por eles. Por exemplo, você poderia abrir a porta 80 para apenas tráfego HTTP e para determinadas aplicações, sites ou serviços que você deseja permitir. É uma mistura de firewall, IPS e funcionalidades de qualidade de serviços (QoS) em uma só solução.

Abaixo vamos resumir algumas funcionalidades de um NGFW:

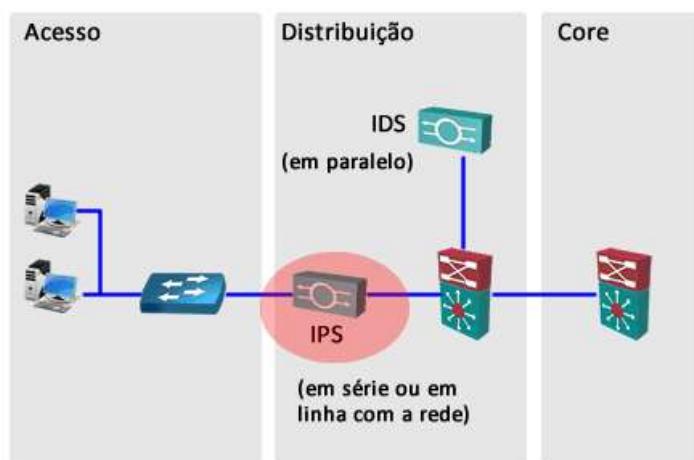
- **Firewall Convencional:** um NGFW suporta os recursos de filtragem, NAT/PAT e VPN que um firewall convencional oferece.
- **Application Visibility and Control (AVC):** esse recurso permite uma inspeção em nível de aplicação, indo além de protocolos e números de portas TCP ou UDP. Esse recurso permite a proteção contra ataques variados em diferentes portas procurando por falhas em aplicações.
- **Advanced malware protection (AMP):** permite ao NGFW analisar arquivos para descobrir ameaças escondidas ou disfarçadas, atuando como um anti-malware de rede rodando no próprio firewall, bloqueando transferência de arquivos suspeitos e até mesmo salvando esses arquivos para análise posterior.
- **Filtragem de URL:** analisa e filtra URLs, categorizando os sites acessados e limitando acesso conforme regras de tráfego configuradas. Pode ser integrado com o Talos security group que monitora e cria scores de reputação para cada domínio conhecido na Internet, possibilitando que essas informações sejam utilizadas como base na categorização, filtragem e limite de tráfego pelo NGFW.
- **NGIPS:** o NGFW pode rodar dentro dele recursos de prevenção de intrusos, possibilitando uma análise contextual em tempo real, mapeamento da rede e priorização de ameaças de forma automática.

4.7 IPS versus Next-Generation IPS (NGIPS)

Em linhas gerais a função do IPS (Intrusion Prevention System) é ser um dispositivo de segurança de rede que monitora o tráfego e/ou atividades dos sistemas em busca de comportamentos maliciosos ou não desejáveis em tempo real, com a finalidade de bloquear ou prevenir essas atividades.

Um IPS baseado em rede, por exemplo, vai operar em linha para monitorar todo o tráfego em busca de códigos maliciosos ou ataques.

Quando um ataque é detectado, é possível bloquear os pacotes danosos enquanto o tráfego normal continua seu caminho.



O IPS utiliza **assinaturas** para detectar desvios de padrões de tráfego na rede.

Uma assinatura é um conjunto de regras que IPS utiliza para detectar uma atividade intrusiva, ou seja, cada ataque tem uma característica as quais são mapeadas e armazenadas em um banco de dados de assinaturas e comparadas com o tráfego entrante.

Caso o tráfego malicioso tente entrar na rede e será detectado e o IPS pode tomar uma ação conforme configurado pelo administrador de rede, sendo desde emitir um alarme até bloquear aquele tráfego.

Um **NGIPS** ou **IPS de Próxima Geração** deve ser capaz de fazer tudo o que um IPS faz e suportar outros recursos mais avançados, tais como:

- **Efetividade superior (Superior effectiveness)**: ser capaz de parar mais ameaças, sejam elas conhecidas ou desconhecidas, com recursos de proteção avançados. Deve acelerar o tempo de detecção de um malware e reduzir o impacto dele sobre os dispositivos, assim como sua disseminação pela rede.
- **Visibilidade Contextual (Contextual awareness)**: visibilidade em tempo real, tendo maior controle e ação sobre os usuários, aplicações, dispositivos, ameaças e vulnerabilidades na rede.
- **Rápida Proteção e Contenção de Ameaças (Advanced threat protection and rapid remediation)**: ser capaz de detectar, bloquear, conter e remediar ameaças através do AMP e outras soluções. Ser também capaz de se atualizar virtualmente e instantaneamente quando um novo software ou assinatura for disponibilizada.

- **Automação da Segurança (Security automation)**: ser capaz de correlacionar eventos de ameaças, informações contextuais e vulnerabilidades, agilizando o trabalho da equipe de segurança e implementando uma melhor segurança e velocidade em investigações forenses.
- **Visibilidade Granular de Aplicações e Controle (Granular application visibility and control)**: ser capaz de reduzir as ameaças de rede com controle preciso de mais de 4000 aplicações comerciais e ter suporte a aplicações customizadas.
- **Integração com o “Global threat intelligence from Cisco’s Talos Security Intelligence and Research Group”**: ser capaz de se beneficiar da análise já realizada de mais de 35.000 regras de IPS e adicionar proteção contra IPs, URLs e DNS maliciosos através de uma inteligência externa que é realizada constantemente.

4.8 Controllers (Controladoras)

Atualmente os dispositivos de rede tem uma arquitetura de controle (control plane) e gerenciamento (management plane) descentralizada, isso porque cada dispositivo ou caixa tem seu próprio controle e gerenciamento, simples assim.

Por exemplo, quando você precisa ativar um protocolo de roteamento como OSPF o que é preciso fazer?

Entrar em cada dispositivo e configurar o OSPF no control plane de cada um deles manualmente, seja através da CLI (com ou sem script) ou uma interface Web, mesmo assim aplicar essa implementação (deploy) é uma tarefa feita dispositivo a dispositivo manualmente.

E após configurado cada dispositivo roda sua própria instância de OSPF localmente, portanto alterações mais uma vez precisam ser realizadas em cada dispositivo isoladamente.

Sem discutir vantagens e desvantagens de arquiteturas centralizadas em relação a distribuídas, a centralização do control plane permitiria, por exemplo, que alterações em vários dispositivos fossem mais simples, pois as informações de controle estariam centralizadas em um único ponto, facilitando a distribuição dessas novas regras para todos os dispositivos.

As redes programáveis e o SDN (Software Defined Network) normalmente utilizam-se desse conceito de arquitetura de rede centralizada (centralized architecture), com a separação e centralização do control plane em uma controladora ou “controller”.

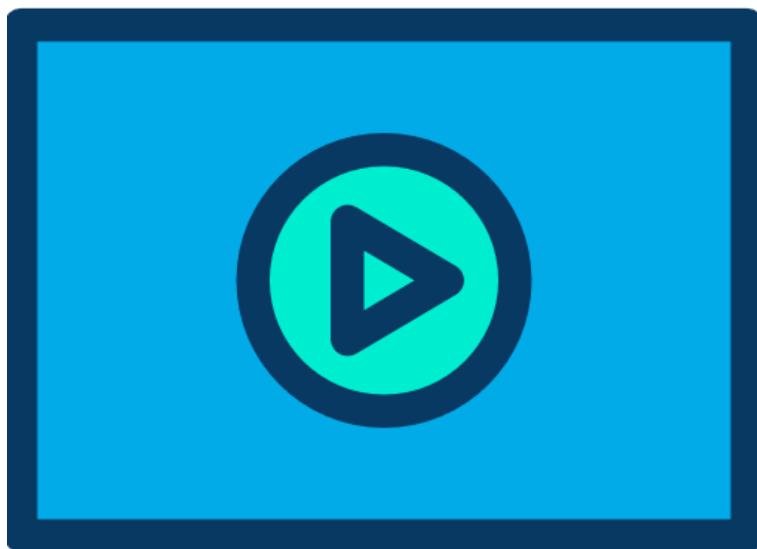
Essa controladora (controller ou SDN controller) tem, portanto, a função de centralizar o controle dos dispositivos de rede, sendo que o nível de controle pode variar conforme a implementação e/ou fabricante, indo de um controle completo de todas as funções do control plane, controle parcial ou até somente estar ciente do trabalho dos control planes distribuídos em dispositivos tradicionais.

Outro exemplo de controladoras é o que já estudamos quando falamos dos Access Points, que são as Wireless LAN Controllers, apesar de uma filosofia diferente do SDN, as WLCs permitem a configuração, gerenciamento e monitoração de uma rede de APs de forma centralizada, tirando a “inteligência” das pontas e centralizando as funções nelas.

Esse assunto inicia aqui, porém para quem está na trilha do CCNA 200-301 ele volta quando formos estudar Automação e Programabilidade.

Vamos a seguir estudar mais sobre as WLCs, o Cisco DNA Center (controladora para redes empresariais) e o ACI (sistema centralizado para Data Centers).

4.8.1 Wireless LAN Controllers



Nós já estudamos um exemplo disso quando tratamos dos Access Points (AP) para redes sem fio, por exemplo, um AP pode funcionar de forma autônoma, ou seja, cada dispositivo é controlado e configurado localmente, ou de forma centralizada com o uso de um Wireless LAN Controller ou WLC.

Nesse modo centralizado chamamos também de “Controller Based Network” ou Rede Baseada em Controladora.

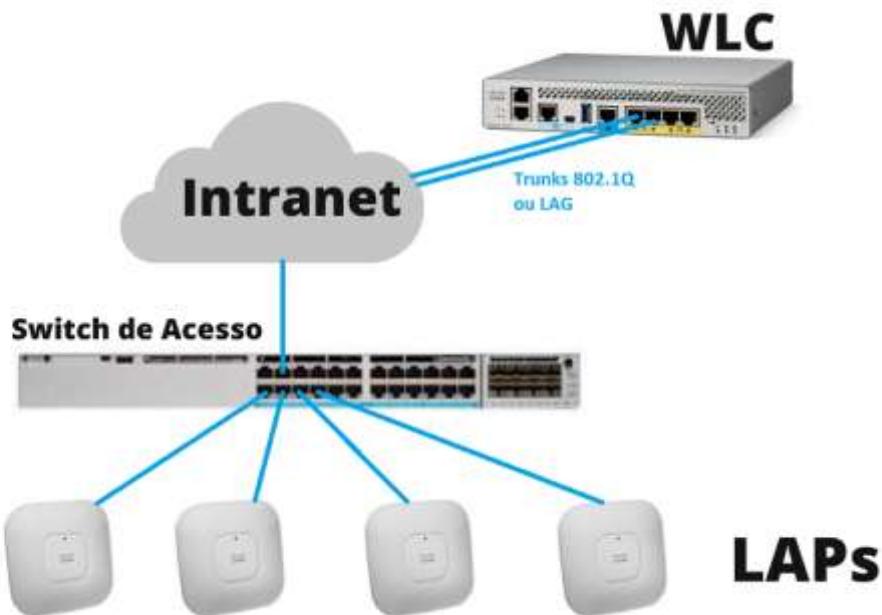
Imagine uma rede com 10 Aps, é relativamente simples entrar um a um e configurá-los, concorda? Vamos fazer algumas configurações básicas nesses 10 APs:

1. Fazer o login inicial no AP
2. Alterar usuário e senha de acesso
3. Definir um SSID (identificador da rede sem fio)
4. Definir o modo de segurança e criptografia da rede sem fio (WEP, WPA, WPA2, etc)
5. Definir o uso dos canais a serem utilizados e padrão 802.11, os quais podem ser escolhidos automaticamente também em Aps residenciais ou de pequenas empresas

Então temos a grosso modo 5 etapas para cada AP o que nos dá 50 passos para configurar essa rede, correto?

Agora aumenta isso para 1000 APs...
... **50x1000=50.000 passos para executar!**

Em uma rede com APs controlados por uma WLC isso seria reduzido drasticamente, pois essas configurações seriam realizadas na controladora e repassadas para os APs à medida que eles forem entrando na rede.



Portanto a principal vantagem de utilizar uma WLC em uma rede sem fio é eliminar a necessidade de configuração dos APs um a um, porém existem muitas outras vantagens no uso de WLCs.

Com uma WLC podemos ter funções em tempo real (Real Time Functions) e gerenciamento (Management Functions).

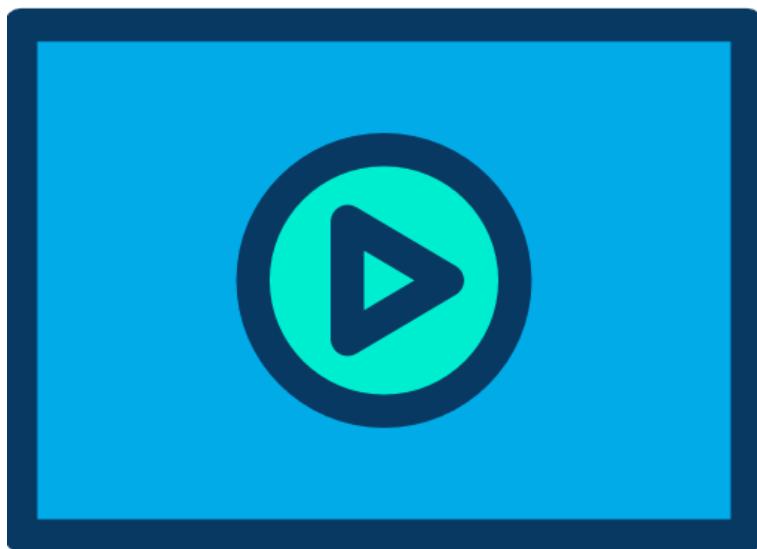
As funções em tempo real permitem analisar transmissão e recepção que estão sendo feitas via rádio freqüência, gerenciamento dos MACs (Media Access Control Layer) e criptografia.

Essas funções envolvem o envio de frames 802.11, mensagens como beacon e probe, realizar a criptografia dos dados em tempo real por pacotes.

Com as funções de gerenciamento o WLC pode gerenciar as rádios freqüências, fazer a associação de APs e roaming (movimentação entre diferentes células sem queda da conexão), autenticação dos clientes, políticas de segurança e qualidade de serviços (QoS).

Tudo isso de forma centralizada!

4.8.2 Cisco DNA Center



O Cisco DNA Center é o sistema de gerenciamento de rede, controladora e plataforma de análise de redes da Cisco, ele é o elemento chave da nova filosofia de redes baseadas em intenções da Cisco ou IBN (Intent-Based Network).

Além do gerenciamento e da configuração do dispositivo, o Cisco DNA Center oferece às equipes de TI a capacidade de:

- Controlar o acesso por meio de políticas usando o acesso definido por software ou SD-Access.
- Provisionar automaticamente por meio do Cisco DNA Automation.
- Virtualizar dispositivos por meio da virtualização de funções de rede da Cisco ou Network Functions Virtualization (NFV).
- Reduzir riscos de segurança por meio de segmentação e análise de tráfego criptografado ou Encrypted Traffic Analysis (ETA).

Além disso, o Cisco DNA Assurance coleta dados de telemetria de dispositivos em toda a rede e usa AI ou em português IA (Inteligência Artificial) e aprendizado de máquina (machine learning) para ajudar a garantir o alinhamento da operação da rede com a intenção do negócio.

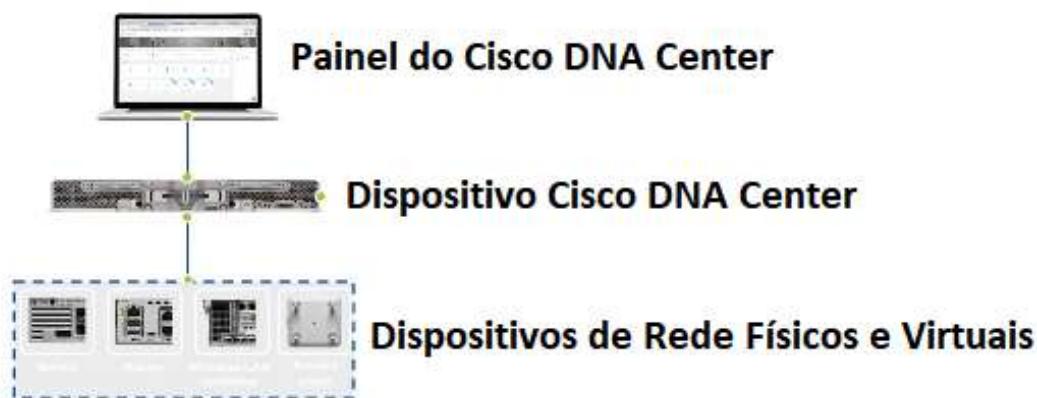
Ao fazer isso, o Cisco DNA Assurance otimiza o desempenho da rede, aplica políticas de rede e reduz o tempo gasto em tarefas mais simples e repetitivas de solução de problemas.

A plataforma Cisco DNA Center também oferece extensibilidade de 360 graus (360-degree extensibility) com um amplo ecossistema de parceiros e ISVs (Independent Software Vendors ou Desenvolvedores de Software Independentes) que permitem tornar a rede ágil e totalmente sintonizada com as prioridades dos negócios.

O DNA Center da Cisco é o único sistema de gerenciamento de rede centralizado a trazer toda essa funcionalidade para um único plano.

Resumindo a operação do Cisco DNA Center, a infraestrutura de rede programável envia dados para o dispositivo Cisco DNA Center, o qual ativa recursos nos componentes de rede usando o software Cisco DNA e tudo é gerenciado a partir do painel do Cisco DNA Center.

Cisco DNA Center



Dica: É necessário ter uma licença do software Cisco DNA para cada roteador, switch, WLC e access point sem fio.

4.8.2.1 RESUMO DOS RECURSOS E BENEFÍCIOS DO Cisco DNA CENTER

Gerenciamento

- Visualização granular de toda a rede, a partir de um único painel
- Gerenciamento do ciclo de vida do dispositivo
- Integração de vários domínios
- Aberto e extensível

Automação

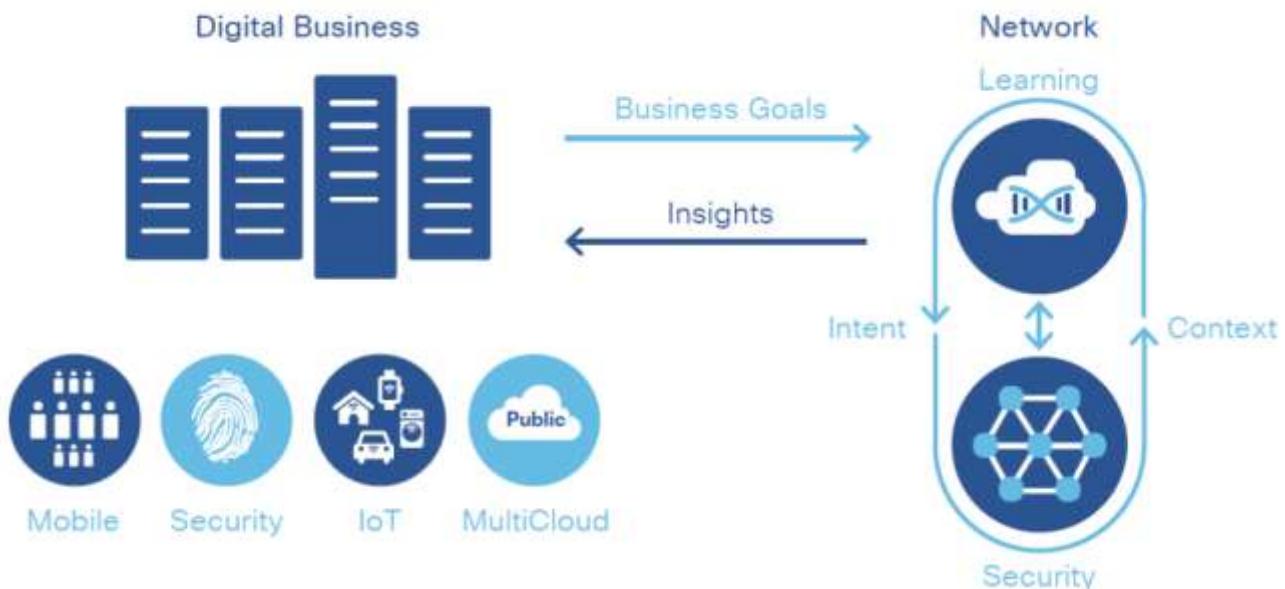
- Descoberta de dispositivos automatizada
- Criação de política Drag-and-drop (de arrastar e soltar)
- Implantação automatizada de dispositivos e gerenciamento do ciclo de vida
- Qualidade de serviço (QoS) automatizada
- Uso de Controladoras e APIs abertos

Análise de IA/ML

- Tudo como um sensor
- Análise guiada por contexto
- Mais de 150 insights úteis
- Análise de IA no local e na nuvem

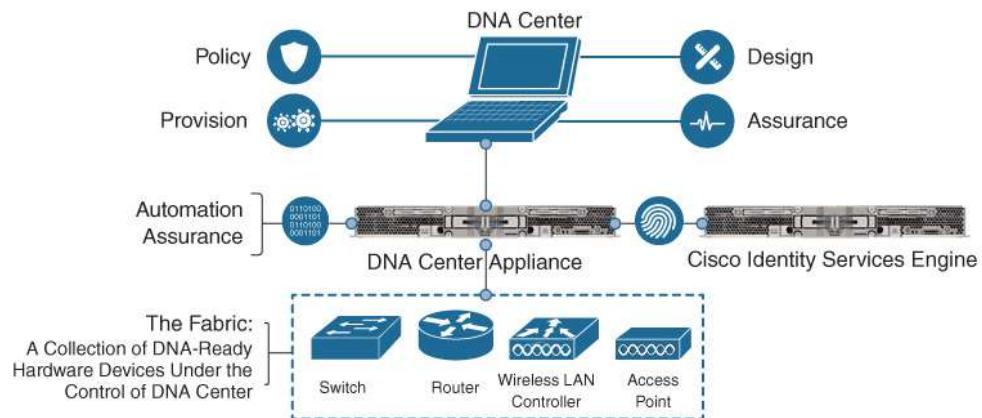
Segurança

- Detecção e resposta a ameaças
- Integração entre o Stealthwatch e o ISE
- Análise de tráfego criptografado (ETA)
- Segmentação extremamente segura



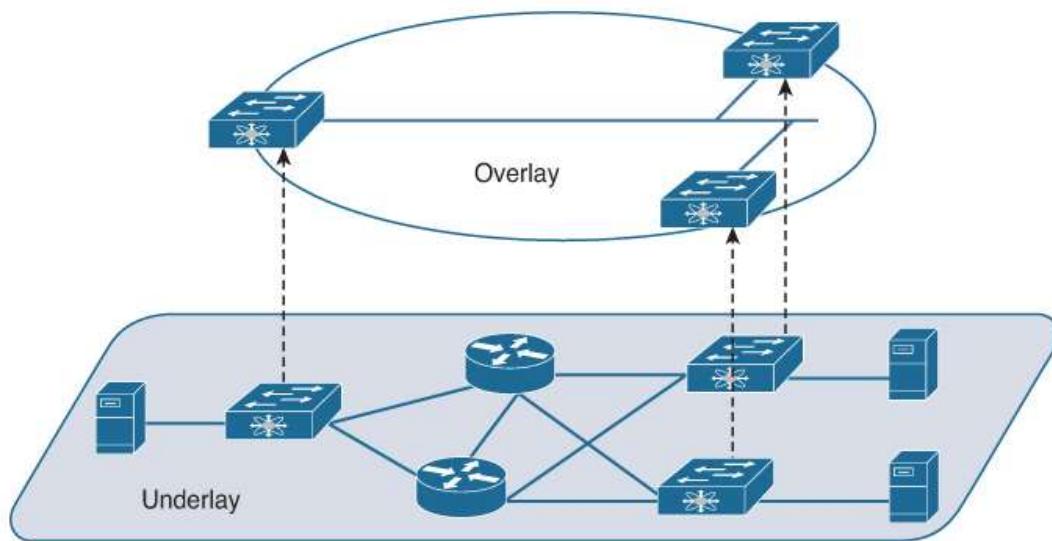
4.8.2.2 UNDERLAY, OVERLAY E FABRIC

O Cisco DNA Center na prática separa a rede física da rede lógica.



A rede física com seus equipamentos passa a se tornar um Underlay (camada inferior) que conectará os endpoints de uma forma que não precisamos mais nos preocupar com a rede física. Uma vez montado o Underlay dificilmente precisaremos configurá-los novamente.

Essa conexão entre os endpoints é feita no Overlay (camada superior), o qual forma o “Fabric”.



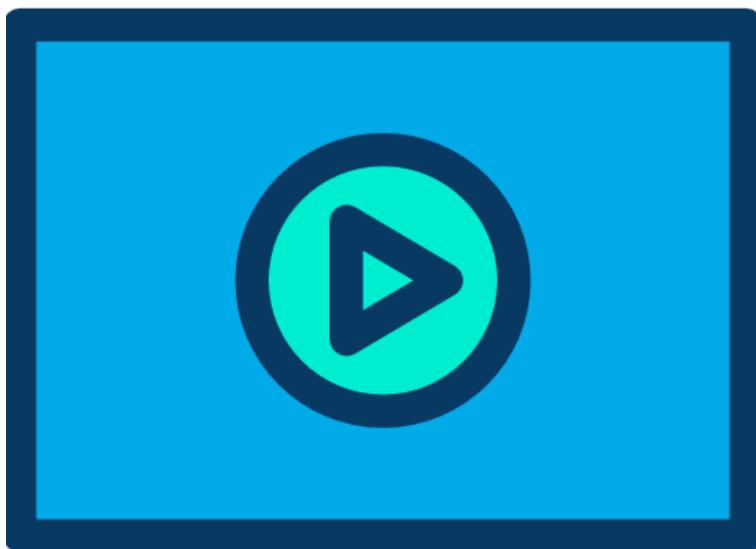
O Fabric é a combinação da parte lógica do Overlay com a parte física da Rede que está suportando tudo isso.

Veja que o conceito de Underlay/Overlay não é novo, ele é utilizando no CAPWAP, GRE, MPLS VPNs e outras tecnologias. Por exemplo, um túnel VPN usa toda a infraestrutura para conectar duas redes distintas de forma segura sem ao menos essas duas redes ter que interagir com os dispositivos que estão no meio do caminho entre elas, concorda?

Portanto, em uma rede que utiliza o SD-Access e o DNA Center, quando dois servidores, hosts, computadores ou endpoints quaisquer quiserem se comunicar é como se eles estivessem conectados à rede superior, sem a complexidade da rede inferior do desenho anterior.

Na prática é criada uma VXLAN entre os dispositivos para que eles se comuniquem. (Esse assunto foge do escopo desse curso e será tratado em cursos mais avançados).

4.8.3 ACI (Application Centric Infrastructure - Datacenter)



O Application Centric Infrastructure ou simplesmente ACI é a solução Cisco similar ao DNA Center, porém voltada para Data Centers.

O ACI ao invés de pensar primeiro na rede tem um foco inicial nas aplicações e cria uma infraestrutura ao redor dessas aplicações.

Um exemplo disso é a maneira que o ACI trata as rotinas de iniciar, parar e mover VMs em um Data Center.

Por exemplo, algumas VMs precisam ter comunicação entre si e outras não, assim como elas podem ter a necessidade de movimentação nesse ambiente virtualizado em nuvem, por isso ter uma implementação/configuração por interface de switch ou roteador pode tornar o sistema mais travado e não tão flexível e elástico como um ambiente em nuvem precisa, muitas vezes essa visão pode até dificultar o “self-service” necessário para implementação de serviços em nuvem como estudamos nos tópicos anteriores.

Portanto a Cisco definiu para o ACI o conceito de endpoints e policies (terminais e políticas), onde os endpoints são VMs ou até mesmo servidores físicos.

Como vários endpoints tem as mesmas necessidades eles podem ser agrupados e ter políticas comuns entre si, ou seja, ter políticas por grupos de VMs ou servidores.

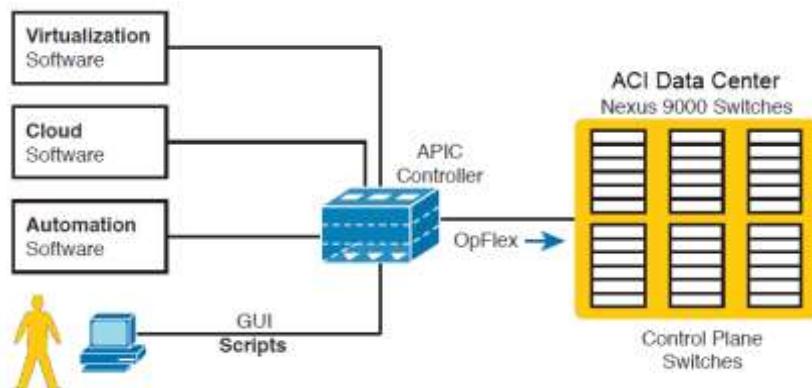
Essas políticas podem definir como esses endpoints e seus grupos podem se comunicar (ou não) entre si e entre outros grupos. Além disso, parâmetros de QoS e outros serviços podem estar definidos nessa política.

Uma coisa deve ter ficado claro no parágrafo anterior, em nenhum momento foi falado em VLAN, link, porta ou coisas desse tipo, certo? Isso porque agora temos uma visão da rede centrada em aplicações ou “application-centric”.

Uma vez definidos os endpoints, grupos, políticas e demais detalhes a controladora vai direcionar a rede para que os objetivos definidos sejam cumpridos, ou seja, ela vai configurar as tabelas de encaminhamento para que a rede atue da forma definida.

Com isso a rede vai reagir corretamente aos processos como inicialização, parada ou movimentação das VMs ou servidores do Data Center.

Na arquitetura definida pelo ACI a controladora chama-se Application Policy Infrastructure Controller ou APIC, portanto o APIC tem a função de centralizar a criação e aplicação das políticas na infraestrutura do data Center, conforme mostra a figura a seguir.



O APIC pode ser configurado por interface gráfica (GUI) e o poder de programar a rede através do controle via software.

Além disso, os softwares de virtualização, nuvem e automação (virtualization, cloud e automation software) e até mesmo scripts escritos pelos administradores de redes podem definir os grupos de endpoint, políticas e assim por diante dentro do APIC.

Tudo isso sem que o administrador de redes e sua equipe precisem entrar nos equipamentos via CLI e configurá-los.

Mais tarde nesse mesmo curso vamos estudar as topologias de rede e dentro delas vamos ver o Spine and Leaf, a qual é a estrutura utilizada pelo ACI.

5 Topologias de Rede

Os dispositivos de rede, sejam eles quais forem, devem seguir uma arquitetura tanto física como lógica que permita uma fácil administração, crescimento, manutenção, gerenciamento e controle.

Para isso devemos definir uma Arquitetura dessa Topologia de rede.

Nesse capítulo vamos estudar as mais importantes tanto para nossa vida profissional como para o exame CCNA, mas antes vamos fazer um exercício que não tem uma resolução correta...

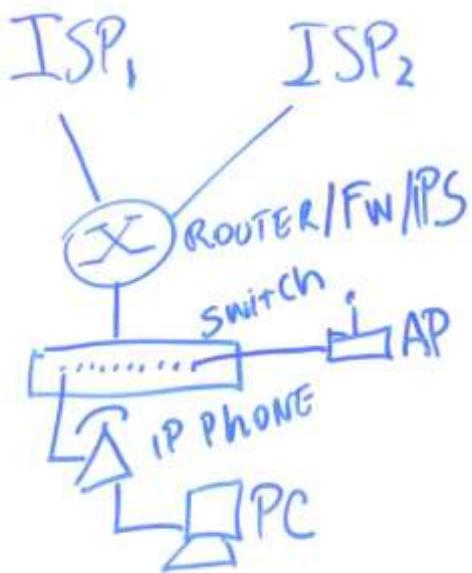
... "como assim?" Você deve estar se perguntando!

Pegue papel e caneta, de preferência, e faça um esboço da topologia de rede da sua casa e da empresa que você trabalha.

Sobre a empresa, se você trabalhar em uma empresa muito grande, desenhe o que você imagina que seja a topologia, não precisa ser exato nem perfeito.

Leve em conta o que estudamos até o momento e coloque onde estão os dispositivos de rede: roteadores, switches, access points e endpoints.

Eu fiz um desenho simples da topologia que utilizamos em nosso escritório, que é basicamente um Router-on-a-stick, ou seja, um roteador com um switch "pendurado" nele.



Não coloquei todos os pontos de rede, fiz somente um endpoint que usa um Telefone IP com o lap-top conectado à ele, chegando em um switch de acesso, o qual também conecta nossos APs e por fim esse mesmo switch é conectado a um roteador que tem duas saídas de Internet.

Bem simples, sendo que o roteador faz a função de roteador, central telefônica IP, Firewall e IPS, tudo em apenas um dispositivo.

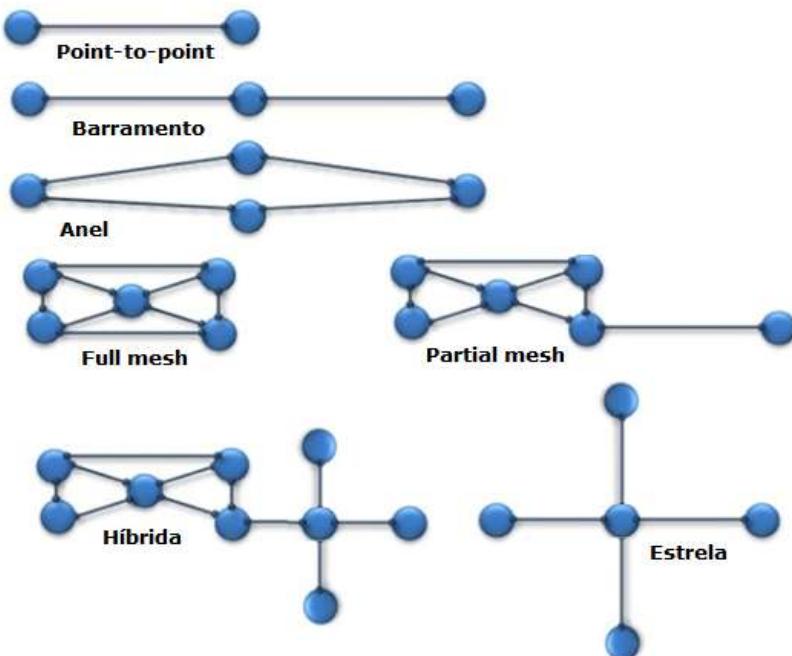
Você vai estudar a seguir que essa é uma topologia típica de um pequeno escritório ou small office.

5.1 Como Podemos Conectar Dispositivos em Rede?

Vamos começar fazendo uma conversa sobre como podemos conectar os dispositivos de rede.

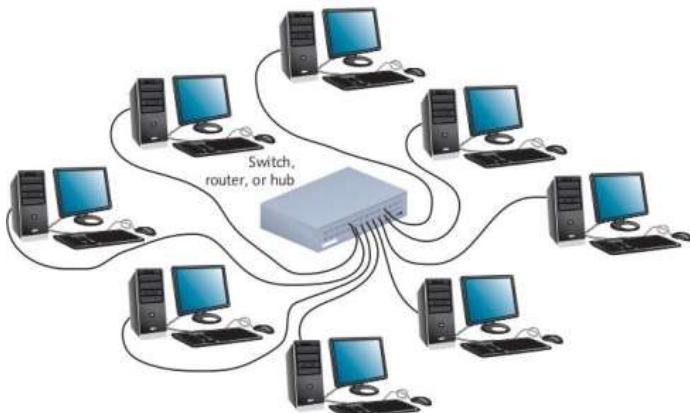
Basicamente podemos ter dispositivos conectados das seguintes maneiras:

- **Ponto a ponto ou point-to-point:** principalmente utilizadas em links WAN.
- **Barramento:** em desuso, mas pode representar logicamente redes Ethernet.
- **Anel ou ring:** utilizada em redes SDH (telecomunicações).
- **Em estrela ou star:** topologia física dos switches e hubs.
- **Conexão total ou malha completa ou full mesh:** muito difícil de ser implementada em topologias físicas devido ao grande número de interfaces, porém utilizada como topologia lógica por diversas tecnologias.
- **Conexão parcial ou malha mista ou partial mesh:** muito utilizada em redes e telecomunicações.
- **Híbrida ou hybrid:** também muito utilizada nas topologias 2 tier e 3 tier.

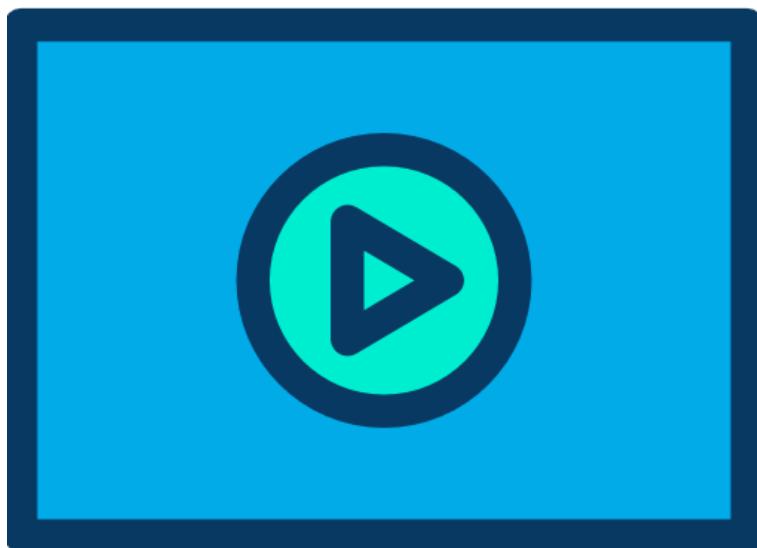


Lembre-se que existem dois tipos de topologia: a **física** e a **lógica**.

Por exemplo, um hub ou switch tem a topologia física em estrela, mas logicamente muitas bibliografias tratam essas conexões como se fossem um barramento.



5.2 Small Office/Home Office (SOHO)



Se você traduzir literalmente esses nomes você terá: pequeno escritório/escritório em casa.

Essas topologias ou arquiteturas de rede são as mais conhecidas porque já utilizamos em nossas casas, pois trabalhando ou não remotamente você tem um ponto de acesso à Internet, seus computadores, smartphones, tablets e demais endpoints conectados à sua rede normalmente.

5.2.1 Home Office

Para trabalhar em home office o usuário vai precisar de um acesso à Internet e uma maneira de acessar os serviços de rede, aplicativos e arquivos da empresa de forma remota.



Normalmente os dispositivos de rede são pequenos com poucos requisitos de número de portas, sendo que na maioria dos casos o acesso dos endpoints é realizado via rede sem fio, utilizando um padrão 802.11.

Existe a possibilidade de conexão utilizando cabo UTP (metálico), porém é algo mais raro ou devido a algum requisito de segurança muito específico.

O roteador que conecta os endpoints até a Internet é geralmente um roteador sem fio, o qual se conecta com o provedor de serviços de Internet ou ISP (Internet Service Provider) utilizando uma tecnologia de última milha como ADSL, Cable Modem ou links de Fibra Óptica (FTTH – Fiber to the Home).

Esse roteador sem fio ou wireless router tipicamente possui uma entrada para conectar a Internet, um pequeno switch integrado com 4 portas (densidade mais comum de portas) e um access point (AP) interno, tudo isso integrado ao mesmo dispositivo.

Se os aplicativos, arquivos ou o que o trabalhador remoto tenha que utilizar estiverem em uma nuvem pública ou servidores da empresa que estão diretamente conectados à Internet não é preciso mais nada para que esse funcionário desempenhe suas tarefas.

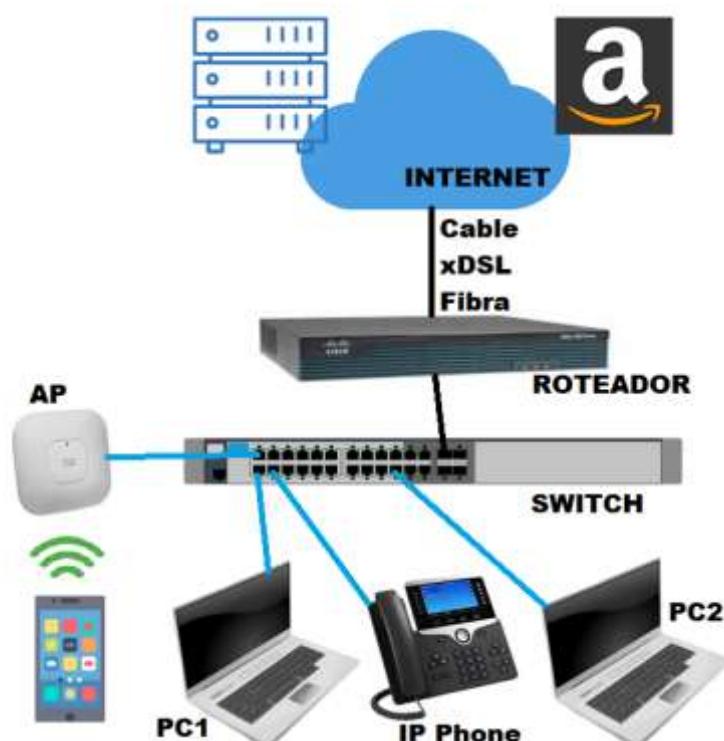
Já se houver a necessidade de conexão com uma nuvem privada ou então à servidores que estão dentro da rede da empresa será necessário ainda fechar ou estabelecer uma VPN (Virtual Private Network) para proteger os dados que serão trafegados entre o trabalhador remoto e a empresa.

Essa VPN pode ser realizada do roteador para empresa ou então com um cliente que pode ser instalado diretamente no PC ou no Smart Phone do funcionário remoto.

Note que essa arquitetura serve tanto para um trabalhador remoto como para um pequeno escritório, onde as exigências não sejam tão grandes com relação ao suporte de tecnologias e ferramentas para monitoração remota da rede. Normalmente esses dispositivos pertencem ao ISP e não permitem tanto controle por parte da empresa.

5.2.2 Small Office ou Branch Office

Em empresas e pequenos escritórios remotos (branch offices) a topologia de rede mais comum segue o desenho que fizemos sobre ao escritório da nossa própria empresa, veja figura abaixo com um desenho “mais caprichado”.

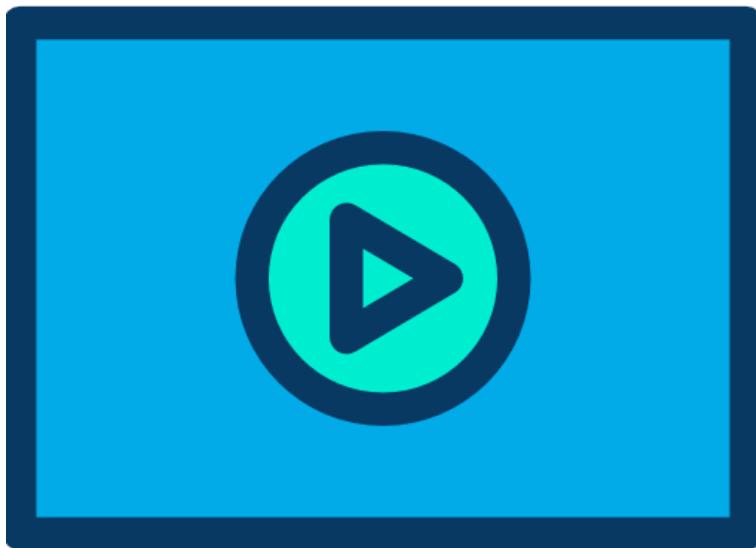


Portanto em uma empresa normalmente teremos:

- Um switch ethernet para conectar os endpoints que precisem de UTP como meio físico (par metálico), assim como para conectar um AP.
- O wireless access point ou AP para conectar dispositivos sem fio à rede, tais como smart phones, tablets e até mesmo computadores e lap-tops (PCs).
- Um roteador para encaminhar os pacotes IP de forma transparente para a Internet, saindo para uma nuvem pública, privada ou para a rede privada remota sem que o cliente precise instalar nenhum aplicativo em sua máquina.
- Um firewall, o qual pode estar integrado no próprio roteador que se conecta à Internet, por isso mesmo ele foi omitido da figura.

Essa rede pode ter um ou mais switches, uma ou mais saídas de Inernet, tudo depende da quantidade de usuários e necessidade de redundância do escritório.

5.3 Two Tier



Você notou uma coisa nas topologias anteriores? O que elas têm em comum?

Ambas têm apenas uma camada na LAN, seja somente com um roteador wireless ou na topologia com switch separado temos apenas uma camada na LAN. O porquê é simples: quantidade de usuários pequena ou, falando em termos mais técnicos, baixa densidade de portas.

Normalmente com a topologia anterior você pode até ter mais um ou dois switches conectados em cascata com o primeiro switch, mas imagine que sua rede comece a crescer e você vá inserindo switches até chegar 40 switches na rede...

Vamos fazer umas contas aproximadas... ao conectar um switch na rede precisamos de no mínimo duas conexões para termos redundância, portanto para conectar TODOS os switches precisaríamos de no mínimo 39×2 conexões, ou seja, aproximadamente 78 portas para interconectar esses switches.

E como vamos conectar esses switches?

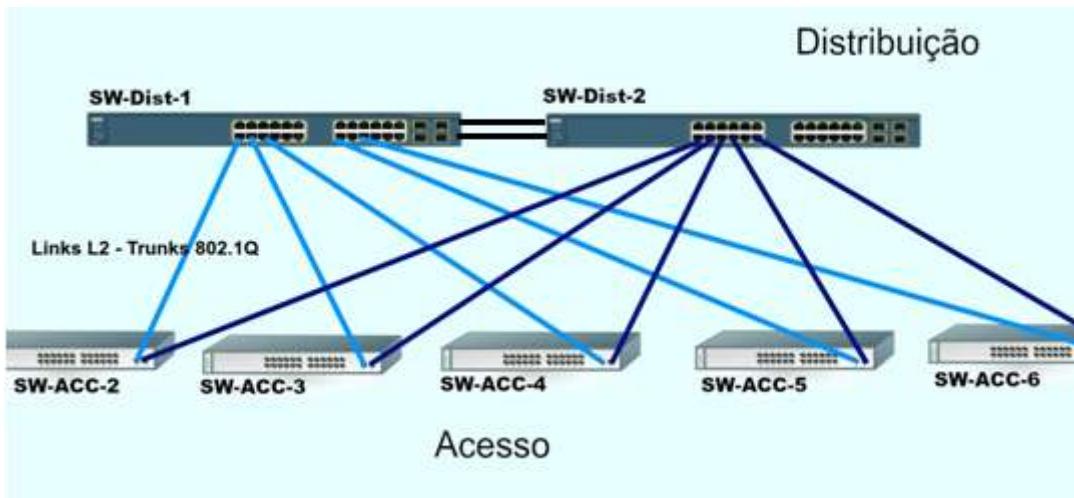
Podemos conectar todos os switches entre si, formando uma cascata de switches, ou então conectar todos os switches a um switch central em estrela, todos entre si formando uma rede full mesh... ou seja, as opções são inúmeras, porém os problemas também.

Se formos conectar em cascata, se perdemos a conexão com o segundo switch nenhum computador abaixo dele acessa mais a Internet. Se conectarmos todos a um switch em estrela, se esse switch central falhar, toda a rede para. Conexões full mesh entre 40 switches seriam necessárias no mínimo 39 interfaces por switch somente para conexão aos seus vizinhos.

Então como resolver esse problema? O nome do tópico já diz tudo!

O que é uma arquitetura **2 tier** ou em **duas camadas**?

É dividir a LAN em dois tiers ou camadas (óbvio rsrs), sendo uma camada para conectar os endpoints (chamada de acesso ou access) e a segunda para conectar os switches da camada inferior (chamada distribuição ou distribution).



Portanto, utilizamos dois switches na distribuição para conectar os switches de acesso.

Note que essa topologia tem uma regra de conexão entre os switches de acesso e distribuição, você deve conectar um switch de acesso a cada um dos switches de distribuição, garantindo redundância de link e equipamento.

Se um link ou uplink entre o switch de acesso e distribuição cair, teremos um segundo link para continuar o tráfego de dados.

E se um dos switches de distribuição falhar, ficar sem energia ou tiver uma quebra qualquer, o segundo switch assume a rede.

Isso garante no mínimo 99,9% de disponibilidade da rede LAN, ou seja, 8 horas e 46 minutos no máximo de downtime (indisponibilidade da rede) por ano.

Além disso, em uma arquitetura 2 tier, a camada de distribuição pode conectar os dispositivos que fazem conexão com a rede WAN, Internet e os servidores corporativos.

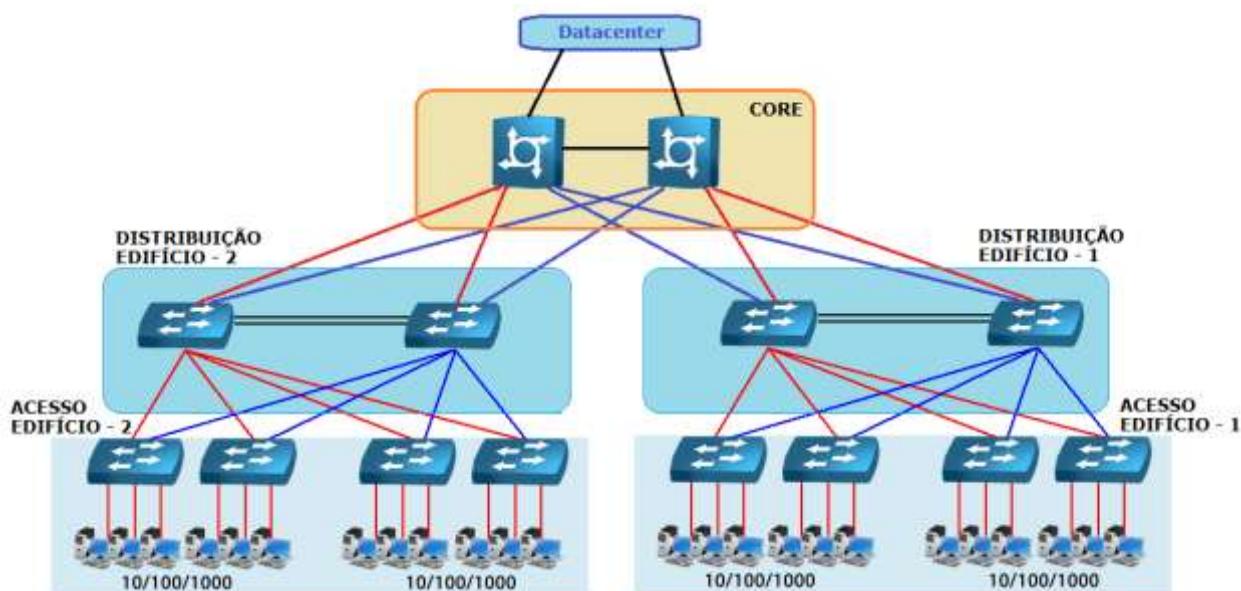
Note que essa topologia é um exemplo de arquitetura híbrida, pois ela usa no acesso uma arquitetura em estrela e entre acesso e distribuição partial mesh.

A arquitetura em 2 camadas ou 2 tier é também conhecida como "**Collapsed Core**" ou **Core Colapsado**, você vai entender o porquê no próximo tópico.

5.4 Three Tier



Esse é o modelo tradicional e mais utilizado até os dias de hoje em projetos de redes mais complexas, dividindo a rede em três camadas: **Acesso, Distribuição e Núcleo (Access, Distribution e Core)**. Veja a figura abaixo.



Nessa topologia temos um campus com switches de acesso em seus andares, os quais são agregados nos switches de distribuição em cada edificação, normalmente switches layer-3.

Por sua vez os switches de distribuição dos diversos prédios são agregados em um ou mais switches de núcleo, conforme a necessidade de redundância e porte da rede.

Note que no acesso ou access estão os switches onde conectamos os dispositivos dos usuários, a distribuição ou distribution agrupa os switches de acesso em blocos, os quais por sua vez são interconectados através do núcleo ou core da rede.

Note que essa estrutura permite que qualquer usuário na camada de acesso se comunique com outro dando no máximo três saltos entre switches, ou seja, o diâmetro da rede é fixo e sempre bem conhecido.

Resumindo, as funções de cada camada são:

- **Acesso - Access Layer:** Fornece conectividade aos grupos de trabalho, estações, Access points, telefones IP, estações de vídeo conferência, etc. Eles não encaminham quadros diretamente entre si em condições normais, sempre os quadros passam pela distribuição para chegar a diferentes switches de acesso.
- **Distribuição - Distribution Layer:** Faz a conectividade ou agregação entre as diversas camadas de acesso intermediando os dados entre a camada de acesso e o Core da rede com base em políticas. Normalmente formam blocos de switches que podem ser prédios ou grupos de setores de uma empresa. Eles fazem o encaminhamento dos quadros e pacotes entre os switches de acesso, porém normalmente não conectamos endpoints diretamente aos switches de distribuição.
- **Núcleo - Core Layer:** Fornece agregação dos switches de distribuição chaveamento rápido entre eles.

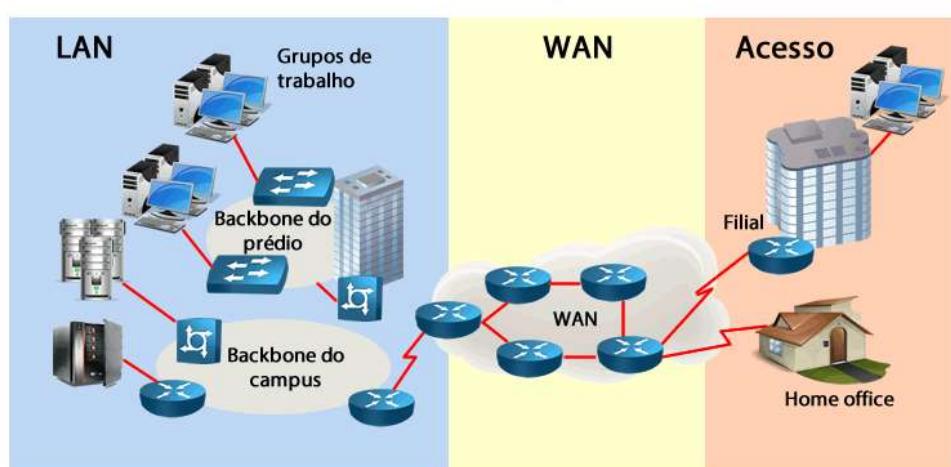
A vantagem desse modelo é a possibilidade de termos links de backups na camada de acesso, assim como links e equipamentos backups nas camadas de distribuição e núcleo, o que possibilita um modelo altamente redundante, ou seja, com uma alta disponibilidade (tolerante a falhas – fault tolerant).

5.5 WAN

Nos itens anteriores estudamos topologias típicas de uma rede LAN com o SOHO, 2 tier e 3 tier, mas agora você precisa interconectar as diversas redes locais da sua empresa que estão situadas distantesumas das outras, para isso podemos utilizar redes **MAN** (redes metropolitanas ou **Metropolitan Area Networks**) e **WAN** (redes de longa distância ou **Wide Area Network**).

O que é uma WAN?

Wide Area Network
(Rede de Longa Distância)



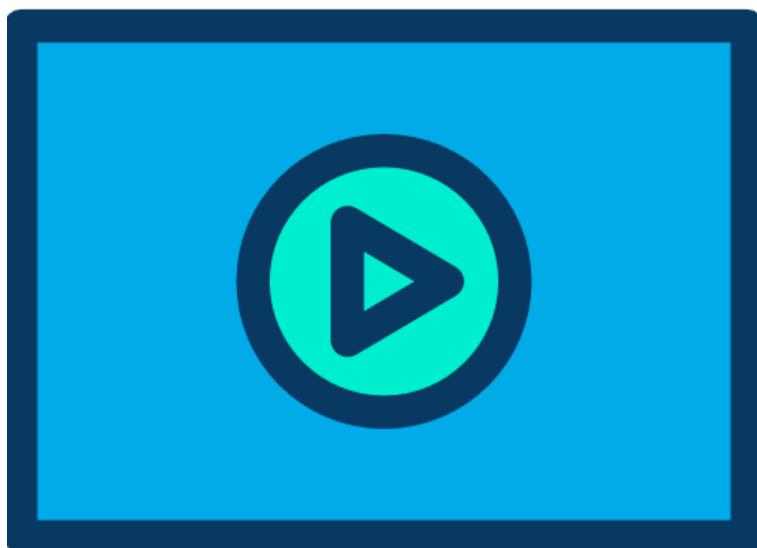
Na prática acabamos chamando qualquer link entre duas unidades de WAN, por isso não se preocupe com essa terminologia, vamos utilizar no CCNA apenas os termos LAN, para redes locais, e WAN para conexões entre as unidades.

Temos duas opções para conectar unidades distantes umas das outras: construir a própria infraestrutura (normalmente realizada para distâncias muito curtas) ou utilizar um Provedor de Internet (ISP – Internet Service Provider) ou de Serviços de Telecomunicações (SP ou Service Provider).

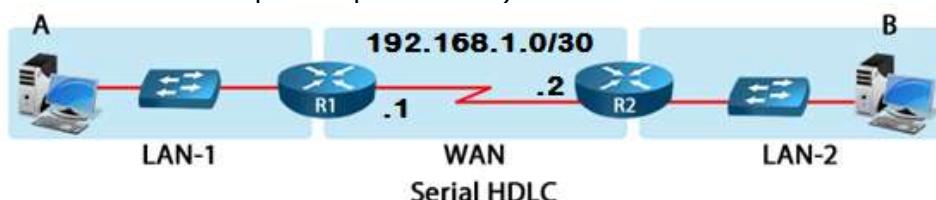
Na WAN podemos encontrar topologias ponto a ponto, full mesh, partial mesh e alguns termos mais específicos como hub-and-spoke e ponto para multiponto (point-to-multipoint).

As tecnologias também podem ser diferentes do que utilizamos normalmente em uma LAN corporativa, pois um service provider tem dois problemas que as empresas (segmento Enterprise) não tem: distância e volume de clientes.

5.5.1 Tecnologias Ponto a Ponto e Hub-and-spoke



São redes que tem apenas dois pontos, portanto precisam de apenas dois endereços de camada-3, normalmente redes /30 ou /31, apesar da última não ser tão comum em campo é uma opção de uso se os roteadores suportarem essa máscara (vamos estudar máscaras e endereços IP nesse curso em capítulos posteriores).



Em redes ponto a ponto utilizamos tecnologias como PPP e HDLC para realizar a conexão lógica (camada-2) e links dedicados via fibra óptica ou pares metálicos para realizar a conexão física entre os dispositivos, porém essas tecnologias estão cada vez mais caindo em desuso.

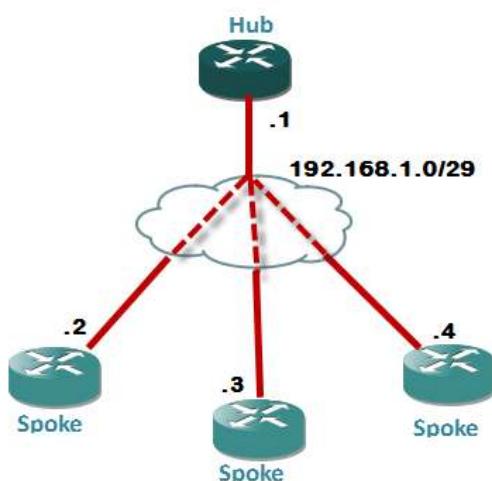
Apesar que existe o serviço ethernet ponto a ponto provido pela Metroethernet chamado “**Ethernet Line Service**” ou **E-Line**.

As redes Hub and Spoke são redes muito comuns nas tecnologias Frame-relay, DMVPN (Dynamic Multipoint VPN), metroethernet E-LAN (full mesh) e E-Tree (hub-and-spoke, partial mesh ou ponto-a-multiponto).

No hub-and-spoke temos um roteador (chamado de Hub ou matriz) e vários Spokes (chamados de unidades remotas).

Para que os Spokes falem entre si eles precisam passar pelo Hub, ou seja, o Hub faz o papel de ponto focal da rede e tem a função de fazer acesso entre as unidades remotas ou até com outros serviços de rede como a Internet.

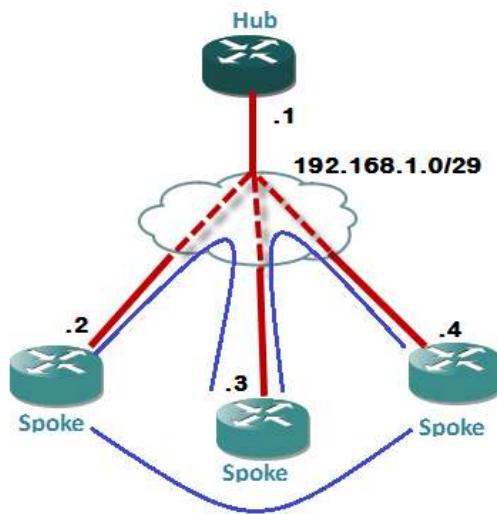
Nesse tipo de topologia normalmente utilizamos uma rede IP que comporte o número de componentes da rede, pois eles compartilham a mesma rede ou sub-rede IP. Veja no exemplo abaixo.



A topologia Hub and Spoke na realidade é uma topologia “**partial mesh**”, ou seja, não tem a totalidade de links interconectados entre si.

A topologia full meshed ou full mesh faz conexão de todos os links possíveis entre os sites da empresa, ou seja, não é preciso de intermediário para que dois pontos se comuniquem como no hub and spoke, pois todos os componentes da rede têm links entre si.

Veja exemplo abaixo onde fizemos as conexões faltantes para que o exemplo do hub and spoke fosse convertido em uma rede full mesh.

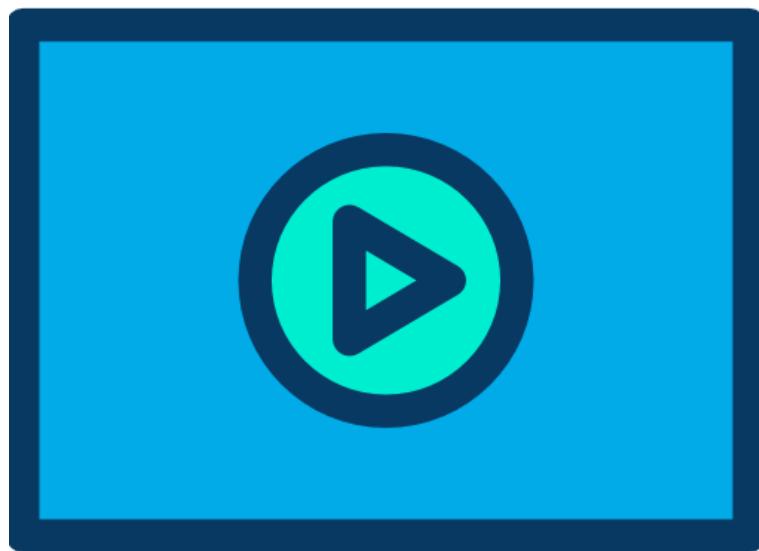


Note que agora existem links entre todas as unidades, ou seja, não é necessário mais do Hub para que os spokes falem entre si.

Se você prestar bastante atenção a topologia parece o rosto de um palhacinho... só para descontrair... (risos)

Em comparação a topologia full mesh é muito mais cara que a hub and spoke ou partial mesh, pois ela vai precisar de muito mais links, sejam eles físicos ou virtuais, para completar a topologia.

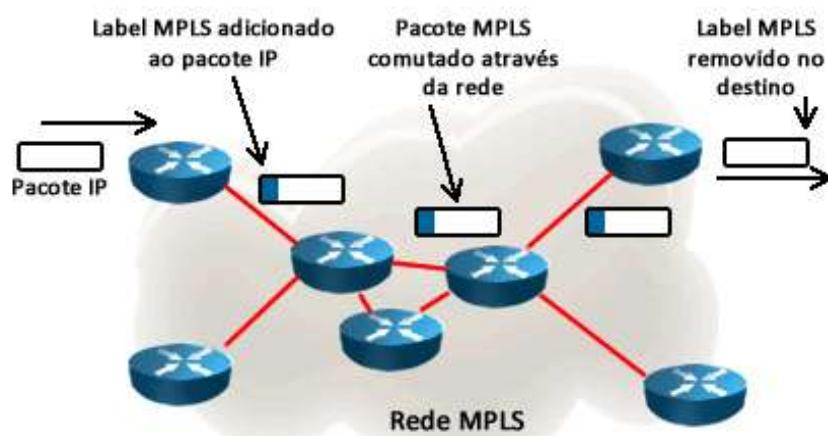
5.5.2 MPLS - MultiProtocol Label Switching



O **MPLS** ou **MultiProtocol Label Switching** é uma tecnologia de encaminhamento de pacotes baseada em rótulos (labels) que funciona com base na adição de um rótulo (label) nos pacotes de tráfego na entrada do backbone (chamados de roteadores de borda) e, a partir daí, todo o encaminhamento pelo backbone passa a ser feito com base neste rótulo.

Comparativamente ao encaminhamento de quadros realizados pelos protocolos de camada-2 que estudamos até o momento, o MPLS torna-se mais eficiente uma vez que dispensa a consulta das tabelas de roteamento.

Outra vantagem do MPLS é de ser indiferente ao tipo de dados transportado, podendo ser tráfego IP ou qualquer outro protocolo de camada 3. O MPLS atua praticamente como um protocolo de camada-3, em algumas bibliografias chegam a colocá-lo como um protocolo de camada "2,5", ou seja, entre as camadas 2 e 3 do modelo OSI. Veja a figura abaixo com a topologia típica do MPLS.

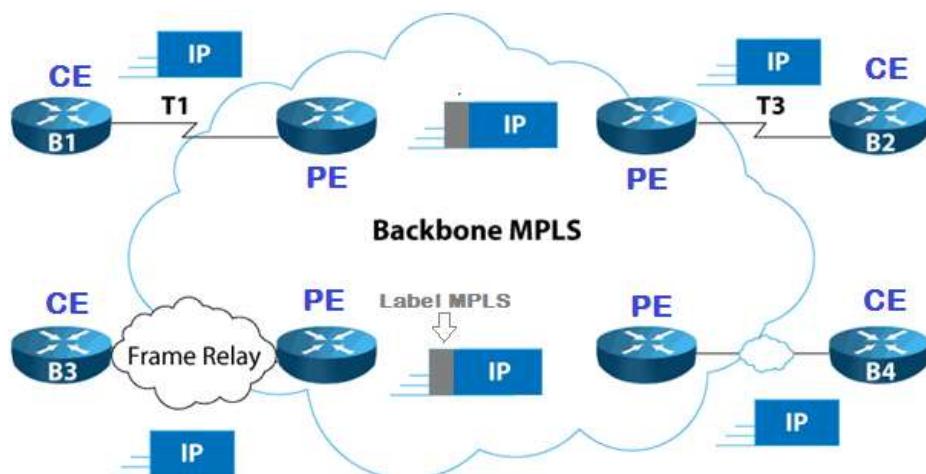


Este protocolo permite a criação de Redes Virtuais Privadas (VPNs) garantindo um isolamento completo do tráfego com a criação de tabelas de "labels" (usadas para roteamento) exclusivas de cada VPN.

Além disso, é possível realizar QoS (Quality of Service) com a priorização de aplicações críticas, dando um tratamento diferenciado para o tráfego entre os diferentes pontos da VPN.

O QoS cria as condições necessárias para o melhor uso dos recursos da rede, permitindo também o tráfego de voz e vídeo, sendo um dos diferenciais do MPLS.

Com o MPLS podemos utilizar diversas tecnologias como links de acesso, pois sua missão é "etiquetar" os pacotes e encaminhá-los através da rede.



Portanto não se assuste ao verificar nos roteadores da empresa onde você trabalha a rede MPLS utilizando links frame-relay ou PPP chegando a sua interface serial ou gigabitethernet.

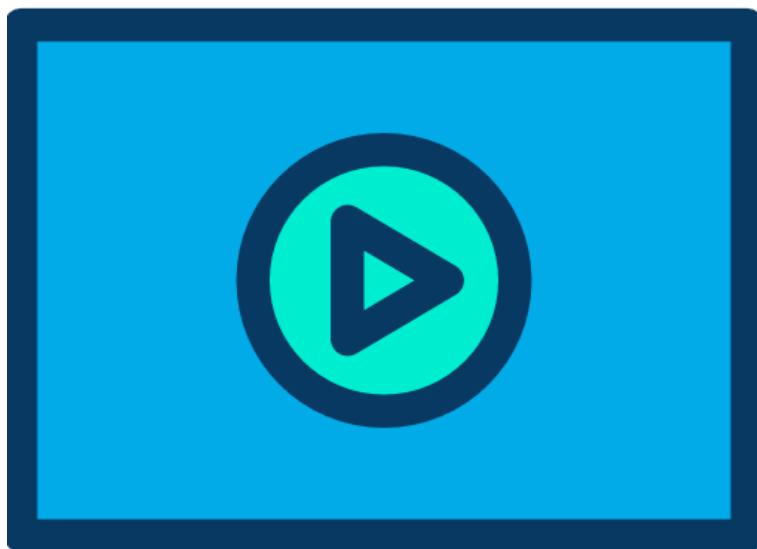
Como toda tecnologia de WAN o MPLS tem algumas terminologias próprias, sendo que o mais importante são os termos: **Customer Edge (CE)** e **Provider Edge (PE)**.

O customer edge (CE) é normalmente um roteador que está no lado do cliente, em inglês "customer site", ou seja, na empresa que está adquirindo o serviço de conexão via MPLS.

Já o provider edge (PE) fica nas pontas do provedor de serviços (SP – Service Provider), na outra ponta do link de acesso que conecta à rede do cliente com a rede do provedor de serviços.

Analizando a figura anterior podemos dizer que B1 a B4 são roteadores CEs e os roteadores sem nome, os quais estão dentro do backbone MPLS são os PEs.

5.5.3 Metro Ethernet



Utilizar redes Ethernet em áreas Metropolitanas e geograficamente distribuídas através do uso conjunto da tecnologia Ethernet permite que links de 100Mbps até 10Gbps sejam utilizados através de fibra óptica para acesso entre os provedores de serviços e seus clientes.

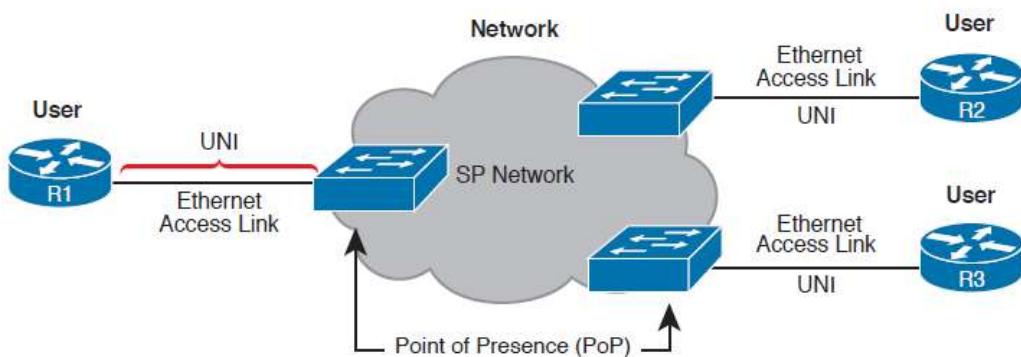
Utilizando esse tipo de serviço para o cliente existe a impressão de que ele tem um link ethernet ponto a ponto, pois a meio de transmissão entre os dispositivos da operadora é transparente para o cliente.

Falando mais especificamente da rede “metropolitan-area Ethernet”, “Ethernet MAN” ou “Metro Ethernet network”, é uma arquitetura baseada em padrões Ethernet para conectar clientes a rede do provedor de serviços, seja para conexão de Internet ou entre pontos da empresa cliente.

A vantagem para o cliente é que ele recebe um ponto de rede no padrão Ethernet que é amplamente conhecido e dominado no mercado.

O padrão Metro Ethernet (MEN – Metro Ethernet Network) define uma topologia composta de switches no service provider (SP – provedor de serviços), que ficam em um ponto de presença (PoP – Point of presence), próximo aos clientes e conecta-se a eles utilizando um link de acesso (last mile) normalmente via fibra óptica padrão Ethernet.

Tudo o que acontece com o link está definido em uma “User Network Interface” ou UNI (interface de rede de usuário), onde o termo “rede” (network) refere-se a rede do SP, enquanto o cliente (enterprise ou a própria empresa cliente) é o usuário (user) da rede.



O usuário remoto ou site remoto é também chamado de folha ou leaf e o site central ou matriz é chamado de root.

O SP tem a função de encaminhar os quadros Ethernet através da WAN entre os usuários da rede, ou seja, switches (L2 ou L3) ou roteadores dos clientes. Esse encaminhamento é realizado através do cabeçalho dos quadros 802.1Q encaminhados pelos trunks indicando cada VLAN configurada, porém os detalhes de como isso é feito dentro do SP não é relevante nesse material.

As conexões UNI são definidas pelos padrões Ethernet, os quais alcançam distâncias muito maiores via fibra que cabos metálicos UTP. Os seguintes padrões podem ser utilizados nos links de acesso:

Padrão	Velocidade	Distância
100Base-LX10	100 Mbps	10 Km
1000Base-LX	1 Gbps	5 Km
1000Base-LX10	1 Gbps	10 Km
1000Base-ZX	1 Gbps	100 Km
10GBase-LR	10 Gbps	10 Km
10GBase-ER	10 Gbps	40 Km

Você pode encontrar também o termo "carrier Ethernet" ao invés de Metro Ethernet para definir esse serviço, o que significa a grosso modo "Ethernet para Provedores de Serviço".

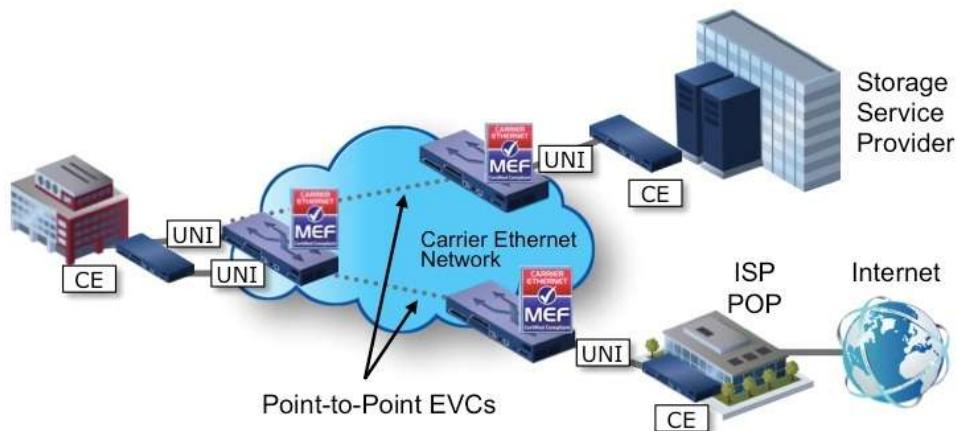
O Metro Ethernet oferece várias vantagens para provedores e assinantes, tais como não necessidade de roteador na ponta do cliente, diminuindo custo, flexibilidade, fácil manutenção e gerenciamento, o cliente lida com uma interface Ethernet comum e bem conhecida, integrando-se perfeitamente a LAN já instalada, etc.

5.5.3.1 TOPOLOGIAS METRO ETHERNET

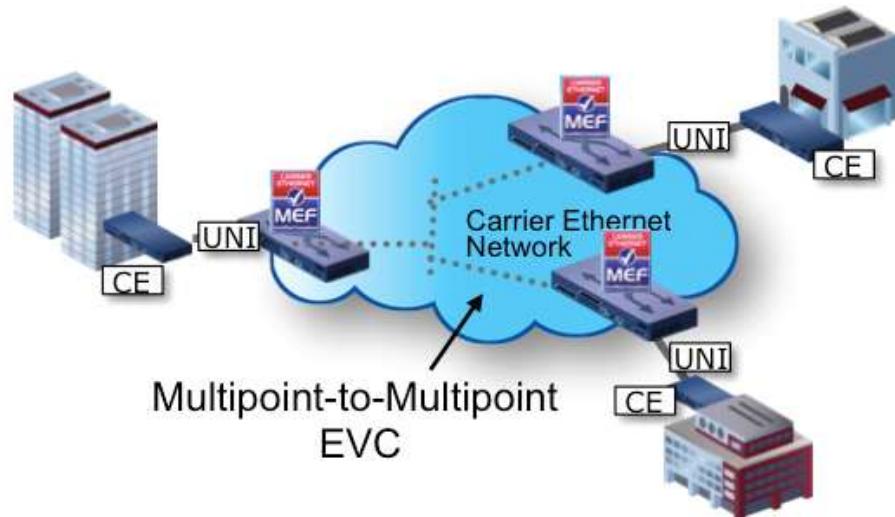
A conexão física dos clientes a uma rede Metro Ethernet é normalmente um cabo de fibra óptica no padrão Ethernet, como citado anteriormente, porém o MEF (Metro Ethernet Fórum) define vários padrões de conexão lógica entre os dispositivos da rede Metro Ethernet.

Vamos estudar aqui três tipos de especificações, as citadas na bibliografia oficial da Cisco:

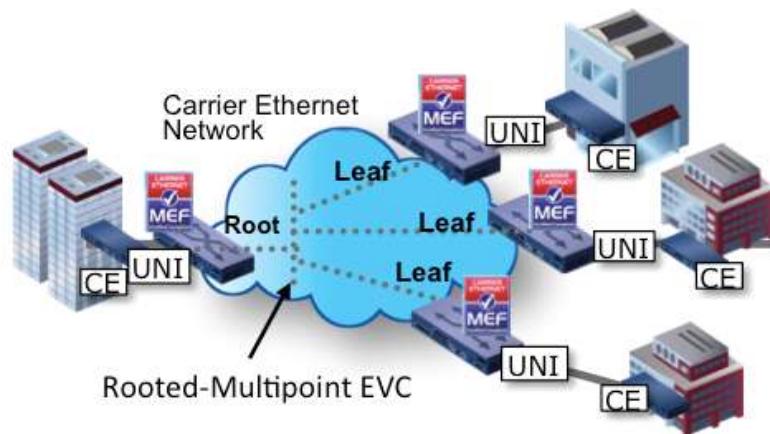
- **Ethernet Line Service ou E-Line** (topologia ponto a ponto): dois customer premise equipment (CPE) trocando quadros Ethernet entre si, como linhas dedicadas ponto a ponto. Os links são chamados e EVCs ou “Ethernet Virtual Connection” (conexão ethernet virtual).



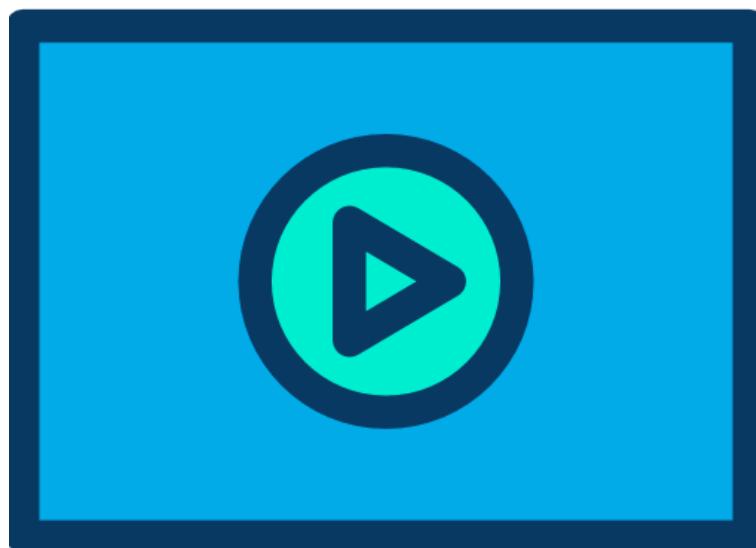
- **Ethernet LAN Service ou E-LAN** (topologia full mesh): o mais parecido com uma LAN, onde todos os CPEs podem trocar quadros entre si. Nessa topologia são criados EVCs entre todos os usuários, por exemplo, com 3 dispositivos serão necessários 3 EVCs, porém com 6 sites você precisará de 15 EVCs para fazer a topologia full mesh.



- **Ethernet Tree Service ou E-Tree** (topologia hub-and-spoke/partial mesh/ponto-multiponto): como já estudamos nessa topologia o Hub (switch central) faz o “meio de campo” para que os demais switches possam se comunicar, ou seja, o Hub fala com todos os Spokes, porém os Spokes não falam entre si diretamente.



5.5.4 Internet como WAN



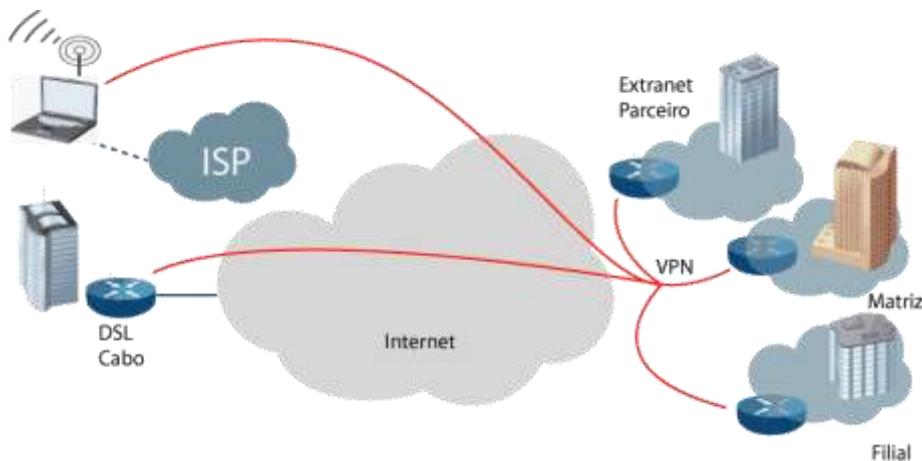
Cada vez mais as empresas estão abandonando os circuitos dedicados de alto custo e migrando suas conexões entre suas Unidades através da Internet, afinal ela é a “WAN das WANs”.

Com opções de conexão cada vez mais rápidas (banda larga), mais seguras e confiáveis a Internet tem dois grandes problemas a serem resolvidos: **segurança** e **privacidade**.

Para resolver esse problema podemos utilizar as VPNs para garantir o tráfego de dados de forma transparente entre as diversas LANs da empresa, de forma segura e privada.

Uma Rede Virtual Privada ou Virtual Private Network (VPN) tem a função principal de permitir a criação de redes privadas através da Internet, permitindo privacidade e tunelamento de protocolos dentro TCP/IP, visando acesso remoto de usuários que trabalham em Home Office ou de Unidades Remotas através da Internet.

As VPNs são usadas diariamente para dar acesso corporativo à rede para usuários remotos, conectividade a escritórios remotos utilizando um meio público como a Internet, sendo uma opção mais barata que circuitos dedicados. Também podem ser uma opção para links de contingência utilizando tecnologias como ADSL ou Internet via cabo coaxial. Veja na figura uma topologia básica de aplicação de uma VPN em um ambiente corporativo.



Na construção de uma VPN são empregadas diversas técnicas combinadas como autenticação, criptografia e tunelamento (as VPNs não são foco desse curso, serão estudadas em cursos específicos).

Os protocolos mais comuns para realização de VPNs ou tunelamento via IP são:

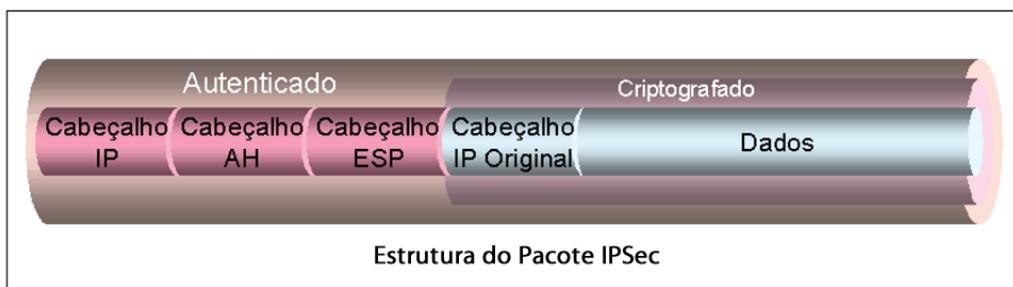
- Layer 2 Forwarding (L2F)
- Point-to-Point Tunneling Protocol (PPTP)
- Layer 2 Tunneling Protocol (L2TP)
- Generic Routing Encapsulation (GRE)

Note que uma VPN é um protocolo encapsulado e criptografado passando dentro do pacote IP, o que gera um grande overhead (cabeçalho adicional) devido às técnicas de tunelamento e criptografia utilizadas.

Na realidade o tunelamento não garante segurança, para isso temos que usar um protocolo como o IPSec em conjunto.

O IPSec (Internet Protocol Security) é um framework padrão do IETF, definido pela RFC 4301, que proporciona confidencialidade, integridade e autenticação dos dados.

Com o IPSec podemos criar um túnel entre dois pontos, por onde os “dados sensíveis” (dados que necessitam ser protegidos) são enviados. Veja a figura abaixo com um pacote protegido pelo IPSec.



O **IPSec** pode transportar as informações em dois modos, **Transporte** ou **Túnel**.

No modo transporte, somente a mensagem (payload) é criptografada, sendo que o cabeçalho IP permanece intacto. Já no modo de tunelamento, o pacote IP é criptografado por inteiro. Deve, assim, encapsular um novo pacote IP para distribuí-lo.

O tunelamento é usado para comunicações da rede-a-rede (túneis seguros entre roteadores, chamadas de VPNs site-to-site) ou comunicações de host-a-rede e de host-a-host através da internet.

5.5.5 SD-WAN ou Software Defined WAN

Opa, SD-WAN não está no blueprint do CCNA!!! Por que você vai falar disso?

Simples, porque você precisa ter uma noção do assunto! Você vai provavelmente ter isso implantado em sua Rede ou vai surgir em uma conversa de trabalho.

Lembre-se de tudo o que estudamos sobre as tecnologias WAN até o momento.

Quais as características de uma WAN e sua administração utilizando as tecnologias atuais?

1. Formada por diversos equipamentos, centenas, milhares de roteadores se comunicando através da uma série de tecnologias.
2. Essas tecnologias são diferentes umas das outras e cada uma administrada de uma maneira diferente.
3. Configurações manuais e feitas em sua maioria via CLI (linha de comando).
4. Devido às configurações manuais são demoradas e sujeitas a falhas humanas.
5. O mesmo se aplica para mudanças, desinstalações, novas instalações e na resolução de problemas.

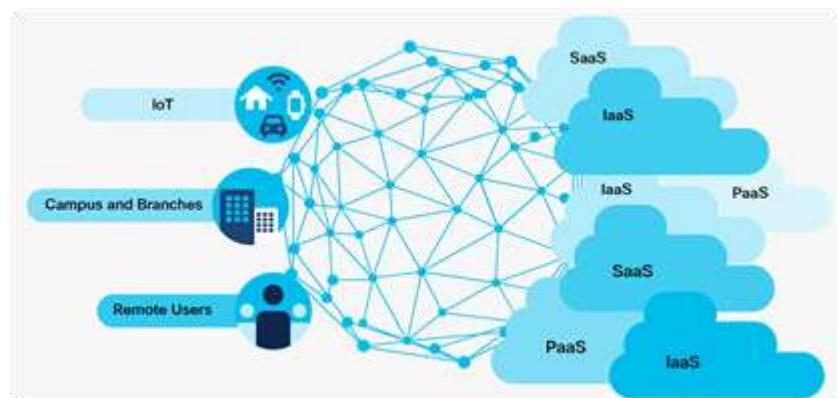
Implementar diversos sites em uma WAN tradicional pode levar dias, semanas e até meses, pois circuitos MPLS não são tão simples de serem implementados como uma conexão de Internet.

O mesmo processo é similar se usamos a Internet como WAN e VPNs para conectar os sites remotos.

As configurações em redes convencionais são manuais e demoradas, testes não são automatizados e a operação da rede é dispositivo a dispositivo.

Outro ponto é que nas WANs tradicionais quem decide por onde um pacote será encaminhado tipicamente é um protocolo de roteamento, o qual analisa apenas características do seu próprio algoritmo, sem considerar necessidades dos usuários ou aplicações da rede.

Na prática o SD-WAN é você fazer toda a sua rede de longa distância controlada por software, você terá como no DNA Center, que vimos anteriormente, um Underlay e um Overlay, separando as funções de rede.



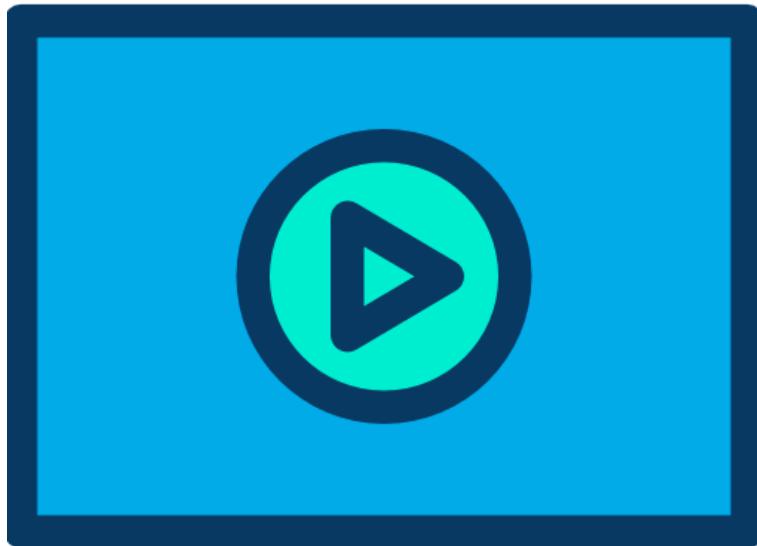
Isso permite que você controle as conexões através de políticas, agrupe essas políticas e as aplique a diversos equipamentos simultaneamente.

Outra habilidade de uma rede SD-WAN é a escolha do melhor caminho utilizando outros parâmetros que não sejam uma simples métrica calculada por um protocolo de roteamento, permitindo que a escolha do caminho priorize usuários, aplicações e necessidades mais específicas que somente "largura de banda".

Ela pode misturar links de Internet, utilizando VPNs, MPLS e outras tecnologias para formar uma WAN definida por software.

Ela consegue juntar agilidade, pois as configurações e resolução de problemas podem ser centralizadas e aplicadas em diversos equipamentos ao mesmo tempo, melhora a performance da WAN porque é capaz de analisar e escolher os melhores caminhos que cada usuário ou aplicação necessita, e, por último, consegue reduzir os custos com implantação e manutenção de novos sites inseridos na rede.

5.6 Spine and Leaf



Já estudamos topologias e tecnologias para redes LAN e WAN, porém agora vamos ver uma topologia utilizada em Data Centers para conectar os diversos servidores, sejam eles físicos ou virtuais.



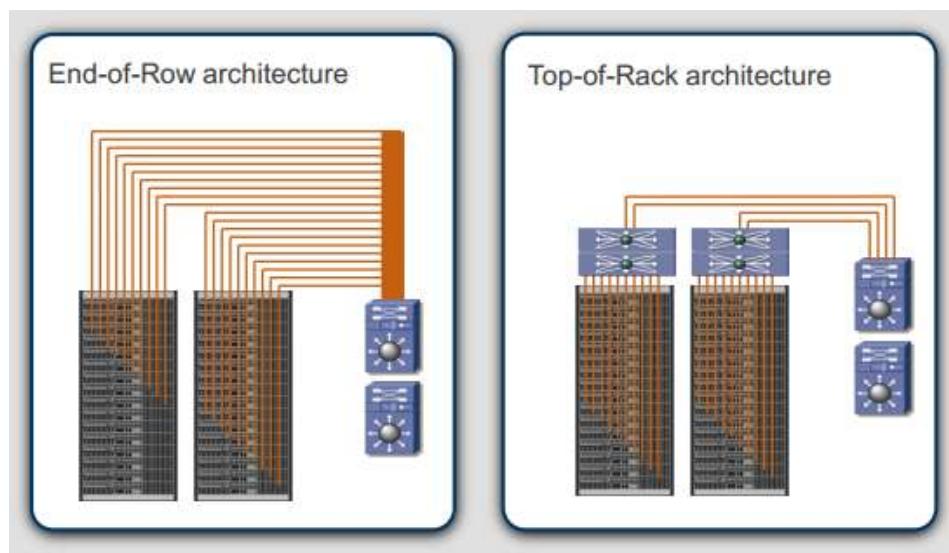
Um Data Center pode estar localizado dentro de uma empresa ou em um Provedor de Serviços.

É um ambiente projetado para concentrar servidores, switches, roteadores e outros dispositivos de Rede.

Ele tem a finalidade de abrigar milhares de servidores e bancos de dados, e processar grandes quantidades de informação, os equipamentos geralmente são montados em racks ou armários metálicos.

Na foto anterior dá para se ter ideia da quantidade de conexões entre servidores e switches que um data center requer! Para isso, por muito tempo utilizou-se a arquitetura em três camadas para fazer essas conexões.

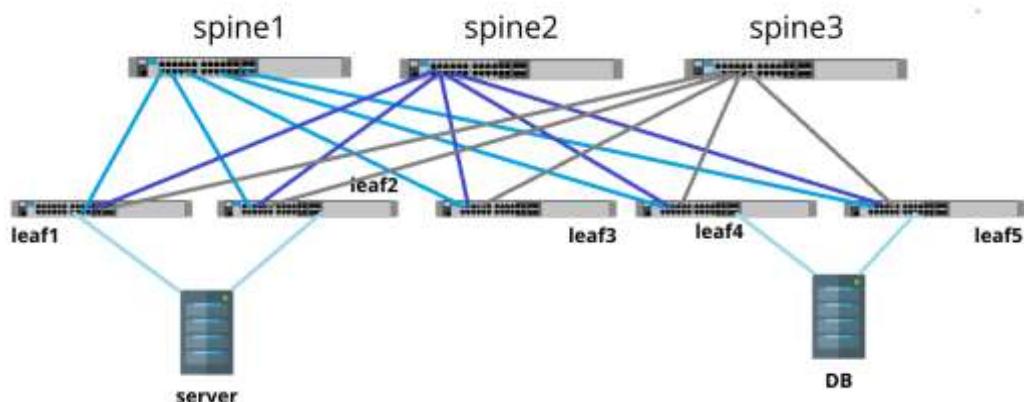
A topologia física típica dos data centers ou DCs é a **top-of-rack** e **end-of-row** (topo de rack e final da fila, respectivamente). Switches de acesso no topo dos racks de servidores, agregando as conexões de rede, e no final da fila um rack com switches de distribuição e core.



Porém a arquitetura em três camadas para data centers é complexa de se administrar e pode trazer mais de três saltos entre os servidores, pois nem sempre teremos apenas um core devido a grande densidade de portas para servidores que um data center exige.

Para tratar desse problema, já adequando o sistema ao conceito de SD-Access (acesso definido por software) a topologia Spine and Leaf veio para substituir a arquitetura em três camadas.

Ela possui apenas duas camadas: switches de acesso que são chamados agora de "**leaf switches**" e os switches que agregam o acesso chamados de "**spine switches**". Veja imagem a seguir.



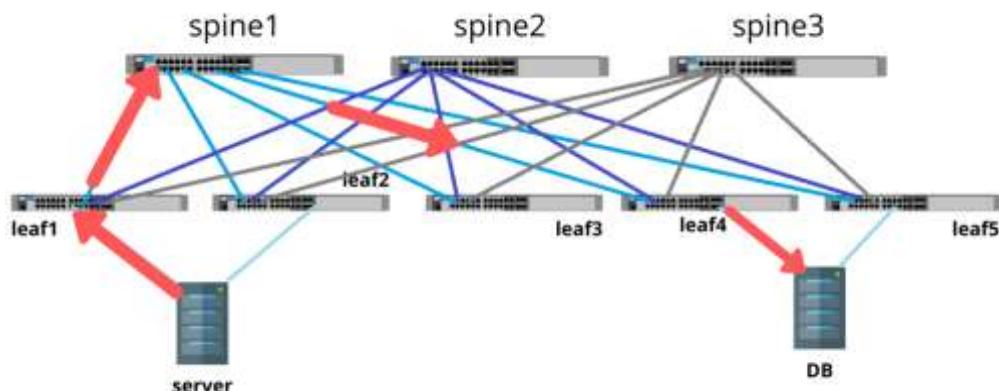
Na arquitetura spine and leaf temos sempre as seguintes **regras de design**:

- Cada “leaf switch” deve conectar a cada “spine switch”
- Cada “spine switch” deve se conectar a cada “leaf switch”
- “Leaf switches” não podem conectar-se entre si
- “Spine switches” também não podem conectar-se entre si
- Endpoints conectam-se apenas aos “leaf switches”

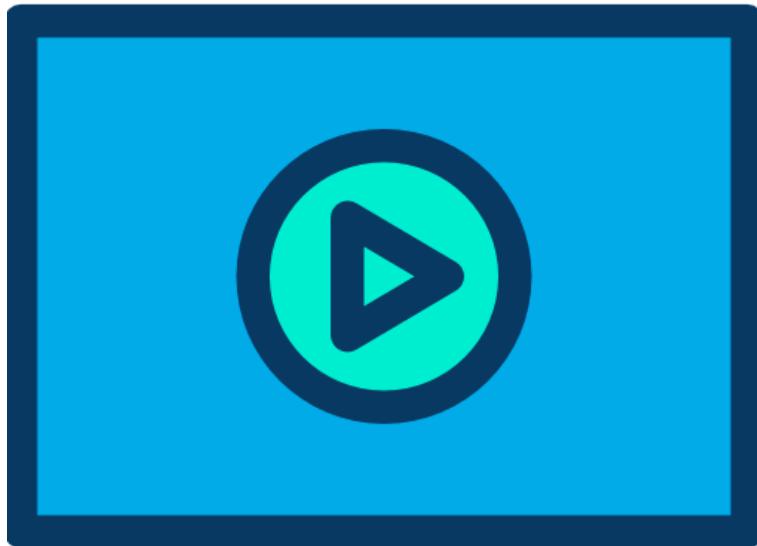
Os servidores podem ser virtualizados e dentro deles várias VMs podem estar rodando simultaneamente, porém não há variação na topologia. Além disso, os servidores podem conectar-se a mais de um leaf switch por questões de redundância.

Note que não importa onde o servidor esteja posicionado na topologia spine and leaf que ele sempre dará no máximo dois (2) saltos até o destino.

Por exemplo, para o server comunicar-se com o servidor de banco de dados (DB) ele pode sair pela interface do switch leaf1, chegar ao spine1, o qual pode encaminhar o quadro até o leaf4, o qual fará o quadro chegar ao seu destino final.



5.7 On-premises e Cloud



Nesse tópico vamos estudar sobre cloud computing services, iniciando com as características que esse serviço deve ter segundo o NIST (National Institute of Standards and Technology – US):

- **On-demand self-service:** Provisionamento dinâmico de recursos sob demanda, com mínimo de esforço e sem interação direta com o time do provedor de serviços.
- **Broad network access:** O serviço deve ser acessível via diversos tipos de dispositivos e redes, inclusive via Internet. Assim como de qualquer localização geográfica de forma transparente ao cliente final.
- **Resource pooling:** Os recursos alocados não devem ser dedicados ao cliente, eles devem ser alocados dinamicamente e independente de um hardware específico.
- **Rapid elasticity:** Para o usuário o sistema deve parecer ilimitado, ou seja, se ele precisa crescer é só solicitar ou preencher uma nova requisição para rapidamente ser atendido, muitas vezes até dinamicamente. Muitas vezes o serviço é chamado como elástico.
- **Measured service:** O provedor deve ser capaz de medir o uso e emitir relatórios para os clientes, tornando a cobrança simples e transparente.

Você provavelmente já utiliza serviços em nuvem nas suas atividades pessoais ou até na empresa que trabalha.



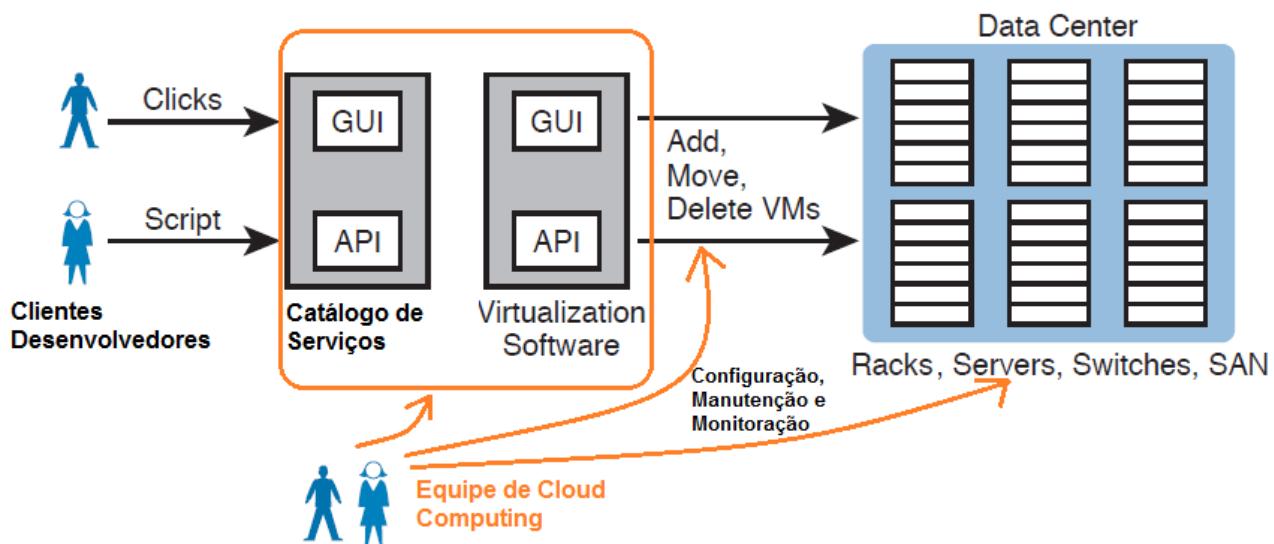
Uma nuvem pode ser **On-Premise** (nuvem privada ou private cloud) ou **pública** (public cloud ou apenas **cloud**). Existem também as nuvens híbridas, uma mistura dos dois tipos de nuvens anteriores, porém não é importante para o escopo do CCNA, por isso vamos focar nas públicas e privadas.



Uma nuvem privada é aquela construída e administrada pela própria empresa, ou seja, quem é "dono" da nuvem e quem a utiliza é a mesma empresa.

A vantagem de uma nuvem privada em relação ao serviço virtualizado seria que os serviços estariam disponíveis em um catálogo de serviços, nos quais os desenvolvedores e operadores poderiam preencher uma requisição, dar alguns cliques e em minutos teriam suas VMs criadas, tudo de forma automatizada e sem intervenção humana.

Na realidade o time de TI nesse caso iria criar o sistema de nuvem privado, configurá-lo, criar o catálogo, implementar os serviços e administrar o sistema como um todo, não precisariam mais intervir em todas as requisições realizadas pelos clientes internos, o que traz mais agilidade ao processo.



Em uma nuvem pública ou public cloud o provedor de serviços (SP ou Service Provider) é o “dono” da nuvem e comercializa serviços para outras empresas a partir dessa plataforma.

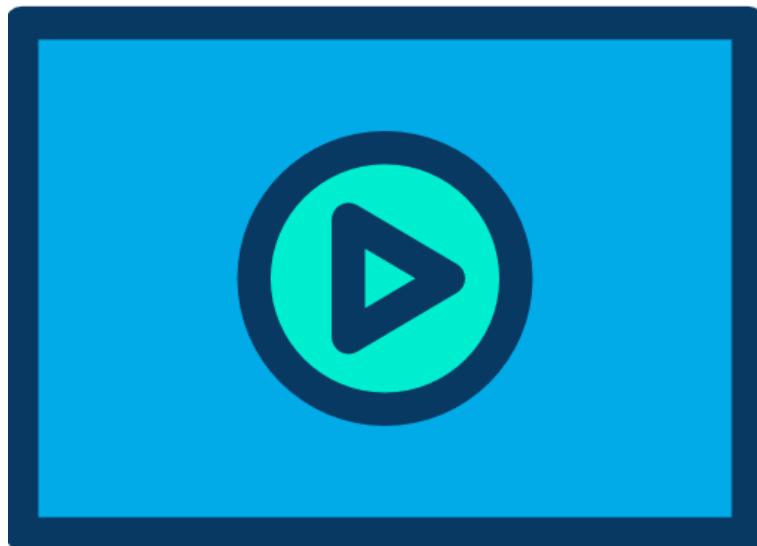
É o mesmo princípio de um provedor de serviços de Internet, porém ao invés de disponibilizar conexão o provedor está comercializando VMs, bancos de dados, softwares e demais serviços em nuvem.

A conexão do cliente com a nuvem do provedor de serviços pode ser realizada diretamente via Internet ou se o cliente requisitar mais segurança pode ser feita via VPN ou até mesmo com um link de WAN dedicado, por exemplo, via MPLS.

Note que essa é uma grande diferença entre uma nuvem privada e pública, pois a nuvem privada pertence a empresa, por isso não tem problema de acesso externo porque tudo está na mesma infraestrutura de redes. Isso traz mais segurança também.

Porém, o custo é muito maior, pois um provedor de serviços pode compartilhar o custo entre vários clientes de tornar o valor muito mais atrativo.

5.7.1 A Nuvem como Serviço



Atualmente, a computação em nuvem é dividida em sete tipos (vamos detalhar as três primeiras):

- **IaaS - Infrastructure as a Service:** na Infraestrutura como Serviço o cliente se utiliza uma percentagem de um servidor, geralmente com uma configuração que se adeque à sua necessidade, por exemplo, Softlayer e Amazon Web Services (AWS).

Esse serviço é o que mais se aproxima ao que estudamos até o momento e o mais simples de ser entendido, pois ele se assemelha a comprar um computador, onde você especifica as capacidades de CPU, memória RAM, armazenamento, sistema operacional e tem seu servidor em nuvem preparado para instalação dos seus aplicativos.

Um dos serviços mais comuns é o Amazon Web Services (AWS), um provedor de nuvem pública onde você cria sua VM com parte do serviço de IaaS. Veja tela abaixo com exemplo de máquina virtual EC2 chamada de "micro" com 1 vCPU e 1Gb de memória RAM.

The screenshot shows the AWS EC2 instance creation process at Step 2: Choose an Instance Type. The 'Currently selected' row is highlighted with a blue border and contains the text 't2.micro (Variable ECUs, 1 vCPU, 2.5 GHz, Intel Xeon Family, 1 GB memory, EBS only)'. An arrow points from the text above to this row. Below the table, the 'General purpose' family is selected. The table lists the following instance types:

Family	Type	vCPUs	Memory (Gb)	Instance Storage (Gb)	EBS-Optimized Available	Network Performance
General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate
General purpose	t2.micro (highlighted)	1	1	EBS only	-	Low to Moderate
General purpose	t2.small	1	2	EBS only	-	Low to Moderate
General purpose	t2.medium	2	4	EBS only	-	Low to Moderate
General purpose	t2.large	2	8	EBS only	-	Low to Moderate

- **SaaS - Software as a Service:** o Software como Serviço é o uso de um software via web, por exemplo, Google Docs, Drop Box, Apple iCloud e Microsoft SharePoint Online. Além disso, maioria dos serviços de e-mail são considerados SaaS atualmente, até a Microsoft já está oferecendo a opção de utilização do Exchange como serviço, ou seja, você pode ter seus e-mails via Exchange sem precisar da licença instalada em seus servidores, pois o serviço está em nuvem.

É importante lembrar que nessa modalidade de serviços o cliente não escolhe a máquina virtual que rodará o serviço de software ou suas características, ele apenas escolhe as opções da aplicação que deseja utilizar.

- **PaaS - Platform as a Service:** na Plataforma como Serviço, como o nome sugere, você tem uma plataforma para desenvolvimento com sistema operacional, programming language execution environment (ambiente de programação), banco de dados, servidor web, etc. Exemplos: AWS Elastic Beanstalk, Windows Azure, Heroku, Force.com, Google App Engine e Apache Stratos.

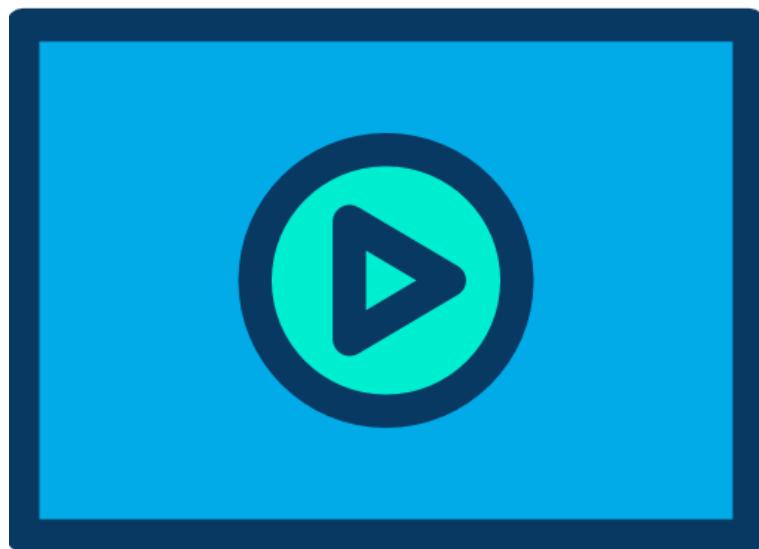
O PaaS vai além do IaaS, sendo uma solução para desenvolvimento de aplicações, apesar de que em ambas as opções o cliente pode escolher o número de VMs, CPU, memórias, no PaaS existem mais opções de ferramentas de software além do sistema operacional.

Portanto, a grande vantagem do PaaS é para ambientes de desenvolvimento, onde ferramentas adicionais que são necessárias em produção são extremamente úteis para quem desenvolve aplicações, normalmente chamado de Integrated Development Environment (IDE – ambiente de desenvolvimento integrado).

- **DaaS - Development as a Service:** no Desenvolvimento como Serviço as ferramentas de desenvolvimento tomam forma na computação em nuvem como ferramentas compartilhadas, ferramentas de desenvolvimento baseadas em web e serviços baseados em mashup.
- **CaaS - Communication as a Service:** a Comunicação como Serviço é o uso de uma solução de Comunicação Unificada hospedada em um Data Center do provedor de serviços ou fabricante, por exemplo, Microsoft Lync.
- **EaaS - Everything as a Service:** Tudo como Serviço... o nome já diz tudo... é quando se utiliza tudo, infraestrutura, plataformas, software, suporte, enfim, tudo o que envolve Tecnologia da Informação e Comunicação como um Serviço.
- **DBaaS - Data Base as a Service:** o Banco de dados como Serviço é quando o cliente utiliza a parte de servidores de banco de dados como serviço.

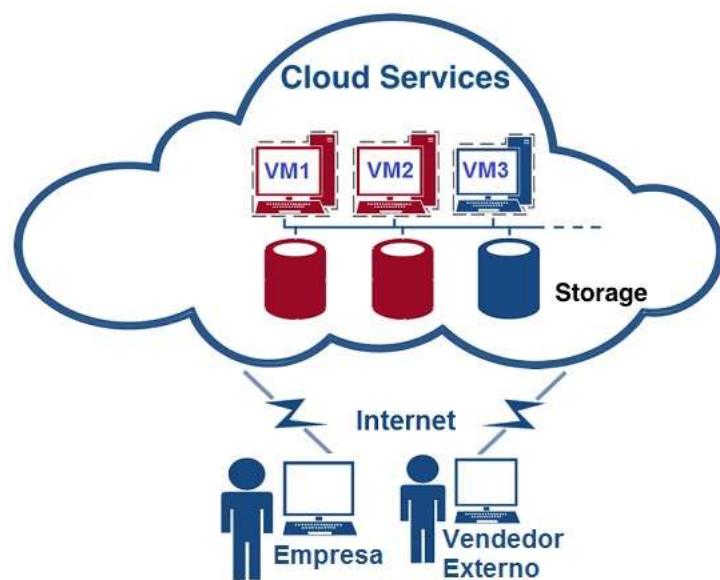
Os três primeiros são os mais comuns e por isso são os mais importantes para o exame do CCNA.

5.7.2 Conectando-se com a Nuvem Pública via Internet



Como já foi citado anteriormente, se a nuvem for privada não precisamos nos preocupar em como fazer a conexão, pois os recursos estão todos no mesmo ambiente de infraestrutura de redes.

O mesmo não ocorre quando a conexão é entre a empresa e serviços que estão em nuvens públicas, pois nesse caso será necessária a conexão através da WAN, seja ela através de um link dedicado ou via rede pública através da Internet.



Se pensarmos no fluxo (workflow) de uma nuvem pública tudo se inicia com o cliente acessando o portal de serviços do provedor de Cloud Computing, escolhendo um serviço do seu catálogo, por exemplo, a criação de uma VM para hospedagem de um determinado aplicativo, a seguir a VM é criada e o cliente recebe os devidos acessos para instalar seus aplicativos. Tudo realizado de forma automatizada e sem intervenção humana por parte do provedor para criar a VM.

Veja que até esse ponto temos um tráfego leve, apenas o responsável da TI da empresa cliente especificando e criando sua VM.

Uma vez instalado e testado o aplicativo ele é liberado para uso interno dos funcionários da empresa ou setor que vai utilizar aquela aplicação. Nesse momento o tráfego vai aumentar, pois mais pessoas farão conexão com esse aplicativo para realizar suas tarefas.

Além disso, pode haver uma comunicação entre servidores (físicos ou virtuais) que estão na rede da empresa, por exemplo, um servidor de autenticação em uma DMZ, e o aplicativo instalado na VM em nuvem.

Portanto, existem vários acessos entre a empresa e suas VMs ou serviços em nuvem, por isso os dois principais pontos a serem analisados são: largura de banda e segurança.

Os links entre a empresa e o provedor de serviços devem suportar a largura de banda necessária para rodar os serviços contratados, por exemplo, a empresa tem um IaaS com servidores virtuais em nuvem e um PaaS utilizado pelo time de desenvolvimento para desenvolver e testar as aplicações que os diversos setores da empresa utilizam para realizar suas tarefas, sendo que o acesso nesse primeiro exemplo será diretamente via Internet.

A largura de banda do link de Internet deve suportar os acessos do dia a dia mais o fluxo entre a rede interna e a nuvem, pois esse serviço em nuvem soma ao que já estava sendo utilizado normalmente pela empresa em termos de link de Internet.

Lembre-se que normalmente um serviço em nuvem retira o que estava sendo utilizado internamente com servidores locais e move o serviço para a nuvem do provedor de serviços, por isso esse tráfego é novo para a WAN ou Internet.

Outro ponto é que se esses dados forem enviados sem nenhuma proteção (sem criptografia), eles podem ser capturados, lidos ou até alterados nesse fluxo entre o cliente e seu provedor de serviços em nuvem.

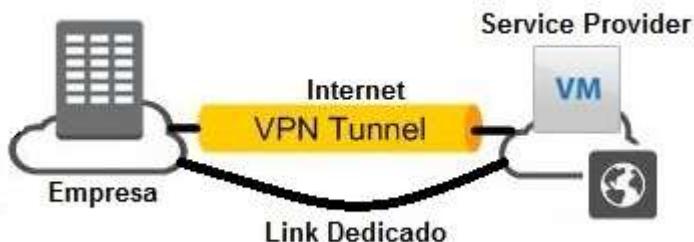
Os pontos positivos da nuvem pública são agilidade, pois tudo está pronto para uso e não é necessário passar pelo processo de compra de uma nuvem privada, a Internet permite acesso de usuários de qualquer localização geográfica, por exemplo, equipes de vendas podem acessar a aplicação de registro e controle de pedidos de qualquer dispositivo onde quer que eles estejam. Por último é a facilidade de migração em caso de problemas ou sobrecarga, pois todos os provedores de serviço estão na Internet e fica muito mais fácil essas movimentações.

As desvantagens desse acesso são segurança, pois os dados da empresa passarão a trafegar em uma rede pública aumentando o risco de espionagem ou ataques de Man-in-the-Middle (MITM).

Outro ponto é a sobrecarga no tráfego de Internet, que pode levar a aumento de custos de conexão. Além disso, na Internet não tem QoS, por isso fatores como delay e perda de pacotes podem afetar as aplicações mais sensíveis a esses fatores. É claro que normalmente links de Internet não oferecem SLA ou acordos de nível de serviço como em links WAN dedicados.

5.7.3 Conectando-se com a Nuvem Pública via VPN ou Link Dedicado

Como especificado pelo NIST as nuvens devem ser acessíveis de várias formas diferentes, por isso os provedores de serviços de nuvem pública oferecem as opções de conexão via VPN ou até mesmo via link dedicado, por exemplo, via MPLS layer 2 ou layer 3.



Para criar um túnel VPN até o provedor de serviços em nuvem podemos utilizar os mesmos conceitos estudados aqui nesse material em capítulos anteriores, somente adaptando para as especificações passadas pelo provedor, o qual normalmente já oferece essa opção com um roteador que ficará pré-configurado do lado dele.

Ou o cliente pode subir um roteador virtual, por exemplo, a Cisco oferece o Cloud Services Router (CSR) para fazer a mesma coisa que um roteador físico, porém rodando em uma VM do provedor de cloud, podendo inclusive fechar VPNs. Essa opção pode até economizar recursos, pois a empresa usa seu próprio roteador virtual ao invés de pagar para usar um que seria do provedor de serviços.

Para fazer uma conexão via links dedicados através de Multiprotocol Label Switching (MPLS) VPN ou Ethernet WAN vai precisar trabalhar tanto com o provedor de nuvem como com o provedor de serviços de WAN, principalmente se forem empresas diferentes.

Por isso mesmo esse tipo de conexão exige um planejamento extra, pois dependem de vários fatores, configurações, localização para terminação dos links dedicados, etc. Grandes provedores de public cloud como Amazon Web Services, Google Compute Cloud, Microsoft Azure e Rackspace oferecem esse tipo de conexão e disponibilizam informações sobre suas especificações, configurações e localizações onde os circuitos podem ser terminados.

Portanto, utilizar links WANs dedicados resolve o problema de segurança em relação ao uso da Internet sem VPN, além disso, os links MPLS permitem que você faça QoS e priorize o tráfego mais importante.

Por outro lado, esses tipos de link são mais caros e necessitam de mais planejamento, por exemplo, se o link for fornecido por um provedor diferente do seu provedor de nuvem podem ocorrer atrasos nas implantações, principalmente nos casos de migração para outros provedores. Você perde a agilidade que a Internet traz para ter mais segurança.

O meio termo para a questão de segurança é o uso da Internet com adição de uma VPN, porém mesmo com mais segurança você continua sem QoS.

Além disso, o uso da Internet com ou sem VPN torna necessidades de migração entre provedores muito mais simples, porém vamos falar desse assunto no próximo tópico.

6 Conexões, Interfaces e Tipos de Cabeamento

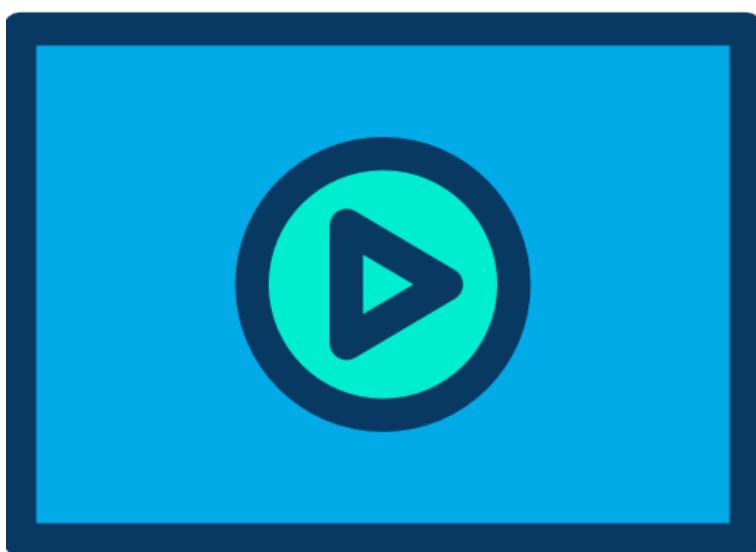
Até agora estudamos os dispositivos de rede, como fazer uma topologia, como conectar esses dispositivos, mas ainda não estudamos as opções físicas e reais de conexão.

Nesse tópico vamos falar sobre como conectar fisicamente os dispositivos de redes e endpoints.

Basicamente em redes corporativas podemos conectar os dispositivos via cobre (pares metálicos), fibras ópticas ou através de ondas eletromagnéticas ou wireless.

Normalmente a escolha entre as tecnologias depende de distância, ruídos e interferências eletromagnéticas, requisitos de segurança e financeira.

6.1 Cabos Metálicos



O principal cabo metálico utilizado nas redes é o par trançado, os quais podem ser blindados ou não blindados e possuem 4 pares por cabo. Cada par é separado por cores para facilitar a conectação.

As principais vantagens de uso do cabo par trançado são taxa de transmissão, baixo custo do cabo e baixo custo de manutenção de rede. As taxas usadas nas redes com o cabo par trançado são:

- 10 Mbps (Ethernet)
- 100 Mbps (Fast Ethernet)
- 1000 Mbps (Gigabit Ethernet)
- 10.000 Mbps ou 10Gbps (10Gigabit Ethernet)

O mais utilizado na prática é o cabo não blindado denominado UTP (Unshielded Twisted Pair ou Par Trançado sem Blindagem), o qual pode ser utilizado para transmissão tanto de dados como voz.



Para a conexão dos cabos UTP são utilizados os conectores RJ-45 macho ou fêmea. Os conectores machos são utilizados como terminação das conexões e os fêmeas, conhecidos como keystone jacks, são utilizados nos painéis de distribuição (de patch-panels), nas tomadas de telecomunicações (utilizadas nas mesas e paredes), placas de rede e assim por diante.



Os cabos UTP foram padronizados pelas normas da EIA/TIA-568-B, sendo divididos em categorias, levando em conta o nível de segurança e a bitola do fio, onde os números maiores indicam fios com diâmetros menores.

Em todas as categorias, a **distância máxima permitida é de 100 metros**.

Veja abaixo um resumo das principais características de cada categoria.

Category	Speed	Frequency
CAT 1	Carry only voice	1MHz
CAT 2	4Mbps	4MHz
CAT 3	10Mbps	16Mhz
CAT 4	16Mbps	20Mhz
CAT 5	100Mbps	100Mhz
CAT 5e	1000Mbps	100Mhz
CAT 6	1000Mbps	250MHz
CAT 7	10Gbps	600MHz
CAT 7a	10Gbps	1000Gbps
CAT 8	25Gbps	2000Mhz

6.1.1 Montagem e Testes dos Cabos de Pares Trançados

Essa montagem pode ser basicamente de dois tipos cabos, um chamado cabo direto e outro chamado cabo cruzado (cross), as quais estão baseadas nos padrões T568A e T568B.

Antes de vermos os padrões vamos conhecer as cores dos fios, que são:

- Laranja e branco
- Laranja
- Verde e branco
- Azul
- Azul e branco
- Verde
- Castanho (ou marrom) e branco
- Castanho (ou marrom)

A norma EIA/TIA-568-B prevê duas montagens para os cabos, denominadas T568A e T568B.

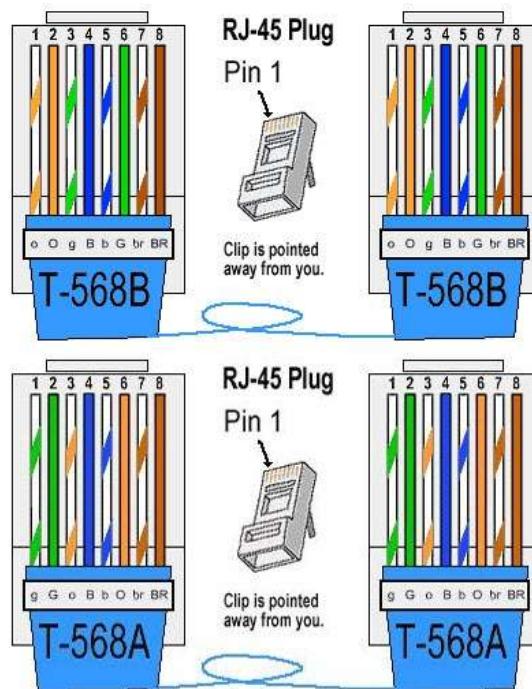
A montagem T568A usa a sequência branco e verde, verde, branco e laranja, azul, branco e azul, laranja, branco e castanho, castanho.

A montagem T568B usa a sequência branco e laranja, laranja, branco e verde, azul, branco e azul, verde, branco e castanho, castanho.

Um cabo cujas duas pontas usam a mesma montagem é denominado "Cabo Direto" (T568B-T568B), e serve para ligar estações de trabalho e roteadores a switches ou hubs.

Um cabo em que cada ponta é usada um padrão diferente (T568A-T568B) é denominado "Cabo Crossover", e serve para ligar equipamentos do mesmo tipo entre si.

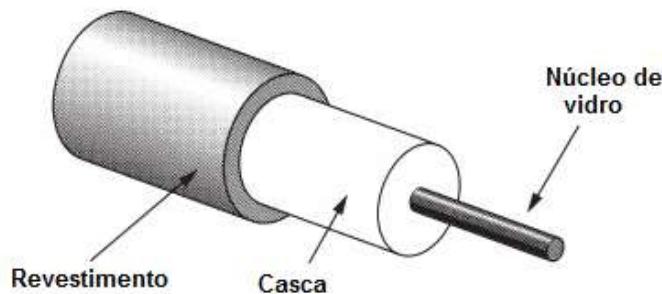
Veja na figura a seguir os padrões de montagem de cada cabo.



6.2 Fibras Ópticas

A fibra óptica pode ser representada como um tubo flexível de vidro onde a luz se propaga.

Essa é uma representação básica da fibra óptica.



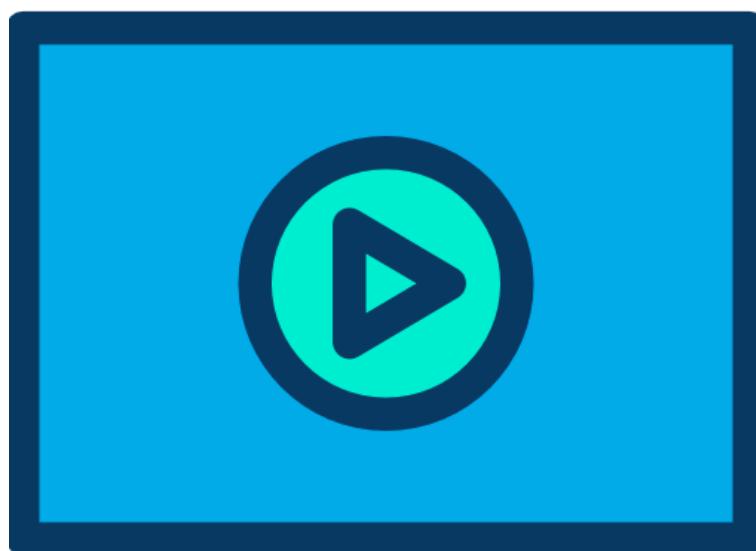
Esse tubo é chamado de núcleo e, portanto, é o meio onde a luz se propaga.

O núcleo é coberto com uma casca que tem a função de proteger e garantir que a luz fique confinada dentro do núcleo.

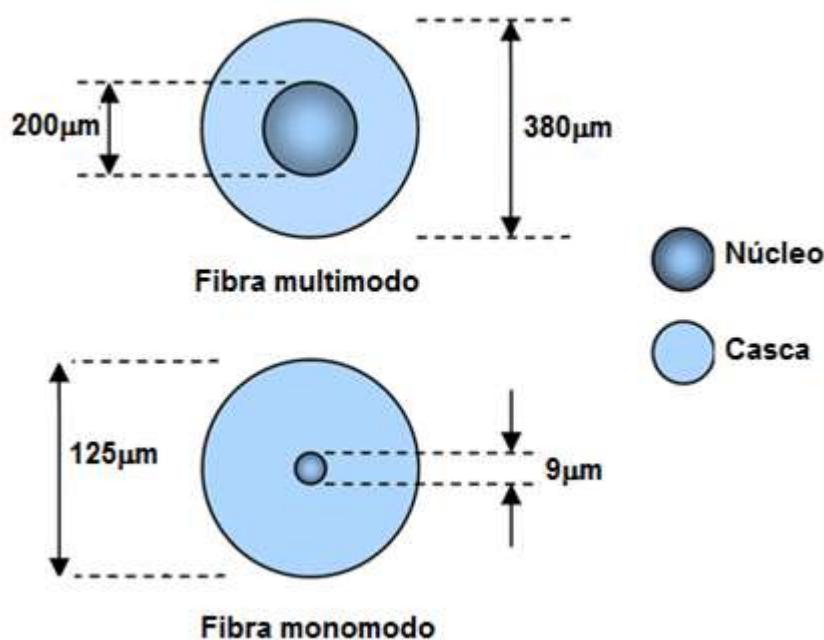
A casca, por sua vez, também é coberta por um revestimento de proteção.

Na prática os cabos possuem diversos revestimentos de proteção conforme a sua aplicação.

6.2.1 Tipos de Fibra Óptica



Você vai ver que existem diversos tipos de fibras ópticas e abaixo temos a representação dos diâmetros típicos de fibras do tipo multimodo e monomodo.



A luz de um LED ou um laser é colocada na ponta do núcleo e então ocorre a propagação até o destino.

A forma com que a luz se propaga no núcleo é o objeto de estudo da óptica, assim como os tipos de fibra óptica.

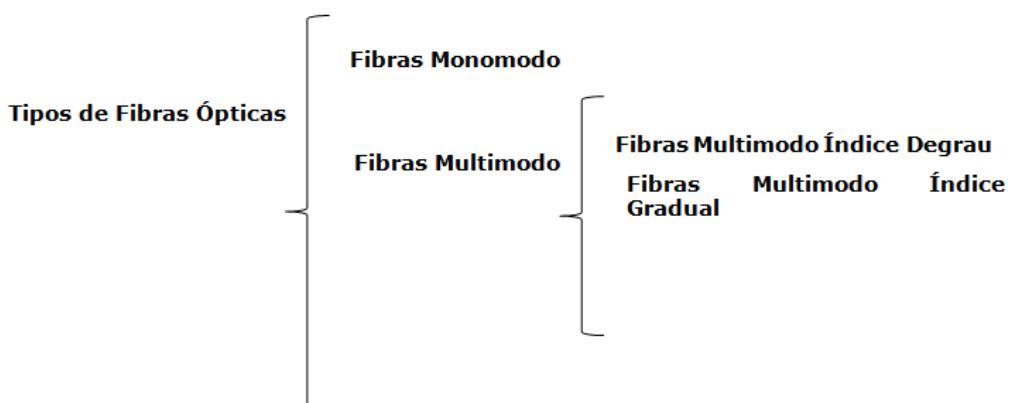
A lei de Snell, os conceitos de refração e dispersão são aplicados diretamente na tecnologia de fabricação das fibras.

Isso faz toda a diferença na hora de projetar e dimensionar um sistema de comunicações ópticas, pois dependendo da distância e uso da fibra óptica podemos baratear ou onerar um projeto de rede.

As Fibras ópticas são divididas em 2 grupos:

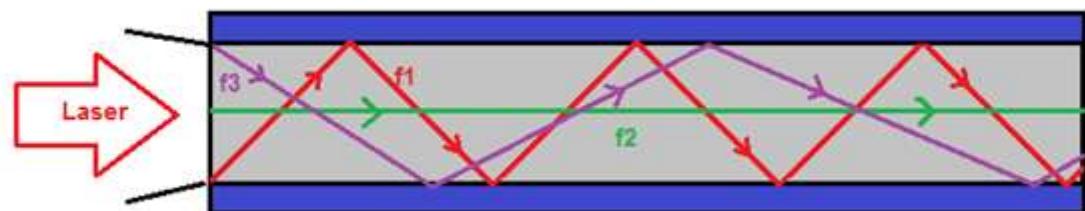
- Fibras Multimodo
- Fibras Monomodo

As Fibras multimodo podem ser de índice degrau ou índice gradual.



6.2.2 Fibras Ópticas Multimodo

Imagine uma fibra óptica com um laser na ponta como na figura a seguir.



Observe que a luz que sai do laser se propaga de vários modos:

1. Um feixe (f1) sai da parte de baixo do laser e reflete na parte de cima do núcleo da fibra óptica e vai se propagando em zigue-zague até o destino.
2. Um segundo feixe (f2) sai da parte do meio do laser e se propaga em linha reta na fibra óptica até chegar do outro lado da fibra.
3. E finalmente, um feixe (f3), sai da parte de cima do laser e reflete na parte de baixo do núcleo da fibra óptica e vai se propagando em zigue-zague até a outra extremidade.

Como esses 3 feixes, "n" feixes saem do laser resultando em "n" modos de propagação, portanto, dentre os tipos de fibra óptica, aquela que proporciona esse tipo de propagação é chamada de fibra multimodo.

As fibras multimodo foram as primeiras a surgir e possuem um núcleo maior que as fibras monomodo, o que resulta nos "n" modos de propagação.

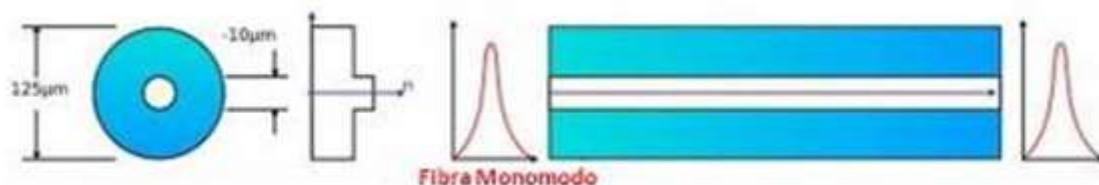
Como elas são menos "exigentes" no modo que a luz se propaga são também mais "baratas", porém suportam distâncias menores que as monomodo que vamos estudar a seguir.

6.2.3 Fibras Ópticas Monomodo

Antes de mais nada, imaginemos uma fibra com um núcleo tão fino que quando a luz do laser é acoplada, o feixe de luz transportado permite somente um modo de transmissão.

Nesse caso existe somente um caminho possível para a propagação, ou seja, somente um modo.

Entre os diversos tipos de fibra óptica, as fibras com essas características são denominadas fibras monomodo.



A fabricação de fibras ópticas monomodo é mais complexa devido à dificuldade mecânica de fibras tão finas.

Nas fibras monomodo anula-se a dispersão modal e obtém-se uma menor atenuação.

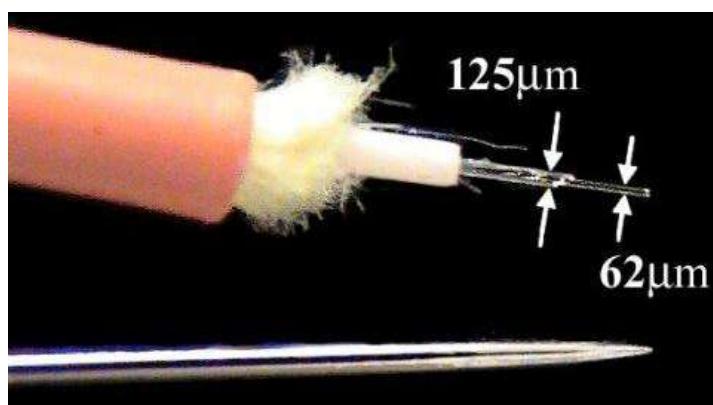
A conectividade do laser, contudo, é mais difícil o que exige que o laser utilizado seja mais preciso de alta qualidade elevando o custo de todo o sistema.

A princípio as fibras monomodo são utilizadas em sistemas de média e longas distâncias, cabos de fibras estaduais, backbones de grandes distâncias e inclusive em comunicações intercontinentais (cabos submarinos) onde há a transmissão de altas taxas de dados.

Por exemplo, podem ser utilizadas em cabos submarinos.



Para você ter uma ideia das dimensões de uma fibra veja a figura a seguir, trata-se de uma fibra multimodo em que a casca tem 125 mícrons e o núcleo 62,5 mícrons, abaixo tem uma agulha para comparação das dimensões.



6.2.4 Onde Devo Utilizar os Tipos de Fibra Óptica Monomodo e Multimodo na prática?

A grande vantagem da fibra monomodo cabos de fibra óptica é a possibilidade de transmissão de sinais em longa distância.

Normalmente essas distâncias podem ser de até 120 quilômetros sem o uso de regeneradores ópticos.

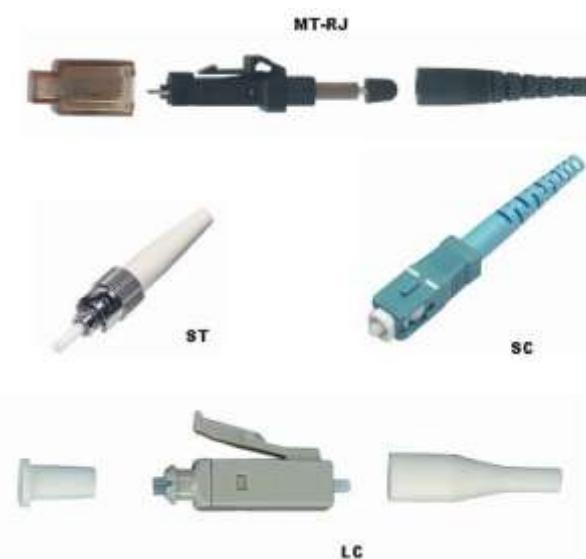
Já as fibras multimodo tem uma faixa máxima de transmissão é de cerca de 2 km.

Portanto, se sua empresa tem links internos de até 2km conectando os switches de Core, Distribuição e Acesso, as fibras multimodo podem ser utilizadas tranquilamente.

Agora, se houver necessidade de links com distâncias superiores a 2km até 120km o uso de uma fibra óptica monomodo é mais recomendado.

6.2.5 Principais Tipos de Conectores Ópticos

Os conectores ópticos tem a função de deixar a fibra perfeitamente alinhada nos pontos de conexão para que o sinal luminoso possa ser transmitido sem grandes perdas. Os quatro tipos de conectores mais comuns são LC, SC, ST e MT-RJ, veja a figura abaixo.



Os conectores ST e SC eram os mais populares até pouco tempo atrás, mas os LC têm crescido bastante em popularidade e podem vir a tornar-se o padrão dominante.

Os conectores MT-RJ também têm crescido em popularidade devido ao seu formato compacto, mas ainda estão restritos a alguns nichos. Como cada conector oferece algumas vantagens sobre os concorrentes e é apoiada por um conjunto diferente de empresas, a escolha recai sobre o conector usado pelos equipamentos que pretender usar.

O LC (Lucent Connector) é um conector miniaturizado que, como o nome sugere, foi originalmente desenvolvido pela Lucent. Ele tem bastante popularidade, sobretudo no uso de fibras monomodo. Ele é o mais comumente usado em transceivers 10 Gigabit Ethernet.

É possível também utilizar conectores diferentes dos dois lados do cabo, usando conectores LC de um lado e conectores SC do outro, por exemplo. Além disso, existem adaptadores para que você possa conectar fibras do mesmo tipo ou de tipos diferentes. Veja a figura a seguir com um cordão com conector MT-RJ em uma ponta e outra com conector LC. O cordão óptico também é conhecido como "pigtail".

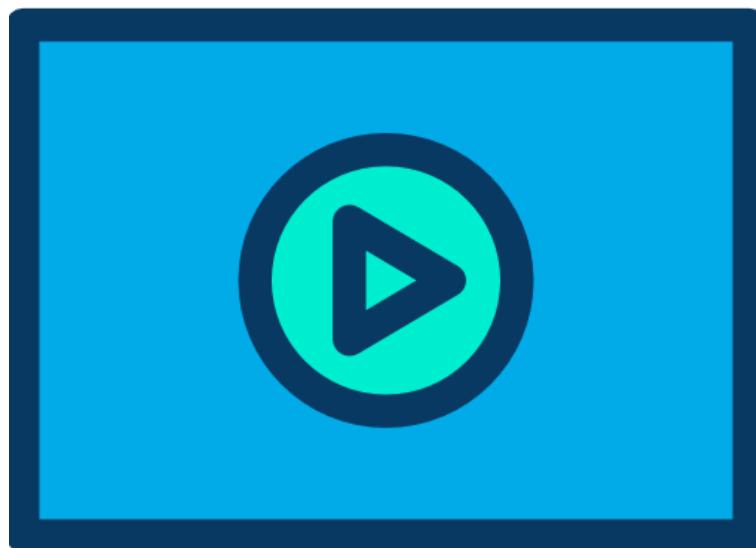


Outro equipamento muito comum de ser encontrado em redes que utilizam fibras ópticas são as caixas de distribuição ópticas (que podem ser também caixas de emendas ópticas ou caixas de terminações ópticas), utilizadas para acomodar as conexões de fibra e é onde normalmente fica terminado um circuito de fibra.

Elas são utilizadas para conectar do equipamento, como um switch ou conversor óptico à fibra de maneira segura, pois como a fibra é mais sensível que um cabo óptico deixá-la solta seria muito arriscado, seria similar ao patch panel de uma rede metálica. Veja a figura seguinte com uma caixa de terminações ópticas.

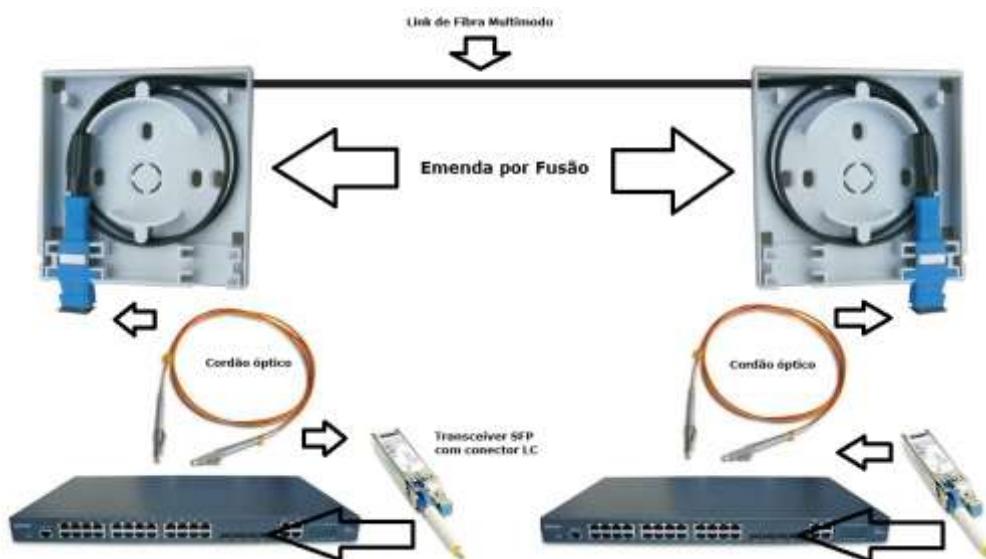


6.2.6 Exemplo de Link Óptico entre Dois Switches

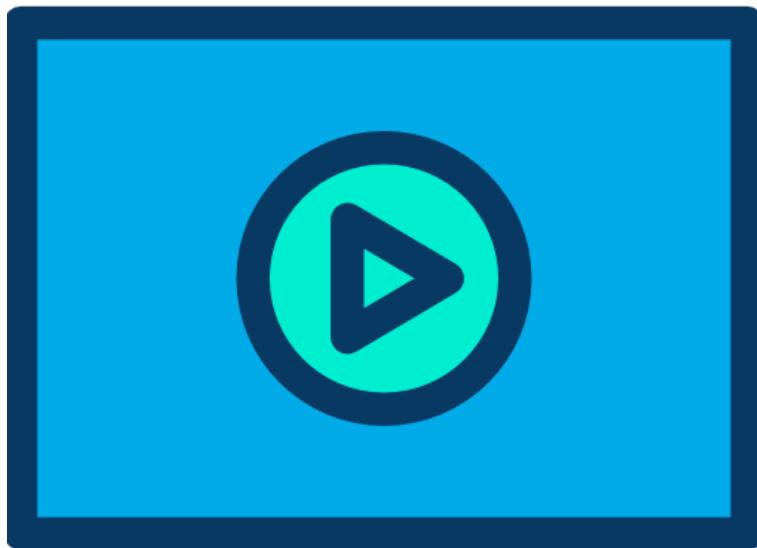


Vamos agora montar um circuito simples com uma conexão óptica entre switches de uma empresa. Por exemplo, temos dois switches com interface SFP com conectores do tipo LC que utilizam fibra multimodo (MM). Portanto, vamos precisar de um cabo de fibra multimodo e duas caixas de terminação ópticas com conectores do tipo LC, lançar um cabo com fibras entre os dois pontos e fazer emendas nas caixas de terminação óptica.

Uma vez o circuito montado o caminho precisa ser testado e depois precisaremos de cordões ópticos para ligar das portas dos switches para a caixa de terminação óptica.



6.3 Opções de Conexões em Switches Cisco Catalyst



Em termos de tecnologia de conexão e cabos os switches Cisco basicamente trabalham com portas da família Ethernet a 10Mbps (Ethernet), 100Mbps Fast Ethernet, 1000Mbps ou 1Gbps (Gigabit Ethernet) e 10Gbps (10-Gigabit Ethernet).

Essas velocidades são suportadas em quase todas as linhas de switches Cisco Catalyst.

Outras opções mais recentes são conexões de 40Gbps e de 100Gbps, principalmente utilizadas em Datacenters e soluções para provedores de serviços.

Quando falamos das tecnologias 10/100/1000 Mbps podemos utilizar tanto cabos UTP categoria 5 ou superior com conector RJ-45 para distâncias até 100m ou fibras ópticas para links mais longos ou conexões entre switches.

Todas essas tecnologias tem a mesma raiz no 802.3 e seguem o mesmo formato de quadro, operação do CSMA/CD, full duplex e outras características do Ethernet, porém o padrão específico do Gigabit Ethernet é definido no 802.3z, pois a sua camada física teve que sofrer alterações devido ao aumento da velocidade de transmissão.

Veja alguns padrões e suas respectivas distâncias a seguir.

Padrão/Tecnologia	Tipo de cabo	Pares	Comprimento do enlace
10BASE-T	UTP categoria 3, 4 e 5	2	100m
100BASE-TX	UTP categoria 5	2	100m
100BASE-FX	Fibra óptica multimodo 62,5/125 (MMF)	1	400m half-duplex ou 2000m full-duplex
	Fibra óptica monomodo (SMF)	1	10km
1000BASE-T	UTP categoria 5	4	100m
1000BASE-SX	Fibra óptica multimodo 62,5/125 (MMF)	1	275m
	Fibra óptica multimodo 50 micrônico e laser 850nm (MMF)	1	550m
1000BASE-LX/LH	Fibra óptica multimodo 62,5/125 e laser de 1300nm (MMF)	1	550m
	Fibra óptica multimodo 50 micrônico e laser 1300nm (MMF)	1	550m
	Fibra óptica monomodo 9 micrônico e laser de 1300nm (SMF)	1	10km
1000BASE-SX	Fibra óptica monomodo 9 micrônico e laser de 1550nm (SMF)	1	70km
	Fibra óptica monomodo 8 micrônico e laser de 1550nm (SMF)	1	100km

Já o 10-Gigabit Ethernet segue a 802.3ae que difere das antecessoras na camada física (PHY – Physical layer) operando apenas com full-duplex.

Além disso, são definidos vários tipos de transceivers utilizados como Protocol Media Dependent ou PMD e classificados como:

- **LAN-PHY:** utilizado em LANs predominantemente no Core.
- **WAN-PHY:** utilizado em interfaces SDH/Sonet para conectar principalmente em redes MAN.

Assim como para os padrões antecessores o 10-Gigabit tem nomenclaturas e padrões que determinam o meio físico e distâncias cobertas pelos enlaces, vamos ver os principais exemplos a seguir.

10GBASE-SR/SW (850 nm serial)	Fibra óptica multimodo 50 micrônico (MMF)	66m
	Fibra óptica multimodo 50 micrônico (MMF – 2GHz km modal bandwidth)	300m
	Fibra óptica multimodo 62,5 micrônico (MMF)	33m
10GBASE-LR/LW (1310 nm serial)	Fibra óptica monomodo 9 micrônico (SMF)	10km
10GBASE-LR/LW (1550 nm serial)	Fibra óptica monomodo 9 micrônico (SMF)	40km
10GBASE-SR/SW (850 nm serial)	Fibra óptica multimodo 50 micrônico (MMF)	300m
	Fibra óptica multimodo 62,5 micrônico (MMF)	300m
	Fibra óptica monomodo 9 micrônico (SMF)	10km
10GBASE-CX4	Par metálico CX4 com conector Infiniband	15m
10GBASE-T	UTP categoria 6A ou 7	100m

Normalmente encontramos switches de acesso com portas 10/100 Mbps ou 10/100/1000 Mbps através de portas UTP de 8, 12, 16, 24 e 48 portas com duas ou até quatro SFPs que são entradas para módulos de fibra.

As conexões de 10G normalmente são disponibilizadas em módulos chamados XENPAKs, X2 e SFP+, sendo que os módulos X2 são menores que as XENPAKs e as SFP+ são menores ainda que as duas, permitindo a conexão em switches menores, pois as duas outras normalmente são utilizadas em módulos de switches como 4500 e 6500.

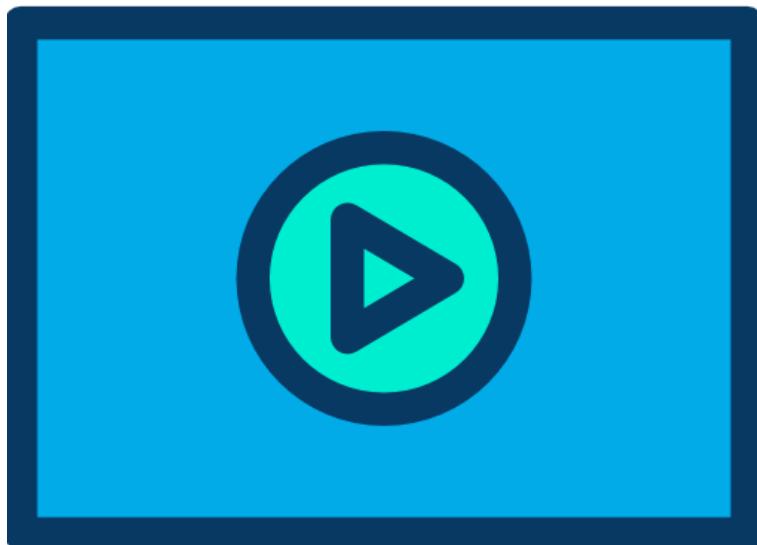
Veja algumas imagens com diferentes padrões de módulos de fibra.



Outro tipo de conexão que podemos encontrar em campo é **GigaStack**, **StackWise** e **StackWise Plus** utilizados para o empilhamento (stacking) de switches através de conectores proprietários que permitem altas taxas de transmissão. Veja exemplo abaixo onde temos uma pilha de switches conectados através de **StackWise** deixando as portas liberadas para conexão de clientes.



6.4 PoE – Power Over Ethernet



Um dispositivo de rede e um endpoint, que são muito utilizados nas redes, normalmente necessitam de uma fonte de alimentação, os quais são:

- Telefones IP
- Access Points
- Câmeras IP

Imagine uma rede com 500 telefones IP e 50 access points, note que isso não é uma rede de grande porte. Pense que teríamos que ter 550 tomadas a mais, além das que já precisamos para alimentar esses dispositivos.

Mas isso não poderia ser resolvido se o próprio ponto de rede que conecta esses dispositivos já fornecesse a energia necessária para que eles funcionassem?

Essa é a função do PoE ou Power over Ethernet (em português alimentação via cabo Ethernet)!

Além disso, estamos entrando na era dos dispositivos IoT, os quais muitos serão alimentados via PoE também.

Existe uma família de padrões que tem a função de fornecer energia a endpoints, porém chamamos todas de uma maneira geral como Power over Ethernet ou PoE.

Numa arquitetura com PoE precisamos ter uma fonte de energia, a qual pode ser a fonte de um switch ou réguas de alimentação PoE ou até mesmo apenas um alimentador simples, porém aqui vamos focar nos switches.

Esse equipamento é chamado de PSE ou Power Sourcing Equipment.

A energia será fornecida pelo mesmo cabo UTP que conecta o endpoint, o qual na arquitetura PoE é chamado de PD ou Powered Devices. Veja imagem a seguir.

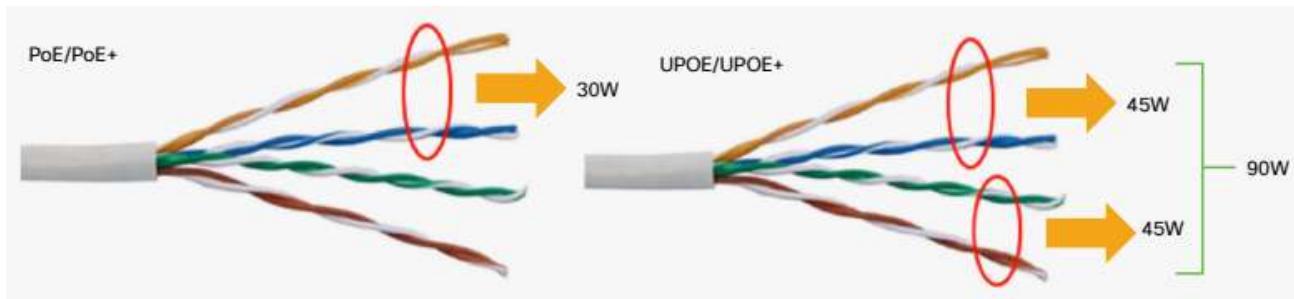


Podemos ter PoE padronizados pela IEEE (PoE e PoE+) e suportados por quaisquer dispositivos ou proprietários da Cisco (UPOE e UPOE+). Além disso, existe um padrão mais antigo também proprietário da Cisco chamado Inline Power (ILP).

Abaixo segue um quadro com as características de cada padrão de PoE.

	PoE	PoE+	Cisco UPOE	Cisco UPOE+
Categoria Mínima	Cat 5e	Cat 5e	Cat 5e	Cat 6a
Padrão IEEE	802.3af	802.3at	Cisco	Cisco
Potência Máx. no PSE	15.4W	30W	60W	90W
Potência Mín. para o PD	12.95W	25.5W	51W	71.3W
Quantidade de pares	2	2	4	4
Distância	100 m			
Performance	sem impacto			

Veja a imagem abaixo para fixar o número de pares e como a potência é fornecida de acordo com os padrões anteriores.



6.4.1 Detecção e Negociação de Potência via PoE

Cada dispositivo alimentado pelo PoE tem uma necessidade específica de energia, assim como uma rede elétrica temos equipamentos 110V e 220V temos diversos níveis de potência e energia que podem ser danificados caso recebam a quantidade de energia errada.

Para evitar esse tipo de problema a IEEE estendeu o processo de autonegociação utilizado pelo Ethernet para o PoE.

Portanto, antes de iniciar a fornecer a energia necessária ao PD existe esse processo de negociação ou autonegotiation, o qual ocorre antes mesmo do PD ser iniciado.

O primeiro passo quando um endpoint é conectado a um switch que suporta PoE, ou seja, um PSE, é que ele precisa verificar se esse endpoint é ou não um PD.

Para isso o PSE envia um pulso de detecção de voltagem no cabo para medir a corrente elétrica.

Se o PSE detecta uma assinatura válida (conforme voltagens definidas pela IEEE 802.3af/at), um PD é detectado.

A partir desse momento o PSE manda pulsos curtos de voltagem nos pares e mede quanta potência o PD necessita.

O PD responde aos pulsos com uma quantidade de corrente elétrica pré-determinada para que o PSE determinar a classe de dispositivo que esse PD pertence conforme tabela a seguir. Note que Class é a classe e Power é a Potência.

Class	Power (W)	Class (mA)
0	0.44 - 12.95W	0 - 4 mA
1	0.44 - 3.84W	9 - 12 mA
2	3.84 - 6.49W	17 - 20 mA
3	6.49 - 12.95W	26 - 30 mA
4	12.96 - 25.5W	36 - 44 mA

Se ambos PSE ou o PD são tipo 1 (PSE suportando máximo de 15.4W ou PD Classe 0 a 3), esse handshake via hardware é finalizado e a potência necessária (até 12.95W) é fornecida conforme classe do PD provisionada na porta do PSE.

Por padrão um PSE tipo 1 fornece apenas classificação em um evento (one-event classification), conforme descrito anteriormente e não importando o tipo do PD que está na ponta.

Se o PSE e o PD forem tipo 2 pode ocorrer um segundo passo de negociação ou um segundo handshake.

Pode haver uma classificação via hardware em dois eventos ou dois passos ou então uma classificação via CDP (Cisco Discovery Protocol) ou LLDP (Link Layer Discovery Protocol).

Esses dois métodos de classificação são utilizados para determinar a potência de dispositivos que necessitam de maior energia, podendo chegar até 90W de potência.

Falando ainda sobre o gerenciamento da potência que pode ser realizado pelo CDP e LLDP, que são protocolos para troca de informações de vizinhança (serão estudados em curso a parte), existem um ajuste previsto na IEEE 802.3af chamado "Inline Power IEEE Power Classification Override".

Esse classification override monitora um PD e exige que ele use menos potência que o previsto pela IEEE, caso a comparação do consumo feito pelo PD com o consumo previsto pela IEEE 802.3af ultrapassa o limite definido na norma o PD será desconectado.

A porta onde esse PD está conectada é colocada em shutdown (desligada), um informe de error-disable é mostrado na Interface (show interfaces) e uma mensagem será gerada via syslog (serviço de envio de avisos).

6.4.2 PoE e Design de LANs

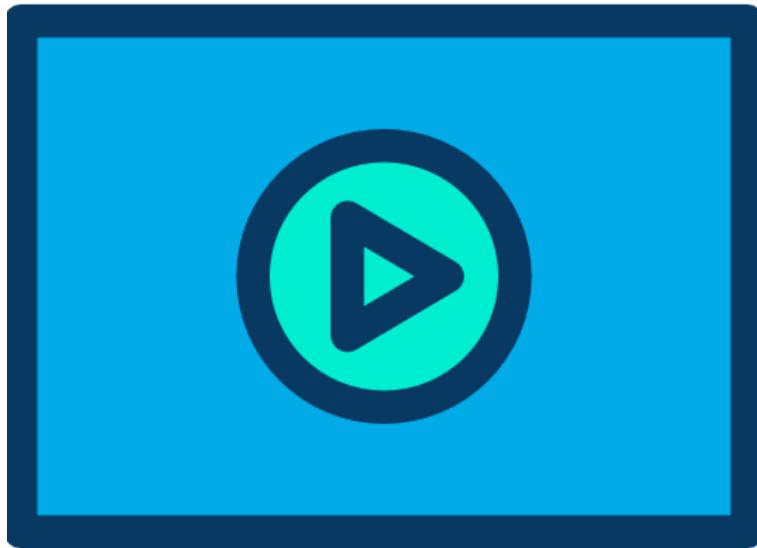
Apesar de parecer simples, existem alguns fatores sobre o uso do PoE que nem sempre são claros nas documentações. Veja abaixo os principais pontos a se considerar em uma LAN que necessita de PoE:

- **Powered Devices:** verifique o tipo de PD que você irá utilizar na rede, os padrões que ele suporta e quanto de energia que você deverá fornecer para cada um deles.
- **Requisitos de Potência:** tenha todos os tipos e quantidades de PDs a serem utilizados na rede para determinar seu "power budget" ou orçamento de potência. Com esse valor você saberá quanto de potência cada switch precisará fornecer para a rede.
- **Portas dos Switches:** alguns switches não suportam PoE em todas as portas, por isso cuidado com os modelos a serem escolhidos para cada parte de rede.
- **Power Supplies:** alguns switches podem trabalhar com mais de uma fonte de alimentação ou power supply. Dependendo do seu power budget será necessário escolher switches que suportem os requisitos, pois não é porque um switch tem 24 portas PoE que você vai conseguir alimentar 24 dispositivos.

Além disso verifique se os padrões utilizados não estão gastando mais que o endpoint usado como PD necessita, por exemplo, você pode ter dois dispositivos que suportam PoE+, o qual suporta até 30W, mas o PD precisa somente 9W.

Isso pode no final das contas dar um aumento no consumo de energia que está simplesmente sendo desperdiçado.

6.5 Identificando os Principais Problemas em Interfaces e Cabeamento



Falar sobre problemas com cabeamento e interfaces em dispositivos Cisco é falar do comando “show interfaces”.

No “show interfaces” são mostrados os contadores de erro que uma interface pode estar sofrendo. Caso você deseje zerar esse contador para monitorar uma interface a partir daquele certo momento utilize o comando “clear counters interface eth|fast|giga x/y” (o professor explicará a nomenclatura das interfaces durante as vídeo aulas).

Os problemas mais comuns envolvendo interfaces LAN são:

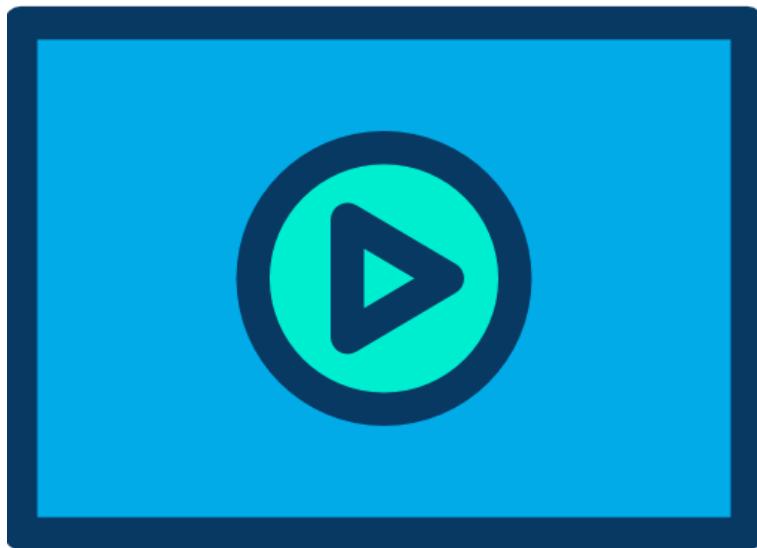
1. **Problemas físicos:** cabos rompidos ou instalados de maneira errada.
2. **Falta do comando “no shut” para ativar a interface:** a interface fica em Administratively Down.
3. **Problemas com “duplex mismatch”:** interfaces configuradas com o duplex em modo errado em uma das pontas.
4. **Colisões ou Collisions:** podemos ter colisões e colisões atrasadas ou late collisions, causadas principalmente pelo comprimento do cabo exceder 100m.
5. **Speed Mismatch:** velocidade da porta configurada errada em uma das pontas.

Vale a pena relembrar abaixo o status que o **show interfaces** pode nos fornecer (*grave muito bem cada uma das condições, seu significado, problemas e como resolvê-los quando aplicável*):

- **up, line protocol is up:** Camadas 1 e 2 funcionando perfeitamente.
- **down, line protocol is down:** Essa saída indica problema na camada física. Pode ser, por exemplo, cabo desconectado nessa interface ou na interface remota. Na prática estes são os problemas mais comuns, ou seja, cabos com problemas ou mal conectados, portanto a resolução passa por verificar o cabeamento ou se a interface remota não está ativada (em shutdown).
- **up, line protocol is down:** Nesse caso a camada física está ok, mas a camada de enlace não. Normalmente são encapsulamentos ou o protocolo de camada-2 configurado errado (raro em interfaces LAN).
- **is administratively down, line protocol is down:** Essa saída indica que a sua interface foi localmente colocada no estado de shutdown. Entre na configuração da interface e dê um “no shutdown”.

- **down, line protocol is down (err-disabled)**: ocorreu algum problema em um protocolo ou recurso de segurança que desabilitou a porta, por exemplo, falha de segurança no port-security, classification override (PoE detectou que o PD usou mais energia que o previsto no padrão IEEE), etc.

6.5.1 Um pouco mais sobre Comando Show Interfaces



Apesar de o comando **show interfaces** ser bem conhecido, a maioria das vezes ele é utilizado apenas para ver se a interface está up ou down. No entanto, muitas outras informações úteis podem ser retiradas da saída desse comando.

O comando pode ser utilizado para exibir informações de todas as interfaces (show interfaces) ou para uma interface específica (show interfaces GigabitEthernet1/1 – ou simplesmente sh int gig1/1). Veja o exemplo da saída do comando abaixo para uma interface serial.

```
Switch# show interfaces GigabitEthernet1/1
GigabitEthernet1/1 is up, line protocol is down
Hardware is Gigabit Ethernet Port, address is 0004.dd46.7700 (bia 0004.dd46.7700)
Internet address is 192.168.1.1/24
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Auto-duplex, Auto-speed
ARP type: ARPA, ARP Timeout 04:00:00
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
```

Vamos agora ver as informações mais importantes do show interfaces e os problemas que podem gerar crescimento nos contadores de erros.

Dividiremos as explicações em dois blocos.

- **Internet address is 192.168.1.1/24** - esse campo nos diz o endereço IP configurado na interface.
- **MTU** – O MTU (Maximum Transmission Unit ou Unidade Máxima de Transmissão) é 1500 bytes. O MTU refere-se ao tamanho máximo do datagrama que uma camada de um protocolo de comunicação pode transmitir.
- **BW 1000000 Kbit** – essa parte nos mostra a largura de banda configurada na interface (comando bandwidth). Caso esse parâmetro não seja configurado em interfaces seriais será adotado o valor padrão de 1544 Kbit/sec e as Interfaces LAN mostram o valor correto, não sendo necessário o bandwidth. Lembre-se que o parâmetro bandwidth é utilizado por alguns protocolos de roteamento (EIGRP, por exemplo) para calcular a métrica de uma rota. Para as interfaces LAN (Eth, Fast e Giga) não é preciso configurar o bandwidth.
- **DLY** – representa o Delay ou atraso padrão de uma interface. Esse valor é padrão e cada tipo de Interface tem um atraso pré-definido medido em micro segundos, por exemplo, o atraso dessa interface serial é de 20.000 micro segundos, ou seja, 0.02 segundos. Já para uma interface giga é de 10 micro segundos.
- **Reliability** – é a confiabilidade da interface medida em um máximo de 255, portanto o 255/255 representa que essa interface está 100% confiável. Caso a confiabilidade caia o primeiro valor ficará menor que 255 e quando chegar à zero quer dizer que a interface está inoperante.
- **Tx Load e Rx Load** – é a carga da Interface, ou seja, quantos por cento da largura de banda está sendo utilizada pela Interface. A medida é parecida com o da confiabilidade, ou seja, 1/255 representa que a interface está praticamente sem tráfego, já 255/255 representa que está 100% da sua capacidade de banda em uso.
- **Encapsulation**– mostra o tipo de encapsulamento utilizado. O padrão para interfaces Ethernet é o ARPA.
- **Last input, output** - número de horas, minutos e segundos desde que o último pacote foi recebido ou transmitido com sucesso. Essa informação é útil nos casos de falha da interface para verificar a quanto tempo ela está com problemas.
- **Input queue** – exibe informação sobre o número de pacotes na fila de entrada. Size/max/drops = número atual de quadros na fila / número de máximo permitido de quadros na fila antes de começar a descartar quadros / número atual de quadros descartados devido a ter excedido o máximo permitido.
- **Total output drops** – número de pacotes descartados devido à fila está cheia. Por exemplo, imagine que uma grande quantidade de tráfego está chegando ao seu roteador através de interfaces com largura de banda de 2Mbps e que todo esse tráfego está saindo por uma outra interface com um link de 64Kbps. Esse excesso de tráfego na interface de 64Kbps pode fazer com que o parâmetro total output drops aumente, pois ela pode não conseguir processar todas as informações e enviá-las a tempo.
- **Output queue** – após os pacotes serem processados, eles são enviados para fila de saída da interface de saída. Essa linha nos mostra o tamanho da fila de saída, o número máximo permitido e os descartados.
- **Minute input/output rate** – exibe a média da taxa de entrada e saída na interface nos últimos 5 minutos. Aqui podemos ver se nossa interface está sobrecarregada ou não.

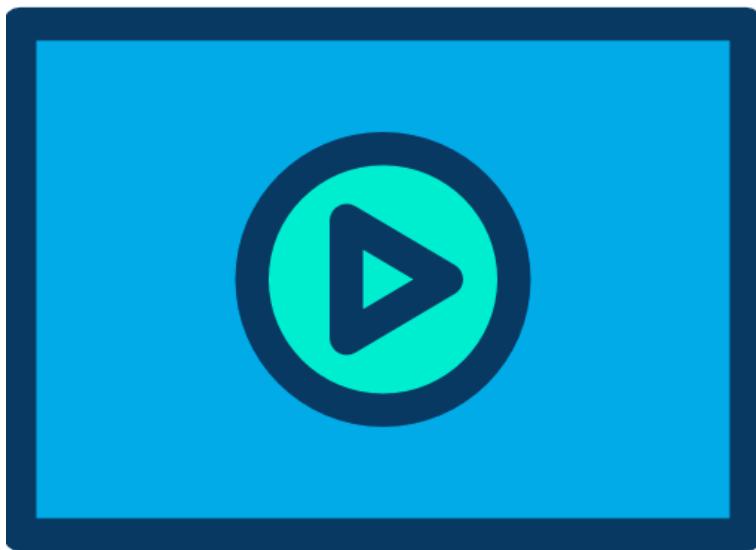
O segundo bloco da saída do comando exibe informações dos contadores de erros. São esses campos que o comando **clear counters** irá zerar, quando executado. Vamos ver os tipos de erros abaixo.

```
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 input packets with dribble condition detected
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
```

- **Packets input/output** – número de total de pacotes recebidos/transmitidos pela interface. Monitorar o incremento desse contador é útil para verificarmos se o tráfego está fluindo corretamente pela interface.
- **Broadcasts** - número total de pacotes de broadcast ou multicast recebidos.
- **Runts** - número de quadros recebidos que são menores do que o tamanho de quadro mínimo do IEEE 802.3 (64 bytes para Ethernet) e com inconsistência no CRC. Possível causa podem ser incompatibilidade no modo duplex ou problemas físicos, como cabeamento, porta ou placa de rede no dispositivo conectado.
- **Giants** - número de quadros recebidos que superam o tamanho máximo permitido pelo IEEE 802.3. Na maioria dos casos esse erro é causado por problema na placa de rede de algum dispositivo (NIC). Procure pelo dispositivo com problema e retire-o da rede. Outro motivo é o recebimento de Jumbo-Frames sem configurar a interface para suportar pacotes acima do MTU.
- **Throttles** - número de vezes que a recepção na porta foi desabilitada, possivelmente devido a uma sobrecarga no buffer do processador. Se exibir um asterisco (*) logo após o valor, significa que a interface está apresentando o problema no exato momento que o comando foi rodado. Exemplos de pacotes que podem sobrecarregar o buffer do processador são pacotes IP com opções, TTL expirado, encapsulamento non-ARPA, fragmentação, tunelamento, pacotes ICMP e outros.
- **Input Errors** - somatório de todos os erros, incluindo runts, giants, no buffer, CRC, frame, overrun e ignored counts. Outros tipos de erros também podem incrementar esse contador e alguns quadros podem apresentar mais de um tipo de erro.
- **CRC** - esse contador incrementa quando o CRC (campo FCS do quadro ethernet) gerado pelo dispositivo remoto não coincide com o checksum calculado no receptor. Geralmente é um indicativo de ruído ou problema na transmissão. Um elevado número de erros de CRC geralmente é um resultado de um elevado número de colisões, mas também pode ser um indicativo de problemas físicos (cabeamento, NIC) ou disparidade no modo duplex configurado.
- **Frame** - número de pacotes recebidos incorretamente com erros de CRC e um número não inteiro de octetos (erro de alinhamento). Geralmente são causados por colisões, problemas físicos (cabeamento, NIC) ou disparidade no modo duplex configurado.
- **Overrun** - número de vezes que o hardware do receptor não foi capaz de suportar os dados recebidos no hardware do buffer. Ou seja, o tráfego de entrada excedeu a capacidade do receptor.
- **Ignored** - número de pacotes recebidos e ignorados pela interface devido a uma baixa na performance do hardware dos buffers internos da interface. Pode ser causado por tempestades de broadcast e tráfego com rajadas de ruídos.
- **Bytes** - número total de bytes transmitido pelo sistema, incluindo dados e encapsulamento MAC.

- **Underruns** - número de vez que o transmissor do dispositivo remoto operou mais rápido do que o receptor do lado local pode suportar. Isso pode ocorrer, por exemplo, em situações onde uma interface esteja recebendo uma grande quantidade de tráfego em rajadas vindo de outras interfaces. Durante uma situação de overrun a interface pode reiniciar.
- **Output Errors** - somatório dos erros que impediram a transmissão final dos datagramas para fora da interface. Geralmente é causado por um tamanho reduzido da fila de saída.
- **Collisions** - número de vezes que ocorreu uma colisão antes que a interface pudesse transmitir o quadro para o meio com sucesso. Colisões são comuns quando a interface está configurada com half-duplex e não deve ocorrer em interfaces full-duplex. Se o número de colisões aumentarem pode ser indicativo de alta utilização do link ou erro na configuração do modo duplex (um lado full e outro half – o correto é ambos serem full ou half).
- **Interface Resets** - número de vezes que a interface foi completamente resetada.
- **Late collision** - colisões atrasadas ocorrem normalmente fora do esperado do padrão que é até o 64º byte do quadro Ethernet. A possível causa de uma late collision são inconsistências no modo de operação **full-duplex/half-duplex** (os dois lados devem ter a mesma configuração), exceder os limites do tamanho do cabo Ethernet (100m), excesso de hubs na rede ou defeito na placa de rede.

6.5.2 Problemas Comuns e Testes em Interfaces LAN



O recomendado para testar problemas de conectividade em interfaces LAN é iniciar da camada física e depois testar a camada de enlace.

Normalmente em interfaces seriais os problemas são detectados pelo incremento dos Input Errors (erros de entrada) e CRC simultaneamente.

O CRC é um check de redundância cíclica que calcula um valor através de um algoritmo (normalmente paridade) e faz uma comparação com um valor previamente calculado na origem. Geralmente Input Errors acompanhados de erros de CRC significam problemas com a linha de transmissão ou o cabo de rede.

Já o output erros em uma interface serial pode significar que a própria placa está com problemas.

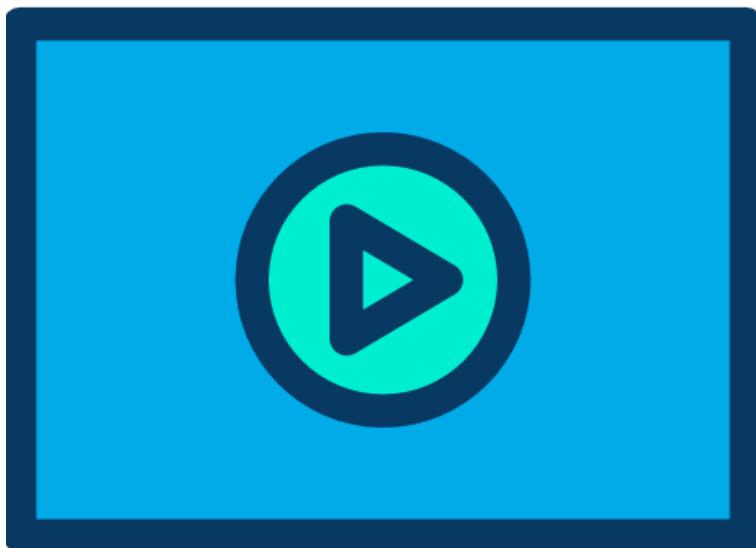
Outros problemas comuns são cabos com padrão errado para conexão dos dispositivos (cross ou direto) e configuração errada da velocidade e/ou modo de operação Duplex/Half-Duplex.

Quando ligamos um cabo errado a interface não irá subir, ou seja, ficará Down/Down.

Existem switches, como os da linha 2960, que possuem o recurso de **Auto-MDIX**, o qual permite que você conecte qualquer tipo de cabo, cruzado ou direto, com o switch que ele irá internamente converter o padrão e fazer a interface funcionar.

No CCNA normalmente não temos o recurso de auto-mdix nos equipamentos e temos que lembrar que entre dois switches, switch/HUB, Roteador/Computador, Computador/Computador e HUB/HUB utilizam-se cabos cruzados, já entre Roteador/Switch ou HUB, Computador/Switch ou HUB utiliza-se cabos diretos.

6.5.3 Problemas com Half/Full-Duplex

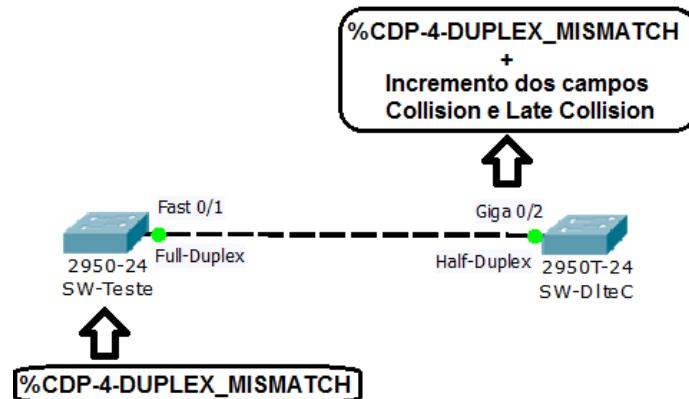


Quando o problema entre duas interfaces LAN é o modo de operação, no roteador ou switch será gerada uma mensagem de erro do tipo "**Mismatch**" (tipo errado ou descasamento de configurações entre as duas pontas).

As mensagens de mismatch são geradas quando em uma das pontas não temos o protocolo ou processo correto configurado, abaixo segue a mensagem que o equipamento dá quando uma das pontas é Half e deveria ser Full-Duplex:

```
14:46:13: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on FastEthernet0/1  
(not half duplex), with SW-DlteC.dltec.com.br GigabitEthernet0/2 (half duplex).
```

Traduzindo a mensagem o switch local detectou que sua interface fast 0/1 está conectada ao switch remoto SW-DlteC.dltec.com.br via Interface Giga 0/2, a qual é Half-Duplex, porém ela está como Full-Duplex, por isso o erro está acontecendo. Veja a figura abaixo.



Como a interface que está configurada como Full-duplex desativa o circuito de detecção de colisões (não detecta mais colisões), os campos de **Collisions** e **Late Collisions** tendem a ser **incrementados** somente na interface que está **configurada como Half-Duplex** nos casos de descasamento do modo de operação.

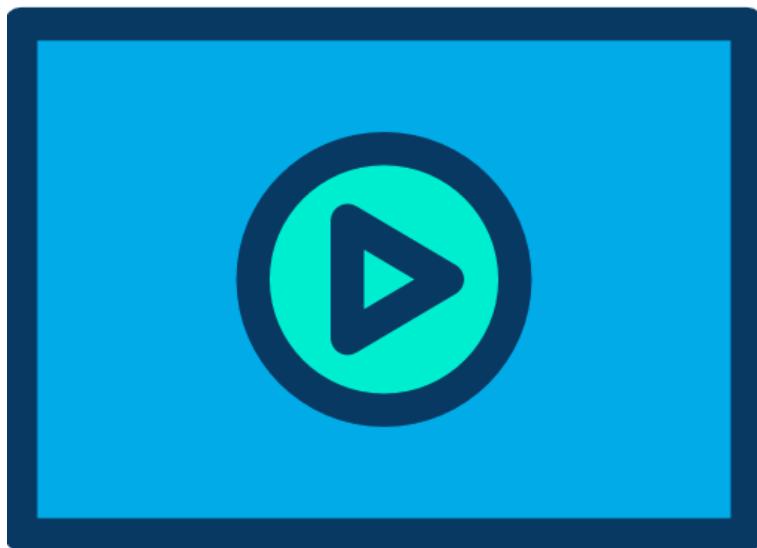
Para visualizar o status das interfaces em **switches**, se elas são half ou full e a velocidade utilize o comando “**show interface status**”, veja exemplo abaixo.

SW-DlteC#sho interfaces status

Port	Name	Status	Vlan	Duplex	Speed	Type
Fa0/1	portas sem telefon	connected	10	a-full	a-100	10/100BaseTX
Fa0/2	portas sem telefon	notconnect	10	auto	auto	10/100BaseTX
Fa0/3	portas sem telefon	connected	10	a-full	a-100	10/100BaseTX
Fa0/4	com vlan de voz	connected	10	a-full	a-100	10/100BaseTX
Fa0/5	com vlan de voz	notconnect	10	auto	auto	10/100BaseTX
Fa0/6	com vlan de voz	notconnect	10	auto	auto	10/100BaseTX
Fa0/7	com vlan de voz	notconnect	10	auto	auto	10/100BaseTX
Fa0/8	com vlan de voz	notconnect	10	auto	auto	10/100BaseTX
Fa0/9	portas sem telefon	notconnect	10	auto	auto	10/100BaseTX
Fa0/10	portas sem telefon	notconnect	10	auto	auto	10/100BaseTX
Fa0/11	com vlan de voz	notconnect	10	auto	auto	10/100BaseTX
Fa0/12	com vlan de voz	notconnect	10	auto	auto	10/100BaseTX
Fa0/13	com vlan de voz	notconnect	10	auto	auto	10/100BaseTX
Fa0/14	com vlan de voz	notconnect	10	auto	auto	10/100BaseTX
Fa0/15	com vlan de voz	notconnect	10	auto	auto	10/100BaseTX
Fa0/16	com vlan de voz	notconnect	10	auto	auto	10/100BaseTX
Fa0/17	com vlan de voz	notconnect	10	auto	auto	10/100BaseTX
Fa0/18	com vlan de voz	notconnect	10	auto	auto	10/100BaseTX
Fa0/19	com vlan de voz	notconnect	10	auto	auto	10/100BaseTX
Fa0/20		notconnect	10	auto	auto	10/100BaseTX
Fa0/21		notconnect	1	auto	auto	10/100BaseTX
Fa0/22		notconnect	20	auto	auto	10/100BaseTX
Fa0/23	Portas da sala de	notconnect	20	auto	auto	10/100BaseTX
Fa0/24		notconnect	1	auto	auto	10/100BaseTX
Gi0/1		connected	trunk	a-full	a-100	10/100/1000BaseTX
Gi0/2		notconnect	trunk	auto	1000	10/100/1000BaseTX

Note que o comando traz várias informações úteis para o dia a dia da administração de redes com switches Cisco, tais como porta, VLAN, o estado se a porta está conectada ou não, etc. O prefixo “a-” em frente do estado de **Duplex** e **Speed** (velocidade) significa que esse parâmetro foi autonegociado.

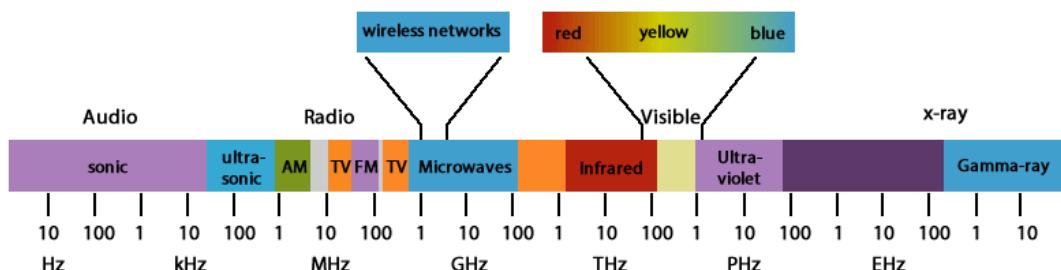
6.6 Conexões Sem Fio – 802.11



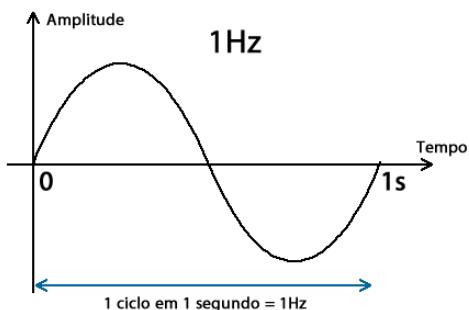
O uso de tecnologias de transmissão sem fio em redes de computadores não é tão novo como se pensa. As primeiras transmissões sem fio aconteceram na década de 70 com redes ponto a ponto utilizando a frequência de 900MHz, porém através de protocolos proprietários e bastante lentas em relação aos padrões atuais.

Para que as redes que conhecemos atualmente do padrão 802.11 fossem desenvolvidas foi necessária a padronização da tecnologia e regulamentação do uso das frequências, pois as frequências de rádio disponíveis são utilizadas por diversos serviços essenciais, tais como polícia e bombeiros, assim como para transmissão de rádio (AM/FM), televisão, telefonia celular e muitas outras aplicações. Essa padronização nasce com a definição do uso de frequências para Aplicações Industriais, Científicas e Médicas (ou ISM) nas décadas de 80 e 90. Em paralelo a IEEE em 1997 define a primeira norma 802.11 que descreve como o sinal deve ser enviado utilizando a faixa de frequências ISM, portanto a maioria dos protocolos que utilizamos atualmente foram desenvolvidos entre 1997 e 2003.

Para entender melhor a transmissão sem fio, vamos analisar a figura abaixo com as faixas de frequência que podem ser transmitidas em meio aéreo ou em “espaço livre”.



Hertz – Hz: A medida de frequência dos sinais é medida em Hz (Hertz), que representa a unidade de frequência derivada do SI (Sistema Internacional de Medidas) para frequência, a qual é expressa, em termos de **ciclos por segundo**, a frequência de um evento periódico, oscilações (vibrações) ou rotações por segundo. Um de seus principais usos é descrever ondas senoidais, como as de rádio ou sonoras.



Note que as frequências mais baixas são as de áudio, sendo que as audíveis pelo ouvido humano estão entre 20Hz e 20KHz (20.000Hz). Depois temos o ultrassom, frequências da rádio AM, FM, sinais de televisão, as quais estão na faixa de KHz (Quilo Hertz - 1.000Hz) e MHz (Mega Hertz - 1.000.000Hz) e então vem as micro-ondas que estão na faixa do GHz (Giga Hertz - 1.000.000.000Hz).

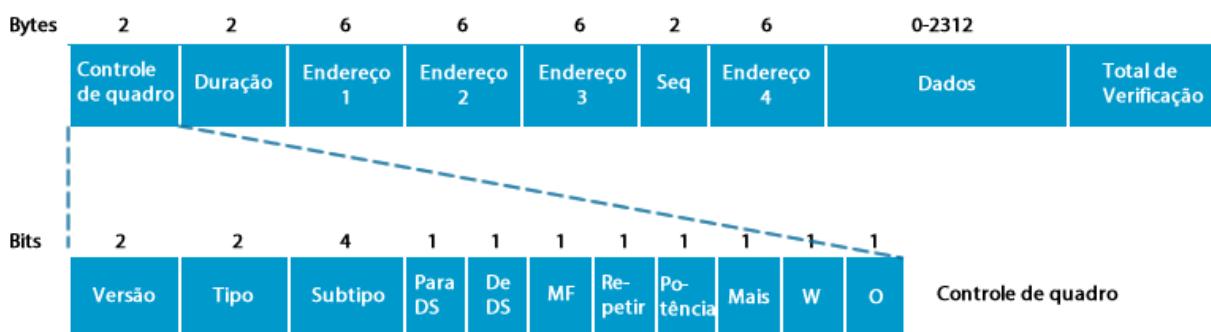
Os sinais das redes 802.11 estão na faixa de frequência entre 1GHz a 5GHz, ou seja, entre um bilhão e cinco bilhões de ciclos por segundo! Acima disso começamos a entrar no infravermelho, o qual também foi e é utilizado até hoje para transmissão de curtas distâncias com velocidade mais baixa, depois temos a luz visível, passando para o ultravioleta, raios-X e raios-gama.

6.6.1 Rede Cabeada versus Wireless

Se compararmos uma rede sem fio com a rede cabeada poderemos entender melhor o que é uma rede sem fio e suas características. Veja abaixo algumas semelhanças e diferenças entre estes dois tipos de redes LAN:

- Ambas são IEEE 802, sendo que as redes com fio fazem parte da família 802.3 e as redes sem fio da 802.11. Isso significa que, para o usuário, se ele estiver acessando uma rede LAN com ou sem fio o acesso será transparente. Tirando a placa de rede que uma tem um conector para plugar o cabo e outra não, o acesso aos dados em uma rede LAN com ou sem fio é transparente para os usuários finais. Veja uma topologia com redes wireless na figura abaixo.
- As redes 802.3 e 802.11 definem o acesso das camadas física e de enlace, sendo que ambos padrões utilizam endereços MAC no mesmo padrão de 48 bits divididos em 12 algarismos Hexadecimais.
- Os mesmos tipos de protocolos das camadas 3 a 7 continuam sendo suportados, pois o 802.11 é apenas um meio de transporte dentro de uma rede LAN sem fio, sendo transparente seu uso para as camadas superiores. Continuamos podendo utilizar o IP, ICMP, HTTP, IPSec, FTP, ou seja, quaisquer protocolos que são utilizados em uma rede com fio continuam valendo para as redes sem fio.

- A principal diferença é que o meio de transmissão utilizado em uma rede sem fio do tipo 802.11 é o ar e não mais cabos metálicos ou fibras ópticas como no padrão 802.3. A transmissão dos dados digitais é realizada por **RF (rádio frequência)** utilizando a faixa das micro-ondas, conforme já estudamos anteriormente. Portanto a primeira e mais gritante diferença está na camada 1 do modelo OSI que utiliza o ar como meio de transmissão para as redes sem fio.
- As redes com fio utilizam o **CSMA/CD** para transmitir os dados, porém como em uma rede sem fio não há como detectar uma colisão ela precisa de um novo protocolo de acesso aos meios, chamado de **CSMA/CA** ou **Carrier Sense Multiple Access with Collision Avoidance**. Nas redes com fio tínhamos a detecção da colisão, porém nas redes sem fio temos que “evitar uma colisão”, por isso o termo “CA – Collision Avoidance”. Portanto, ambos tipos de redes (com e sem fio) utilizam a detecção de portadoras ou “Carrier Sense”, a diferença é que nas redes com fio as colisões são detectadas e nas redes sem fio são evitadas com o uso do protocolo RTS (Request to Send – requisição para enviar) e CTS (Clear to Send – Pronto para enviar). Como em uma rede sem fio não é possível que a estação transmita e receba ao mesmo tempo fica impossível de detectar uma colisão.
- Os quadros do 802.3 e do 802.11 também são diferentes, pois as comunicações sem fio precisam de protocolos adicionais para funcionar, porém os dois utilizam os MACs de origem e destino para montar seus quadros. Veja a figura abaixo, note que o quadro tem quatro campos de endereço, pois deve conter origem e destino para a transmissão e origem e destino para envio até o Access Point.



- As redes sem fio enfrentam mais problemas de conectividade e de privacidade (segurança) que uma rede cabeada. Podemos citar problemas como refração, reflexão, absorção, caminhos múltiplos do sinal (multipath), etc. Além disso, como é muito difícil evitar que o sinal saia dos domínios da empresa, ou seja, que não vaze para fora de um edifício, por exemplo, a parte de segurança é um aspecto fundamental da implementação de uma rede sem fio. Caso contrário, uma invasão ou até mesmo o uso dos recursos da rede por pessoas não autorizadas seria muito simples de se fazer.
- As redes sem fio suportam mobilidade (mobility), facilidade parecida com o **roaming** dos telefones celulares, onde ao cruzar células de rádio sua ligação não cai e sim é “transferida” para a nova célula que você está entrando. Isso possibilita o uso de diversas facilidades em redes corporativas, tais como telefonia IP sem fio.
- As redes sem fio dependem da regulamentação do uso do espectro de frequência de cada País.

Em uma rede cabeada nosso sinal é convertido em impulsos elétricos ou ópticos para serem transmitidos no meio físico, essa é a característica das tecnologias da família 802.3 (Ethernet). Já nas redes sem fio, que pertencem à família 802.11, os bits a serem transmitidos são convertidos em ondas de RF e os bits são codificados ou modulados utilizando diversas tecnologias de espalhamento espectral ou Spread Spectrum.

Algumas empresas fabricantes de equipamentos de rede e placas de rede, tais como 3Com, Nokia, Lucent Technologies (atualmente Alcatel-Lucent) e Symbol Technologies (adquirida pela Motorola) se uniram para criar um grupo para lidar com este tema em meados de 1999, nascendo assim a Wireless Ethernet Compatibility Alliance (WECA), que passou a se chamar Wi-Fi Alliance em 2003. Assim como acontece com outros consórcios de padronização de tecnologias, o número de empresas que se associam à Wi-Fi Alliance aumenta constantemente. Atualmente o grupo conta com a participação de mais de 500 empresas e entidades. Por isso muitas vezes as tecnologias da família 802.11 são chamadas de **Wi-Fi**.



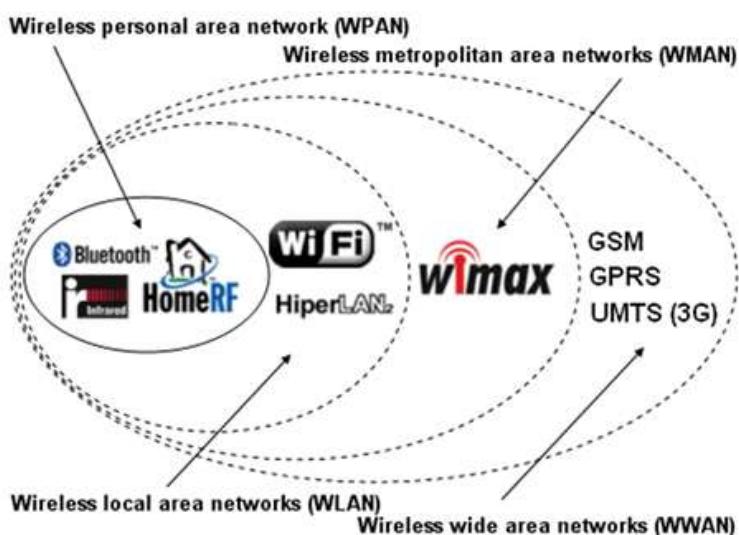
Segundo a Wi-Fi Alliance atualmente existem mais dispositivos WI-Fi em uso do que a quantidade de pessoas na terra, e mais da metade do tráfego da internet passa por uma rede Wi-Fi.

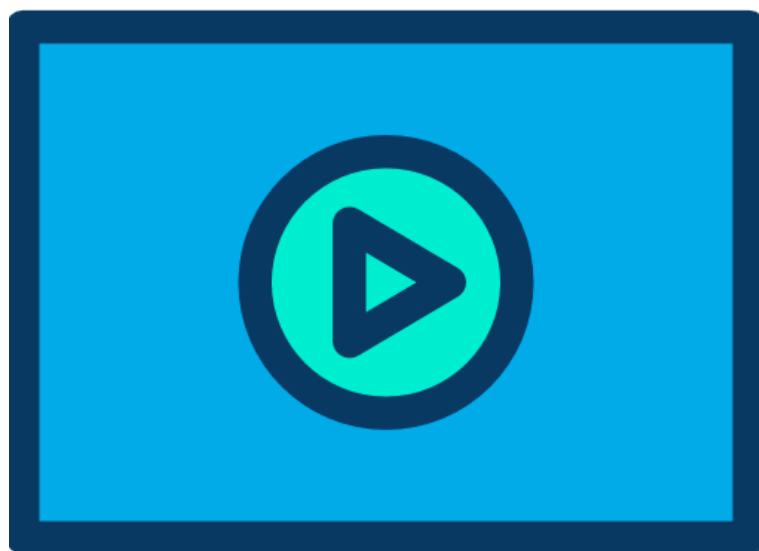
Lembre-se que no Brasil o órgão que regulamenta o uso das frequências é a **Anatel** (Agência Nacional de Telecomunicações).

6.6.2 Tipos de Redes Sem Fio

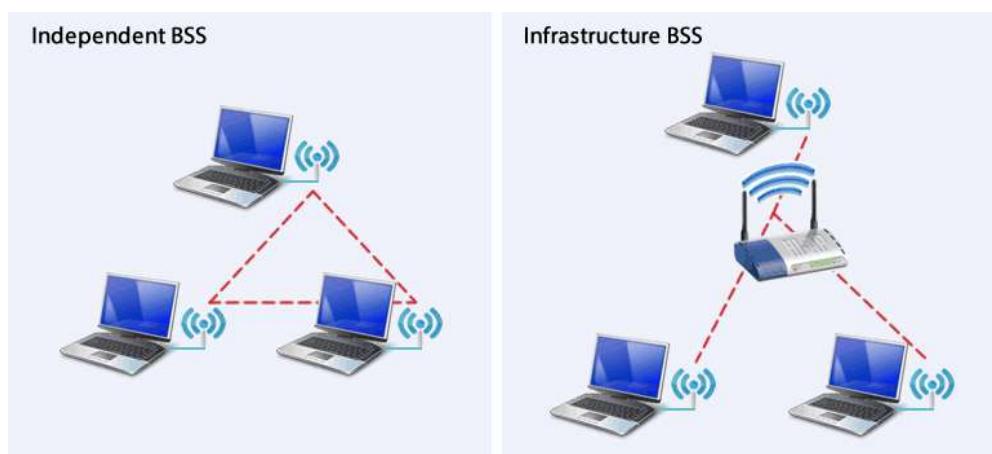
As redes sem fio podem ser divididas em quatro tipos principais (veja a figura abaixo):

- Redes pessoais ou curta distância (**WPAN**)
- Redes locais (**WLAN**)
- Redes metropolitanas (**WMAN**)
- Redes geograficamente distribuídas ou de longa distância (**WWAN**).



6.6.3 Modos de Operação de uma WLAN – Ad-hoc e Infraestrutura

As redes sem fio locais podem operar de dois modos, sendo o primeiro chamado **Ad-hoc** ou **IBSS** (Independent Basic Service Set), e o segundo de Infraestrutura (Infrastructure), a qual pode ser dividida em dois tipos de operação: **BSS** (Basic Service Set) e **ESS** (Extended Service Set). Estes modos definem como a comunicação entre os diversos dispositivos de uma rede local vai ser estabelecida.



6.6.4 Arquiteturas WLAN Ad-Hoc

Em uma rede Ad-hoc ou **IBSS**, temos a comunicação direta entre os equipamentos sem fio, sem a necessidade de um intermediário. É como se criássemos um domínio, ou grupo de trabalho, onde os componentes podem trocar informação direta entre si.



As redes Ad-hoc também são conhecidas como redes sem fio P2P (Peer to Peer) ou IBSS (Independent Basic Service Set – Grupo ou Conjunto de Serviço Básico Independente).

Nesse modo de operação redes com poucos dispositivos podem ser criadas diretamente utilizando os computadores de algumas pessoas e suas placas de rede sem fio para compartilhar informações, por exemplo. Como cada computador em uma rede Ad-hoc está utilizando apenas um rádio, a comunicação feita entre os dispositivos será do tipo half-duplex, assim como acontecia anteriormente com os HUBs em uma rede cabeada.

6.6.5 Arquiteturas WLAN Infraestrutura

As redes em modo Infraestrutura tem sua principal diferença das redes Ad-hoc pela utilização obrigatória de um **ponto de acesso** ou **Access Point (AP)**.

No modo infraestrutura não há comunicação direta entre dois clientes de rede sem fio, pois eles obrigatoriamente precisarão passar pelo AP para falar entre si ou com o restante dos dispositivos da rede cabeada ou com dispositivos que estejam em outras células sem fio distantes.

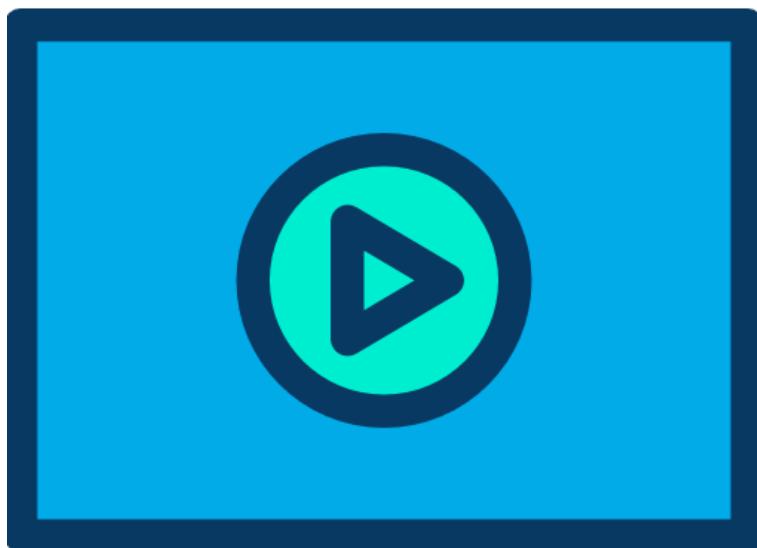


O link ou entroncamento entre o switch e o AP é denominado **DS** (Distribution System ou Sistema de Distribuição), o qual permite que os computadores dessa célula de rede sem fio possam acessar os demais recursos da rede. Este link pode ser, por exemplo, um tronco 802.1Q como vimos no capítulo relacionado às VLANs e switching, o qual seria utilizado para passar uma ou mais VLANs (subredes) da rede física para a rede sem fio.

Os APs não necessariamente terão apenas uma rede vinculada a sua interface aérea, pois existem modelos de AP que possuem mais de uma interface de rádio e permitem a configuração de múltiplas redes LAN sem fio (WLANs) em um mesmo dispositivo. Esta facilidade é utilizada, por exemplo, para fornecer acesso à rede conhecida como **Guest**, ou seja, uma rede disponibilizada para visitantes ou parceiros poderem acessar a Internet com segurança, sem precisar passar pela rede corporativa da empresa.

Agora vamos analisar os dois modos de Infraestrutura sem fio que podemos encontrar na prática: **BSS** e **ESS**.

6.6.5.1 BSS - BASIC SERVICE AREA



A **Basic Service Area** é um modo de operação onde os APs trabalham de forma independente uns dos outros na rede ou temos apenas **um AP isolado**. Este tipo de arquitetura é a que utilizamos em nossas residências ou pequenos escritórios.

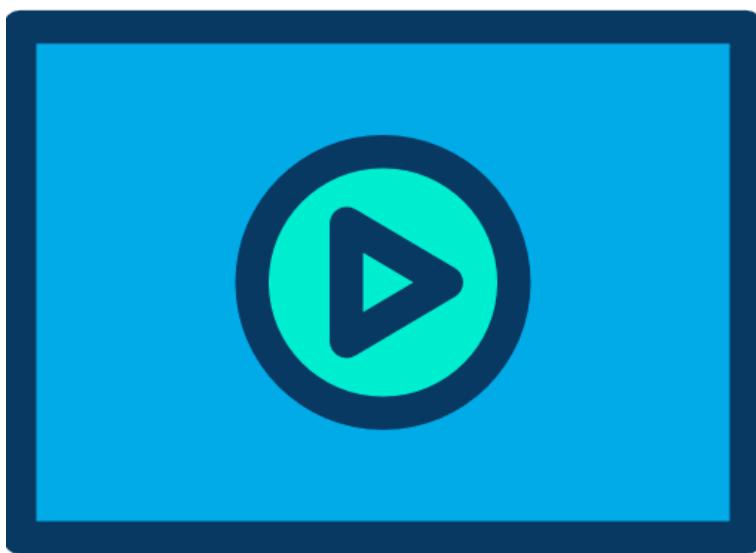


Em uma rede de infraestrutura, as estações devem efetuar a **associação a um AP** para ter acesso aos serviços de rede, a qual é semelhante à função de ligar o cabo ethernet. Um terminal sem fio pode tentar se conectar a qualquer AP, porém é o AP quem decide se permite ou não o seu registro. A função de solicitar a associação é exclusiva do terminal, o qual pode estar associado a um AP por interface sem fio.

Os APs seguem o mesmo conceito de célula da telefonia celular, pois cada AP tem uma área de cobertura e a célula está delimitada pela região que o AP consegue dar cobertura de sinal aos seus clientes. Esta área de cobertura é o BSS ou Grupo de Serviços Básico que o AP irá fornecer aos seus clientes, sendo que a identificação da rede sem fio se dá através do **identificador do grupo de serviços**, conhecido como **SSID** ou **Service Set Identifier**. Veja o detalhe na figura anterior, onde o AP divulga sua rede com o SSID "DLteC".

O padrão 802.11 não impõe nenhuma limitação ao número de terminais que podem estar associados a um AP, porém esta limitação é normalmente baseada nos requisitos de taxa de transmissão necessária para os clientes e por recomendações dos fabricantes. Por exemplo, APs do fabricante Cisco conseguem suportar até 2048 endereços MAC em sua tabela de endereços MAC, porém o fabricante não recomenda mais do que 50 usuários por AP para não afetar o throughput da rede.

6.6.5.2 ESS - EXTENDED SERVICE AREAS



A BSS (rede com 1 AP ou APs isolados) tem apenas a capacidade de cobertura para pequenos escritórios ou instalações pessoais, conforme estudamos anteriormente. Porém, o padrão 802.11 permite a criação de redes wireless de área estendida a partir do **agrupamento de várias BSSs** em uma **ESS (Extended Service Set** – Grupo ou Conjunto de Serviço Estendido).

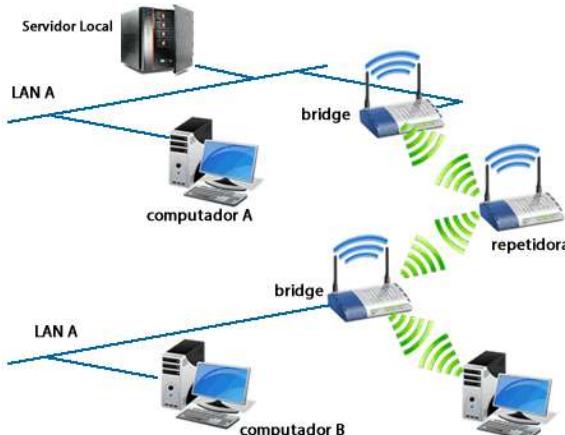
As ESSs são criadas agrupando todas as BSSs utilizando uma rede backbone, sendo que todos os AP na ESS tem configurado **o mesmo SSID** (Service Set Identifier), que funciona como o nome da rede do ponto de vista dos clientes. Um detalhe é que essa tecnologia utilizada na rede backbone não é especificada pelo padrão 802.11, o qual define apenas uma série de serviços obrigatórios que a ESS deve fornecer a seus clientes.

A principal vantagem do uso do modo ESS em rede sem fio é a possibilidade do **Roaming**, ou seja, trocar de célula (trocar de AP) sem perder a conexão de rede. Esse roaming é semelhante ao de uma rede de telefonia celular, onde não há queda da chamada quando você passa de uma célula para outra, pois senão não seria possível falar ao celular quando nos deslocamos de carro ou ônibus. O roaming possibilita implementar recursos de “**mobilidade**” na WLAN com ESS, permitindo que recursos como a telefonia IP sem fio seja possível.

Para a implementação do ESS a maioria dos fabricantes exige o uso de controladoras de redes sem fio, chamadas de **Wireless LAN Controllers** ou simplesmente **WLC** (já estudadas anteriormente).

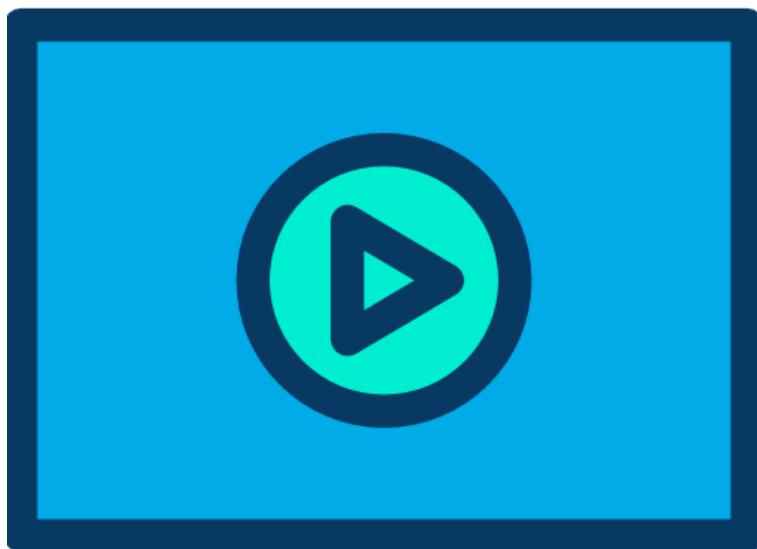
6.6.5.3 OUTROS MODOS DE OPERAÇÃO DOS APs

Além do que já vimos, os APs podem operar com **bridges**, ou seja, apenas uma ponte entre duas redes ou uma extensão para a rede cabeada, porém agora sem fio. Em modo bridge o AP também pode funcionar como uma estação repetidora para aumentar o alcance de uma rede sem fio.



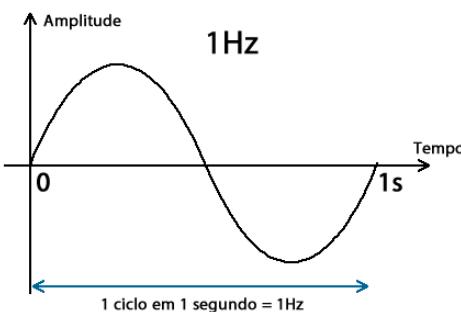
Existem modelos de AP que podem também atuar como um link ponto a ponto em modo bridge, bastando conectar uma antena correta para essa aplicação. Dessa forma, empresas podem estender a comunicação entre suas edificações que está em linha de visada (que dá para enxergar sem obstáculos) sem o uso de cabos metálicos ou fibras ópticas.

6.6.6 Técnicas de Modulação – Enviando um Bit via RF



Como já estudamos anteriormente, em uma rede 802.3 podemos ter as interfaces físicas metálicas e ópticas. Com pares metálicos os bits são transmitidos através de níveis de tensão, por exemplo, +5V para o bit 1 e -5V para o bit zero. Já para uma transmissão óptica é ligando e desligando o laser ou led que representamos os bits um e zero respectivamente. Mas e com uma rede sem fio, como os bits são representados?

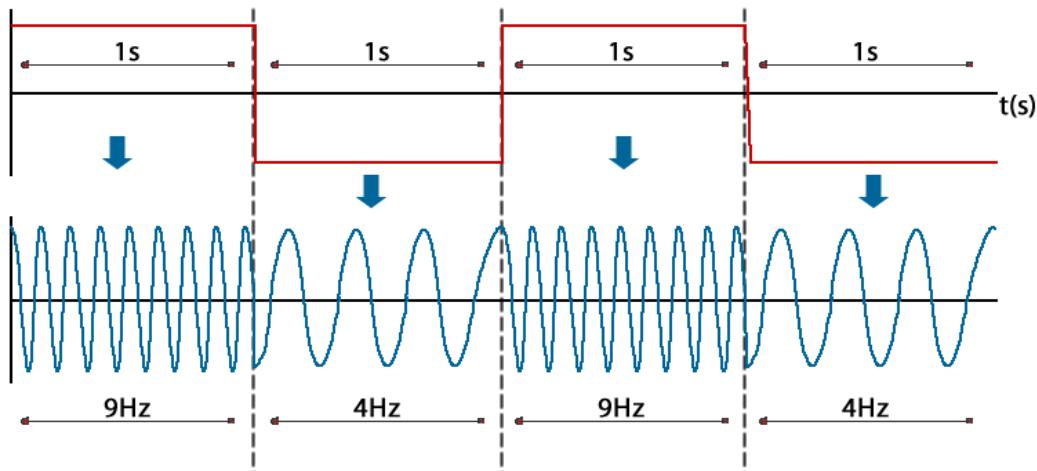
Vamos primeiro analisar o que é uma onda. Veja na figura ao lado que a onda eletromagnética é um sinal que varia com o tempo e tem duas características básicas: Amplitude e Frequência.



A amplitude está na vertical do gráfico e representa a altura da onda eletromagnética, ou seja, quanto menor a amplitude mais difícil de um receptor perceber aquela onda. Em outras palavras, a onda com uma amplitude muito baixa pode ser tão fraca que será impossível do receptor perceber ou ler aquela informação. O oposto é que a amplitude pode ser tão grande que pode ser demais para o receptor e pode danificá-lo ou simplesmente ficar irreconhecível para leitura.

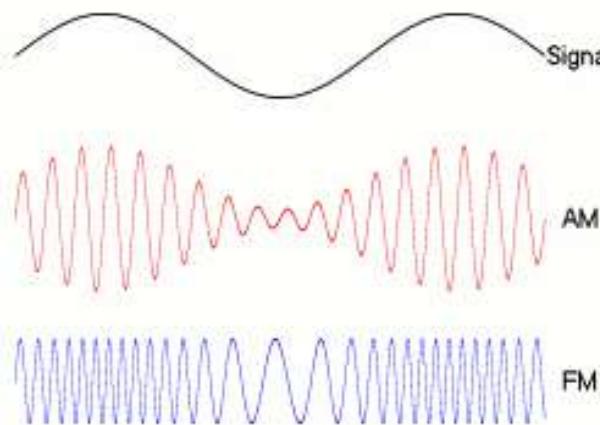
A variação dessa amplitude no tempo é cíclica e a cada ciclo completado em um determinado período tempo representa a frequência que essa onda tem, a qual é medida em Hertz. No exemplo da figura a onda completa um ciclo em um segundo, o que caracteriza um Hertz ou 1Hz. Quanto mais ciclos por segundo a onda completar maior a frequência dela, por exemplo, se ela completar 10 ciclos em 1 segundo ela tem 10 Hz. Lembre-se do início desse capítulo onde vimos que os sinais sem fio estão entre 1 e 5 Giga Hertz, isso quer dizer que os sinais completam cinco bilhões de ciclos em um segundo!

Agora podemos utilizar estes dois parâmetros básicos para criar exemplos de modulação, ou seja, representar um sinal elétrico através de uma onda eletromagnética. Por exemplo, podemos utilizar a frequência para representar dois níveis de um sinal elétrico, veja o exemplo na figura ao lado onde temos um sinal elétrico quadrado que varia de um em um segundo (1Hz) em um nível de tensão positivo e outro negativo. Nesse exemplo de modulação do sinal elétrico utilizamos a frequência de 9Hz para representar o sinal positivo e de 4Hz para representar o sinal negativo.



Quando o receptor captar o sinal de 9Hz ele irá converter para a tensão positiva e o sinal de 4 Hz para a negativa. Note que esse é um exemplo apenas ilustrativo, pois as modulações que são utilizadas nos padrões 802.11 são muito mais complexas, porém este é o princípio básico de uma modulação de um sinal em redes sem fio.

Além da frequência, podemos utilizar a amplitude e a fase do sinal para implementar técnicas de modulação, podendo ainda fazer técnicas compostas que utilizam mais de uma característica para compor a técnica de modulação. Veja a figura abaixo (na matéria online temos uma animação sobre isso) comparando a modulação em frequência e amplitude de uma onda senoidal.

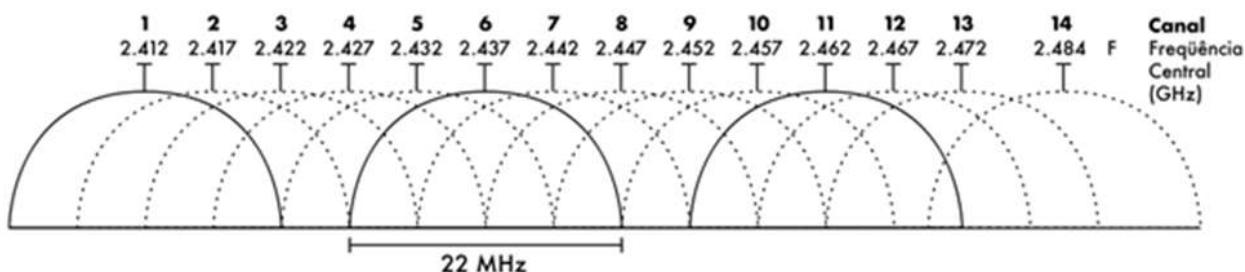


Na prática os padrões 802.11 utilizam basicamente técnicas de espalhamento espectral (Spread Spectrum) para transmitir o sinal com as modulações do tipo:

- **Frequency-hopping Spread Spectrum (FHSS)**: foi utilizado pela primeira versão de 802.11 (versão original) e não é utilizado atualmente.
- **Direct-sequence Spread Spectrum (DSSS)**: utilizado pelos padrões 802.11b e 802.11g.
- **Orthogonal Frequency-division Multiplexing (OFDM)**: utilizado pelos padrões 802.11a, 802.11g, 802.11n e 802.11ac.

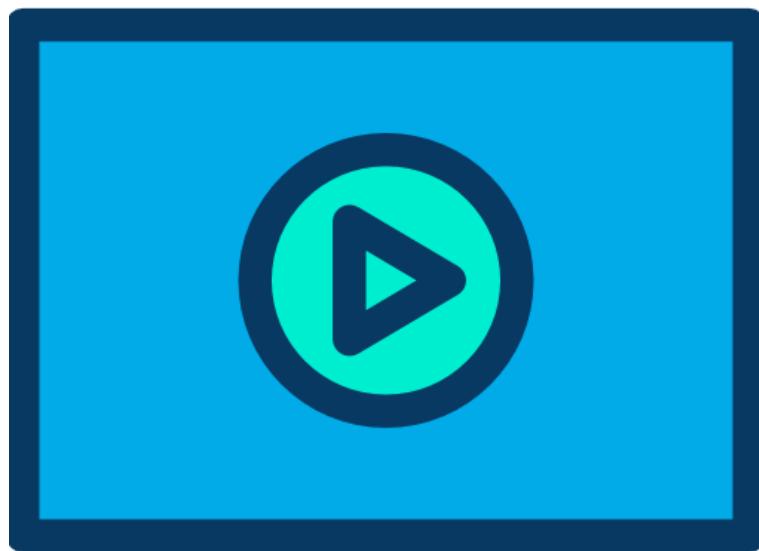
O espalhamento espectral consiste em codificar e modificar o sinal de informação executando o seu espalhamento no espectro de frequências, ou seja, ao invés de utilizar uma frequência específica o sinal passa em várias faixas de frequência ou **canais**. Portanto, o sinal espalhado ocupa uma banda maior que a informação original, porém acaba utilizando menos potência e baixa relação sinal/ruído. O receptor deve estar sincronizado com o transmissor, ou seja, deve saber previamente a sequência de canais onde o transmissor vai saltar para poder sintonizar estes canais e receber os pacotes transmitidos.

Ainda nesse capítulo, quando estudarmos os padrões 802.11, você poderá visualizar os canais que cada tecnologia utiliza. Veja agora o exemplo dos canais que o 802.11g pode utilizar na figura abaixo. Note que o padrão 802.11g utiliza 14 canais e cada um deles ocupa 22MHz de largura de banda de RF, isso significa que se utilizarmos dois APs 802.11g próximos um do outro precisaremos escolher canais que não interferem entre si. Por exemplo, em um deles podemos utilizar o canal 1 e no outro o canal 6, conforme destacado na figura. Note que os canais de 2 a 4 utilizam uma faixa de frequências que podem interferir no canal 1 e o canal 5 está no limite, ou seja, “colado” com o canal 1. Por isso a escolha dos canais 1 e 6, porque há um espaço de frequências seguro entre os dois, evitando possíveis interferências.



No projeto de redes sem fio de maior porte, onde são utilizados diversos APs e o modo ESS de Infraestrutura sem fio, a escolha dos canais para garantir a sobreposição segura entre as células é fundamental. Na prática os engenheiros e técnicos de campo costumam chamar a atividade de escolha dos canais de “**canalização**” ou “**non-overlapping channels**” (canais sem sobreposição).

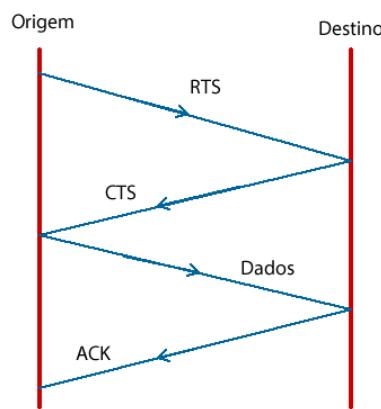
6.6.7 Funcionamento Básico do CSMA-CA



O **CSMA/CA** ou “**Carrier Sense Multiple Access with Collision Avoidance**” (Acesso múltiplo com verificação de portadora com prevenção de colisão) é um método de controle de acesso ao meio sem fio que, ao contrário do CSMA/CD, antes de transmitir efetivamente um pacote (dados), a estação transmissora **avisa sobre a transmissão e em quanto tempo** irá realizar a tarefa para **prevenir** (evitar) que uma colisão ocorra.

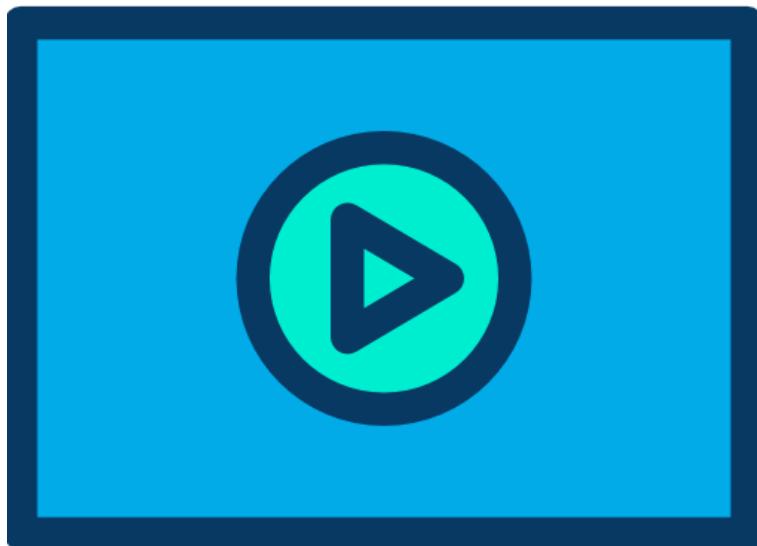
Por isso o termo “**Collision Avoidance**” (prevenção de colisão) substituiu o termo “**Collision Detection**” (detecção de colisão) nas redes sem fio em relação às redes cabeadas. Nas redes cabeadas existem meios de detectar uma colisão, enquanto em uma rede sem fio não é possível.

Os dispositivos de uma rede (WLAN) devem sentir (ouvir) o meio para verificar alimentação (estímulo de RF acima de certo limite) e esperar até que o meio esteja livre antes de transmitir, ou seja, verificar a **portadora**. Para evitar as colisões no ambiente sem fio é utilizado um recurso chamado “**solicitar para enviar**” e “**livre para enviar**” (**Request to Send - RTS / Clear to Send - CTS**).



Portanto, o **RTS/CTS** do **CSMA/CA** lembra muito o handshake triplo realizado pelo TCP para estabelecer uma conexão antes de iniciar o envio dos segmentos, porém aqui estamos em camada 1.

6.6.7.1 DESCOBRINDO UMA REDE SEM FIO (SCAN)



Pela natureza das redes sem fio, o ponto de acesso precisa **anunciar** a existência da rede para que os clientes possam se conectar e utilizar os serviços e recursos de rede. Uma rede sem fio é reconhecida pelo seu identificador chamado **SSID**. O SSID é um valor único, normalmente alfanumérico, com comprimento que varia de 2 a 32 caracteres.

Para este “anúncio” da rede, o AP utiliza quadros especiais chamados de **beacons** (em português, balizas), os quais são enviados periodicamente para facilitar a descoberta de uma rede sem fio e informar as capacidades que os APs têm, como o próprio SSID, taxa de dados, etc.

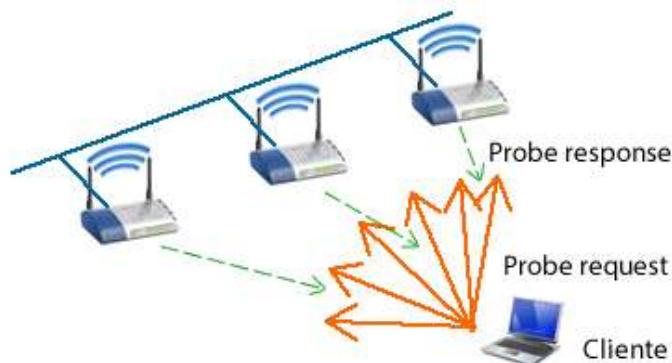
Portanto, quando instalamos, configuramos e iniciamos um cliente de rede sem fio, o primeiro passo que será executado por ele, será verificar a existência de alguma rede sem fio ao seu alcance. Caso haja, o cliente deverá verificar se há possibilidade de associação com a rede sem fio em questão. Este processo é chamado de **scanning** (varredura).

O scanning da rede pode ser feito de duas maneiras: **Ativo** e **Passivo**. No modo passivo os clientes procuram por beacons em cada canal por um determinado período assim que ele é inicializado. Os beacons, portanto, são enviados pelo AP e as estações procuram nesses beacons o SSID da rede que eles desejam se conectar. Se estiver, a estação então tenta entrar na rede através do AP que enviou o beacon.



Em configurações em que há vários APs, vários beacons serão enviados e, nesse caso, a estação tenta entrar na rede através do AP que tiver o **sinal mais forte**.

No modo ativo são as estações que iniciam o processo, tornando-se, portanto, parte ativa do processo de descoberta de redes. Quando a estação está procurando por uma rede, ela envia um frame chamado **probe request**, contendo o SSID da rede que ela está procurando. O AP que tiver o SSID em questão envia um **probe response**.

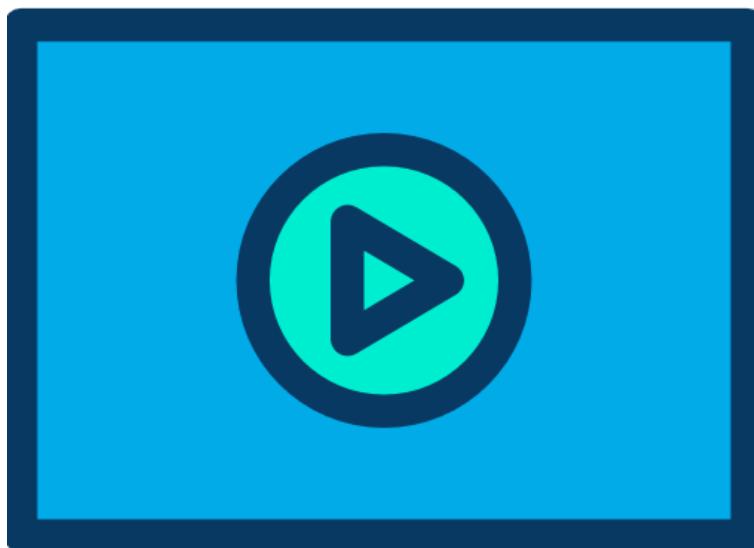


Se houver vários APs, somente aquele que tiver aquele SSID envia o probe response. Por outro lado, se o SSID de broadcast (que indica "qualquer rede") for enviado no probe request, **todos os APs** enviarão um probe response.

Uma vez que o AP com o SSID específico tenha sido encontrado, a estação inicia os passos de **autenticação e associação** para entrar na rede através daquele AP.

Note que se tivermos muitos SSIDs, quanto o AP tiver mais de um rádio e suportar essa facilidade, podemos ocupar demais a rede com o envio de Beacons, por isso mesmo não é recomendado criar mais que três ou quatro SSIDs por AP.

6.6.7.2 AUTENTICAÇÃO, CRIPTOGRAFIA E ASSOCIAÇÃO DE CLIENTES



A autenticação é a primeira etapa do processo e serve para o cliente estabelecer a sua identidade com um ponto de acesso. Existem dois tipos de autenticação: Sistema de autenticação aberta ou Autenticação com Chave Compartilhada (shared key).

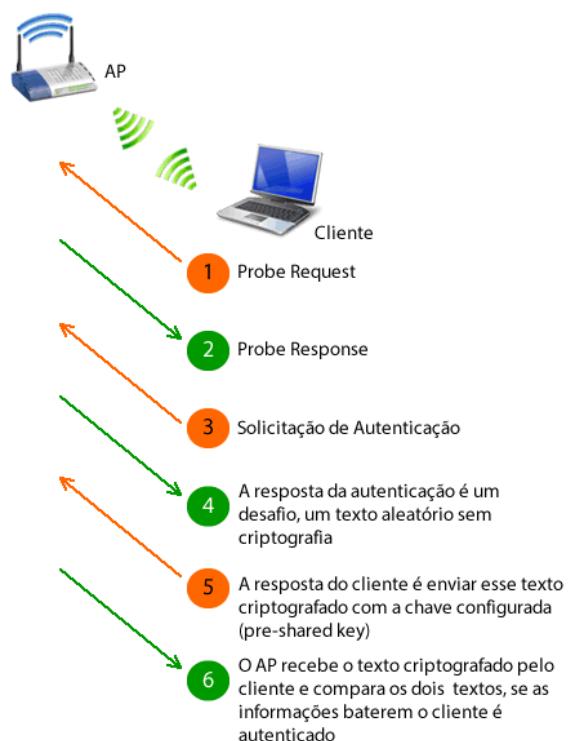
O sistema de autenticação aberto consiste em duas etapas. A primeira é uma solicitação de autenticação pelo cliente, a qual é seguida de uma resposta de autenticação por parte do AP contendo uma mensagem de sucesso ou falha. Veja a figura ao lado com a troca de mensagens até a associação do cliente ao AP com autenticação aberta.



Já no processo de autenticação e criptografia com chaves compartilhadas, uma chave ou senha é definida manualmente em ambos os equipamentos (AP e Cliente). Há vários tipos de autenticação de chave compartilhada disponíveis para usuários residenciais ou de pequenas empresas, sendo que as principais são:

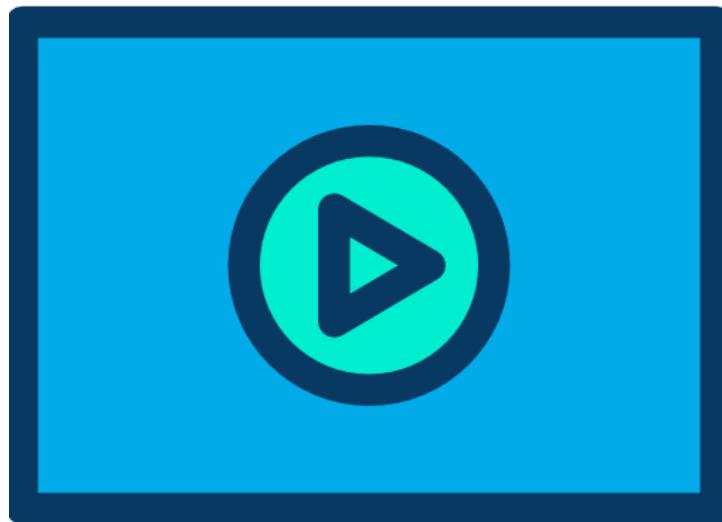
- **WEP (Wired Equivalent Privacy)**: WEP não é recomendado mais para uso em redes sem fio, pois possui diversas vulnerabilidades. Um dos principais riscos de segurança é a possibilidade de um hacker capturar quadros que são trocados no início do processo (usando softwares específicos) e usar as informações para quebrar criptografia.
- **WPA (Wi-Fi Protected Access)**: WPA já é um protocolo considerado seguro e aumenta significativamente o nível de proteção de dados e de controle de acesso (autenticação) para uma rede sem fio. WPA utiliza a autenticação 802.1X e a troca de chaves só funciona com chaves de criptografia dinâmicas, já no WEP as chaves são estáticas. Existem alguns tipos de WPA, os mais utilizados são o WPA-Pessoal, WPA-PSK (Pre-shared key - chave pré-compartilhada) e WPA-Home.
- **Wi-Fi Protected Access 2 (WPA2)**: WPA2 implementa uma melhoria de segurança para o WPA, sendo que os dois não são interoperáveis. Normalmente o WPA e o WPA-2 suportam as criptografias via TKIP e AES.

Veja na figura abaixo a troca de mensagens de autenticação quando utilizamos chaves compartilhadas. Note que ao invés de enviar os dados abertos da autenticação, é enviando um challenge ou desafio, que significa que aquela informação está criptografada.



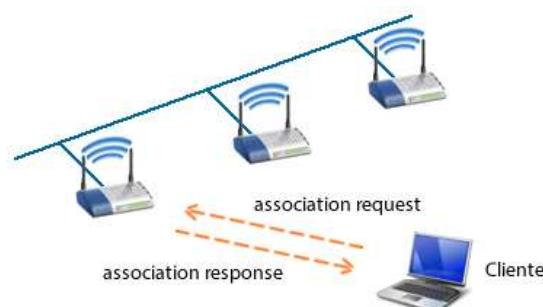
A vantagem do uso da criptografia na transmissão dos dados é que as informações trocadas entre o cliente e o AP são protegidas (codificadas com um protocolo de criptografia). Assim, caso as informações sejam capturadas por um hacker elas não conseguirão ser decodificadas, a não ser que ele consiga descobrir chave utilizada (configuradas no AP e nos clientes), porém utilizando sistemas de criptografias fortes isto é praticamente impossível ou pelo menos muito difícil.

6.6.7.3 ASSOCIAÇÃO



Assim que a autenticação termina os clientes podem se associar (registrar) com o AP para ter acesso completo aos recursos de rede. Na associação o AP vincula o cliente com um identificador de associação (ID), vinculado ao endereço MAC daquela estação.

Veja a figura abaixo que o cliente envia uma requisição de associação ao AP (association request) e o AP responde informando se o cliente está ou não associado (association response).



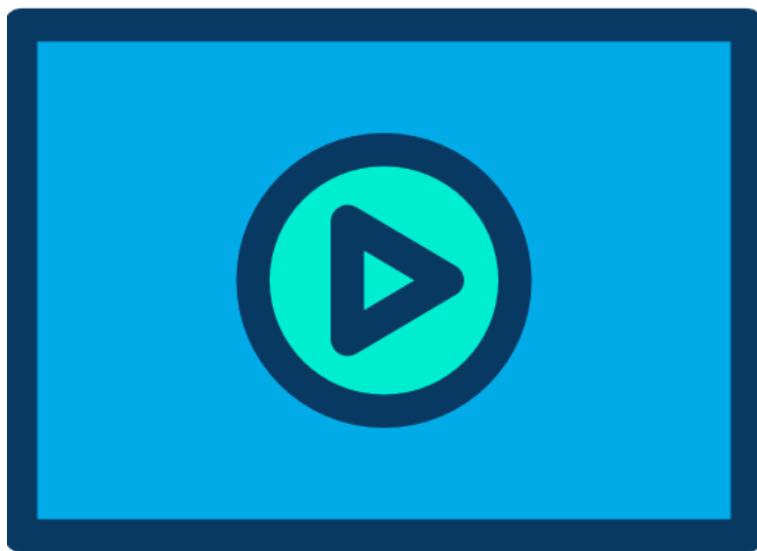
Ao final do processo de associação os clientes podem estar nos seguintes estados:

- **Não autenticado e não associado** – Nesta fase inicial o nó wireless está desconectado da rede e incapaz de encaminhar seus quadros através do AP. Os APs geralmente mantêm uma tabela de status de conexão de clientes conhecida como tabela de associação.
- **Autenticado e não associado** – Nessa segunda fase, o cliente está autenticado, mas não associado com o AP. O status da tabela de associação do AP mostrará AUTENTICADO, mas o cliente ainda não pode passar dados através do AP.
- **Autenticado e associado** – Esta é a última fase, o cliente por estar associado já pode encaminhar seus dados através do AP, ou seja, está totalmente conectado à rede. A tabela de associação agora mostrará o status ASSOCIADO.

Dica: os quadros ou frames trocados pelo 802.11 basicamente podem ser divididos em 4 tipos:

- **Management:** mensagens de associação (association), reassociação (Reassociation), probes, beacons e autenticação (Authentication).
- **Control:** mensagens como CTS e RTS e ACK (reconhecimento).
- **Data:** mensagens com os dados dos usuários e informações de QoS.
- **Reserved:** campo reservado para futuras implementações.

6.6.8 Tecnologias Wireless da Família 802.11



A primeira versão do padrão 802.11 foi lançada em 1997, após aproximadamente 7 anos de estudos. Com o surgimento de novas versões, a versão original passou a ser conhecida como 802.11-1997 ou 802.11 Legacy. Atualmente temos os padrões 802.11 "a", "b", "g" e "n" no mercado, além disso, existem os padrões 802.11ac ou wifi-5 e 802.11ax ou wifi-6.

6.6.8.1 Padrão 802.11b

Em 1999, foi lançada uma atualização do padrão 802.11 que recebeu o nome **802.11b**. A principal característica desta versão é a possibilidade de estabelecer conexões nas seguintes velocidades de transmissão: 1 Mbps, 2 Mbps, 5.5 Mbps e 11 Mbps.

O intervalo de frequências é o mesmo utilizado pelo 802.11 original (entre 2,4 GHz e 2,4835 GHz), mas a técnica de transmissão se limita ao DSSS, uma vez que o FHSS acaba não atendendo às normas estabelecidas pela Federal Communications Commission (FCC) quando operada em transmissões com taxas superiores a 2 Mbps. Para trabalhar de maneira efetiva com as velocidades de 5.5 Mbps e 11 Mbps, o 802.11b também utiliza uma técnica chamada Complementary Code Keying (CCK).

6.6.8.2 Padrão 802.11a

O padrão 802.11a surgiu quase na mesma época que a versão 802.11b. Sua principal característica é a possibilidade de operar com taxas de transmissão de dados nos seguintes valores: 6 Mbps, 9 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps e 54 Mbps.

O alcance do 802.11a é de aproximadamente 50 metros para ambientes indoor e até 5 km para ambientes externos, além disso, sua frequência de operação é diferente do padrão 802.11 original, passando a operar na faixa dos 5 GHz.

O uso desta frequência é conveniente por apresentar menos possibilidades de interferência, afinal, este valor é pouco usado. Por outro, pode trazer determinados problemas, já que muitos países não possuem regulamento para essa frequência. Além disso, esta característica pode fazer com que haja dificuldades de comunicação com dispositivos que operam nos padrões 802.11 original e 802.11b. Além da frequência de 5GHz, o padrão 802.11a pode operar em 3.7GHz, uma opção para países onde o 5GHz não estiver regulamentado.

O padrão 802.11a utiliza uma técnica de modulação conhecida como Orthogonal Frequency Division Multiplexing (OFDM). No OFDM a informação é dividida em vários pequenos conjuntos de dados que são transmitidos simultaneamente em diferentes frequências, com o objetivo de impedir que uma interfira na outra, fazendo com que a técnica OFDM funcione de maneira bastante eficiente.

Apesar de oferecer taxas de transmissão maiores, o padrão 802.11a não chegou a ser tão popular quanto o padrão 802.11b.

6.6.8.3 PADRÃO 802.11g

O padrão 802.11g foi disponibilizado em 2003 e foi tido como o "sucessor natural" da versão 802.11b, pois os dois padrões são compatíveis. Isso significa que um dispositivo que opera com 802.11g pode interoperar com outro que trabalha com 802.11b sem qualquer problema, exceto o fato de que a taxa de transmissão de dados fica limitada ao máximo suportado pelo 802.11b.

A principal vantagem do padrão 802.11g é poder trabalhar com taxas de transmissão de até 54 Mbps, assim como o padrão 802.11a, porém o 802.11g opera com frequências na faixa de 2,4 GHz e possui praticamente o mesmo poder de cobertura do seu antecessor, o padrão 802.11b.

A técnica de transmissão utilizada pelo 802.11g também é o OFDM, porém quando é feita comunicação com um dispositivo 802.11b, a técnica de transmissão passa a ser o DSSS.

6.6.8.4 PADRÃO 802.11n

O desenvolvimento da especificação 802.11n teve início em 2004 e foi finalizado em setembro de 2009. Tem como principal característica o uso de um esquema chamado Multiple-Input Multiple-Output (MIMO), o qual falamos anteriormente, capaz de aumentar consideravelmente as taxas de transferência de dados por meio da combinação de várias vias de transmissão em múltiplas antenas. Com isso, é possível, por exemplo, usar dois, três ou quatro transmissores e receptores para o funcionamento da rede.

Uma das configurações mais comuns neste caso é o uso de APs que utilizam três antenas (três vias de transmissão) e clientes com a mesma quantidade de receptores. Somando esta característica de combinação com o aprimoramento de suas especificações, o padrão 802.11n é capaz de fazer transmissões na faixa de 300 Mbps e, teoricamente, pode atingir taxas de até 600 Mbps.

Em relação à sua frequência, o padrão 802.11n pode trabalhar com as faixas de 2,4 GHz e 5 GHz, o que o torna compatível com os padrões anteriores, inclusive com o 802.11a (pelo menos, teoricamente). Sua técnica de transmissão padrão é o OFDM, mas com determinadas alterações, devido ao uso do esquema MIMO, sendo, por isso, muitas vezes chamado de MIMO-OFDM.

6.6.8.5 PADRÃO 802.11AC

O padrão 802.11ac foi publicado em dezembro de 2013, também identificado como Wi-Fi5 pela WI-Fi Alliance.

O 802.11ac opera apenas na frequência de 5 GHz e possui técnicas mais avançadas de modulação, pois trabalhará com o esquema MU-MUMO (Multi-User MIMO), que permite transmissão e recepção de sinal de vários terminais, como se estes trabalhassem de maneira colaborativa, na mesma frequência.

Com a modulação QAM256 e MIMO 8x8, o 802.11ac consegue atingir uma taxa de transmissão total de 7 Gbit/s. A WI-Fi Alliance certificou os equipamentos em duas fases, chamados Wave1 e Wave2, operando com três e quatro antenas, respectivamente. Outra característica que difere as duas fases é que o Wave1 operava com canal de 80MHz e o Wave2 com 160MHz.

A taxa de transmissão obtida por um dispositivo com duas antenas e canalização de 160MHz pode chegar a 1,69 Gbit/s.

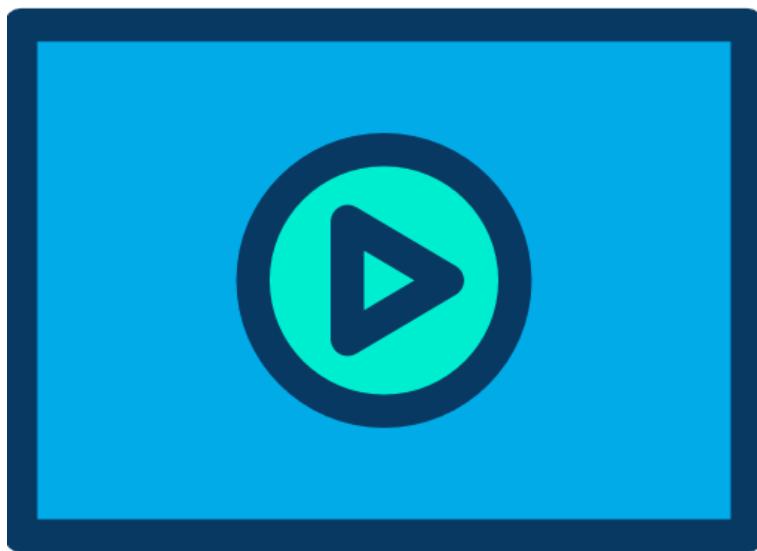
6.6.8.6 PADRÃO 802.11AX

Em maio de 2013 o grupo HEW (High Efficiency WLAN Study Group) do IEEE iniciou o estudo do padrão 802.11ax, chamado de Wi-Fi 6 pela WI-Fi Alliance. Em novembro de 2018 já foi publicada a versão Draft 4.0.

O padrão 802.11ax utiliza a modulação QAM 1024, permitindo taxas muito maiores e o acesso é feito com o OFDMA (Orthogonal Frequency Division Multiple Access) reduzindo o overhead e a latência, atingindo uma taxa de transmissão total de 11 Gbit/s teóricos.

Opera nas frequências de 2,4GHz e 5GHz, os access points 802.11ax deverão suportar o acesso de todas as tecnologias anteriores: 802.11a/g/n/ac.

6.6.9 Non-Overlapping Channels



Já citamos anteriormente esse assunto sobre a canalização que deve ser feita de uma maneira que os canais não se sobreponham com a mesma frequência, ou seja, utilizando “non-overlapping channels” ou canais não sobrepostos.

2.4 GHz (802.11b/g/n)



5 GHz (802.11a/n/ac)

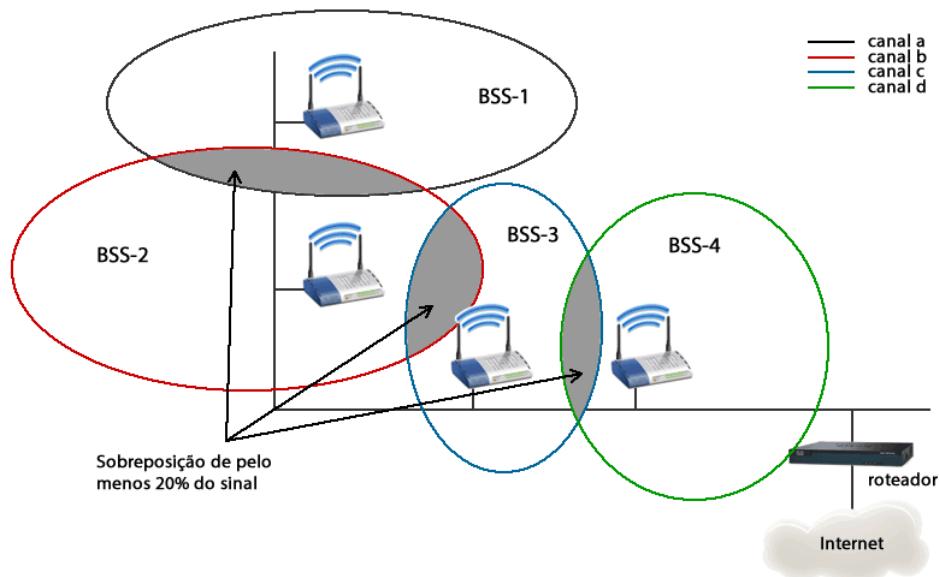


Na imagem acima podemos ver que os canais têm uma numeração e para as tecnologias que utilizam frequência de 2,4GHz podemos utilizar os canais 1, 6 e 11 para planejar uma rede sem sobreposição. Existem outras opções, mas essas são as mais comuns.

Já para tecnologias que utilizam 5Ghz temos mais opções de canais.

Lembre-se que as células ou APs vizinhos precisam estar em canais diferentes, porém deve haver uma sobreposição das células em canais diferentes, pois isso não causa interferência e traz a possibilidade dos clientes fazerem o roaming (mobilidade) sem perder a conexão ao migrar de uma célula para outra.

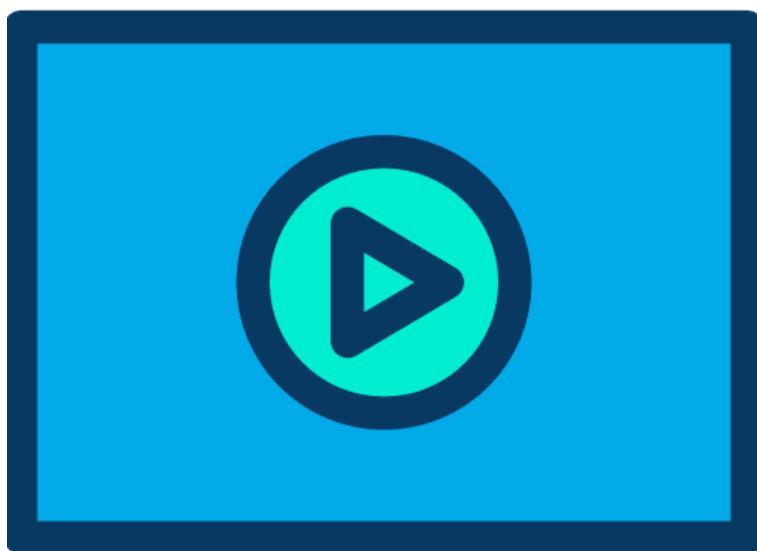
Na figura abaixo temos uma Infraestrutura sem fio ESS formada pela união de 4 BSSs, onde cada AP é configurado com o mesmo SSID. Nessa arquitetura, um cliente pode movimentar-se na área de cobertura do ESS sem ter que se preocupar com os diferentes APs que irá se conectar ao longo do caminho.



Para que uma ESS seja construída, nas áreas limites entre as células deve haver uma sobreposição de sinal de pelo menos 20%, conforme mostra as áreas em cinza da figura. Além disso, para que haja sobreposição de célula e não interferência, cada célula deve estar em um canal distinto, ou seja, cada célula que se sobrepõe deve trabalhar em uma faixa de frequência distinta.

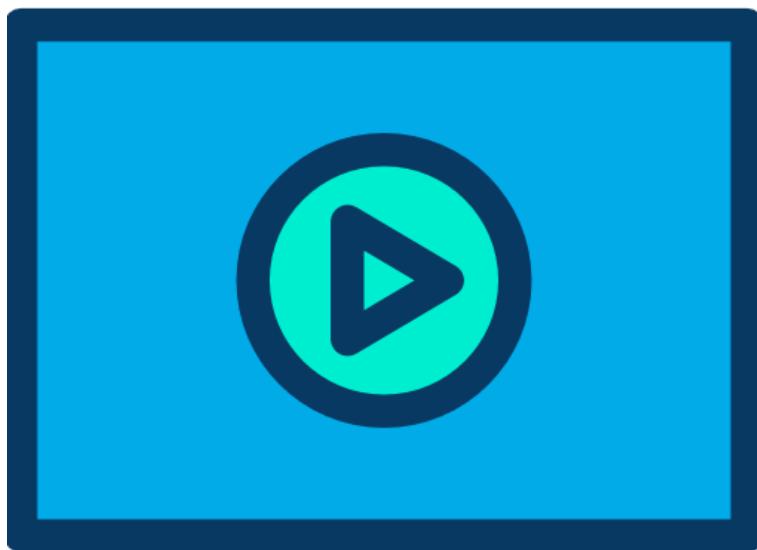
7 TCP versus UDP

7.1 Revisão



Assista a vídeo aula com a revisão sobre o TCP versus UDP.

7.2 Protocolo TCP



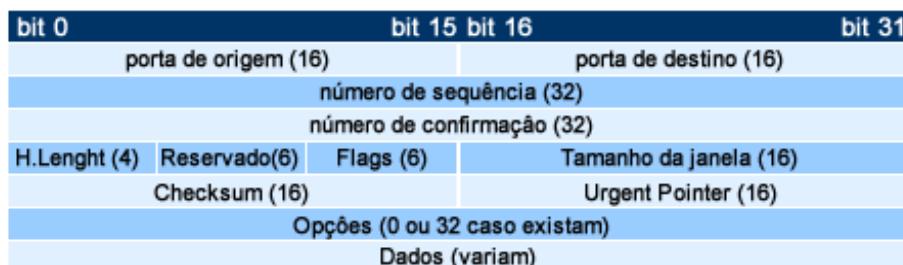
O TCP é um dos principais protocolos da camada transporte do modelo TCP/IP.

Sua versatilidade e robustez o torna adequado a redes globais, uma vez que este protocolo verifica se os dados são enviados de forma correta, na sequência apropriada e sem erros pela rede.

As características fundamentais do TCP são:

- **Orientado à conexão** - A aplicação envia um pedido de conexão para o destino e usa a "conexão" para transferir dados.
- **Ponto a ponto** - uma conexão TCP é estabelecida entre dois pontos.
- **Confiabilidade** - O TCP usa várias técnicas para proporcionar uma entrega confiável dos pacotes de dados, que é a grande vantagem que tem em relação ao UDP, e motivo do seu uso extensivo nas redes de computadores. O TCP permite a recuperação de pacotes perdidos, a eliminação de pacotes duplicados, recuperação de dados corrompidos e pode recuperar a ligação em caso de problemas no sistema e na rede.
- **Full duplex** - É possível a transferência simultânea em ambas as direções (cliente-servidor) durante toda a sessão.
- **Handshake** - Possui mecanismo de estabelecimento e finalização de conexão a três e quatro tempos, respectivamente, o que permite a autenticação e encerramento de uma sessão completa. O TCP garante que, no final da conexão, todos os pacotes foram bem recebidos.
- **Entrega ordenada** - A aplicação faz a entrega ao TCP de blocos de dados com um tamanho arbitrário num fluxo (ou stream) de dados, tipicamente em octetos. O TCP parte estes dados em segmentos de tamanho especificado pelo valor MTU. Porém, a circulação dos pacotes ao longo da rede (utilizando um protocolo de encaminhamento, na camada inferior, como o IP) pode fazer com que os pacotes não cheguem ordenados. O TCP garante a reconstrução do stream no destinatário mediante os números de sequência.
- **Controle de fluxo** - O TCP usa o campo janela ou window para controlar o fluxo. O receptor, à medida que recebe os dados, envia mensagens ACK (=Acknowledgement), confirmindo a recepção de um segmento. Como funcionalidade extra, estas mensagens podem especificar o tamanho máximo do buffer no campo (janela) do segmento TCP, determinando a quantidade máxima de bytes aceita pelo receptor. O transmissor pode transmitir segmentos com um número de bytes que deverá estar confinado ao tamanho da janela permitido: o menor valor entre sua capacidade de envio e a capacidade informada pelo receptor.

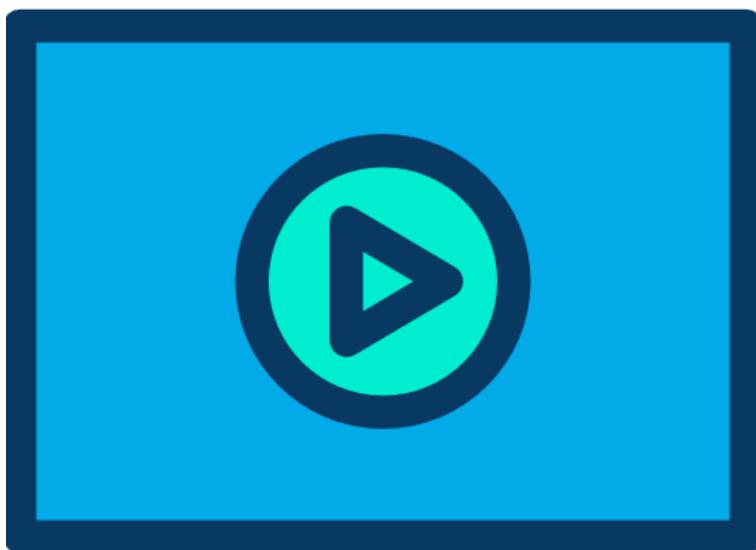
Veja na figura a seguir os campos do cabeçalho do segmento TCP e logo abaixo a explicação de cada campo.



- **Porta de origem**: Número da porta de origem.
- **Porta de destino**: Número da porta de destino.
- **Número de sequência**: Número utilizado para garantir a sequência correta dos dados que estão chegando. Especifica o número do último octeto (byte) em um segmento.
- **Número de confirmação**: Próximo octeto TCP esperado. Especifica o octeto seguinte esperado pelo receptor.
- **H.Length**: Comprimento do cabeçalho do segmento em bytes.
- **Reservado**: Definido como zero.

- **Flags:** Funções de controle, como a configuração e término de uma sessão. Utilizado no gerenciamento de sessões e no tratamento de segmentos.
- **Janela:** Número de octetos que o remetente está disposto a aceitar. É o valor da janela dinâmica, quantos octetos podem ser enviados antes da espera do reconhecimento.
- **Checksum:** Cálculo de verificação feito a partir de campos do cabeçalho e dos dados. Utilizado para verificação de erros no cabeçalho e dados.
- **Urgent Pointer:** Indica o final de dados urgentes. Utilizado somente com um sinalizador URG flag.
- **Opção:** Informações opcionais. Uma opção atualmente definida é o tamanho máximo do segmento TCP.
- **Dados:** Dados de protocolo da camada superior, chamado também de Payload.

7.2.1 Arquitetura Cliente/Servidor



Vamos agora ver como funciona o processo do TCP em um servidor ao executar diversas aplicações.

Cada processo de aplicação sendo executado no servidor é configurado para usar um número de porta, seja no modo padrão ou manualmente através de um administrador do sistema.

Conforme já comentamos em um mesmo servidor não podem existir dois serviços designados ao mesmo número de porta dentro dos mesmos serviços da camada de Transporte.

Por exemplo, um host executando uma aplicação de servidor web e uma aplicação de transferência de arquivo não pode ter ambos configurados para usar a mesma porta.

Quando uma aplicação de servidor ativa é designada a uma porta específica, essa porta é considerada como estando "aberta" (listening) no servidor. Isto significa que a camada de Transporte aceita e processa segmentos endereçados àquela porta.

Qualquer solicitação de cliente que chega endereçada a essa porta é aceita e os dados são transmitidos à aplicação do servidor.

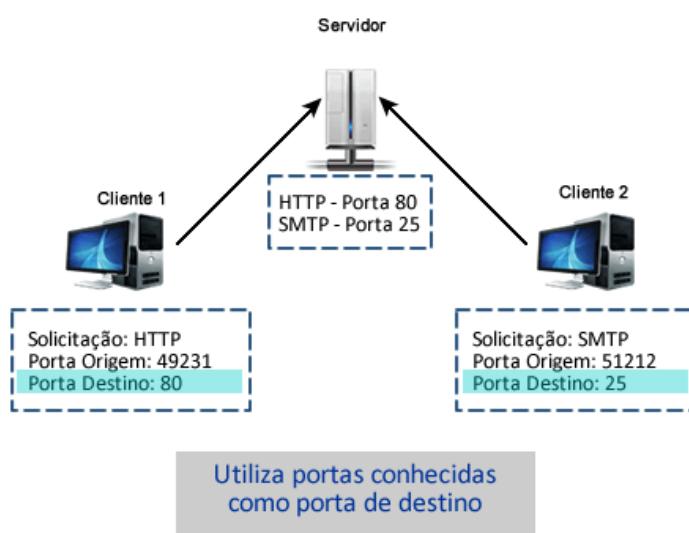
Pode haver muitas portas simultâneas abertas em um servidor, uma para cada aplicação de servidor ativa, pois é comum para um servidor fornecer mais de um serviço, como serviço web e servidor FTP ao mesmo tempo no mesmo servidor.

Esse modelo de acesso a serviços de rede é chamado arquitetura cliente/servidor, pois temos os computadores clientes que precisam acessar informações que são disponibilizadas pelos servidores de rede.

Veja nas figuras a seguir um exemplo de comunicação cliente/servidor através do TCP. Nesse exemplo o computador chamado cliente 1 deseja acessar uma página de Web e o cliente 2 enviar um e-mail. Na primeira figura temos os clientes enviando a solicitação ao servidor utilizando como porta de origem os números 49231 e 51212 respectivamente.

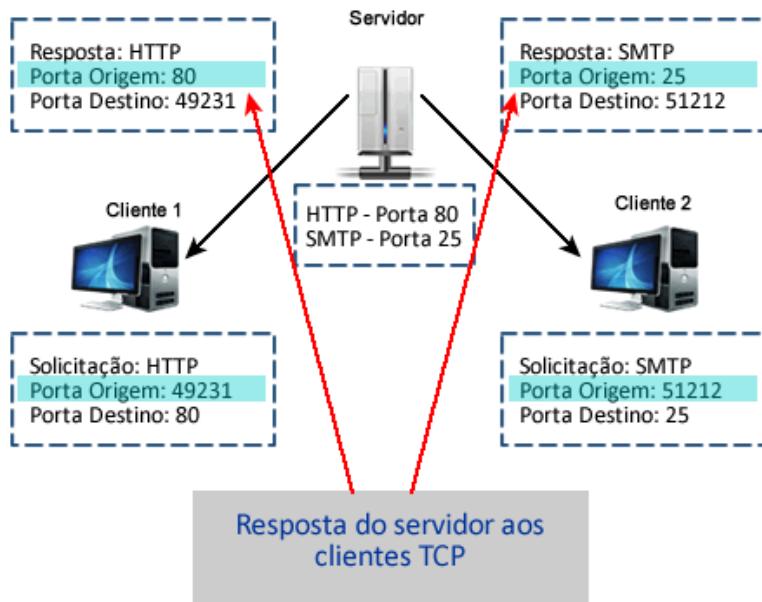


A porta de destino do cliente 1 é a 80, pois ele deseja acessar o serviço de HTTP, já do cliente 2 é 25, pois ele deseja enviar um email através do SMTP. Veja a figura a seguir com as portas destacadas.



O servidor recebe as solicitações, verifica se existe serviço ativo nessas portas e passa as informações recebidas para a camada de aplicação, a qual passa para os aplicativos que cuidam de cada um dos recursos solicitados.

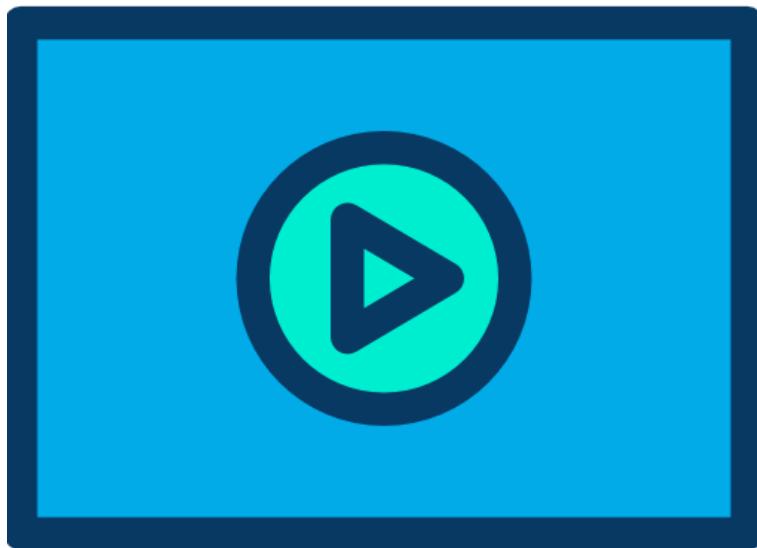
Após os aplicativos tratarem as solicitações, o servidor responde aos clientes utilizando a porta do serviço solicitado como origem e destino a porta que o cliente enviou como origem na sua solicitação.



Essa troca de informações será feita até que a requisição esteja completa ou um problema de rede ocorra e interrompa o tráfego.

A mesma analogia pode ser feita para o protocolo UDP, o qual também funciona no modelo Cliente/Servidor, porém suas portas não têm os estados das portas TCP, pois o UDP não é orientado a conexão.

7.2.2 Estabelecendo uma Conexão TCP



O TCP é classificado como um protocolo orientado a conexão, mas o que significa isso?

Para que dois hosts se comuniquem utilizando o TCP é necessário que seja estabelecida uma conexão antes que os dados possam ser trocados.

Depois da comunicação ter sido completada, as sessões devem ser fechadas e a conexão é encerrada.

É esse mecanismo de conexão e sessão que fornecem a característica de confiabilidade ao TCP.

Dentro do cabeçalho de segmento TCP, existem seis campos de 1 bit que contêm a informação de controle usada para gerenciar os processos TCP. Esses campos são:

- URG - Indicador urgente de campo significativo
- **ACK** - Campo significativo de confirmação
- PSH - função Push
- RST - Restabelecer a conexão
- **SYN** - Sincronizar números de sequência
- FIN - Não há mais dados do remetente

Estes campos são referidos como flags (flags), porque o valor de um desses campos é apenas 1 bit e, portanto, tem apenas dois valores: 1 ou 0, sendo que quando o valor de bit é definido como 1, ele indica que a informação de controle está contida no segmento.

Cada conexão representa dois fluxos de comunicação, ou sessões e para estabelecer uma conexão, os hosts realizam um handshake triplo (negociação em três vias).

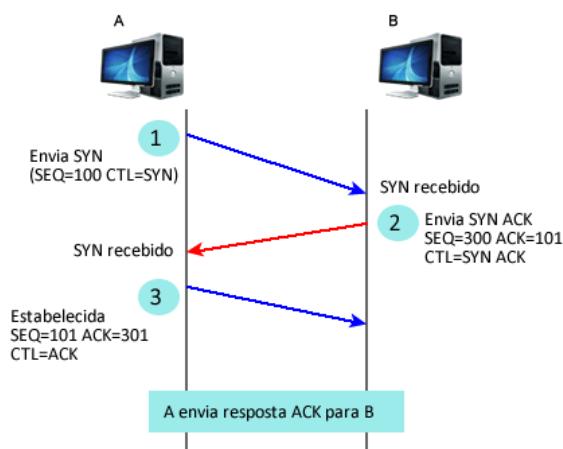
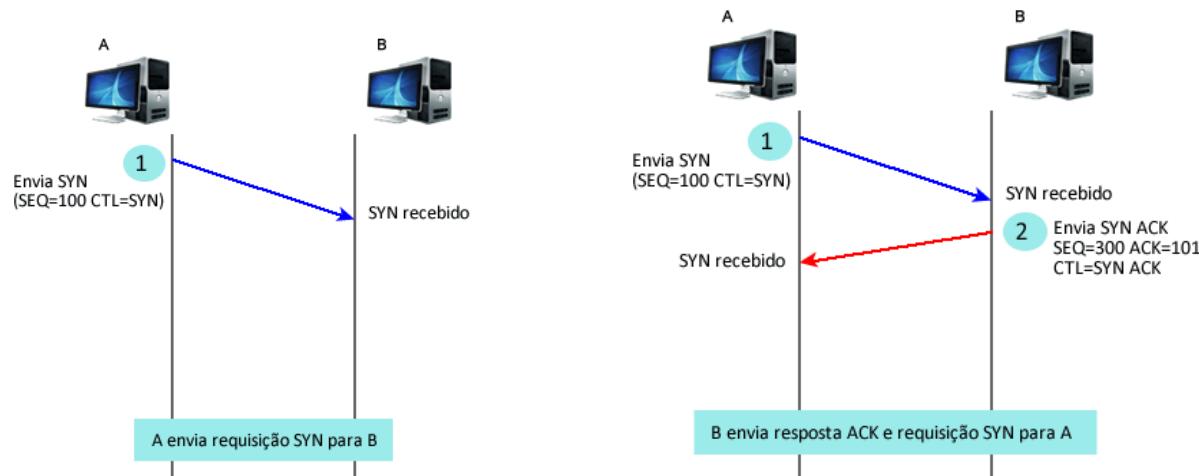
Bits de controle no cabeçalho TCP indicam o progresso e o status da conexão. Abaixo as funções do handshake triplo:

- Confirma que o dispositivo de destino esteja presente na rede.
- Verifica se o dispositivo de destino tem um serviço ativo e está aceitando solicitações no número de porta de destino que o cliente pretende usar para a sessão.
- Informa o dispositivo de destino que o cliente de origem pretende estabelecer uma sessão de comunicação nesse número de porta.

Em todas as conexões TCP, o host que serve como um cliente é quem inicia a sessão para o servidor. Os três passos no estabelecimento de uma conexão TCP são:

1. O cliente envia um segmento contendo um valor sequencial inicial (ISN – Initial Sequence Number) com o flag SYN ativo. Esse segmento serve como uma solicitação ao servidor para começar uma sessão.
2. O servidor responde com um segmento contendo um valor de confirmação igual ao valor sequencial recebido mais 1, mais seu próprio valor sequencial de sincronização (flag SYN e ACK ativos). O valor é maior do que o número sequencial porque o ACK é sempre o próximo Byte ou Octeto esperado.
3. O cliente responde com um valor de confirmação igual ao valor sequencial que ele recebeu mais um. Isso completa o processo de estabelecimento da conexão.

Veja as figuras abaixo com a ilustração da abertura da conexão com handshake de três vias.



7.2.3 Confirmação de Recebimento de Segmentos TCP



Outro campo importante no cabeçalho TCP é o "**número de confirmação**".

O número de sequência definido durante a abertura da conexão TCP e o número de confirmação são utilizados para confirmar o recebimento dos bytes de dados contidos nos segmentos.

O número de sequência é o número relativo de bytes que foram transmitidos na sessão com iniciado pelo ISN definido no início da conexão, já o número de confirmação é o valor recebido mais 1.

O TCP usa o número de confirmação em segmentos enviados de volta à origem para indicar o próximo byte que o receptor espera receber nessa sessão.

Isto é chamado de confirmação esperada ou confirmação positiva.

Dessa forma o TCP assegura que cada segmento atinja o seu destino.

A origem é informada de que o destino recebeu todos os bytes neste fluxo de dados até, mas não incluindo, o byte indicado pelo número de confirmação.

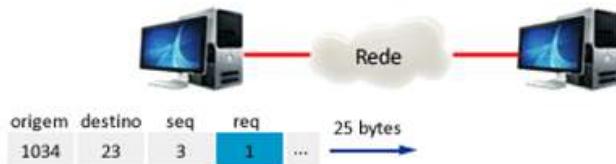
Espera-se que o emissor envie um segmento que utilize um número de sequência que é igual ao número de confirmação.

Lembre-se, cada conexão é na verdade composta por duas sessões unidirecionais. Os números de sequência e de confirmação estão sendo trocados em ambas as direções.

Vamos exemplificar com as figuras a seguir, sendo que a explicação está contida nas próprias imagens.

Porta de Origem	Porta de Destino	Número de Sequência	Número de Reconhecimento	...
-----------------	------------------	---------------------	--------------------------	-----

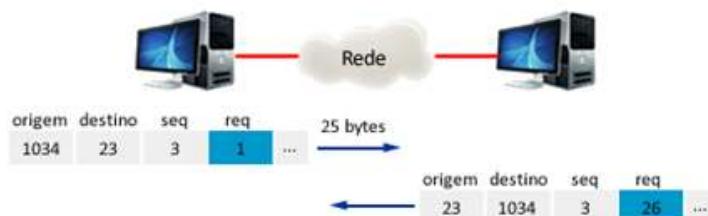
Enviando byte n.3, vou enviar 25 bytes.



Porta de Origem	Porta de Destino	Número de Sequência	Número de Reconhecimento	...
-----------------	------------------	---------------------	--------------------------	-----

Enviando byte n.3, vou enviar 25 bytes.

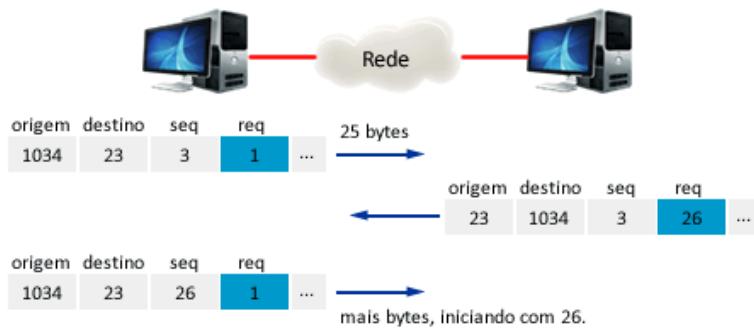
Recebi 25 bytes iniciando com o num.seq 3, espero agora o byte 26.



Porta de Origem	Porta de Destino	Número de Sequência	Número de Reconhecimento	...
-----------------	------------------	---------------------	--------------------------	-----

Enviando byte n.3, vou enviar 25 bytes.

Recebi 25 bytes iniciando com o num.seq 3, espero agora o byte 26.



Vamos supor que o host da esquerda está enviando dados para o host da direita. Ele envia um segmento contendo 25 bytes de dados para essa sessão e um número de sequência igual a 3 no cabeçalho.

O host receptor da direita recebe o segmento na Camada 4 (Camada de Transporte) e determina que o número de sequência é 3 e que ele tem 25 bytes de dados.

O host então envia um segmento de volta ao host da esquerda para confirmar o recebimento deste dado. Neste segmento, o host define o número de confirmação em 26 para indicar que o próximo byte de dados que ele espera receber nessa sessão é o byte número 26.

Quando o host emissor da esquerda recebe essa confirmação, ele pode agora enviar o próximo segmento contendo dados para essa sessão iniciando com o byte número 26.

Examinando esse exemplo, se o host de envio tiver que esperar pela confirmação de recebimento de cada 25 bytes, a rede teria muito overhead.

Para reduzir o overhead dessas confirmações, múltiplos segmentos de dados podem ser enviados e confirmados com uma única mensagem TCP na direção oposta.

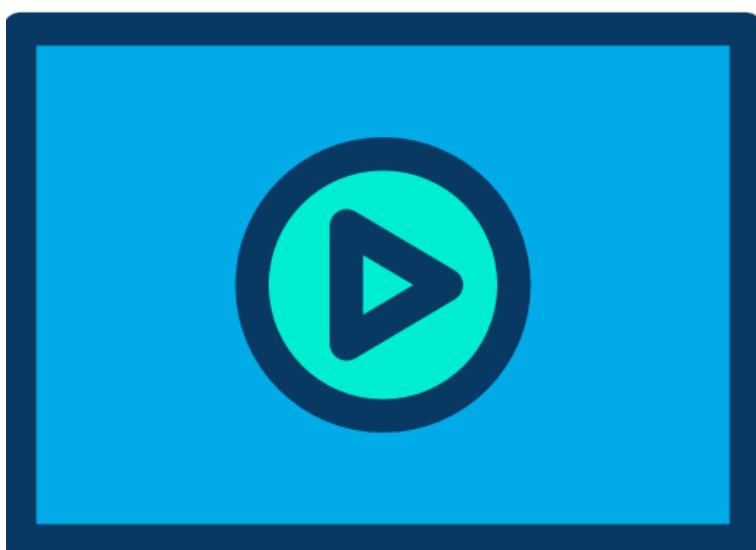
Esta confirmação contém um número de confirmação baseado no número total de bytes recebidos na sessão.

Por exemplo, começando com um número de sequência de 1000, se 10 segmentos de 1000 bytes cada fossem recebidos, o número de confirmação 11001 seria retornado à origem.

```
#####
SIN=1000
10 segmentos de 1000 bytes = 10 x 1000 = 10000
ACK=1000 + 10000 + 1 = 11001
#####
```

A quantidade de dados que a origem pode transmitir antes que uma confirmação seja recebida é chamada de tamanho da janela. O Tamanho de Janela é um dos campos no cabeçalho TCP que habilita o gerenciamento de dados perdidos e o controle de fluxo.

7.2.4 Retransmissão de Segmentos TCP



Por melhor que seja o projeto de uma rede ocasionalmente ocorrerão perdas de alguns dados.

Para contornar essa perda de dados, o TCP possui um mecanismo que retransmite segmentos com dados não confirmados.

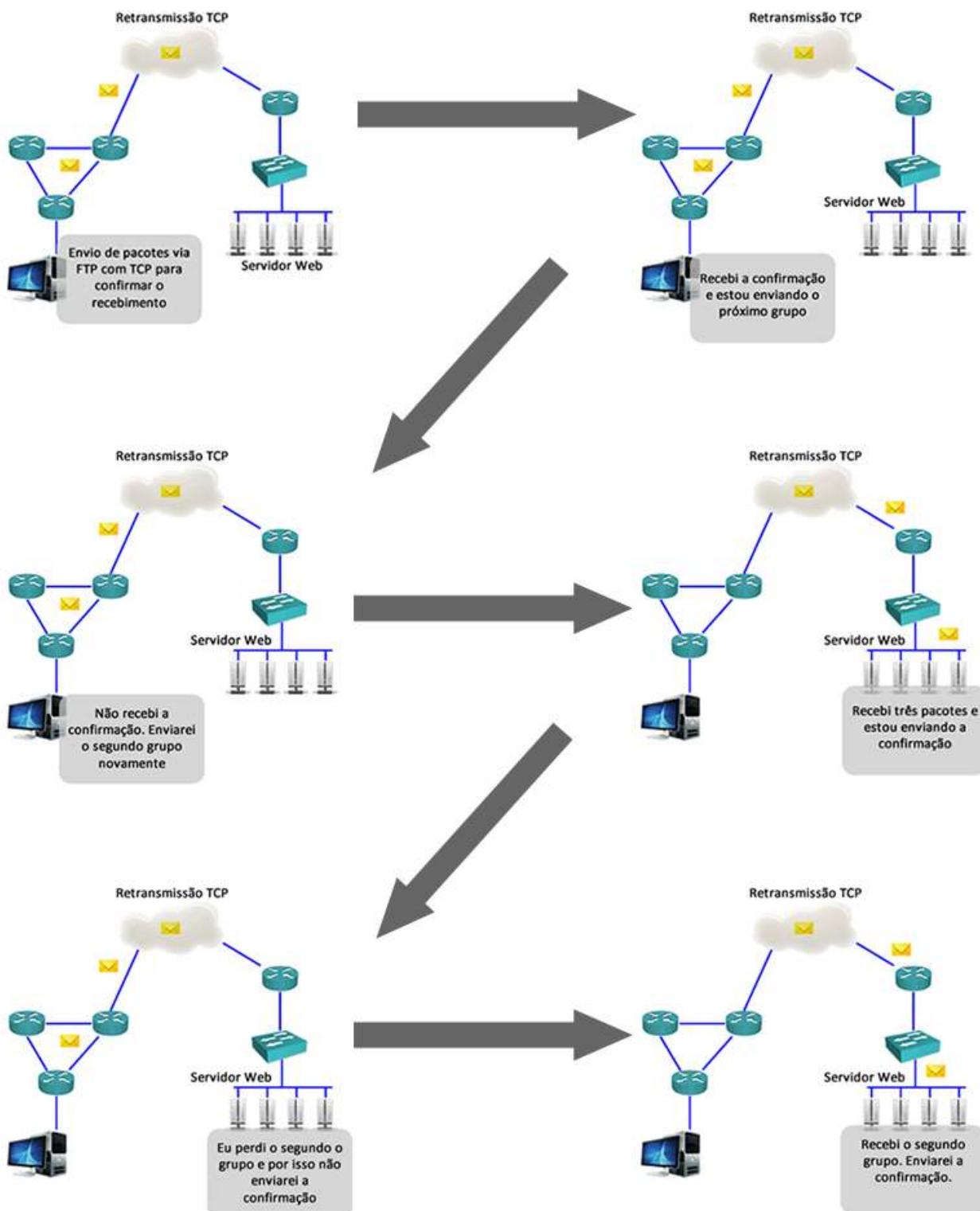
Por exemplo, se os segmentos com números de sequência de 1000 a 3000 e de 4000 a 5000 fossem recebidos, o número de confirmação seria 3001. Isto porque existem segmentos com os números de sequência de 3001 a 3999 que não foram recebidos.

Quando o TCP no host de origem percebe que não recebeu uma confirmação depois de um período pré-determinado de tempo, ele voltará ao último número de confirmação que recebeu e retransmitirá os dados a partir daquele ponto para frente.

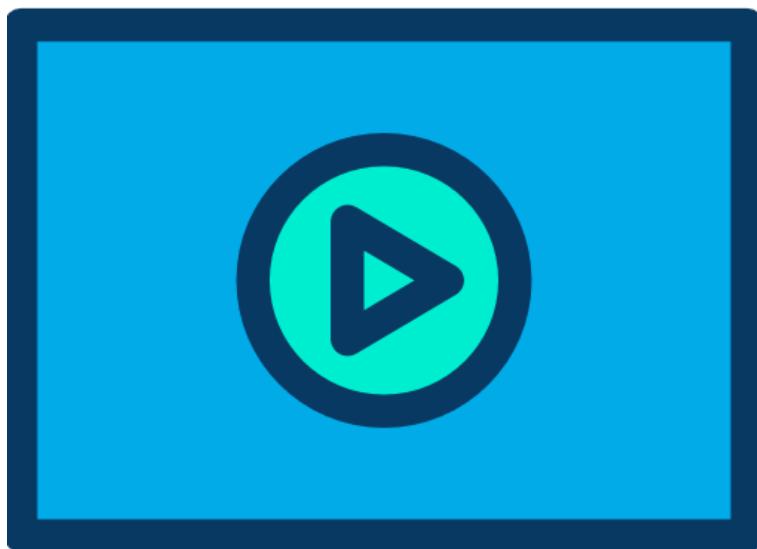
Na prática, se você desconfiar que a sua rede está congestionada verifique o número de retransmissões solicitadas pelos equipamentos, pois se está existindo muita necessidade de retransmissão é sinal que os pacotes não estão chegando ao seu destino e a mais provável causa é uma sobrecarga na rede ou um congestionamento.

Isso pode ser verificado colocando um "Analizador de Protocolo" como o Wireshark para fazer uma varredura dos pacotes que estão sendo trocados na rede.

Veja as figuras a seguir com um exemplo de retransmissão.

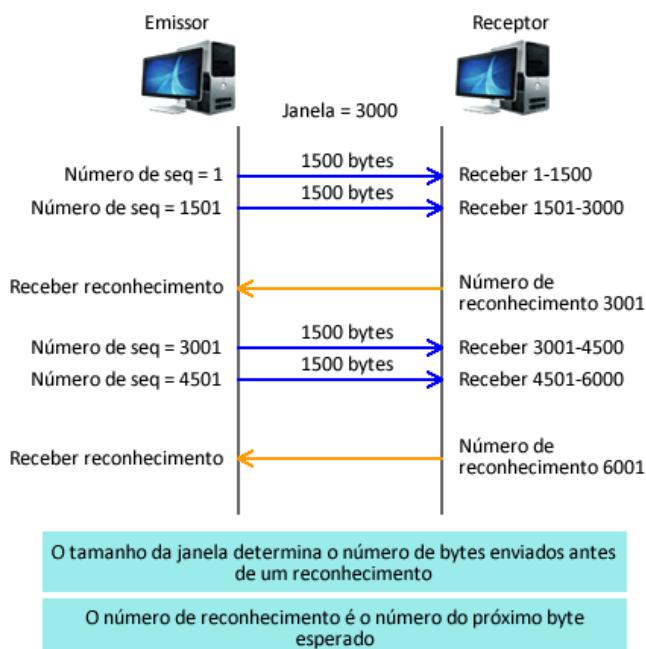


7.2.5 Controle de Congestionamento TCP



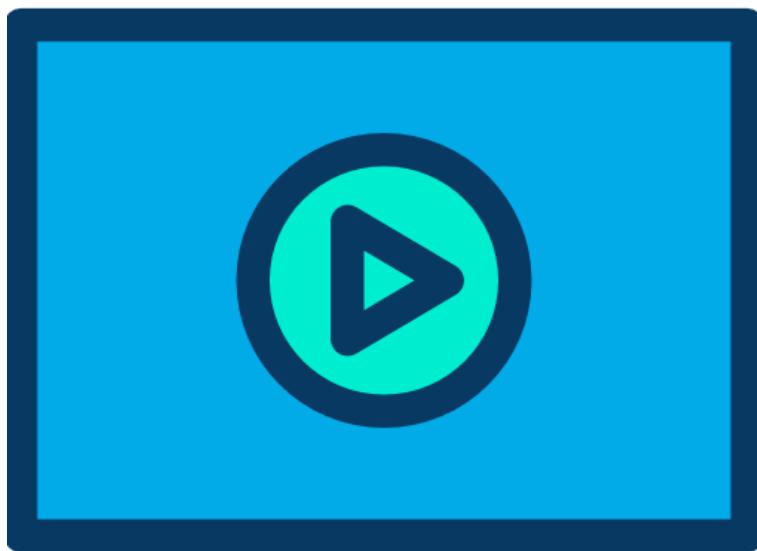
O controle de congestionamento no TCP é realizado através do tamanho da janela de transmissão, ou seja, através de quantos bytes foram confirmados através do número de reconhecimento.

Por exemplo, o computador que iniciou a comunicação tentou mandar uma quantidade de 1500 bytes por janela, se o receptor não conseguir tratar essa quantidade de informações ou a rede estiver lenta, a confirmação não será 1501, como deveria, e sim um número menor até ajustar o tamanho da janela, por isso esse processo é chamado de janelamento ou janela móvel.



Outra forma de controle de congestionamento é chamada “**Slow Start**”, ou seja, o TCP inicia o envio de informações com poucos bytes e vai aumentando o tamanho da janela gradativamente até que seja encontrado o valor ideal. Esse processo é dinâmico e se adapta às condições da rede.

7.2.6 Reagrupamento de Segmentos TCP



Mais uma vez (para gravar bem) vamos reforçar que o TCP é um protocolo orientado a conexão. No entanto, quando algum serviço utiliza o protocolo TCP para enviar dados, os segmentos de dados podem chegar fora de ordem. Mas por quê?

Porque os diversos segmentos podem percorrer caminhos diferentes para chegar no destino.

Um segmento pode ser roteado dentro da rede e percorrer um caminho que tenha uma velocidade mais rápida ou um delay menor.

No entanto, para que a mensagem original seja entendida pelo receptor, os dados desses segmentos precisam ser reagrupados em sua ordem original. Para isso existe no cabeçalho TCP o campo "número de sequência".

Durante a instalação de uma sessão, um número de sequência inicial (ISN) é definido.

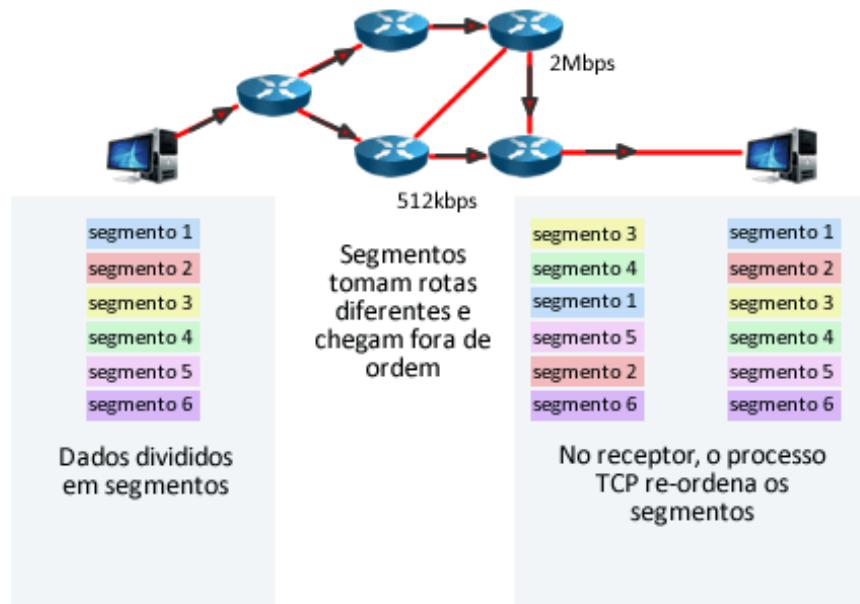
Este número de sequência inicial representa o valor de partida para os bytes para esta sessão. À medida que os dados são transmitidos durante a sessão, o número de sequência é incrementado pelo número de bytes que foram transmitidos.

Dessa forma cada segmento pode ser identificado e reconhecido, pois cada um terá um número de sequência único que seguirá uma ordem definida.

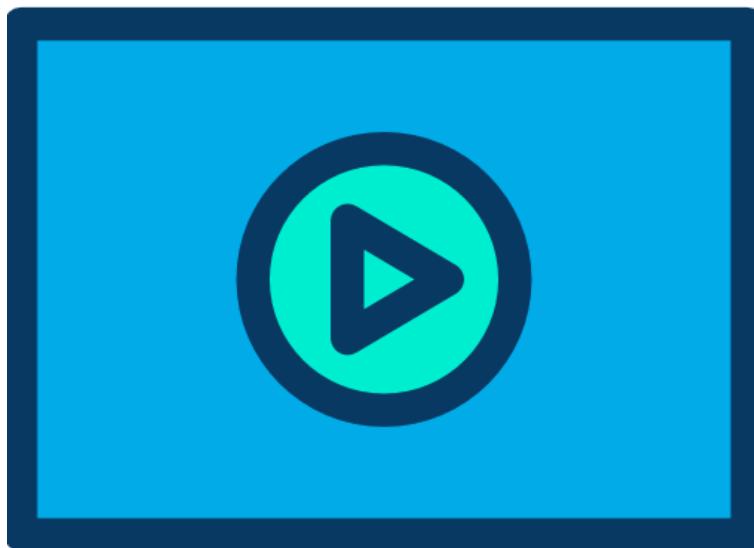
O processo TCP do receptor coloca os dados de um segmento em um buffer. Os segmentos são então colocados na ordem do número de sequência apropriada e passados para a camada de Aplicação quando reagrupados.

Quaisquer segmentos que cheguem com números de sequência não contíguos são retidos para processamento posterior. Então, quando os segmentos com os bytes perdidos chegam, esses segmentos são processados.

Esse processo de sequenciamento é que fornece a confiabilidade do TCP, pois garante que os segmentos serão entregues na ordem corretas e sem faltar nenhum pedaço.



7.3 Protocolo UDP



Ao contrário do TCP o protocolo UDP não é orientado a conexão, portanto não possui mecanismos sofisticados de controle de congestionamento e erros como o TCP.

O UDP transmite os datagramas de forma “best-effort” ou seja “melhor esforço”, ficando a cargo das aplicações tratarem dos erros e controle da transmissão.

O único campo de controle do UDP é o Checksum para verificar a integridade do datagrama recebido. Veja na figura a seguir o datagrama do UDP.

Sobre a comunicação através de portas o funcionamento do UDP é similar ao TCP, tendo portas específicas para determinados serviços.

A grande diferença é que não existe conexão, elas sempre estão preparadas para receber dados de um host remoto que deseja se comunicar.

Pelo fato do UDP ser mais simples, ele acaba se tornando mais rápido e preferido para aplicações onde a velocidade é fundamental, como a voz sobre o protocolo IP ou VoIP.

O protocolo RTP (Real Time Protocol) utiliza o serviço UDP para transmitir a voz entre aparelhos IP.

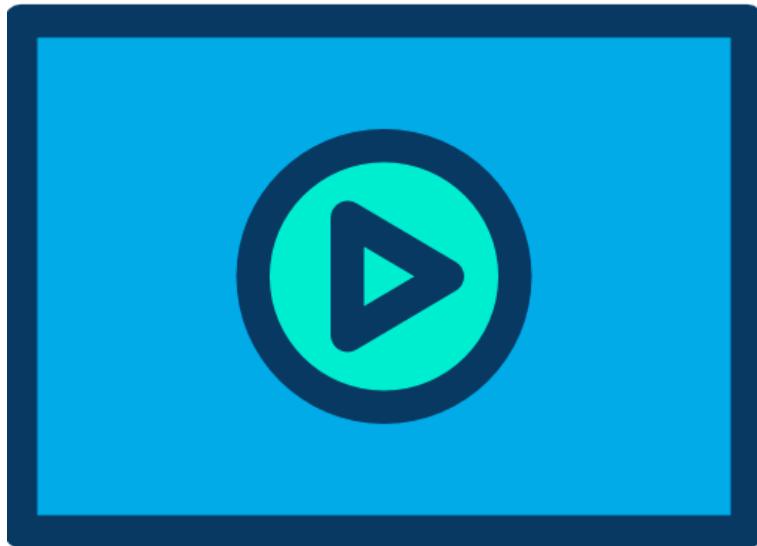
Outro exemplo de aplicação são as VPN's ou redes virtuais privadas, elas também normalmente utilizam serviço UDP para transmissão dos seus dados criptografados, pois os pacotes acabam sendo enviados mais rápidos e com menos cabeçalho, pois o UDP tem bem menos bits de controle que o TCP.

As portas do UDP não tem estado, pois elas estão sempre prontas para receber dados.

bit 0	bit 15	bit 16	bit 31
porta de origem (16)		porta de destino (16)	
comprimento (16)		checksum (16)	
Dados (caso existam)			

- **Porta de origem:** Número da porta chamadora.
- **Porta de destino:** Número da porta chamada.
- **Comprimento:** Número de bytes que inclui cabeçalho e dados.
- **Checksum:** Cálculo de verificação (checksum) feito através de campos do cabeçalho e dados.
- **Dados:** Dados de protocolo de camada superior.

7.4 Identificando Conexões e Aplicações Com Portas TCP e UDP



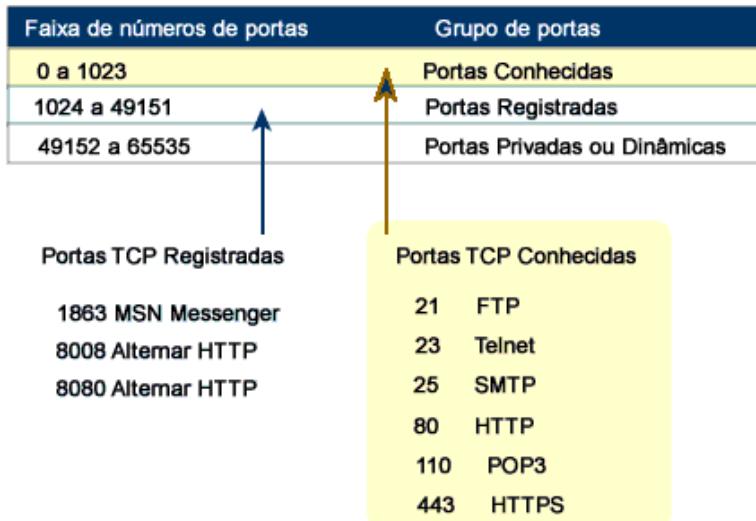
A IANA (Internet Assigned Numbers Authority) é o órgão não governamental responsável pela designação de vários padrões de endereçamento internacionalmente, dentre eles os números de portas. Veja na figura a seguir uma classificação geral dos números de porta alocados pela IANA.

Faixa de números de portas	Grupo de portas
0 a 1023	Portas conhecidas
1024 a 49151	Portas Registradas
49152 a 65535	Portas Privadas ou Dinâmicas

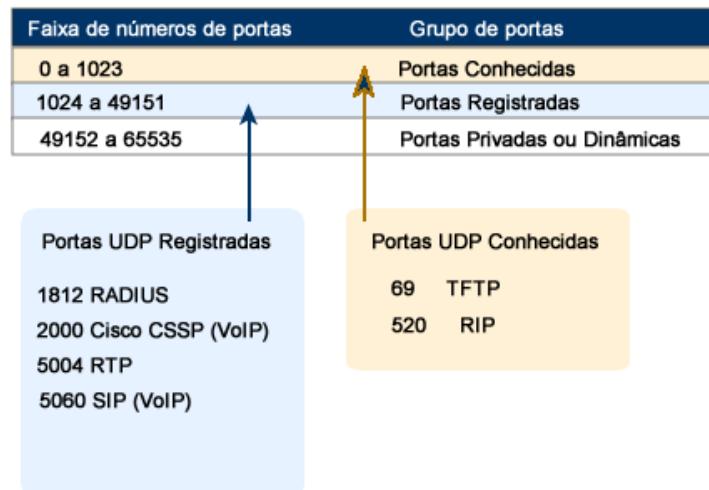
Portanto existem três diferentes tipos de números de portas:

- **Portas Conhecidas (Números 0 a 1023)** - Esses números de portas estão reservados para serviços e aplicações. Eles são comumente usados para aplicações como o HTTP (servidor web) POP3/SMTP (servidor de e-mail) e Telnet. Através da definição destas portas conhecidas para aplicações de servidor, aplicações de clientes podem ser programadas para solicitar uma conexão com essa porta específica e seu serviço associado. São também chamadas como **Well Known Ports**.
- **Portas Registradas (Números 1024 a 49151)** - Estes números de portas são designados para processos ou aplicações de usuário. Estes processos são principalmente aplicações individuais que um usuário escolheu para instalar em vez de aplicações comuns que receberiam uma Porta Conhecida. Quando não usadas para um recurso de servidor, estas portas também podem ser dinamicamente selecionadas por um cliente como sua porta de origem.
- **Portas Dinâmicas ou Privadas (Números 49152 a 65535)** - Elas são geralmente designadas dinamicamente a aplicações de cliente quando se inicia uma conexão. Não é muito comum um cliente se conectar a um serviço usando uma Porta Dinâmica ou Privada, embora alguns programas de compartilhamento de arquivos peer-to-peer o façam.

Exemplo de números portas TCP:



Exemplos de portas UDP:



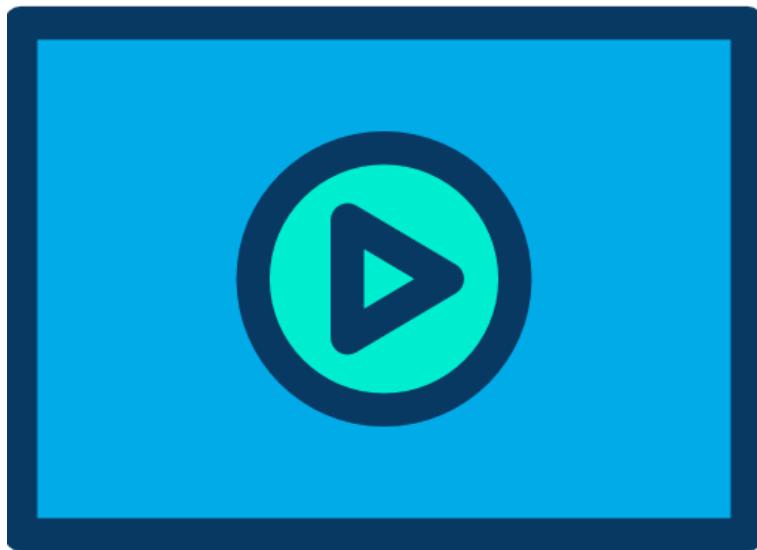
8 Endereçamento IPv4, Sub-Redes e Configurações

É muito importante que você aprenda os conceitos que serão apresentados, pois eles o acompanharão em toda a sua vida no mundo das redes de computadores e administração de redes!

Sendo assim, leia, estude, pesquise, releia o material, faça os exercícios e insista até que tenha assimilado **toda a matéria**, pois várias questões do CCNA dependem desses conceitos.

Como os endereços IP, apesar de escritos em números decimais, são na realidade números binários nada melhor que começar revisando o sistema de numeração binário. Caso a explicação mostrada a seguir não seja suficiente temos ainda uma apostila de sistemas de numeração para ajudá-lo a aprender melhor o assunto.

8.1 IP versão 4 - Formato do Pacote e Endereçamento



Abaixo segue o cabeçalho do protocolo IP versão 4 e logo abaixo a descrição dos campos.

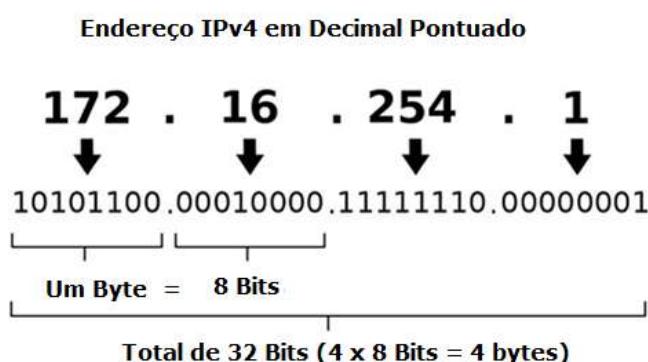
+	0 - 3	4 - 7	8 - 15	16 - 18	19 - 31		
0	Versão	Tamanho do cabeçalho	<i>Tipo de Serviço (ToS)</i> (agora DiffServ e ECN)	Comprimento (pacote)			
32	Identificador			Flags	Offset		
64	<i>Tempo de Vida (TTL)</i>		Protocolo	<i>Checksum</i>			
96	Endereço origem						
128	Endereço destino						
160	Opções						
192	<i>Dados</i>						

- **Versão (version)**: Definido como 4.
- **IHL (header length)**: Comprimento do Cabeçalho da Internet com o número de palavras de 32 bits no cabeçalho IPv4.
- **Tipo de serviço**: Definido na RFC 791 e define o tipo de serviço (ToS – Type of Service), agora DiffServ e ECN utilizados para definir marcação de QoS.
- **Tamanho total (total length)**: Define todo o tamanho do datagrama incluindo cabeçalho e dados. O tamanho mínimo do datagrama ou pacote IP é de vinte bytes e o máximo é 64 Kbytes, porém o MTU mínimo que os hosts precisam suportar é de 576 bytes. Se os pacotes ultrapassarem o MTU precisam ser "fragmentados", ou seja, quebrados em pedaços menores para caberem dentro do tamanho máximo do protocolo do caminho. No IPv4 a fragmentação pode ser feita pelos computadores ou diretamente nos roteadores.
- **Identificador (identifier)**: Usado principalmente para identificar fragmentos do pacote IP original.
- **Flags**: Usado para controlar ou identificar fragmentos.
- **Offset do fragmento**: permite que um receptor determine o local de um fragmento em particular no datagrama IP original.
- **Tempo de vida**: Chamado de TTL (time to live) ajuda a prevenir que os pacotes IP entrem em loop na rede. Utilizado para o teste de traceroute.
- **Protocolo (protocol)**: Define o protocolo que será transportado no pacote, sendo que os protocolos comuns e os seus valores decimais incluem o ICMP (1) e o TCP (6).
- **Checksum**: Campo de verificação de erros para o cabeçalho do datagrama IPv4. Cobre apenas verificação do cabeçalho, não dos dados.
- **Endereço de origem (source)/destino (destination)**: Campos que trazem os endereços de origem (transmissor) e de destino (receptor) de 32 bits cada um. Os endereços IP têm seus campos divididos em 4 conjuntos de 8 bits, ou seja, 4 bytes escritos em decimal pontuado, por exemplo, 192.168.1.1.
- **Opções (options)**: Normalmente não utilizados.
- **Dados (data ou payload)**: Informações das camadas superiores, por exemplo, segmentos TCP ou datagramas UDP.

Sem dúvida alguma os campos de endereçamento de origem e destino são os mais importantes do cabeçalho IP, pois eles que fornecem o endereçamento lógico utilizado para transporte do pacote através da rede.

Lembre-se que o quadro de camada-2 é trocado durante a viagem do IP pela rede conforme o protocolo utilizado pelo link local, já o pacote IP é aberto somente pelo destino da transmissão.

Abaixo segue como um endereço IP é escrito em decimal pontuado e depois em bits.



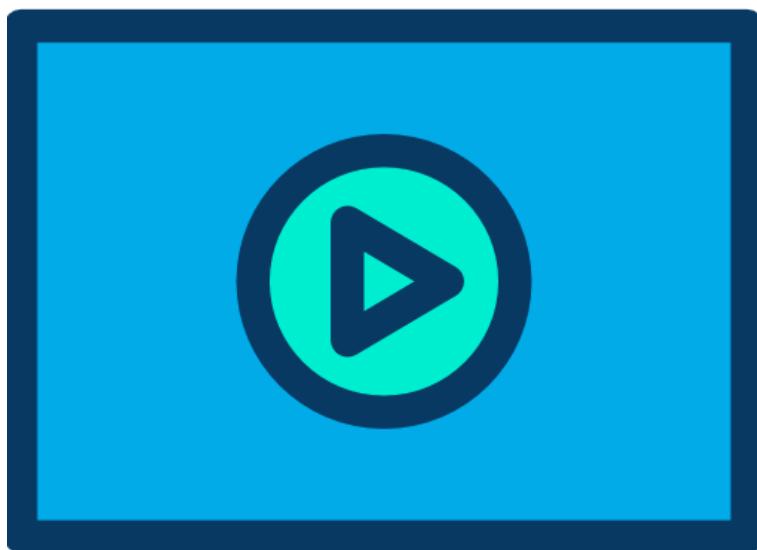
Com 32 bits temos um total de 2^{32} bits ou 4.294.967.296 de possíveis endereços IP. Portanto, o primeiro endereço IP versão 4 possível tem todos os bits em zero e o último todos os bits em 1:

- 1º endereço IP: 00000000.00000000.00000000.00000000 -> 0.0.0.0
- Último endereço IP: 11111111.11111111.11111111.11111111 -> 255.255.255.255

A faixa de variação dos endereços entre o primeiro 0.0.0.0 e o último 255.255.255.255 corresponde a todo espaço de endereçamento IPv4 disponível.

Mais para frente você vai aprender que essa faixa foi dividida no início em classes (A, B, C, D e E) para possibilitar a divisão dos endereços entre instituições e empresas para possibilitar o endereçamento dos computadores na Internet.

8.2 Sistemas de Numeração



Vamos iniciar com o tópico "Matemática para Redes de Computadores", onde iremos rapidamente abordar os seguintes assuntos:

- Sistema de Numeração Decimal.
- Sistema de Numeração Binário.

8.2.1 Sistema Decimal

Os sistemas numéricos consistem em símbolos e regras para a utilização destes símbolos. O sistema numérico mais frequentemente utilizado é o sistema numérico Base 10 ou decimal. Um sistema dito de base 10 significa que são utilizados dez símbolos para sua representação (0, 1, 2, 3, 4, 5, 6, 7, 8 e 9). Estes símbolos podem ser combinados para representar todos os valores numéricos possíveis.

O sistema numérico decimal é baseado em potências de 10. Cada posição colunar de um valor, da direita para a esquerda, é multiplicada pelo número 10, que é o número base, elevado a uma potência, que é o expoente.

A potência à qual é elevado o valor 10 depende da sua posição à esquerda do ponto decimal. Quando um número decimal é lido da direita para a esquerda, a primeira posição, ou a mais à direita representa 10 elevado por 0 (1), a segunda posição representa 10 elevado por 1 ($10 \times 1 = 10$). A terceira posição representa 10 elevado por 2 ($10 \times 10 = 100$). A sétima posição à esquerda representa 10 elevado por 6 ($10 \times 10 \times 10 \times 10 \times 10 \times 10 = 1,000,000$). Esta é a verdade independentemente de quantas colunas sejam ocupadas pelo número.

Sistema de Numeração Base 10

Símbolos: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9

$$\begin{array}{cccc}
 1 & 3 & 4 & 5 \\
 10^3 & 10^2 & 10^1 & 10^0 \\
 1 \times 10^3 & = 1000 \\
 3 \times 10^2 & = +300 \\
 4 \times 10^1 & = + 40 \\
 5 \times 10^0 & = + \underline{5} \\
 & & & 1345
 \end{array}$$

8.2.2 Sistema Binário

Os computadores reconhecem e processam dados, utilizando-se o sistema binário ou Base 2. O sistema binário utiliza dois símbolos, 0 e 1, em vez dos dez símbolos utilizados no sistema numérico decimal.

A posição, ou casa, de cada algarismo da direita para a esquerda em um número binário representa 2, o número base, elevado a uma potência ou expoente, começando com 0.

Exemplo: 1011 base 2 = $(1 \times 2 \text{ elevado por } 3 = 8) + (0 \times 2 \text{ elevado por } 2 = 0) + (1 \times 2 \text{ elevado por } 1 = 2) + (1 \times 2 \text{ elevado por } 0 = 1) = 11$ ($8 + 0 + 2 + 1$).

Sistema de Numeração Base 2

Símbolos: 0, 1

$$\begin{array}{cccc}
 1 & 0 & 1 & 1 \\
 2^3 & 2^2 & 2^1 & 2^0 \\
 1 \times 2^3 & = 8 \\
 0 \times 2^2 & = 0+ \\
 1 \times 2^1 & = 2+ \\
 1 \times 2^0 & = 1+ \\
 & & & \underline{11}
 \end{array}$$

Observação: Os computadores foram concebidos para utilizarem grupos de oito bits. Este grupo de oito bits é denominado byte. Em um computador, um byte representa um único local de armazenamento endereçável. Estes locais de armazenamento representam um valor ou um único caractere de dados, por exemplo, um código ASCII.

O número total de combinações de oito chaves ou bits ligadas ou desligadas é de 256. Já a faixa de valores de um byte é de 0 a 255. Veja abaixo como é o crescimento em binário da sequência entre 0 e 255:

- 00000000 -> 0
- 00000001 -> 1
- 00000010 -> 2
- 00000011 -> 3
- 00000100 -> 4
- 00000101 -> 5
- 00000110 -> 6
- 00000111 -> 7
- 00001000 -> 8
- 00001001 -> 9
- 00001010 -> 10
- 00001011 -> 11
- 00001100 -> 12
- 00001101 -> 13
- 00001110 -> 14
- 00001111 -> 15
- 00010000 -> 16
- ...
- 11111100 -> 252
- 11111101 -> 253
- 11111110 -> 254
- 11111111 -> 255

Os valores em binário dentro de um byte crescem da esquerda para direita somando-se um a cada passo. Por esse motivo cada campo do endereço IP pode ir apenas de 0 a 255, não existe IP 1.1.1.256, por exemplo, pois o valor do quarto byte não é possível com apenas 8 bits!

Outra dica interessante é que os números pares têm o último bit sempre em zero e os ímpares em 1, note na sequência mostrada anteriormente esse fato.

É importante entender o conceito do byte ao trabalhar com computadores e redes.

8.3 Conversão Binária

Vamos ver agora um pouco de como realizar conversão de sistemas numéricos começando pela conversão decimal-binário e na sequência veremos a conversão binário-decimal.

Conversão Decimal-Binário

Existem várias maneiras de realizar a conversão de decimal para binário, vamos mostrar nesse tópico um método simples de comparar o número decimal que queremos converter em binário com os valores de cada bit. A dica é verificar se o número decimal é maior ou menor que cada bit e ir subtraindo antes de passar ao próximo caso ele seja maior. Veja abaixo os valores em decimal de cada bit em um octeto (byte):

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

Sempre comece comparando o decimal a ser convertido com o valor do bit mais significativo (**128**). Veja o exemplo prático a seguir para converter o número decimal 168 em número binário de oito bits utilizando esse método:

- 128 cabe dentro de 168? Sim. Portanto, o bit mais à esquerda do número binário é um.
- Agora fazemos a diferença $168 - 128 = 40$.
- 64 cabe dentro de 40? Não cabe. Portanto, o segundo bit da esquerda é zero.
- 32 cabe dentro de 40? Sim. Portanto, o terceiro bit da esquerda é um.
- Agora subtraímos $40 - 32 = 8$.
- 16 cabe dentro de 8? Não cabe. Portanto, o segundo bit da esquerda é zero.
- 8 cabe dentro de 8? Sim. Portanto, o quinto bit da esquerda é um.
- Agora subtraímos $8 - 8 = 0$. Como o resto foi zero todos os bits à direita serão zero, mesmo assim vamos continuar a análise até o final.
- 4 cabe dentro de 0? Não cabe. Portanto o sexto bit é zero.
- 2 cabe dentro de 0? Não cabe. Portanto o sétimo bit é zero.
- 1 cabe dentro de 0? Não cabe. Portanto o oitavo bit mais à esquerda também é zero.
- Resultado: $10101000 = 168$ decimal

Conversão Binário-Decimal:

Os números binários podem ser convertidos em números decimais, multiplicando os dígitos binários pelo número base do sistema, o qual é Base 2, e elevando-os ao expoente da sua posição.

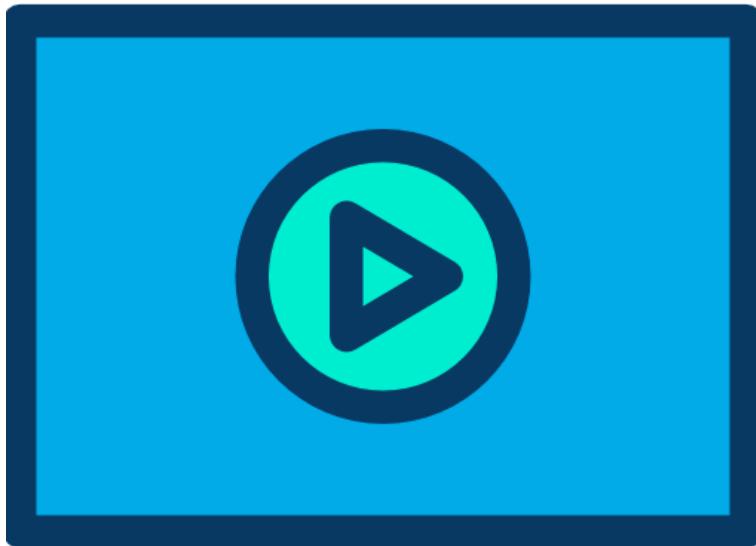
Exemplo: Para converter o número binário 01110000 em um número decimal fazemos o seguinte:

$$\begin{aligned}
0 \times 2 \text{ elevado a } 0 &= 0 \\
0 \times 2 \text{ elevado a } 1 &= 0 \\
0 \times 2 \text{ elevado a } 2 &= 0 \\
0 \times 2 \text{ elevado a } 3 &= 0 \\
1 \times 2 \text{ elevado a } 4 &= 16 \\
1 \times 2 \text{ elevado a } 5 &= 32 \\
1 \times 2 \text{ elevado a } 6 &= 64 \\
0 \times 2 \text{ elevado a } 7 &= 0
\end{aligned}$$

Agora é só somar o valor dos bits e temos o resultado: $0+0+0+0+16+32+64+0 = 112$

Lembre-se que as provas da Cisco não permitem uso de calculadora, por isso é importante que você entenda bem as conversões em binário e interpretar números Hexadecimais (estudados no IPv6).

8.4 Hosts, Redes e Máscaras



Como já estudamos, um endereço IP é representado por um número binário de 32 bits, divididos em quatro conjuntos de oito bits, chamados de octetos ou bytes.

Todo endereço IP é dividido em duas partes, sendo que a inicial identifica a rede e a final é o endereço do host de rede, chamado também de Host-ID (Host Identification ou identificação do host).

A melhor analogia para entender o endereçamento IP é o endereçamento postal, onde para encontrar um destino você necessita do nome da rua e do número da casa, ou seja, o endereço de rede seria o nome da rua e o endereço de host o número da casa. Portanto a principal função do endereçamento IP é **identificar um dispositivo** (micro, roteador, servidor, etc.) **dentro de uma rede**, a qual é um conjunto de computadores.

Quem delimita a porção de rede e de host em um endereço IP é a **máscara de rede** também chamada de **máscara de sub-rede**. Na realidade **não existe endereço IP sem uma máscara de rede**.

A máscara de rede também é representada por 32 bits, sendo que os bits "0" representam a porção de host e os bits "1" a de rede. A máscara sempre inicia com uma sequência de bits 1 e depois têm uma sequência de zeros, nunca veremos bits um e zero intercalados, isso porque o que é rede é rede, não existe uma rede-host para o endereçamento IP.

Por exemplo, uma máscara 1111111.00000000.00000000.00000000 = 255.0.0.0 é válida, já a máscara 11111110.00000000.00000000.11111111 = 254.0.0.255 não é válida.

Usando a mesma máscara acima, se tivermos o endereço IP 1.2.3.4 com a máscara 255.0.0.0 podemos tirar que a porção de rede desse endereço é "**1**" e o host-ID "**.2.3.4**".

A rede que um endereço IP pertence pode ser definida com uma conta binária chamada AND lógico entre o endereço e sua máscara. No AND lógico qualquer número AND zero é zero e um AND um é igual a um, portanto se fizermos o cálculo teremos:

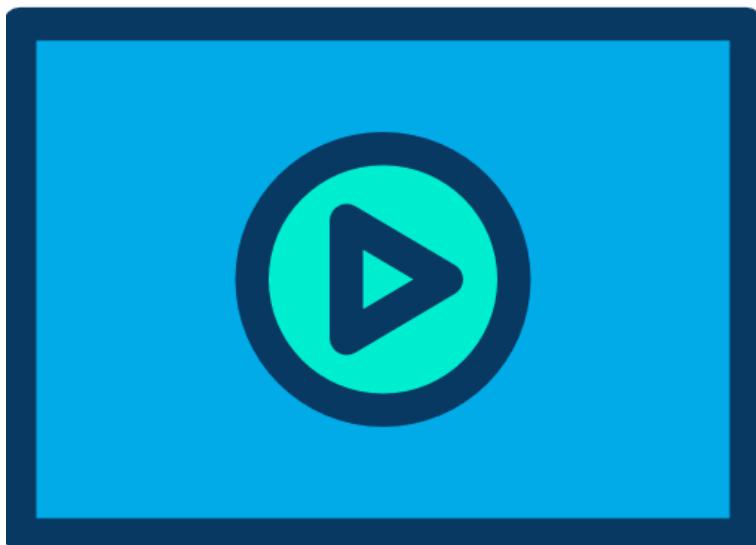
- 1.2.3.4 AND 255.0.0.0
- 00000001.00000010.00000011.00000100 AND
11111111.00000000.00000000.00000000
- 00000001.00000000.00000000.00000000 = 1.0.0.0

Portanto a rede que o IP 1.2.3.4 pertence é 1.0.0.0 com a máscara 255.0.0.0.

Podemos também representar o IP e máscara através da notação de prefixo de rede com a máscara não em decimal, mas representada por uma barra (/) mais o número de bits um nela contidos. Por exemplo, a rede calculada acima pode ser escrita 1.0.0.0/8, porque na máscara 255.0.0.0 temos oito bits um.

Observação: Lembre-se que um endereço IP identifica não uma máquina, mas **uma conexão à rede**. Máquinas com mais de uma interface de rede (roteadores, por exemplo) possuem um endereço IP para cada interface. Até mesmo um computador pode possuir vários endereços IP.

8.5 Endereçamento IP e a Internet



No início da Internet não era prevista essa taxa de adesão tanto de empresas como do setor público em geral, por isso os IP utilizados para endereçar as redes foram divididos em três classes de tamanhos fixos chamadas: **classes A, B e C**.

Essas classes foram baseadas na premissa que teríamos na Internet poucas redes de grande porte (126 redes com mais de 16 milhões de hosts cada uma), as quais estão na classe A, uma quantidade maior de redes de médio porte (aproximadamente 16 mil redes com mais de 65 mil hosts cada uma) que ficariam dentro da classe B e uma quantidade muito maior de redes de pequeno porte que ficariam dentro da classe C (aproximadamente 2 milhões de redes com apenas 254 hosts cada uma).

Para termos uma ideia de como a alocação de IPs foi realizada nos primórdios da Internet as faixas classe A foram distribuídas entre grandes instituições como AT&T, IBM, Xerox, HP, Apple, MIT, Ford, dentre outras. É isso mesmo que você está pensando uma empresa apenas com uma classe A inteira, ou seja, mais de **dezesseis milhões de hosts!**

Outras duas classes foram definidas além das citadas anteriormente, a classe D dedicada a serviços de Multicast e a classe E reservada para estudos e pesquisas.

O roteamento com base em classes é chamado de **Classful**.

Com o crescimento da Internet esse tipo de classificação e distribuição de IPs passou a não ser mais eficiente, pois as classes acabaram ficando muito limitadas em termos de tamanho de rede e flexibilidade.

Atualmente o mundo está vivendo uma fase em que os endereços IP versão 4 disponíveis estão com seus dias contados e já foi dado o início à implementação do IP versão 6, porém como os dois ainda irão conviver por muito tempo temos que saber sobre as duas versões.

Alguns outros fatos históricos interessantes sobre o crescimento da Internet:

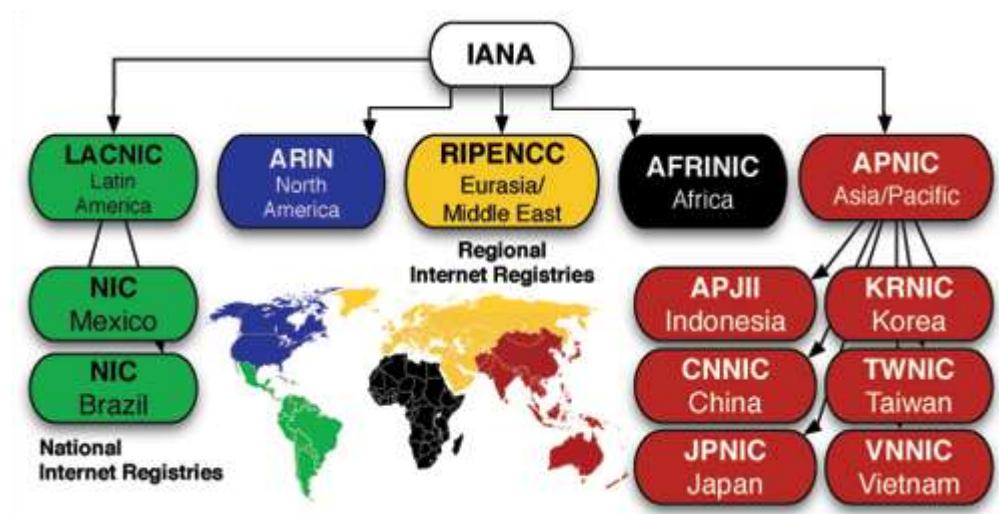
- Em 1990 já existiam 313.000 hosts conectados à Internet.
- Em maio de 1992 38% das faixas de endereços classe A, 43% da classe B e 2% da classe C já estavam alocados, sendo que a rede já possuía 1.136.000 hosts conectados.
- Em 1993, com a criação do protocolo HTTP e a liberação por parte do Governo estadunidense para a utilização comercial da Internet, a quantidade de hosts na Internet passou de 2.056.000 em 1993 para mais de 26.000.000 em 1997.
- Em 2012 a ISC (Internet System Consortium) estimou que existissem até o mês de julho de 2012 aproximadamente **908.585.739** hosts na Internet.

Em novembro de 1991 é formado o grupo de trabalho ROAD (Routing and Addressing) para atuar sobre o problema da escassez de endereços IP versão 4, o qual apresenta como solução a estes problemas a utilização do **CIDR (Classless Inter-domain Routing)**. Basicamente o CIDR tem como ideia central o **fim do uso das classes de endereços**, por isso o nome **classless** ou **"sem classes"**, possibilitando a alocação de blocos de tamanho apropriado conforme a real necessidade de cada rede na Internet.

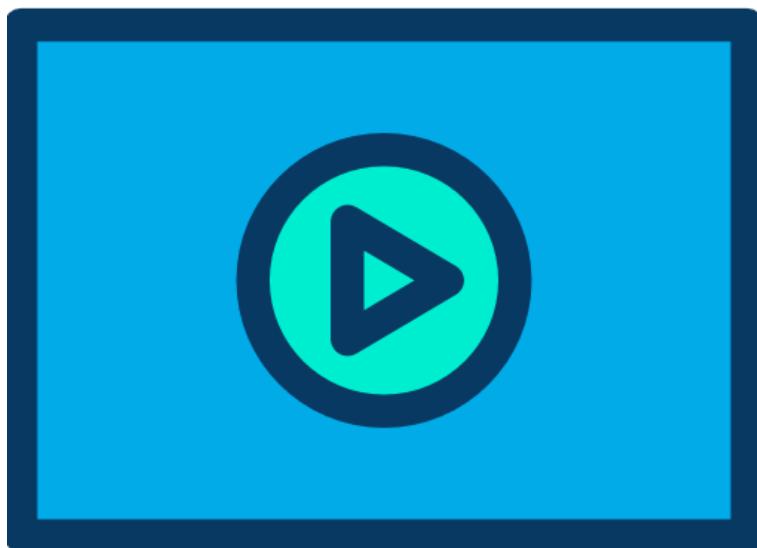
Outras duas técnicas foram desenvolvidas para desacelerar o esgotamento de IPs válidos da Internet foi a introdução dos **endereços IP privados** (RFC 1918) e o uso do **NAT** (Network Address Translation), as quais estudaremos em capítulos posteriores.

Mundialmente quem administra os IPs é a entidade chamada **IANA** (Internet Assigned Numbers Authority), a qual repassa as responsabilidades de alocação em cada região do mundo para outras cinco entidades, sendo que para a América Latina a **LACNIC** é a responsável.

No Brasil a LACNIC delegou a administração dos endereços IP para o **Registro BR** (<http://registro.br>), nesse link você pode registrar domínios, solicitar endereços IPs e também verificar a disponibilidade de domínios. Veja na figura abaixo um organograma das entidades que administram a alocação de IPs ao redor do mundo.



8.6 Classes de Endereços IP



Ao todo foram definidas cinco classes de endereços IP, ou seja, classes A, B, C, D e E. Veja a figura abaixo com as classes e como identificá-las.



O que caracteriza cada classe é o primeiro octeto do endereço IP, sendo que para a Classe A ele sempre inicia em zero, para a Classe B inicia em 10, para a Classe C em 110, na Classe D em 1110 e finalmente para a Classe E em 1111.

Aqui temos o primeiro uso da conversão de decimal para binário, se você enfrentar uma pergunta querendo saber a classe de um endereço IP é só converter o primeiro octeto em binário e seguir a regra estudada anteriormente!

Na figura também podemos tirar uma importante informação sobre quantas redes e endereços de host que as classes A, B e C podem fornecer. Note que para a classe A temos o primeiro octeto para rede e os demais para host, na B temos dois octetos para rede e dois para host e na classe C são três para rede e um para host, o que nos fornece a máscara de rede padrão de cada uma das classes:

- **Classe A** -> Rede.Host.Host.Host = 255.0.0.0
- **Classe B** -> Rede.Rede.Host.Host = 255.255.0.0
- **Classe C** -> Rede.Rede.Rede.Host = 255.255.255.0

As classes D e E não utilizam o conceito de rede e host, elas utilizam somente endereçamento de host, por isso não possuem máscara de rede.

Portanto, a faixa de endereços de Internet não vai de 0.0.0.0 a 255.255.255.255, ela está limitada aos endereços das classes A, B e C.

Além disso, temos diversas faixas de endereços reservados. A mais conhecida é a **RFC 1918** que define endereços para uso privativo, ou seja, para criação de Intranets, evitando o uso de endereços válidos para Internet em ambientes corporativos. Abaixo seguem as faixas de endereços privados:

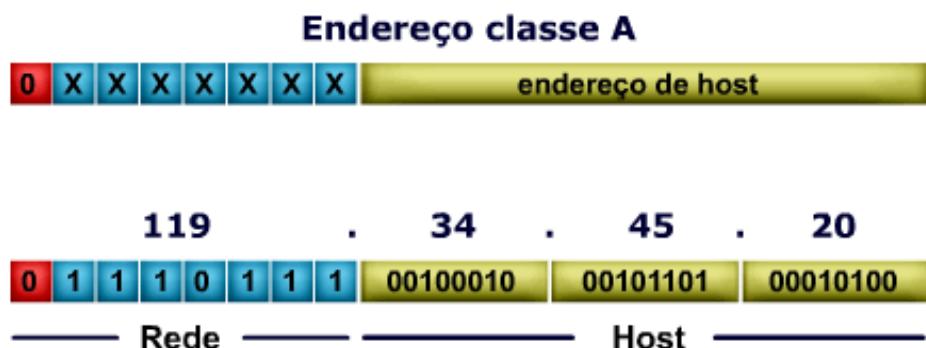
- **Classe A**: de 10.0.0.0 até 10.255.255.255
- **Classe B**: de 172.16.0.0 até 172.31.255.255
- **Classe C**: de 192.168.0.0 até 192.168.255.255

Os endereços começados em zero também não são utilizados para endereçar computadores, pois a rede 0.0.0.0 com a máscara 0.0.0.0 representa a Internet. Outra faixa reservada é a 127.0.0.0 a 127.255.255.255, a qual representa a faixa de loopback utilizada pelos computadores para endereçar a própria interface de rede. Se você pingar o endereço 127.0.0.1 no Windows, Linux ou MAC OS-X deve receber 100% de retorno, pois você está pingando sua própria placa de rede, portanto se ela não responder você está com sérios problemas.

Outra faixa de endereço reservada e não utilizada na Internet é a iniciada em 169.254.0.0 com a máscara 255.255.0.0, esses endereços são reservados para o **Zeroconf**, uma autoconfiguração da placa de rede quando o computador não encontra um servidor DHCP na rede. Se você entrar com um ipconfig no Windows ou ifconfig no Linux e verificar um endereço na faixa de 169.254.0.1 a 169.254.255.254 é sinal de que sua placa de rede encontrou um servidor DHCP para fornecer os dados necessários para seu correto funcionamento.

8.6.1 Endereço IP Classe A

Os endereços da classe A sempre terão o primeiro bit do primeiro octeto igual a 0 (0xxxxxxxx), veja figura abaixo ilustrando o endereço.



Ao lado segue a variação completa do primeiro octeto que representa as redes da classe A.

Note que o primeiro bit nunca será diferente de "0". Uma dica interessante para descobrir em que classe o endereço IP está situado é converter o primeiro octeto em binário e verificar os primeiros bits.

0 0 0 0 0 0 0 0 → 0
 0 0 0 0 0 0 0 1 → 1
 0 0 0 0 0 0 1 0 → 2

⋮

0 1 1 1 1 1 1 0 → 126
 0 1 1 1 1 1 1 1 → 127

Os endereços de classe A pertencem das redes **1.0.0.0** até a **126.0.0.0**. As redes 0.0.0.0 (Internet) e 127.0.0.0 (127.0.0.0) são de uso especial e não podem ser utilizadas para endereçar redes, conforme já estudamos anteriormente.

A máscara de rede padrão de uma classe A é **255.0.0.0**. Outra forma de representar uma máscara de rede é utilizando a notação decimal, onde a máscara será representada pela quantidade de bits "1" nela contidos, para a classe A o prefixo é "/8".

Para determinar a quantidade de hosts que uma classe possui, ou seja, o número de computadores que ela pode endereçar utiliza-se a fórmula abaixo:

$$* \text{ Número de hosts} = 2^n - 2$$

(onde n representa o número de bits 0 da máscara de rede)

Máscara da classe A

255 . 0 . 0 . 0	11111111 . 00000000 . 00000000 . 00000000
	<u>24 bits "0"</u>

$$\text{Número de hosts} = 2^{24} - 2 = 16.777.216 - 2$$

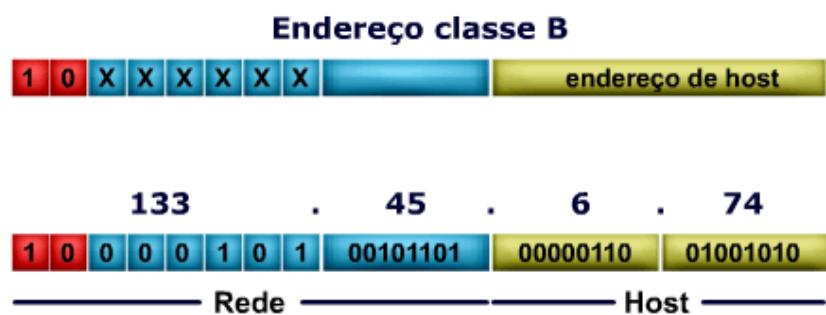
$$\text{Número de hosts} = 16.777.214$$

Note que na fórmula diminuímos dois endereços IPs do total, isso porque o primeiro representa a própria rede e o último representa o endereço de broadcast, e ambos não podem ser utilizados para endereçar computadores.

As **126** redes da classe A possuem endereços suficientes para endereçar até **16.777.214** hosts (computadores) cada uma.

8.6.2 Endereço IP Classe B

Os endereços da classe B sempre terão os dois primeiros bits do primeiro octeto igual a 10 (10xxxxxx), veja ilustração abaixo.



Abaixo segue a variação completa dos dois primeiros octetos que representam as redes da classe B.

1 0 0 0 0 0 0 0 . 0 0 0 0 0 0 0 0 → 128.0	1 0 1 0 1 0 1 0 . 0 0 0 0 0 0 0 0 → 170.0
1 0 0 0 0 0 0 0 . 0 0 0 0 0 0 0 1 → 128.1	1 0 1 0 1 0 1 0 . 0 0 0 0 0 0 0 1 → 170.1
1 0 0 0 0 0 0 0 . 0 0 0 0 0 0 1 0 → 128.2	1 0 1 0 1 0 1 0 . 0 0 0 0 0 0 1 0 → 170.2
⋮	⋮
1 0 0 0 0 0 0 0 . 1 1 1 1 1 1 1 0 → 128.254	1 0 1 1 1 1 1 0 . 1 1 1 1 1 0 1 1 → 190.251
1 0 0 0 0 0 0 0 . 1 1 1 1 1 1 1 1 → 128.255	1 0 1 1 1 1 1 0 . 1 1 1 1 1 1 0 0 → 190.252
1 0 0 0 0 0 0 1 . 0 0 0 0 0 0 0 0 → 129.0	1 0 1 1 1 1 1 0 . 1 1 1 1 1 1 0 1 → 190.253
1 0 0 0 0 0 0 1 . 0 0 0 0 0 0 0 1 → 129.1	1 0 1 1 1 1 1 0 . 1 1 1 1 1 1 1 0 → 190.254
1 0 0 0 0 0 0 1 . 0 0 0 0 0 0 1 0 → 129.2	1 0 1 1 1 1 1 0 . 1 1 1 1 1 1 1 1 → 190.255
⋮	⋮
1 0 0 0 0 0 0 1 . 1 1 1 1 1 1 1 0 → 129.254	1 0 1 1 1 1 1 1 . 1 1 1 1 1 1 0 1 → 191.253
1 0 0 0 0 0 0 1 . 1 1 1 1 1 1 1 1 → 129.255	1 0 1 1 1 1 1 1 . 1 1 1 1 1 1 1 0 → 191.254
1 0 0 0 0 0 1 0 . 0 0 0 0 0 0 0 0 → 130.0	1 0 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 → 191.255

Conforme mostrado acima, as redes classe B variam de 128.0.0.0 até 191.255.0.0, sendo que a máscara de rede padrão de uma classe B é 255.255.0.0 ou /16.

O número de redes classe B é o número de bits 1 que podem variar na máscara elevado a dois, ou seja, como temos 16 bits de rede e dois deles são fixos (**10xxxxxxxx.xxxxxxxxxx**) temos 2^{14} endereços de classe B o que dão **16.384 redes**.

Para determinar a quantidade de hosts que uma classe possui, ou seja, o número de computadores que ela pode endereçar utiliza-se a fórmula abaixo (mesma conta utilizada para a classe A):

$$* \text{ Número de hosts} = 2^n - 2 \quad (\text{onde } n \text{ representa o número de bits 0 da máscara de rede})$$

Máscara da classe B

255 . 255 . 0 . 0
11111111 . 11111111 . <u>00000000 . 00000000</u>
16 bits "0"

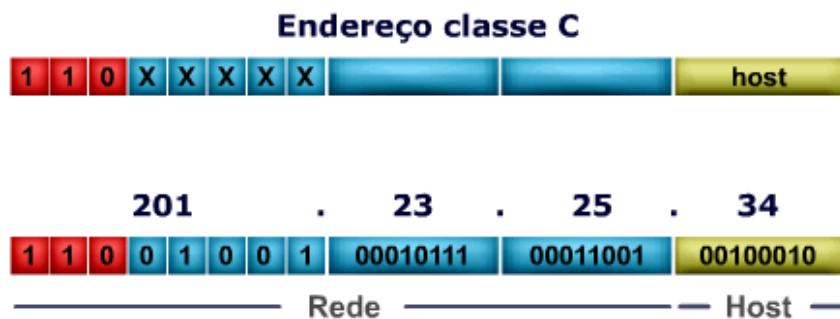
$$\text{Número de hosts} = 2^{16} - 2 = 65.536 - 2$$

$$\text{Número de hosts} = 65.534$$

Portanto a classe B possui endereços suficientes para endereçar **16.384 redes** diferentes com até **65.534 hosts** (estações) cada uma.

8.6.3 Endereço IP Classe C

Os endereços da classe C sempre terão os três primeiros bits do primeiro octeto igual a 110 (110xxxx), conforme figura abaixo.



As redes classe C variam de 192.0.0.0 (**110**000000.00000000.00000000.00000000) até a 223.255.255.0 (**110**11111.11111111.11111111.00000000), sendo que a máscara de rede padrão de uma classe C é 255.255.255.0 ou /24.

O número de redes classe C segue o mesmo princípio que utilizamos para a classe B, ou seja, temos 24 bits de host com os três primeiros do primeiro octeto fixos em "110", portanto podemos ter 2^{21} (24-3) redes classe C, ou seja, um total de **2.097.152 redes**.

Para determinar a quantidade de hosts que uma classe possui, ou seja, o número de computadores que ela pode endereçar utiliza-se a mesma fórmula das classes A e B (**o cálculo de host nunca varia!**):

$$* \text{ Número de hosts} = 2^n - 2$$

(onde n representa o número de bits 0 da máscara de rede)

Máscara da classe C

$$\begin{array}{ccccccccc} 255 & . & 255 & . & 255 & . & 0 \\ \textcolor{green}{11111111} & . \textcolor{green}{11111111} & . \textcolor{green}{11111111} & . \textcolor{orange}{00000000} \\ \hline & & & & & & 08 \text{ bits "0"} \end{array}$$

$$\text{Número de hosts} = 2^8 - 2 = 256 - 2$$

$$\text{Número de hosts} = 254$$

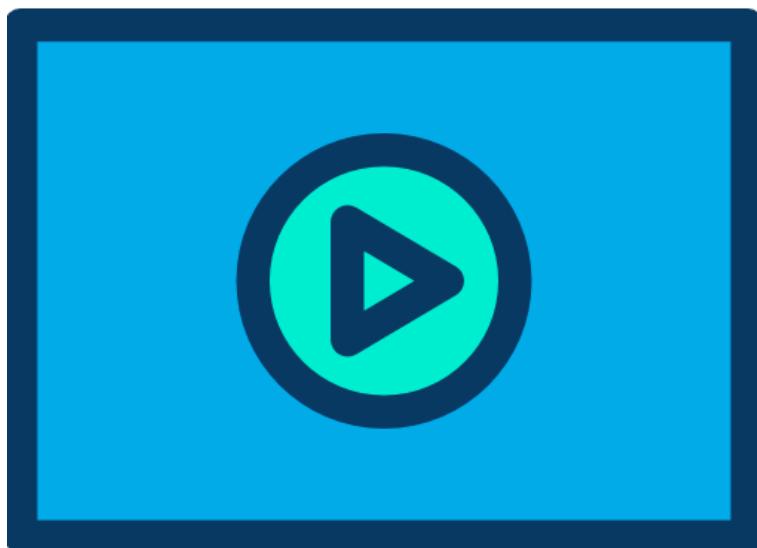
Portando a classe C possui endereços suficientes para endereçar **2.097.152** redes diferentes com até **254** hosts cada uma.

8.6.4 Endereço IP Classe D e Classe E

Os endereços da classe D são utilizados para **multicasting** e variam dos Ips 224.0.0.0 até 239.255.255.255. Os demais IPs pertencem à classe E, à qual é reservada para testes e estudos.

classe D	1 1 1 0	endereço de multicast
classe E	1 1 1 1 0	reservado para uso futuro

8.7 Tipos de Comunicação Suportada pelo Protocolo IP

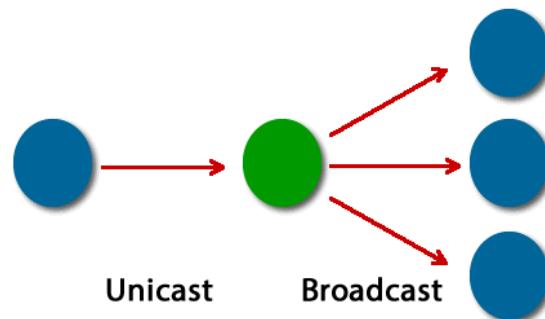


Conforme vimos anteriormente os endereços IP foram divididos em classes, sendo que nas **Classes A, B e C** temos os endereços utilizados pelos computadores para que eles possam se comunicar em rede, chamados de endereços de **Unicast**.

Além disso, nessas três classes de IP temos também os endereços de **Broadcast**, utilizados para comunicação com **todos os hosts** de uma rede.

Portanto, a comunicação **Unicast** é realizada de **um para um**, ou seja, **host a host**, já a comunicação em **broadcast** é de **um para todos**, ou seja, quando um pacote é endereçado no destino para um endereço de broadcast **todos os hosts** daquela rede **irão receber e processar** aquele pacote IP.

Veja a figura ao lado.



Em uma rede IP o primeiro endereço representa a própria rede para o roteamento e **não pode ser utilizado para endereçar hosts**. Este endereço recebe o nome de “**endereço de rede**” ou “**endereço de subrede**” e é utilizado para criar “**rotas**” para as redes IP.

Os endereços de Unicast vão do segundo ao penúltimo IP de cada rede ou sub-rede, por exemplo, na rede classe C 192.168.1.0 os endereços de Unicast vão de 192.168.1.1 até 192.168.1.254, pois o endereço 192.168.1.0 é o endereço de rede e o último IP 192.168.1.255 é o endereço de broadcast dessa rede.

Os endereços de Unicast são chamados de **endereços de Host (hosts válidos ou IPs válidos)** e podem ser **utilizados para endereçar os hosts ou interfaces de rede**, já os **endereços de rede e broadcast NÃO podem ser utilizados para endereçar os hosts ou interfaces dos roteadores**.

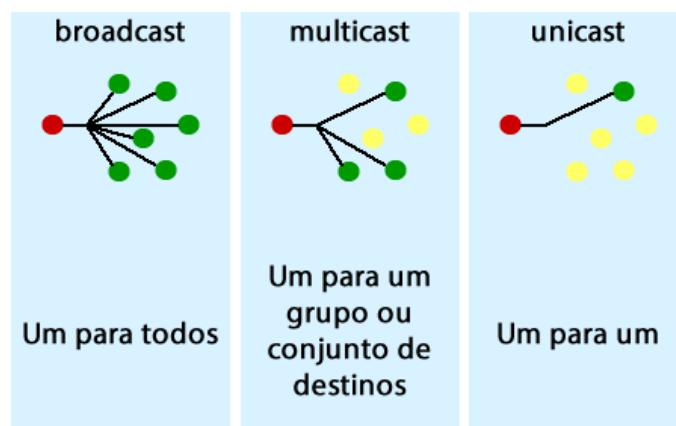
O endereço de broadcast que representa **todos os IPs** (de qualquer classe) é o endereço IP **255.255.255.255**, porém cada rede ou sub-rede IP tem também um endereço de broadcast que representa todos os IPs daquela rede ou sub-rede específica, o qual é o **último IP de cada rede ou subrede**. Por exemplo, na rede classe C 192.168.1.0 o IP 192.168.1.255 é o broadcast direcionado dessa rede, o que significa se você fizer um “ping 192.168.1.255” todos os IPs dessa rede irão responder, ou seja, os computadores configurados com IPs de 192.168.1.1 até 192.168.1.254.

Normalmente esse teste proposto acima não deve funcionar, pois ele permite um tipo de ataque chamado de Smurf e por isso normalmente o ping para endereços de broadcast não são respondidos por muitos sistemas operacionais.

Os **broadcasts direcionados** a uma sub-rede específica, ou seja, para o **último IP** de uma rede ou sub-rede, por padrão não são encaminhados entre interfaces de um roteador, porém esse comportamento pode ser alterado com o comando “**ip directed-broadcast**” que pode ser inserido nas interfaces dos roteadores e permitir o envio do broadcast direcionado por aquela interface. Esse comando vem por padrão desabilitado.

Já uma mensagem de broadcast para o endereço **255.255.255.255** nunca será encaminhado pelas interfaces, mesmo com o comando citado acima.

Já os endereços de **Classe D** são utilizados para a comunicação Multicast, a qual é uma comunicação de **um para um grupo**, ou seja, utilizada para **comunicação em um grupo** de elementos que possuem o **mesmo endereço de Multicast**. Veja a figura abaixo com a diferença entre os três tipos de comunicação.



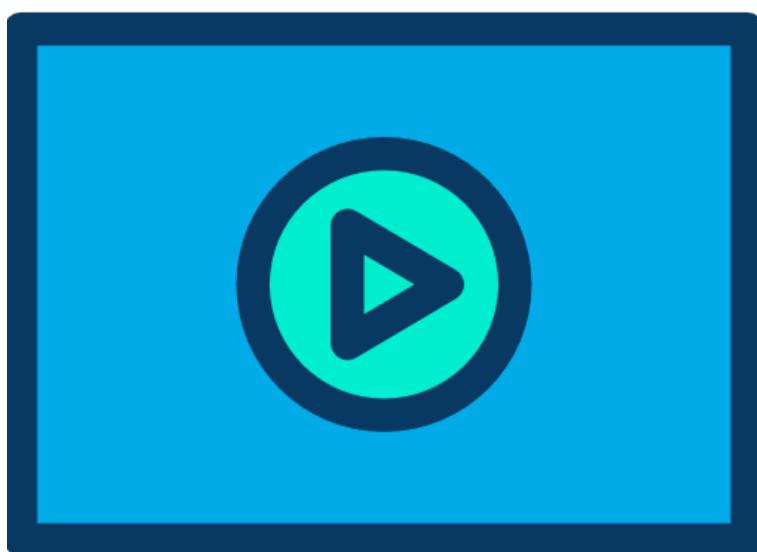
Por exemplo, quando um roteador é configurado com o EIGRP como protocolo de roteamento, as informações de roteamento trocadas entre os roteadores são feitas utilizando o **multicasting**.

Os roteadores que estão rodando o EIGRP recebem o endereço IP classe D 224.0.0.10 e se um roteador em uma rede LAN enviar uma mensagem de roteamento e houver mais roteadores OSPF todos receberão essa mensagem, porém diferente do broadcast somente os roteadores com o IP 224.0.0.10 irão processar essa informação.

Note que todos os roteadores EIGRP enviam e recebem informações de roteamento pelo mesmo endereço classe D 224.0.0.10, por isso o termo "**grupo de multicast**".

No Unicast precisamos ter um IP de origem e outro de destino **únicos** na rede, já no broadcast temos um endereço de origem do host que está enviando o pacote e o destino será 255.255.255.255 ou um dos endereços de broadcast direcionados de uma rede, por exemplo, 192.168.1.255.

8.8 Endereçamento IPv4 na Prática



Na prática um endereço IP versão 4 possui 32 bits e é dividido em quatro "**octetos**", ou seja, quatro conjuntos de oito bits e escritos em formato decimal. O que define que parte do endereço é rede ou host é a "**máscara de rede**" ou "**máscara de sub-rede**". Por exemplo, se tivermos o endereço **192.168.10.65** e não dermos mais nenhuma característica não seria nada mais que um número qualquer, pois se não pudéssemos dividir os endereços IPs em redes não teríamos uma "**hierarquia**" e não poderíamos dividir as redes entre as diversas empresas e corporações.

Tenha em mente que a “**rede IP**” representa um **conjunto de endereços**, assim como no endereçamento postal de um país se não tivéssemos os Estados, Cidades, Ruas e números das casas não conseguíramos enviar cartas. Imagine se tivéssemos apenas o País Brasil e você deseja enviar uma carta para uma pessoa, como seria possível encontrar o João da Silva que tem seu endereço “Brasil”? Precisamos de uma hierarquia, ou seja, vamos mandar uma carta para o Sr João da Silva, que mora no Brasil, na cidade de São Paulo, na rua tal, número tal apartamento 100, agora sim faz sentido concorda? A mesma coisa acontece com as redes IP, para que possamos encontrar um host, que é relativo a uma pessoa ou casa no endereçamento postal, precisamos saber onde ele está e isso quem nos diz é a rede ou sub-rede IP e quem nos mostra isso é a máscara de rede ou de sub-rede.

Vamos completar agora o endereço 192.168.10.65 com a máscara padrão de um endereço de **classe C** que é o **255.255.255.0**. Veja que cada octeto da máscara corresponde ao octeto do endereço, portanto onde temos o bit um na máscara indica que o número que está no endereço IP representa uma rede, convertendo a máscara em binário temos **11111111.11111111.11111111.00000000**, ou seja, os três primeiros octetos representam a rede e o último octeto o host. Isso significa que temos um conjunto de micros dentro da rede 192.168.10 e o que procuramos é o que tem o final 65.

Na prática uma rede é quando **todos os bits de host estão zerados**, portanto representamos a rede que o host final 65 pertence como: 192.168.10.**0**, pois é no último octeto que estão os bits de host.

Os Hosts, ou seja, os endereços que posso configurar em um computador, laptop, impressora, switch ou interface de um roteador vão do primeiro IP após o endereço de rede até o penúltimo número da sequência (um antes do broadcast).

Lembrem-se endereços de host são também chamados de endereços de **Unicast**, para utilização de comunicação entre dois terminais apenas, já o último valor representa o **broadcast direcionado** daquela rede, ou seja, se enviamos um ping para o último valor da sequência de IPs de uma rede todos os hosts que estiverem ativos dessa rede deveriam responder. Colocamos a palavra “**deveriam**” porque essa ação pode ser bloqueada em algumas redes por questões de segurança.

Vamos então entender o que é uma rede IP finalizando a análise do endereço 192.168.10.65 com a máscara 255.255.255.0.

Já sabemos que sua rede é o 192.168.10.0, que o broadcast é o último valor da sequência (quando todos os bits de host estão em um) e os hosts válidos estão entre a rede e o broadcast, portanto teremos:

- **Rede:** 192.168.10.0 (192.168.10.**00000000** - quando todos os bits de host estão zerados).
- **Broadcast (último valor):** 192.168.10.255 (192.168.10.**11111111** -> o último valor é quando todos os bits de host estão setados em um).
- **Endereços que podemos utilizar nos hosts:** 192.168.10.1 (192.168.1.**00000001** - o próximo após a rede) até 192.168.10.254 (192.168.10.**11111110** - um a menos que o broadcast).

Portanto essa é a definição de uma rede IP, ou seja, ela possui um **endereço de rede** (todos os bits de host estão zerados), os **hosts válidos** (um após a rede até um antes do broadcast) e um **endereço de broadcast** (todos os bits de host estão em 1 – último IP antes da próxima rede).

Lembre-se que outra maneira de encontrar a rede que um endereço pertence, a qual é utilizada pelos roteadores e computadores, é fazendo o **AND lógico** entre o IP e a máscara. Um AND lógico é uma conta em binário que diz que qualquer valor AND zero dá zero e um AND um dá um. Vamos fazer a conta com o endereço 192.168.10.65 AND 255.255.255.0.

Onde temos 255 é tudo 1 e onde temos zero é tudo zero, ou seja, temos oito bits um no número 255 e oito bits zero no ponto zero. Fazendo o AND temos que:

- 192 AND 255 = 192
- 168 AND 255 = 168
- 10 AND 255 = 10
- 65 AND 0 = 0

Portanto a rede é a 192.168.10.0 com a máscara 255.255.255.0.

Outro ponto importante é a quantidade de redes e hosts por rede e como isso tudo pode ser calculado. Se você conhecer bem o binário conseguirá responder essa pergunta sozinho, senão vamos aprender ou revisar na sequência.

Quem dá a quantidade de redes ou hosts que teremos são quantos bits vamos utilizar para fazer as redes e hosts, ou seja, os **bits um** da máscara que podemos utilizar dão a quantidade de **redes** e os **bits zero** dão a quantidade de **hosts**.

Por exemplo, foi citado que uma classe C tem sempre os três primeiros bits fixos em "110" e como ela utiliza os três primeiros octetos para rede e somente o quarto octeto para host temos o seguinte cenário:

- 21 bits 1 (r - rede) para redes (24 menos 3 que são fixos) e 8 bits (h - hosts) para fazer os hosts.
- 110~~rrrrrr.rrrrrrrr.rrrrrrrr.hhhhhh~~

Para calcular as redes basta você fazer dois (base do binário) elevado à quantidade de bits de rede que sobraram nesse caso 21, ou seja, 2^{21} (dois elevado a vinte e um) será igual a 2.097.152 de redes classe C.

Já para os hosts temos um detalhe importantíssimo, pois o primeiro IP é utilizado para dar o endereço rede e o último o broadcast, portanto temos que descontar dois IPs da conta, por isso a fórmula para hosts são dois elevados ao número de bits zero da máscara menos dois, pois temos que descontar a rede e o broadcast que não são utilizados para endereçar hosts. No caso da classe C temos $(2^8 - 2) = (256 - 2) = 254$ IPs.

Seguindo o mesmo princípio, se tivermos que escolher redes Classe A e B o que varia são as quantidades de redes e hosts que temos por classe.

Por exemplo, se fossemos endereçar uma LAN com a rede 172.16.0.0 classe B, a qual tem a máscara padrão 255.255.0.0 ou o prefixo /16 temos as seguintes características:

- 172.16.0.0 é o endereço de rede, ou seja, quando todos os bits de host estão em zero.
- Como máscara é 255.255.0.0 temos os dois últimos octetos variando como host, pois ela é uma classe B (**10rrrrrr.rrrrrrrr.hhhhhhhh.hhhhhhhh**).
- O último endereço IP é o broadcast dessa rede (todos os bits de host estão em um), o qual será 172.16.1111111.11111111 ou 172.16.255.255.
- Tudo que está entre 172.16.0.0 e 172.16.255.255 você pode utilizar para endereçar hosts.
- Portanto temos os endereços válidos iniciando em 172.16.0.1 e o último 172.16.255.254 (um a menos que o broadcast).

Em termos quantitativos, para uma classe B temos 14 bits (pois os dois primeiros do primeiro octeto são sempre 10) de rede e 16 bits de host. O que nos dá 2^{14} redes (16.384) e " $2^{16} - 2$ " endereços de host (65.534 hosts válidos).

Agora vamos a um exemplo com a classe A, endereçando uma LAN com a rede 10.0.0.0, a qual tem a máscara padrão 255.0.0.0 ou /8 temos as seguintes características:

- 10.0.0.0 é o endereço de rede, ou seja, quando todos os bits de host estão em zero.
- Como máscara é 255.0.0.0 temos os dois últimos octetos variando como host, pois ela é uma classe A (**10rrrrrr.hhhhhhhh.hhhhhhhh.hhhhhhhh**).
- O último endereço IP é o broadcast dessa rede (todos os bits de host estão em um), o qual será 10.1111111.1111111.1111111 ou 10.255.255.255.
- Tudo que está entre 10.0.0.0 e 10.255.255.255 você pode utilizar para endereçar hosts.
- Portanto temos os endereços válidos iniciando em 10.0.0.1 e o último 10.255.255.254 (um a menos que o broadcast).

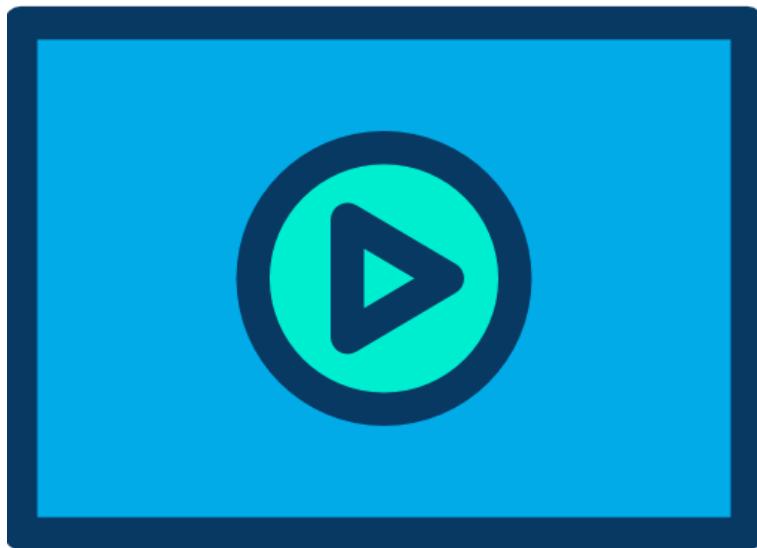
Em termos quantitativos, para uma classe A temos 7 bits de rede (pois o primeiro octeto é sempre 0 na classe A) e 24 bits de host. O que nos dá 2^7 redes (128) e " $2^{24} - 2$ " endereços de host (16.777.214 hosts válidos). Porém ao invés de termos 128 temos 126 redes na classe A, pois temos que descontar as redes iniciadas com zero (0.0.0.0) e com 127 (127.0.0.0).

Lembre-se que elas são redes especiais, sendo que a zero é reservada para representar todas as redes ou a Internet e a 127 é reservada para loopback.

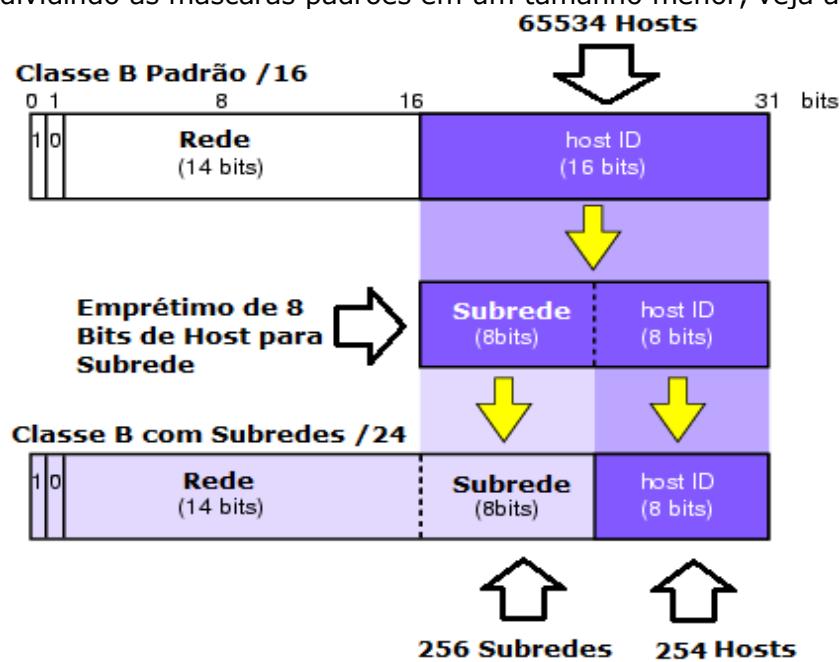
Na prática cada rede LAN, VLAN ou WAN precisa de uma rede IP **própria e única**, portanto endereçar é atribuir uma rede a uma interface de um roteador ou a uma VLAN e distribuir os endereços de host para essas interfaces e demais terminais.

O que estudamos aqui são as **redes IP baseadas em classes** ou **classfull**. Mais para frente no curso vai dividir essas redes em **sub-redes** e analisar o cálculo de **redes classless** ou **CIDR**, ou seja, como a Internet funciona atualmente, desconsiderando as classes de IP e utilizando **prefixos** ao invés de máscaras de sub-rede.

8.9 Dividindo Redes IPv4 em Sub-redes



Dividir redes classful em sub-redes é “emprestar” ou “roubar” bits da máscara padrão para criar sub-redes, dividindo as máscaras padrões em um tamanho menor, veja a figura abaixo.



Nessa figura temos uma máscara classe B padrão **255.255.0.0**, em binário **11111111.11111111.00000000.00000000**, portanto onde temos bits 1 na máscara são endereços fixos e não podemos alterar, agora podemos sim “emprestar” bits de host (zero) da máscara de rede para criar redes menores ou sub-redes. Nesse exemplo emprestamos oito bits da máscara de rede para criar 256 sub-redes (2^8 bits emprestados) cada uma com 254 hosts (2^8 bits zero que sobraram na máscara de sub-rede). Com isso a máscara de rede padrão 255.255.0.0 vira a máscara de sub-rede 255.255.**255**.0, pois emprestamos 8 bits dela para criar sub-redes.

Se estivermos utilizando a rede 128.0.0.0, no total ela tem dos IPs 128.0.0.1 até 128.0.255.255, agora vamos subdividir esses IPs em sub-redes menores iniciando em 128.0.0.0 até 128.0.0.255, depois 128.0.1.0 até 128.0.1.255, 128.0.2.0 até 128.0.2.255 e assim segue até a última sub-rede 128.0.255.0 até 128.0.255.255.

Vamos elaborar melhor essa necessidade entendendo o problema e suas soluções:

- **Problema 1:** as classes dividem as redes e hosts em valores fixos e não flexíveis, por exemplo, se eu precisar de uma máscara que suporte pelo menos 1000 hosts por sub-rede não é possível com classe A, B e C pura sem exceder ou ter a necessidade de dividir esses hosts em redes menores.
- **Problema 2:** Minha rede corporativa é composta por 50 segmentos, assim como no exemplo anterior não temos uma máscara que suporte o mais próximo possível de 50 redes sem termos desperdício de endereços.
- **Problema 3:** Uma rede precisa de 128 sub-redes cada uma com até 1000 hosts. Idem aos dois exemplos anteriores.
- **Solução:** para os três problemas é escolher uma classe que melhor se encaixe nas quantidades mínimas de endereçamento e utilizar a divisão em sub-rede para encontrar uma máscara mais precisa.

Os problemas citados acima são de projeto, onde é passado um requisito de quantidade de hosts ou de sub-redes para que o aluno calcule a melhor máscara.

Outro modelo de questão de sub-rede é a análise do endereçamento dado um endereço e máscara. Por exemplo, a questão fornece o endereço 192.168.1.10 com a máscara 255.255.255.240 e realiza perguntas como:

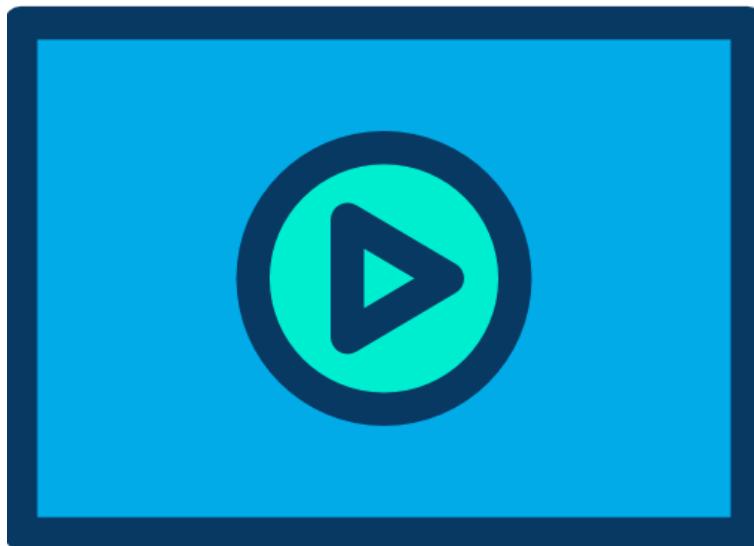
- Qual o endereço de sub-rede desse host?
- Qual o endereço de broadcast dessa sub-rede?
- Quais endereços em uma lista pertencem à mesma sub-rede que aquele host?
- Dada uma lista de endereços reconheça IPs válidos (que podem ser endereçados em hosts)?

Além desse conceito poder ser cobrado em conjunto com questões práticas, por exemplo, configure uma interface LAN do roteador, sendo que seu endereço IP é o primeiro IP válido pertencente à quinta sub-rede de 192.168.0.0/29. Nesse caso o aluno terá que calcular a sub-rede que o IP pertence e aí sim poder realizar a configuração da interface LAN.

Para realizar esses cálculos existem vários métodos, porém desenvolvemos uma metodologia simples e principalmente veloz de resolução de problemas de sub-rede, a qual estudaremos ao longo do capítulo.

Nesse capítulo vamos ensinar os cálculos utilizando sempre exemplos práticos, além de mais produtivo é muito mais simples de ensinar e aprender!

8.9.1 Método Tradicional de Análise de Endereços IP



A maneira tradicional de analisar um endereço IP é utilizando a definição, ou seja, fazendo o AND lógico entre o endereço e sua máscara de sub-rede. Com esse método conseguiremos descobrir seu endereço de rede, faixa de valores válidos para endereçamento em hosts e também o broadcast direcionado da sub-rede em questão.

Vamos a um exemplo prático, onde temos o endereço 192.168.10.170 com a máscara 255.255.255.240 ou /28.

1. Primeiro passo da análise é descobrir a classe, a qual é C, pois se convertermos o primeiro octeto em binário temos $192 = \underline{\text{110}}00000$.
2. Em seguida vamos fazer o AND lógico. Essa conta é realizada em binário, porém como qualquer bit com zero é zero e somente bit um com bit um dá um não precisamos converter todos os octetos, pois somente quando a máscara é diferente de zero (tudo zero) ou 255 (tudo um) que precisaremos converter, veja a seguir.

192.168.10 .170
AND 255.255.255.240
192.168.10 .???

Como qualquer coisa com 1 dá ela mesma, $192 \text{ AND } 255 = 192$, $168 \text{ AND } 255 = 168$ e $10 \text{ AND } 255 = 10$, porém com o 240 teremos que transformar o octeto do endereço e da máscara em binário, veja abaixo:

$$\begin{aligned} 170 &= 10101010 \\ 240 &= \underline{11110000} \\ 10100000 &= 128+0+32+0+0+0+0+0 = 160 \end{aligned}$$

Portanto, o endereço pertence à sub-rede **192.168.10.160**.

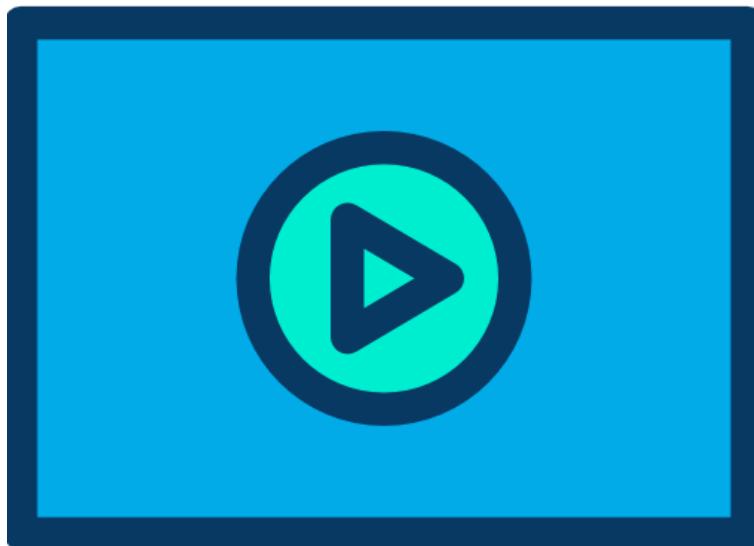
3. Agora vamos encontrar o endereço de broadcast dessa sub-rede. Por definição o broadcast tem todos os bits de host setados em "1", portanto teremos:
 $192.168.10.1010\text{1111} = \text{192.168.10.175}$.
4. Os hosts válidos estão entre o endereço de rede e o broadcast, ou seja, iniciando em 192.168.1.161 e vão até 192.168.1.174, totalizando 14 hosts válidos por sub-rede. Veja a sequência de IPs válidos dessa sub-rede:
 - 1) 192.168.10.1010**0001** → **161** → **1º endereço válido**
 - 2) 192.168.10.1010**0010** → **162**
 - 3) 192.168.10.1010**0011** → **163**
 - 4) 192.168.10.1010**0100** → **164**
 - 5) 192.168.10.1010**0101** → **165**
 - 6) 192.168.10.1010**0110** → **166**
 - 7) 192.168.10.1010**0111** → **167**
 - 8) 192.168.10.1010**1000** → **168**
 - 9) 192.168.10.1010**1001** → **169**
 - 10) 192.168.10.1010**1010** → **170**
 - 11) 192.168.10.1010**1011** → **171**
 - 12) 192.168.10.1010**1100** → **172**
 - 13) 192.168.10.1010**1101** → **173**
 - 14) 192.168.10.1010**1110** → **174** → **último endereço válido (broadcast -1)**

Na prática a cada bit emprestado de uma máscara você divide essa rede em dois elevados a n, onde esse n são os bits emprestados. Note no exemplo acima que temos um endereço classe C com uma máscara /28, como a padrão é /24 emprestamos 4 bits para sub-rede, portanto estamos dividindo essa rede em 2^4 sub-redes, o que nos dá um total de 16 sub-redes.

Como uma classe C tem um total de 256 endereços (primeiro a rede, do segundo ao penúltimo os hosts válidos e o último o broadcast), se dividirmos 256 por 16 teremos que cada sub-rede tem um total de 16 endereços, como cada sub-rede terá seu próprio endereço de sub-rede e um broadcast direcionado, sobrem 14 hosts para cada uma delas.

Se você notou acima, em termos quantitativos as contas continuam basicamente as mesmas, o número de sub-redes são dois elevados à quantidade de bits emprestados e os hosts são dois elevados à quantidade de bits zero que sobraram na máscara de sub-redes.

Existem na Internet os famosos "**subnet calculators**" ou calculadoras de sub-rede, você pode utilizar esses recursos apenas para conferir seus cálculos, porque no CCNA não é permitida calculadora nem qualquer dispositivo de ajuda, as contas são feitas pelo próprio aluno!

8.9.2 Exemplo Prático I – Dividindo Redes Classe A, B e C em duas Sub-redes

Conforme o que já estudamos de sub-rede, para dividir uma rede Classe A, B ou C em duas sub-redes precisamos emprestar apenas um bit de host e transformá-lo em bit de sub-rede (1).

Vamos iniciar utilizando um endereço classe C padrão 192.168.1.0 com máscara 255.255.255.0 (/24). Seus IPs válidos ou de hosts vão de 192.168.1.1 a 192.168.1.254 e o endereço de broadcast é 192.168.1.255.

Agora vamos emprestarmos 1 bit e dividir a rede em duas sub-redes, assim teremos:

- Primeira sub-rede: 192.168.1.0 com máscara 255.255.255.128
 - Hosts válidos 192.168.1.1 a 192.168.1.126
 - Broadcast 192.168.1.127
- Segunda sub-rede: 192.168.1.128 com máscara 255.255.255.128
 - Hosts válidos 192.168.1.129 a 192.168.1.254
 - Broadcast 192.168.1.255

Note que a máscara padrão era 255.255.255.0, se emprestamos um bit ela fica 255.255.255.10000000 ou 255.255.255.128. Com um bit apenas emprestado temos duas opções de sub-rede, quando ele for zero e depois quando for 1, por isso temos a primeira sub-rede 192.168.1.0 e a segunda 192.168.1.128.

Outra forma de analisar é que temos um total de 256 endereços contando todos, incluindo a rede e o broadcast, por isso dividindo em dois conjuntos temos que um tem os endereços de 0 a 127 e o segundo de 128 a 255. Sendo que o primeiro endereço é a sub-rede e o último é o broadcast.

Para as classes A e B a análise de emprestar um bit é parecida, porém em octetos diferentes.

Na classe B os hosts iniciam no terceiro octeto, portanto teremos a máscara 255.255.100000000.00000000 = 255.255.128.0. Se utilizarmos a rede 172.16.0.0 como exemplo teremos as sub-redes 172.16.0.0/17 e 172.16.128.0/17, dividimos na realidade 65.536 endereços (incluindo rede e broadcast) em dois conjuntos de 32.768 endereços. Vamos analisar as sub-redes abaixo:

- Primeira sub-rede: 172.16.0.0 com máscara 255.255.128.0
 - Hosts válidos 172.16.0.1 até 172.16.127.254
 - Broadcast 172.16.127.255
- Segunda sub-rede: 172.16.128.0 com máscara 255.255.128.0
 - Hosts válidos 172.16.128.1 até 172.16.255.254
 - Broadcast 172.16.255.255

Para dividir uma classe A em duas sub-redes temos a máscara /9 ou 255.128.0.0, onde estamos dividindo 2^{24} endereços (16.777.216) em dois conjuntos de 8.388.608 endereços, incluindo o endereço de sub-rede e broadcast. Com isso teremos as seguintes sub-redes para a rede privativa 10.0.0.0/8:

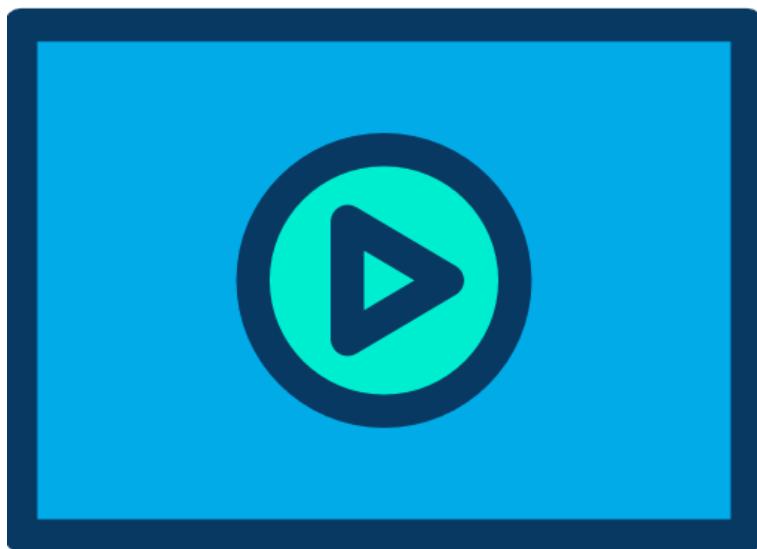
- Primeira sub-rede: 10.0.0.0 com máscara 255.128.0.0
 - Hosts válidos 10.0.0.1 até 10.127.255.254
 - Broadcast 10.127.255.255
- Segunda sub-rede: 10.128.0.0 com máscara 255.128.0.0
 - Hosts válidos 10.128.0.1 até 10.255.255.254
 - Broadcast 10.255.255.255

Portanto, em última análise, fazer sub-rede é adicionar bits "1" nas máscaras padrões das classes A, B e C para permitir a divisão dessas redes em sub-redes.

Seguindo o padrão do binário emprestamos um bit dividimos a rede em duas sub-redes ($2^1=2$), se emprestarmos dois bits dividimos a rede em quatro sub-redes ($2^2=4$), se emprestarmos três bits dividimos a rede em oito sub-redes ($2^3=8$) e assim por diante.

Note que quando falamos em sub-rede a classe continua sendo importante, porque o empréstimo de bits se dá na faixa de hosts, o que é dado pela classe do endereço IP. Na classe A o empréstimo inicia no segundo octeto, já na classe B no terceiro octeto e na classe C no quarto octeto. O mesmo vale para o VLSM.

8.9.3 Exemplo Prático II - Projeto de Sub-redes por Redes



Vamos acompanhar a solução de um problema prático muito comum na vida de um administrador de rede. Suponha que você é o administrador de rede da empresa **Mantra LTDA** e necessita de pelo menos **10 sub-redes** para prover endereçamento para seus grupos de usuários da rede interna. Ele deverá utilizar a rede classe C **192.168.0.0/24** (**255.255.255.0**) para efetuar o endereçamento.

Antes da implementação o gerente da área faz as seguintes indagações sobre esse projeto e o administrador deve respondê-las:

- 1) Quantos bits serão necessários emprestar da parte de host da máscara de rede original para fazer a divisão e obter no mínimo 10 sub-redes?
- 2) Qual a nova máscara de sub-rede?
- 3) Quantos números endereços válidos (hosts) estarão disponíveis em cada sub-rede para endereçar os computadores?
- 4) Qual a faixa de endereços de cada sub-rede (sub-rede, endereços válidos e broadcast).

Lembre-se que criar uma sub-rede nada mais é que “**emprestar bits de host**” (bits zero) para criar novas redes, chamadas sub-redes. Com uma rede Classe C, a qual tem a máscara padrão 255.255.255.0 ou /24, quantos bits precisamos emprestar do **último octeto** para termos 10 sub-redes?

Para responder essa pergunta vamos aos valores de cada binário de um octeto:

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

Para caber 10 sub-redes teremos que emprestar 4 bits da máscara, que dão 16 sub-redes, aí teremos as dez que precisamos mais seis de reserva. Nesse tipo de exercício sempre pegamos a que mais se aproxima do valor pedido.

Agora já podemos responder o item 1, são 4 bits emprestados, assim como o item 2, pois a nova máscara será 255.255.255.**11110000** = 255.255.255.240 (128+64+32+16+0+0+0+0).

Se analisarmos então teremos um total de 16 sub-redes com 14 hosts cada uma, pois temos quatro bits zero sobrando na máscara e o número de hosts é igual a dois elevados ao número de bits zero da máscara menos dois, pois temos que descontar o endereço de rede e de broadcast, por isso temos "**2^4-2 = 16 -2 = 14**" hosts por sub-rede.

A faixa de IPs inicia com a primeira sub-rede chamada "**subnet zero**" ou sub-rede zero e nesse exemplo crescem em múltiplos de 16, veja sequência abaixo iniciando na subnet zero:

0. **192.168.0.0**, sendo que o primeiro IP válido é 192.168.0.1 e o último é 192.168.0.14, já o broadcast é 192.168.0.15. A partir de agora elas variam de 16 em 16.
1. **192.168.0.16** (0+16), sendo que o primeiro IP válido é 192.168.0.17 e o último é 192.168.0.30, já o broadcast é 192.168.1.31.
2. **192.168.0.32** (16+16), sendo que o primeiro IP válido é 192.168.0.33 e o último é 192.168.0.46, já o broadcast é 192.168.1.47.
3. **192.168.0.48** (32+16), sendo que o primeiro IP válido é 192.168.0.49 e o último é 192.168.0.62, já o broadcast é 192.168.1.63.
4. **192.168.0.64** (48+16), sendo que o primeiro IP válido é 192.168.0.65 e o último é 192.168.0.78, já o broadcast é 192.168.1.79.

E assim continua até a última sub-rede (subnet 15) que tem o valor do último octeto igual ao valor da máscara: **192.168.0.240**, endereços válidos de 192.168.0.241 até 192.168.0.254, com broadcast 192.168.0.255. A última sub-rede é chamada de "broadcast subnet", porque todos os bits de sub-rede têm o valor 1: 192.168.0.**1111**0000.

A seguir veremos mais detalhes sobre a subnet zero e a de broadcast.

Note que em binário as sub-redes são a variação dos bits uns da máscara de sub-rede calculada, veja exemplo abaixo:

0. 192.168.0.**0000**0000 → 192.168.0.0
1. 192.168.0.**0001**0000 → 192.168.0.16
2. 192.168.0.**0010**0000 → 192.168.0.32
3. 192.168.0.**0011**0000 → 192.168.0.48
4. 192.168.0.**0100**0000 → 192.168.0.64
5. 192.168.0.**0101**0000 → 192.168.0.80
6. 192.168.0.**0110**0000 → 192.168.0.96
7. 192.168.0.**0111**0000 → 192.168.0.112
8. 192.168.0.**1000**0000 → 192.168.0.128
9. 192.168.0.**1001**0000 → 192.168.0.144
10. 192.168.0.**1010**0000 → 192.168.0.160
11. 192.168.0.**1011**0000 → 192.168.0.176
12. 192.168.0.**1100**0000 → 192.168.0.192
13. 192.168.0.**1101**0000 → 192.168.0.208
14. 192.168.0.**1110**0000 → 192.168.0.224
15. 192.168.0.**1111**0000 → 192.168.0.240

Note uma característica interessante, o que dá o valor de quanto em quanto uma sub-rede varia é o último bit da máscara de sub-rede, por exemplo, na máscara 255.255.255.240 o último octeto é 240, em binário **11110000** e seu último bit vale 16. Isso não é uma coincidência e pode ser utilizado nos cálculos de sub-rede, você verá mais para frente como esse conceito é útil para resolver problemas de sub-rede.

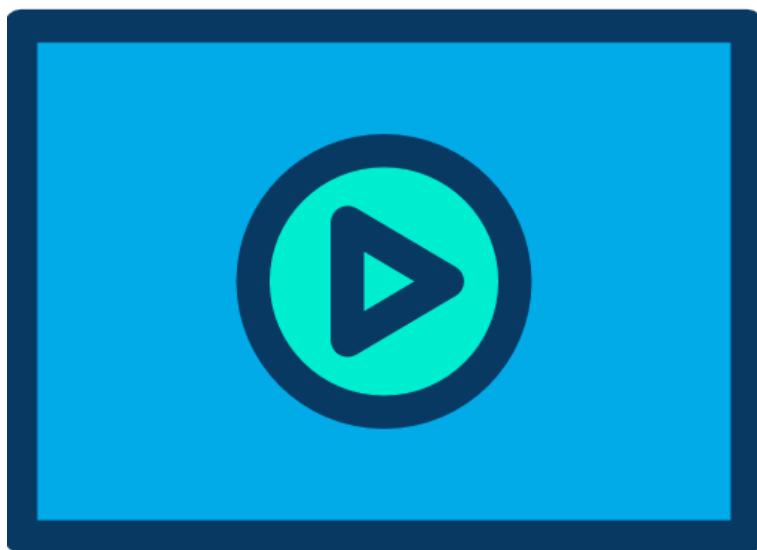
Outro fato importante que podemos tirar dos cálculos realizados até o momento é que o broadcast de uma sub-rede é um valor a menos que a sub-rede seguinte, por exemplo, o broadcast da sub-rede 13 (192.168.0.208/28) é 192.168.0.223, ou seja, o valor da sub-rede 14 192.168.0.224 menos 1. Com isso a faixa de IPs válidos fica fácil de ser encontrada, pois vai de um após a sub-rede "**192.168.0.208 + 1 = 192.168.0.209**" até um a menos que o broadcast "**192.168.0.223 - 1 = 192.168.0.222**".

Esse é outro princípio para facilitar e acelerar os cálculos, achando as sub-redes temos automaticamente os broadcasts, portanto o que está entre o endereço de sub-rede e o broadcast são os endereços válidos.

Resumindo, se você tem a máscara, com o último bit 1 dela você tem também de quanto em quanto as sub-redes variam. Escrevendo as sub-redes uma embaixo da outra, olhando um valor a menos que a próxima você tem o broadcast, por último, tudo que está entre o endereço de sub-rede e o broadcast são os IPs válidos!

Com esse conceito **99,9%** dos exercícios de sub-rede são resolvidos, por isso entenda esse conceito que vamos praticar ao longo desse capítulo!

8.9.4 Entendendo a Subnet-Zero e Broadcast-Subnet



Nos primórdios do endereçamento IP costumava-se não utilizar nem a subnet zero nem a de broadcast, isso devido a implementação nos roteadores, porém atualmente esse tipo de cálculo é uma exceção, pois todos os equipamentos da Cisco utilizam o comando em modo de configuração global "**ip subnet-zero**", o qual ativa no roteador a utilização da subnet zero. A subnet de broadcast já era suportada, porém não utilizada apenas por uma convenção entre os administradores de rede.

Portanto, se inserirmos o comando no roteador “**no ip subnet-zero**” ele não aceitará a configuração de IPs da primeira sub-rede disponível, veja exemplo abaixo:

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#no ip subnet-zero
R1(config)#int f0/0
R1(config-if)#ip address 192.168.0.1 255.255.255.240
Bad mask /28 for address 192.168.0.1
```

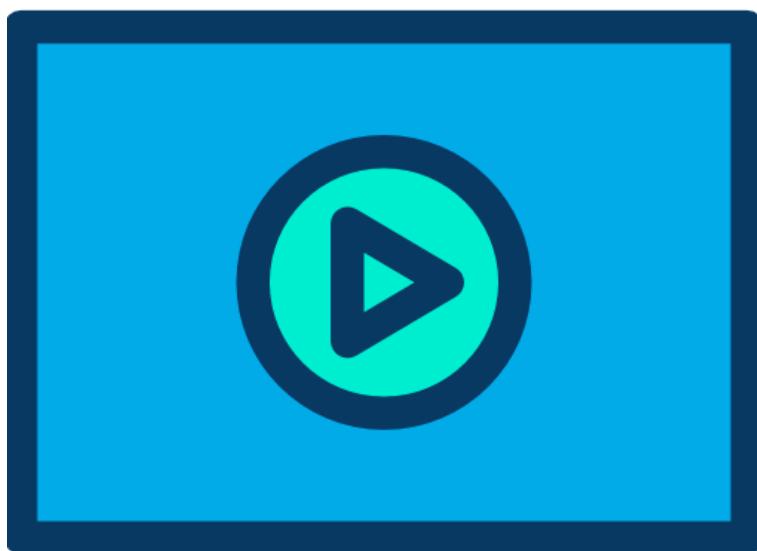
Portanto, com o comando “no ip subnet-zero”, ao tentarmos configurar a interface fast 0/0 com o primeiro IP da subnet zero recebemos uma mensagem de Bad Mask e o comando não foi aceito. Agora note abaixo quando tentamos configurar na sequência um IP da última sub-rede, a de broadcast, note que o roteador irá aceitar sem problemas:

```
R1(config-if)#ip address 192.168.0.254 255.255.255.240
R1(config-if)#do sho ip route
### Saídas omitidas ###

  192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.0.240/28 is directly connected, FastEthernet0/0
L        192.168.0.254/32 is directly connected, FastEthernet0/0
R1(config-if)#

```

É preciso tomar cuidado com esse detalhe da subnet zero ser válida ou não em exercícios de sub-rede, pois podem ser cobradas ambas as filosofias de endereçamento, ou seja, a atual que todas as sub-redes são aceitas ou a antiga onde devíamos desconsiderar a primeira (subnet zero) e a última (broadcast subnet) das nossas contas.

8.9.5 Exemplo Prático III - Projeto de Sub-redes por Hosts

Nesse segundo exemplo prático o administrador de redes recebeu o endereço de classe B 172.16.0.0/16 (255.255.0.0) e precisa descobrir a máscara de sub-rede que suporte no mínimo **1000 endereços válidos para hosts**. Mais uma vez o gerente da área faz as seguintes indagações sobre esse projeto:

1. Quantos bits serão necessários emprestar para fazer a divisão e obter pelo menos 1000 hosts?
2. Qual a nova máscara de sub-rede?
3. Quantas sub-redes estarão disponíveis para esse número de hosts?
4. Listar a faixa de endereços para as cinco primeiras sub-redes iniciando pela sub-rede zero.

No exemplo prático 2, onde fizemos um projeto pela quantidade de sub-redes tivemos que pensar em quantos bits uns teríamos que emprestar para suportar 10 sub-redes. Agora nesse exemplo precisamos projetar nossa máscara utilizando a informação quantitativa de hosts.

Nesse tipo de exercício temos que procurar o número de bits zero temos que deixar na máscara para suportar a quantidade de hosts necessários! Alguns valores em binário são importantes saber, tais como os valores dos oito bits de um octeto e valores como 2^8 , 2^9 e 2^{10} . É simples, já sabemos que 2^7 é 128, portanto elevado a 8 será 256 (128×2), 2^9 será 512 (256×2) e 2^{10} será 1024 (512×2). Portanto, para termos 1000 hosts precisamos deixar 10 bits na máscara de sub-rede.

A máscara de classe B tem 16 bits uns e 16 bits zero, portanto temos 255.255.0.0 ou 11111111.11111111.00000000.00000000, se temos que deixar 10 bits zero basta deixar da esquerda para a direita e depois completar com bits uns! Teremos então 11111111.11111111.11111111.00.00000000 que dá a máscara /22, ou seja, emprestamos 6 bits e deixamos 10 dos dezesseis para os hosts.

As questões 1 e 2 já podem ser respondidas, teremos que emprestar 6 bits uns e teremos a máscara 255.255.252.0 ($11111100 = 128 + 64 + 32 + 16 + 8 = 252$).

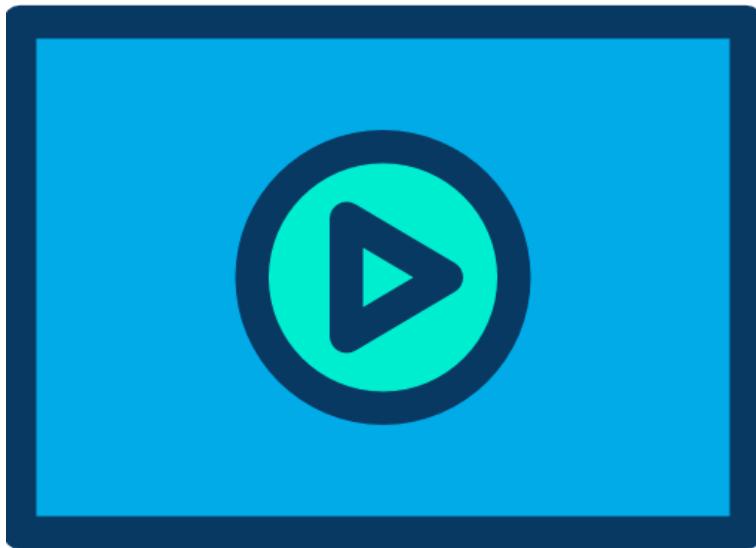
A questão 3 sobre quantas sub-redes teremos se resolve elevando dois ao número de bits emprestados, ou seja, $2^6=64$ sub-redes com até $2^{10-2}=1024-2=1022$ hosts por sub-rede.

A questão 4 confunde muita gente, pois ficamos muito acostumados a calcular sub-redes para classes C, ou seja, de /25 para cima. Para máscaras /23 ou menores temos que tomar cuidado, vamos à resolução. Primeiro vamos descobrir a variação, que é o valor do último bit 1 da máscara: $255.255.111111100.00000000 = 4$, portanto as sub-redes variam de 4 em 4 a partir do terceiro octeto! Veja abaixo como fica:

0. **172.16.0.0** → broadcast 172.16.3.255 e IPs válidos de 172.16.0.1 até 172.16.3.254
1. **172.16.4.0** → broadcast 172.16.7.255 e IPs válidos de 172.16.4.1 até 172.16.7.254
2. **172.16.8.0** → broadcast 172.16.11.255 e IPs válidos de 172.16.8.1 até 172.16.11.254
3. **172.16.12.0** → broadcast 172.16.15.255 e IPs válidos de 172.16.12.1 até 172.16.15.254
4. **172.16.16.0** → broadcast 172.16.19.255 e IPs válidos de 172.16.16.1 até 172.16.19.254
5. **172.16.20.0** (inserida somente para poder encontrar o broadcast)

A sequência de resolução é: escrever as sub-redes, encontrar o broadcast e depois a faixa de IPs válidos.

8.9.6 Análise de Endereços IP com a Metodologia DlteC



Podemos também utilizar a metodologia de análise realizada nos exercícios de projeto para resolver problemas onde envolvem a análise de endereços IP e máscara.

Vamos fazer o mesmo exemplo da análise realizada com o método tradicional com o endereço 192.168.10.170 e máscara 255.255.255.240 ou /28. Vamos descobrir as seguintes informações:

- 1) Qual a sub-rede que o IP pertence?
- 2) Qual o endereço de broadcast da sub-rede?
- 3) Qual a faixa de endereços válidos?

Vamos à resolução!

Passo 1 - Pelo nosso método tudo começa verificando a variação das sub-redes com a máscara /28, que é o valor do último bit "1" da máscara em decimal. A máscara /28 em binário é 11111111.11111111.11111111.11110000, portanto o bit vale 16 em decimal, o que nos leva que as sub-redes variam de 16 em 16.

Passo 2 – Agora escreva as sub-redes uma embaixo da outra até que o endereço a ser analisado (**192.168.10.170**) esteja entre duas das sub-redes escritas (é só somar 16 no último octeto):

0. 192.168.10.0
1. 192.168.10.16
2. 192.168.10.32
3. 192.168.10.48
4. 192.168.10.64
5. 192.168.10.80
6. 192.168.10.96
7. 192.168.10.112
8. 192.168.10.128
9. 192.168.10.144
- 10.192.168.10.160**
- 11.192.168.10.176**

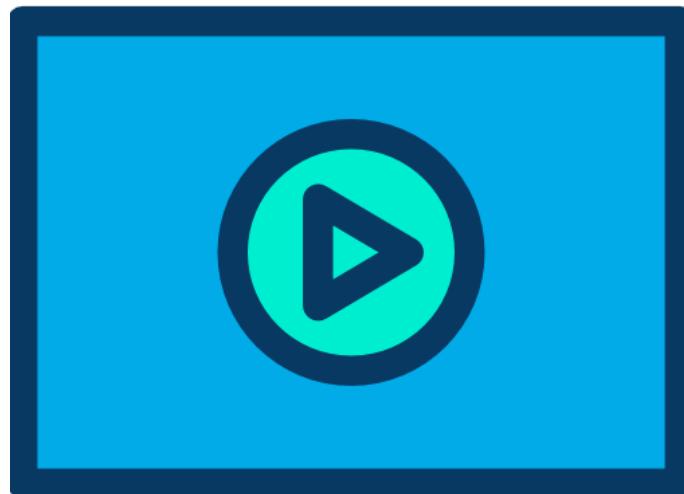
Achamos, o IP 192.168.10.170 pertence à sub-rede 192.168.10.160, agora fica fácil, porque o broadcast é um valor antes da próxima sub-rede (192.168.10.176) e é 192.168.10.175, por isso os IPs válidos estão entre a sub-rede e o broadcast, por isso vão de 192.168.10.161 até 192.168.10.174.

Se o exercício pedisse para reconhecer broadcasts entre redes que iniciam nas redes 192.168.10.0 com a máscara /28 fica simples, porque são os IPs ímpares antes das sub-redes escritas.

Se a pergunta fosse reconhecer endereços de sub-rede seria mais fácil ainda, assim como reconhecer IPs válidos, pois é só escrever as sub-redes como fizemos nesse exercício, anotar também os broadcasts e tudo que não for sub-rede ou broadcast é IP válido!

Nas vídeo aulas do capítulo vamos explorar esses conceitos e ensinar a utilizar essa metodologia que agiliza as contas, pois para exames de certificação a velocidade e automação na resolução de exercícios são muito importantes, pois um dos fatores que mais reprovam é a administração do tempo de prova.

8.9.7 Máximo de Bits de Host Emprestados

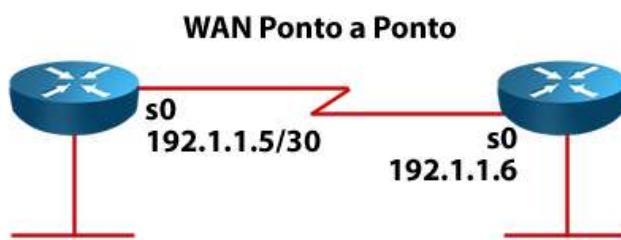


Nesse tópico vamos procurar responder até quantos bits podemos emprestar para criar sub-redes. Para isso lembre-se que uma rede IP tem:

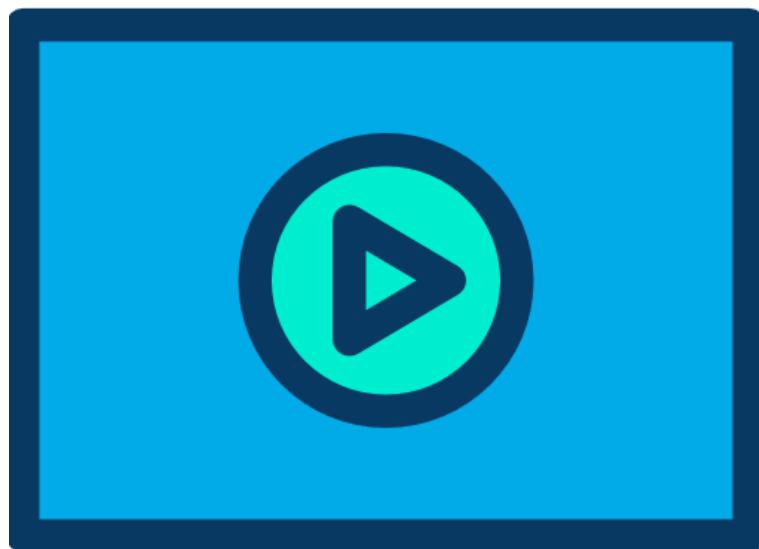
- 1) Endereço de rede
- 2) Hosts válidos
- 3) Endereço de broadcast

Por isso, teoricamente precisamos no mínimo de 3 endereços em uma sub-rede para que ela tenha hosts válidos. Não existe máscara com 3 endereços, lembre-se que as máscaras sempre são valores pares, por isso a última máscara válida para sub-redes é a /30 ou 255.255.255.252, pois com ela temos 4 endereços totais, sendo que o primeiro será a sub-rede, dois endereços de hosts e um broadcast.

Essa máscara é utilizada em redes WAN ponto a ponto, onde precisamos de apenas dois endereços, um para cada ponta do link. Veja figura a seguir, onde temos um link ponto a ponto configurado com IPs da rede 192.168.1.4/30.



Essa recomendação vale para todas as Classes, apesar de atualmente existir a RFC 3021 (Using 31-Bit Prefixes on IPv4 Point-to-Point Links), normalmente no CCNA essas máscaras não são utilizadas, sendo o máximo permitido até a /30.

8.9.8 Resumo das Máscaras de Sub-rede por Classe

As máscaras de sub-rede possíveis por classe tem um número limitado, por exemplo, como a classe A tem por padrão um comprimento de oito bits (/8), suas sub-redes iniciam com nove bits (/9) e vão até /32 (/9, /10, /11, ... , /30, /31 e /32).

Para a classe B, fazendo a mesma análise, temos de /17 até /32, pois o padrão é /16. Já para a classe C, como o padrão é /24 temos de /25 até /32. Lembrando que a /31 depende do suporte à RFC 3021 e a /32 representa um host único, chamada de máscara de host.

Veja na tabela abaixo todas as máscaras possíveis para a classe A.

Classe A (1-126) - Padrão 255.0.0.0 com prefixo /8				
Bits emprestados	Máscara	Prefixo	Sub-redes (2^n)	Hosts ($2^n - 2$)
1	255.128.0.0	/9	2	8388606
2	225.192.0.0	/10	4	4194302
3	225.224.0.0	/11	8	2097150
4	225.240.0.0	/12	16	1048574
5	225.248.0.0	/13	32	524286
6	225.252.0.0	/14	64	262142
7	225.254.0.0	/15	128	131070
8	255.255.0.0	/16	256	65534
9	255.255.128.0	/17	512	32766
10	255.255.192.0	/18	1024	16382
11	255.255.224.0	/19	2048	8190
12	255.255.240.0	/20	4096	4094
13	255.255.248.0	/21	8192	2046
14	255.255.252.0	/22	16384	1022
15	255.255.254.0	/23	32768	510
16	255.255.255.0	/24	65536	254
17	255.255.255.128	/25	131072	126
18	255.255.255.192	/26	262144	62
19	255.255.255.224	/27	524288	30
20	255.255.255.240	/28	1048576	14
21	255.255.255.248	/29	2097152	6
22	255.255.255.252	/30	4194304	2
		n= bits 1 emprestados		n= bits 0

Portanto, podemos iniciar com a máscara /9 temos um bit emprestado para sub-rede, dividindo a rede classe A em duas sub-redes com 8.388.606 hosts cada uma, e emprestar até 22 bits para formar uma máscara /30 com 4.194.304 sub-redes de apenas dois hosts cada uma, utilizados para endereçar redes WAN ponto a ponto.

Para a classe B o empréstimo de bits inicia no terceiro octeto, pois o primeiro e segundo bytes são fixos para rede. Veja a tabela com todas as sub-redes possíveis para endereços classe B abaixo.

Classe B (128-191) - Padrão 255.255.0.0 com prefixo /16				
Bits emprestados	Máscara	Prefixo	Sub-redes (2^n)	Hosts ($2^n - 2$)
1	255.255.128.0	/17	2	32766
2	255.255.192.0	/18	4	16382
3	255.255.224.0	/19	8	8190
4	255.255.240.0	/20	16	4094
5	255.255.248.0	/21	32	2046
6	255.255.252.0	/22	64	1022
7	255.255.254.0	/23	128	510
8	255.255.255.0	/24	256	254
9	255.255.255.128	/25	512	126
10	255.255.255.192	/26	1024	62
11	255.255.255.224	/27	2048	30
12	255.255.255.240	/28	4096	14
13	255.255.255.248	/29	8192	6
14	255.255.255.252	/30	16384	2

Fazendo a mesma análise que realizamos anteriormente para a classe A, para a classe B podemos iniciar com a máscara /17 (um bit emprestado para sub-rede), dividindo a rede em questão em duas sub-redes com 32.766 hosts cada uma, e emprestar até 14 bits para formar uma máscara /30 com 16.384 sub-redes de apenas dois hosts cada uma, utilizadas também para endereçar redes WAN ponto a ponto.

Para a classe C temos um escopo menor de empréstimo, pois ela tem três octetos de rede e apenas um byte de host, por isso temos apenas oito bits para criar sub-redes. Veja a tabela da classe C abaixo.

Classe C (192-223) - Padrão 255.255.255.0 com prefixo /24				
Bits emprestados	Máscara	Prefixo	Sub-redes (2^n)	Hosts ($2^n - 2$)
1	255.255.255.128	/25	2	126
2	255.255.255.192	/26	4	62
3	255.255.255.224	/27	8	30
4	255.255.255.240	/28	16	14
5	255.255.255.248	/29	32	6
6	255.255.255.252	/30	64	2

Para a classe C podemos iniciar com a máscara /25 (um bit emprestado para sub-rede), dividindo a rede em questão em duas sub-redes com 126 hosts cada uma, e emprestar até 6 bits para formar uma máscara /30 com 64 sub-redes de apenas dois hosts cada uma, utilizadas também para endereçar redes ponto a ponto.

Se você prestar bastante atenção perceberá que os octetos das máscaras, não importando a classe podem ser apenas:

- o 0 → 00000000
- o 128 → 10000000
- o 192 → 11000000
- o 224 → 11110000
- o 240 → 11111000
- o 248 → 11111100
- o 252 → 11111110
- o 254 → 11111110
- o 255 → 11111111

A variação das sub-redes é bem conhecida e apenas nos valores conforme abaixo do último octeto da máscara (último bit 1 marcado na lista de valores de octeto anterior):

- o 255 → 1 em 1 (2^0)
- o 254 → 2 em 2 (2^1)
- o 252 → 4 em 4 (2^2)
- o 248 → 8 em 8 (2^3)
- o 240 → 16 em 16 (2^4)
- o 224 → 32 em 32 (2^5)
- o 192 → 64 em 64 (2^6)
- o 128 → 128 em 128 (2^7)

Portanto, se você anotar esses valores antes de iniciar a prova na folha de rascunho também ajudará bastante para agilizar as conversões decimal/binário para encontrar a variação dos bits e resolver questões de sub-rede, VLSM e CIDR.

Maioria dos roteadores Cisco com IOS acima da versão 12 aceitam a máscara /31 para endereçar interfaces WAN ponto a ponto, gerando mais economia de endereços que uma rede /30, assim como a configuração de endereços /32 utilizados para configurar interfaces de loopback nos roteadores, pois as loopbacks não formam redes e sim são endereços lógicos locais dos dispositivos. Veja os exemplos abaixo, onde as saídas referentes a rede /31 estão destacadas em amarelo e da /32 em verde.

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int f0/0
R1(config-if)#ip add 192.118.1.1 255.255.255.254
R1(config-if)#int loop 0
R1(config-if)#ip add 192.168.1.1 255.255.255.255
R1(config-if)#
*Jul 16 12:21:30.775: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0,
changed state to up
R1(config-if)#do sho ip rou
### Saídas omitidas ###

      192.118.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.118.1.0/31 is directly connected, FastEthernet0/0
L        192.118.1.1/32 is directly connected, FastEthernet0/0
      192.168.1.0/32 is subnetted, 1 subnets
C        192.168.1.1 is directly connected, Loopback0
R1(config-if)#

```

As redes /31 no CCNA não são exploradas no material oficial por terem alguns problemas em certos tipos de interfaces, por isso nas respostas de questão de prova normalmente redes ponto a ponto utilizam máscaras /30.

8.9.9 Dicas Finais sobre Exercícios de Sub-rede para o CCNA

No CCNA ou qualquer outra prova que cobre a divisão de uma rede em sub-redes, você poderá encontrar alguns modelos de questões. Vamos a alguns exemplos comuns.

Dado um IP e máscara perguntar:

- o Qual a sua sub-rede
- o Qual a porção de rede ou de host
- o Qual a faixa de IPs válidos dessa sub-rede
- o Qual o broadcast da sub-rede em questão
- o Etc.

Nesse caso os conceitos estudados anteriormente resolvem o problema. Por exemplo, dado o IP 172.16.33.45 com a máscara 255.255.255.248 vamos obter todas as informações possíveis sobre essa sub-rede.

A primeira coisa a fazer é descobrir a sub-rede com um AND lógico:

172. 16 . 33. 45
AND 255.255.255.248
172. 16. 33. ?

obs: lembra-se que no AND qualquer bit com 0 dá 0 e 1 com 1 dá 1.

45 = 00101101
AND 248 = 11111000
00101000 = 40

Portanto sub-rede 172.16.33.40

Para achar a faixa de IPs é só descobrir a próxima sub-rede, analisando a máscara sabemos que a variação será de 8 em 8, portanto a próxima sub-rede será a 172.16.33.48. Com essa informação sabemos que:

- A faixa total de IPs será de 172.16.33.40 a 172.16.33.47.
- Os IPs válidos serão de 172.16.33.41 a 172.16.33.46.
- O broadcast será o 172.16.33.47.

Um “macete” muito útil para quando você tem uma rede de qualquer classe com uma máscara maior que /24 (255.255.255.xxx) e precisa identificar em uma lista de IPs quem é endereço de rede, IPs válidos ou broadcast é o seguinte:

1. Primeiro com a máscara de sub-rede encontre a variação (valor em decimal do último bit 1 da máscara de sub-rede).
2. Com esse valor, divida o último octeto do IP dado no exercício pela variação, os que resultarem em zero na divisão, ou seja, forem múltiplos da variação são endereços de sub-rede.
3. Se você somar 1 e dividir pela variação e resultar em zero, ou seja, der múltiplo da variação é um broadcast.
4. Os demais são endereços válidos.

Outro modelo de questão são os de projeto, onde dado um número de hosts ou de sub-redes você terá que achar qual a máscara que melhor se adapta ao projeto. Nesse caso existem dois tipos de análise para resolução:

1. Quando o projeto é pelo **número de sub-redes** você deve pensar em **quantos bits “emprestar”**, ou seja, quantos bits zero da máscara original você terá que transformar em bits 1 para fazer a sub-rede. Aqui tome cuidado com que fórmula utilizar, pois como já estudamos temos duas abordagens, com ou sem a subnet zero.
2. Quando o projeto é pelo **número de hosts** ou computadores que você terá na rede pense em **quantos bits zero você terá que deixar na máscara** de sub-rede. Aqui a fórmula não muda, sempre será $2^n - 2$, onde o n são os bits zero que você terá na máscara para representar os hosts.

Para resolver esse problema basta utilizar a tabela de potências de 2:

2⁷	2⁶	2⁵	2⁴	2³	2²	2¹	2⁰
128	64	32	16	8	4	2	1

Por exemplo, o exercício fornece um IP de classe A e quer que você a divida em 30 sub-redes. Basta você procurar na tabela o que se encaixa com o 30 e a potência de 2 desse número será o número de bits que você terá que emprestar. Nesse exemplo o melhor é o 2^5 que dá 32, portanto vamos emprestar 5 bits. A máscara de sub-rede será 255.248.0.0, lembre-se que a máscara padrão da classe A é 255.0.0.0.

Cuidado nos exercícios que envolvem sub-redes para certificar **se você deve ou não desconsiderar a sub-rede zero e a broadcast**. Se não falar nada valem todas as sub-redes.

Agora vamos relembrar o projeto a partir dos hosts. Por exemplo, você tem um IP de classe C, máscara padrão 255.255.255.0, e precisa ter 12 hosts por sub-rede. Agora a fórmula é $2^n - 2$, onde o n são os bits zero.

Quanto bit zero precisará deixar na máscara? Analisando a tabelinha são 4, pois $2^4-2=14$, cabem os 12 micros e temos uma sobra de 2. Portanto a máscara será 255.255.255.240 (11111111.11111111.11111111.11110000).

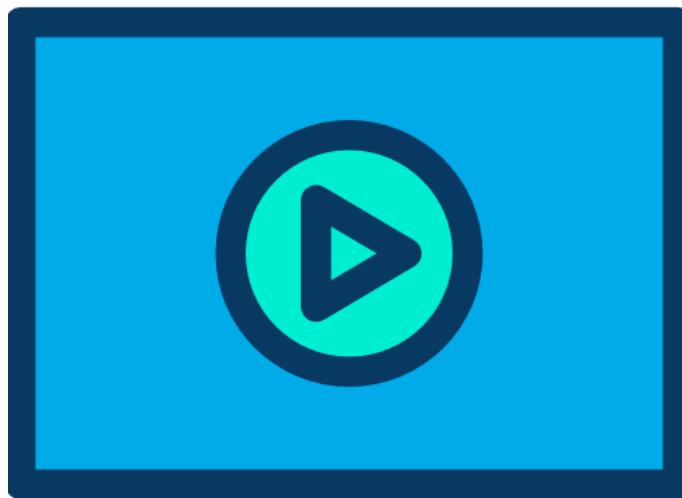
Estude bem esses conceitos, tire dúvidas antes de prosseguir se necessário e no final não se esqueça de fazer as listas de exercícios extras de sub-rede que estão disponíveis na área do aluno. Os gabaritos estão comentados para que vocês possam entender melhor os modelos de questão possíveis e como resolvê-los.

Veja também na área do aluno a “**Folha de rascunho para cálculo de Sub-redes**”, documento em PDF com um “**resumão**” para facilitar na hora das contas relacionadas ao IP. Uma boa dica é decorar o que está sugerido nessa folha de rascunho para anotar no quadro de anotações dado pelas entidades certificadoras da Pearson VUE antes de iniciar a prova do CCNA, isso irá acelerar e facilitar os cálculos de IP e sub-rede.

Nas vídeo aulas ensinaremos a utilizar a folha de rascunho!

Esse capítulo é muito importante para o CCNA e será cobrado isoladamente e em conjunto com outras questões, por exemplo, você terá que calcular uma sub-rede para determinar que IP configurar em uma interface de um roteador, por isso pratique bastante!

8.10 VLSM, CIDR e Sumarização de Rotas



Originalmente o uso de sub-redes era destinado à subdivisão de uma rede baseada em classes em uma série de sub-redes de **mesmo tamanho**, onde a mesma máscara de sub-rede era compartilhada por todos os segmentos.

Por exemplo, a subdivisão de 4-bits de hosts de uma rede classe B produzirá 16 sub-redes do mesmo tamanho, cada uma com 4094 endereços IP.

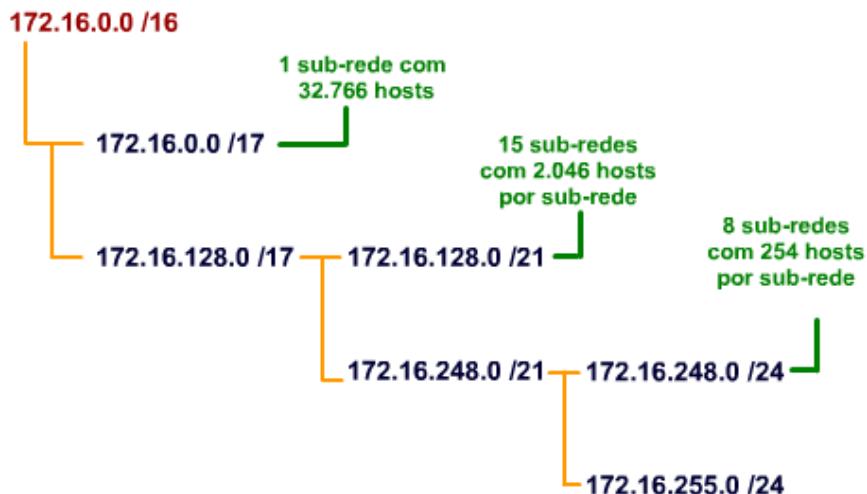
Mas e se um departamento necessitar de apenas 30 endereços IP? Será que esse desperdício de endereçamento pode ser suportado pela organização?

As sub-redes de tamanhos diferentes (**VLSM - Variable Length Subnet Masks**) podem resolver esse problema e melhorar ainda mais a alocação dos endereços IP em redes baseadas em classes.

Com o VLSM um administrador pode criar sub-redes de tamanho variável e que supram as necessidades de cada departamento de sua organização.

Podemos chamar essa técnica de **sub-rede da sub-rede**, pois o VLSM quebra sub-redes em tamanhos menores.

Um exemplo de subdivisão com máscara de tamanho variável da rede 172.16.0.0/16 na figura a seguir.



Vamos entender a divisão realizada na figura anterior.

Tudo começou pegando a rede classe B privativa (RFC 1918) 172.16.0.0/16, depois o administrador quebrou ela em duas sub-redes com uma máscara /17 (emprestado um bit), com isso temos uma sub-rede disponibilizada para endereçar mais de 32 mil hosts e outra que será novamente quebrada em sub-redes.

A segunda sub-rede /17 foi quebrada com a máscara /21, resultando em 16 sub-redes, pois $21-17=4$ e temos 4 bits de sub-rede ($2^4=16$). Desses 16 sub-redes, 15 foram reservadas para segmentos com 2.046 hosts e a última será novamente subdividida.

Para a última sub-rede 172.16.248.0/21 o administrador quebrou utilizando máscaras /24, portanto temos também 3 bits de sub-rede ($24-21=3$), gerando 8 sub-redes /24 com 254 hosts por sub-rede.

Essa subdivisão poderia continuar, por exemplo, poderíamos pegar a sub-rede 172.16.255.0 e quebrá-la em sub-redes /30, criando 64 sub-redes para endereçamento de links ponto a ponto.

Uma dica importante é que na prática costuma-se fazer a divisão das redes com maior número de endereços para a menor, assim você consegue aproveitar melhor a faixa de endereços disponíveis com a rede escolhida para VLSM.

Vamos reforçar o uso da máscara de sub-rede /30 (255.255.255.252) utilizada principalmente para endereçamento de interfaces serias ponto a ponto, pois elas fornecem apenas 2 endereços IP válidos, o suficiente para uma interface serial ponto a ponto, veja figura a seguir.

Com a máscara /30 apenas dois endereços de host são disponíveis.



A sub-rede será 201.100.20.4/30 e os endereços de host disponíveis serão .5 e .6.

Outra vantagem que um projeto com VLSM proporciona é a possibilidade de **hierarquização** da rede e **agregação de rotas** (route summarization ou route aggregation).

Agregar ou sumarizar rotas é representar um conjunto de sub-redes com uma máscara de menor comprimento.

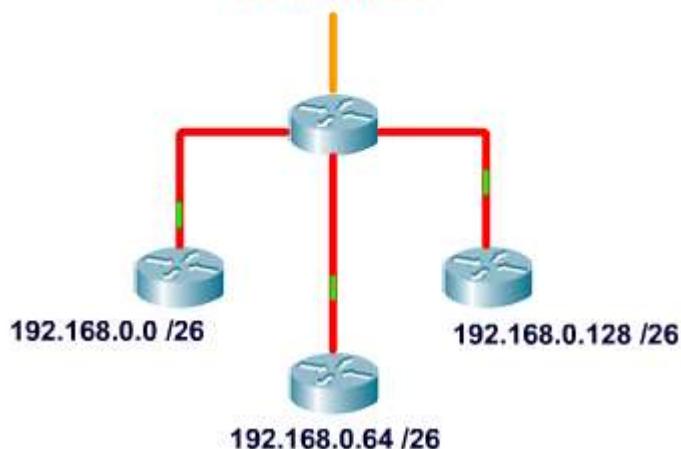
Por exemplo, suponha que abaixo de um roteador você tenha as sub-redes 192.168.0.0/26, 192.168.0.64/26 e 192.168.0.128/26. Você terá que anunciar três rotas para o roteador vizinho, porém você pode agregar essas rotas e representá-las como 192.168.0.0/24, veja figura abaixo.

Eu conheço as rotas para as redes:

192.168.0.0 /26
192.168.0.64 /26
192.168.0.128 /26

E posso anunciar-las somente como:

192.168.0.0 /24



Dentro da rede 192.168.0.0/24 não estão contidos todos os endereços IP das três redes apresentadas? Faça essa conta e confirme.

A única restrição do uso do VLSM é com relação aos **protocolos de roteamento**, pois alguns protocolos como RIP versão 1 e IGRP não suportam esse tipo de endereçamento, porém o RIP versão 2, EIGRP, OSPFv2, IS-IS e BGP suportam tanto o VLSM como o CIDR.

Aproveitando o conceito de máscara de sub-rede com comprimento variável, vamos entender também o que é **Classless Inter-domain Routing**.

O CIDR (**Classless Inter-Domain Routing**) foi introduzido em 1993 como um refinamento para a forma como o tráfego era conduzido pelas redes IP. Permitindo flexibilidade acrescida quando dividindo margens de endereços IP em redes separadas, promoveu assim um uso mais eficiente para os endereços IP cada vez mais escassos.

O CIDR está definido no **RFC 1519**.

O CIDR usa máscaras de comprimento variável, o VLSM (de Variable Length Subnet Masks), para alocar endereços IP em sub-redes de acordo com as necessidades individuais e não nas regras de uso generalizado em toda a rede a partir de classes pré-definidas.

Assim a divisão de rede/host pode ocorrer em qualquer fronteira de bits no endereço.

Porque as distinções de classes normais são ignoradas, o novo sistema foi chamado de **roteamento sem classes** ou **classless**.

Isto levou a que o sistema original passasse a ser chamado de roteamento de classes ou **classful**.

Basicamente com o CIDR **deixamos de utilizar as classes** e passamos a utilizar um prefixo para identificar as redes e um comprimento de prefixo para definir a faixa de IPs contidas nessas redes, sem levar em consideração as classes.

Por exemplo, um provedor que tem as redes IP classe C 200.200.0.0 até 200.200.255.0 poderá representar com o CIDR apenas o bloco ou prefixo **200.200.0.0** com o comprimento **/16** (16 bits de rede ou 255.255.0.0).

Isso possibilita o anúncio de apenas uma rede que representa um bloco de 256 redes classe C, princípio básico de uso da summarização!

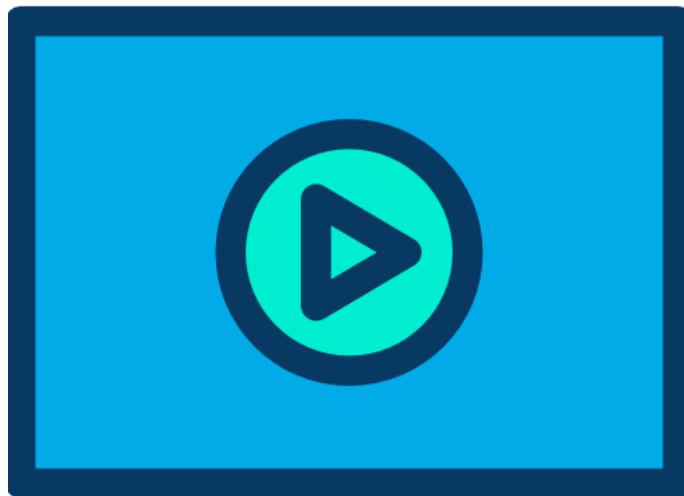
Vamos analisar a faixa de IPs do bloco CIDR do exemplo acima 200.200.0.0/16.

Um prefixo com comprimento /16 é a máscara 255.255.0.0, portanto os hosts estão no terceiro e quarto bytes do endereço IP, temos a seguinte faixa de endereços:

- Rede 200.200.0.0 /16
- Broadcast 200.200.255.255
- IPs válidos: 200.200.0.1 até 200.200.255.254

Então com CIDR posso ter uma classe C com máscara igual a class B? Sim, pois aqui simplesmente ignoramos classes!

Note que a análise de IPs ou cálculos referentes a VLSM e redes classless podem ser realizados com o que aprendemos para sub-redes, por isso que frisamos ao longo do capítulo que aprendendo sub-redes com nosso método você já aprende "de quebra" VLSM e CIDR!

8.11 Configurando Endereços IPv4 em Interfaces de Roteadores e Switches

A configuração básica de uma interface IP, inserindo um endereço estático (manual) utilizando o comando “**ip address**” dentro do modo de configuração global. Veja exemplo abaixo:

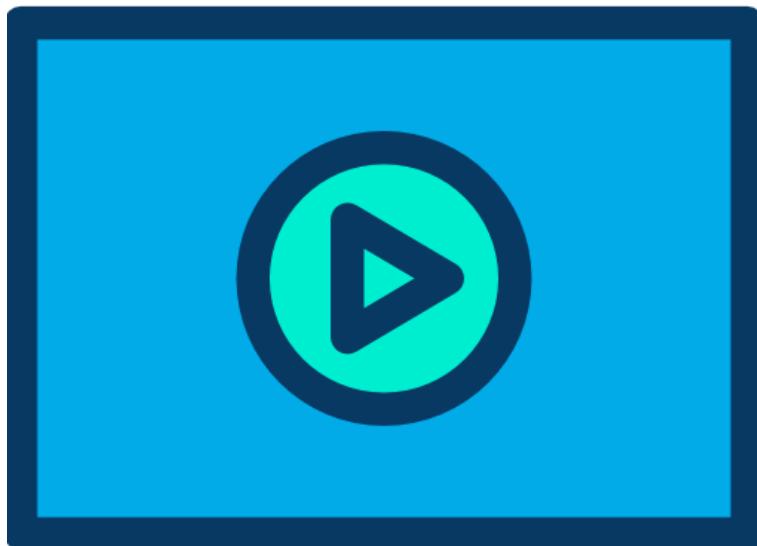
```
R1(config)#interface fast 0/0
R1(config-if)#ip address 172.17.0.1 255.255.255.0
R1(config-if)#description LAN-1
R1(config-if)#no shut
```

Existem outras opções para configurar o IP em uma interface de roteadores e switches Cisco, através do DHCP ou então inserindo endereços IP secundários, o que possibilita que uma interface responda para duas ou mais redes diferentes. Veja a saída do comando **ip address** com o help para ver as opções possíveis em um roteador abaixo:

```
R1(config-if)#ip address ?
  A.B.C.D  IP address
  dhcp      IP Address negotiated via DHCP
  pool      IP Address autoconfigured from a local DHCP pool
R1(config-if)#ip address dhcp
```

Portanto com o comando “**ip address dhcp**” o roteador enviará uma solicitação ao serviço de DHCP local para fazer a atribuição dinâmica de IP na interface, porém não é muito utilizada porque os dispositivos de redes normalmente precisam ter um endereço bem conhecido.

Por exemplo, imagine que o roteador R1 é seu gateway e devido a algum problema no DHCP ele muda de endereço. O que vai ocorrer é que todos os hosts que tinham o IP antigo do roteador não conseguiram mais sair para a Internet através desse gateway.

8.11.1 Endereços IPs Secundários

Cada interface IP possui um endereço principal e para inserir mais endereços na mesma interface você precisa utilizar o comando "secondary" no final da declaração da configuração de IP, veja exemplo abaixo:

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int f0/0
R1(config-if)#ip address 172.16.0.1 255.255.255.0
R1(config-if)#ip address 172.17.0.1 255.255.255.0 secondary
R1(config-if)#ip address 172.18.0.1 255.255.255.0 secondary
R1(config-if)#do show run interface f0/0
Building configuration...

Current configuration : 187 bytes
!
interface FastEthernet0/0
  ip address 172.17.0.1 255.255.255.0 secondary
  ip address 172.18.0.1 255.255.255.0 secondary
  ip address 172.16.0.1 255.255.255.0
  shutdown
  duplex half
end

R1(config-if) #
```

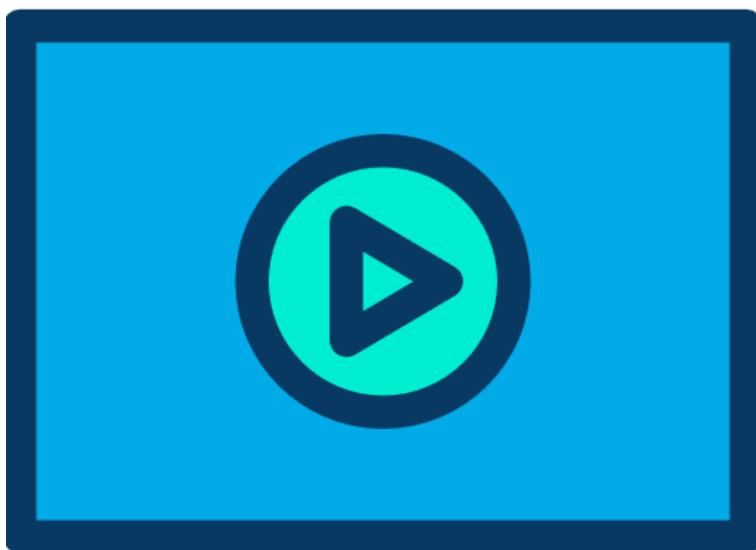
No exemplo acima configuramos o endereço 172.16.0.1 como principal e 172.17.0.1 e 172.18.0.1 como secundários, podemos ter diversos IPs secundários configurados, porém não é muito usual atualmente.

Existe uma desvantagem do uso desse tipo de solução com todos os hosts em uma mesma VLAN e separados por sub-redes diferentes, pois assim você não segregá os broadcasts enviados na rede e também insere mais saltos para que dois hosts em uma mesma rede física se comuniquem, pois eles estão compartilhando o mesmo meio, poderiam estar na mesma sub-rede e simplesmente trocar informações entre si sem precisar enviar para o roteador padrão fazer o encaminhamento entre as sub-redes.

Com switches suportando VLANs é mais comum termos cada rede ou sub-rede IP segregada nos switches em diferentes VLANs, assim realmente segregamos o domínio de broadcast.

Na prática redes secundárias podem servir como medida paliativa para quando uma rede cresce demais e é preciso mudar a máscara de sub-rede. Para evitar transtornos aos usuários, pode-se fazer uma configuração da rede secundária para que os novos computadores tenham acesso à rede até que o projeto de integração completa da rede possa ser configurado nos roteadores.

8.11.2Configurando Endereços IP em Switches



Em switches temos duas situações:

1. **Switches L2:** eles têm o IP de gerenciamento dentro da Interface VLAN 1 por padrão, isso pode e é recomendado ser alterado. As interfaces do tipo VLAN são Switched Virtual Interfaces (SVI), porém em switches L2 apenas uma pode ficar ativa.
2. **Switches L3:** suportam interfaces SVI (Switched Virtual Interface) ou Portas Roteadas (portas L2 configuradas como portas de roteadores com o comando "no switchport").

Os switches camada 2 não suportam endereço IP em suas interfaces físicas (fast ou giga), por isso precisamos configurar o IP em uma "interface vlan", sendo que por padrão essa configuração é feita na "interface vlan 1".

A interface VLAN 1, que é a interface de gerenciamento padrão dos switches L2, é também uma SVI. Nesse tipo de switch apenas uma VLAN de gerenciamento fica ativa e as portas L2 não podem ser configuradas como portas roteadas.

Essa configuração em switches L2 mantém sempre a última interface VLAN ativa, ao dar "no shut" em uma nova interface VLAN, a anterior é desativada automaticamente.

Veja exemplo abaixo:

```
SW-DlteC-L2>en
Password:
SW-DlteC-L2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-DlteC-L2(config)#interface vlan 1
SW-DlteC-L2(config-if)#ip address ?
  A.B.C.D  IP address
  dhcp      IP Address negotiated via DHCP
  pool      IP Address autoconfigured from a local DHCP pool
SW-DlteC-L2(config-if)#ip address 192.168.1.5 255.255.255.0
SW-DlteC-L2(config-if)#no shutdown
```

Perceba acima que a configuração é a mesma do roteador, inclusive permite a configuração de IPs secundários, conforme saída abaixo:

```
SW-DlteC-L2(config-if)#ip address 192.168.1.5 255.255.255.0 ?
  secondary  Make this IP address a secondary address
<cr>
SW-DlteC-L2(config-if)#ip address 192.168.1.5 255.255.255.0 secondary
```

Para que um switch L2 possa trocar informações com outras redes será necessário configurar também o Gateway ou Roteador Padrão dele com o comando “ip default-gateway *ip-do-gateway*”.

```
SW-DlteC-L2(config)#ip default-gateway 192.168.1.1
```

O IP do gateway deve ser o endereço da interface do roteador ou da SVI do switch L3 a qual a VLAN de gerenciamento está conectada.

Em switches L3 todas as SVIs ou interfaces VLAN criadas ficam ativas e têm capacidade de roteamento. Não será necessário utilizar o comando “ip default-gateway” como nos switches L2, pois os switches L3 montam suas tabelas de roteamento.

Veja exemplo abaixo onde vamos criar as interfaces para rotear as VLANs 1, 10 e 20 em um switch L3 (com roteamento IPv4 ativado pelo comando “ip routing”).

```
SW-L3-DlteC(config)#interface vlan 1
SW-L3-DlteC(config-if)#ip address 192.168.1.1 255.255.255.0
SW-L3-DlteC(config-if)#no shutdown
SW-L3-DlteC(config)#interface vlan 10
SW-L3-DlteC(config-if)#ip address 192.168.10.1 255.255.255.0
SW-L3-DlteC(config-if)#no shutdown
SW-L3-DlteC(config)#interface vlan 20
SW-L3-DlteC(config-if)#ip address 192.168.20.1 255.255.255.0
SW-L3-DlteC(config-if)#no shutdown
```

Para configurar uma interface roteada em switches L3 você precisa primeiro transformá-la de L2 para L3 com o comando “no switchport”, pois as interfaces de switches L2 e L3 por padrão são interfaces L2. Veja exemplo abaixo.

```
SW1-L3(config)#interface fast 0/0
SW1-L3(config-if)#no switchport
SW1-L3(config-if)#ip address 192.168.10.1 255.255.255.0
SW1-L3(config-if)#description Interface-de-gerenciamento
SW1-L3(config-if)#no shut
```

Agora essa interface fast0/0 do switch não é mais uma porta L2 e sim uma porta roteada, protocolos como spanning-tree e o encaminhamento de MACs são desativados nessa porta.

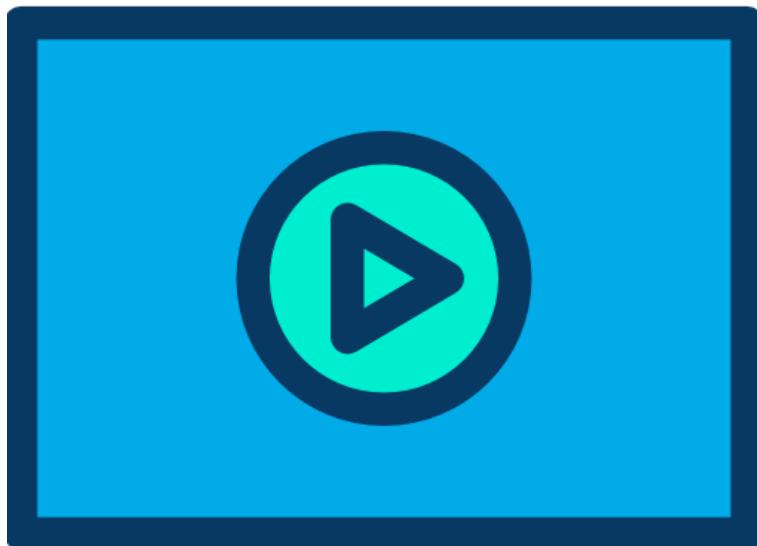
Para verificar a configuração realizada utilize o comando “show running-config interface fast0/0”.

Com esse comando você consegue ver a configuração específica da interface fast 0/0, porém se em uma prova ele não for aceito utilize o “show running-config” e navegue até chegar às configurações da interface.

As interfaces L2 dos switches não aceitam o comando “ip address”, pois elas fazem o encaminhamento em camada-2 e não em camada-3. Isso é o padrão dos switches e realizado devido ao comando “switchport” que já vem configurado em suas portas.

Dica: mesmo sendo L3, os switches normalmente vêm configurados como L2 e você precisa utilizar o comando “ip routing” para ativar o roteamento IPv4 nesse switch.

8.11.3 Erros Comuns ao Configurar Interfaces



Devemos lembrar-nos de algumas regras descritas sobre configuração de endereços IP que servem para todos os dispositivos de rede:

1. Endereços de rede e de broadcast não podem ser utilizados para endereçar Hosts.
2. Endereços IP devem ser únicos na Intranet e/ou na Internet.
3. Cada interface do roteador deve pertencer a uma rede ou sub-rede distinta, não podemos repetir rede ou sub-rede em interfaces diferentes.

Caso você não obedeça a essas regras básicas mensagens de erro serão geradas, veja alguns exemplos abaixo onde.

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int f0/0
R1(config-if)#ip add
R1(config-if)#ip address 10.0.0.0 255.0.0.0
Bad mask /8 for address 10.0.0.0
R1(config-if)#ip address 192.168.1.255 255.255.255.0
Bad mask /24 for address 192.168.1.255
```

Note em amarelo que ao tentar inserir o IP 10.0.0.0/8 o roteador emitiu uma mensagem de "Bad mask", ou seja, com essa máscara esse IP não pode ser configurado nessa interface, pois como já estudamos trata-se de um endereço de rede e não de host.

O mesmo acontece para o exemplo abaixo destacado em verde, ao tentarmos configurar um broadcast na interface recebemos um "Bad mask".

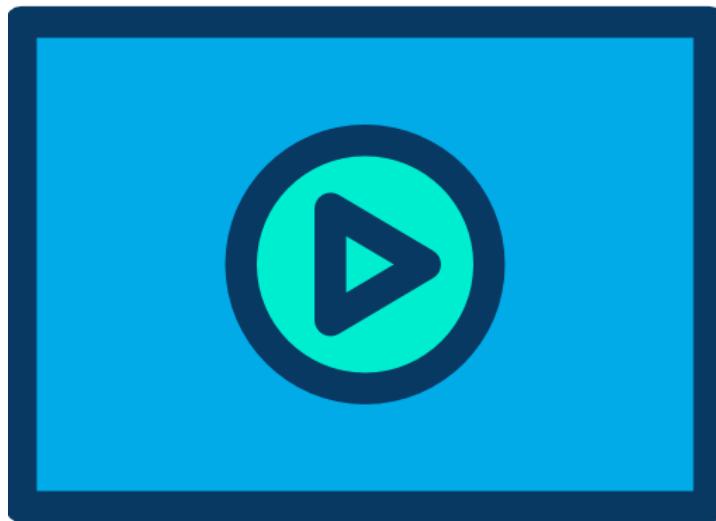
No próximo exemplo vamos tentar inserir um IP de uma rede já configurada em uma das interfaces do roteador.

```
R1(config-if)#int f0/0
R1(config-if)#ip add 10.0.0.1 255.255.255.0
R1(config-if)#int f0/1
R1(config-if)#ip add 10.0.0.10 255.255.255.0
% 10.0.0.0 overlaps with FastEthernet0/0
R1(config-if)#

```

Perceba que nesse segundo exemplo o roteador mostra uma mensagem de erro diferente, na qual ele informa um “**overlap**” indicando que esse IP está na faixa da interface fast0/0.

É importante sempre “ficar ligado” nas mensagens que os roteadores e switches enviam para identificar possíveis erros e não perder tempo!

8.11.4 Apagando e Alterando Endereços Configurados

O comando “ip address” é do tipo substitutivo, ou seja, como cada interface só pode ter um endereço principal, para trocar o endereço é só sobrescrever o comando, veja exemplo abaixo:

```
R1(config)#int f0/0
R1(config-if)#ip address 10.0.0.1 255.255.255.0
R1(config-if)#do sho run int f0/0
Building configuration...

Current configuration : 81 bytes
!
interface FastEthernet0/0
  ip address 10.0.0.1 255.255.255.0
  duplex half
end

R1(config-if)#ip add 10.0.0.2 255.255.255.0
R1(config-if)#do sho run int f0/0
Building configuration...

Current configuration : 81 bytes
!
interface FastEthernet0/0
  ip address 10.0.0.2 255.255.255.0
  duplex half
end
```

Para remover o IP da interface basta entrar com o comando “**no ip address**”. Essa opção apaga o endereço IP principal e os secundários ao mesmo tempo.

Para apagar somente um ip secundário é preciso especificar o IP a ser apagado. Veja exemplo abaixo onde temos três IPs secundários configurados e precisamos apagar apenas o referente à rede 12.0.0.0/8:

```
R1(config-if)#ip address 11.0.0.1 255.0.0.0 secondary
R1(config-if)#ip address 12.0.0.1 255.0.0.0 secondary
R1(config-if)#ip address 13.0.0.1 255.0.0.0 secondary
R1(config-if)#do show run int f0/0
Building configuration...

Current configuration : 204 bytes
!
interface FastEthernet0/0
  ip address 11.0.0.1 255.0.0.0 secondary
  ip address 12.0.0.1 255.0.0.0 secondary
  ip address 13.0.0.1 255.0.0.0 secondary
  ip address 10.0.0.2 255.255.255.0
  duplex half
end

R1(config-if)#no ip add 12.0.0.1 255.0.0.0 secondary
R1(config-if)#do show run int f0/0
Building configuration...

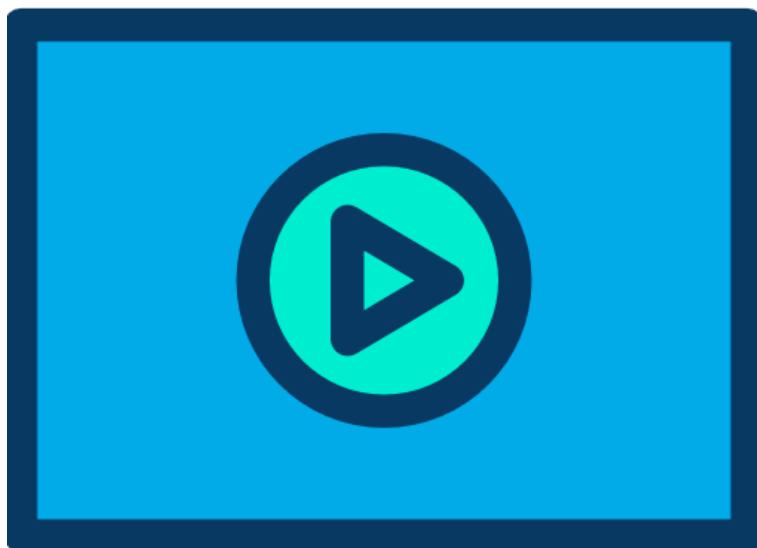
Current configuration : 163 bytes
!
interface FastEthernet0/0
  ip address 11.0.0.1 255.0.0.0 secondary
  ip address 13.0.0.1 255.0.0.0 secondary
  ip address 10.0.0.2 255.255.255.0
  duplex half
end

R1(config-if)#

```

Portanto, para apagar um endereço secundário precisamos inserir a opção "no" mais o comando completo.

8.11.5 Verificando as Configurações das Interfaces



Para verificar as configurações das interfaces você pode utilizar o comando "show running-config" ou especificar apenas a interface que deseja ver as configurações com o "show running-config interface **tipo-interface num-interface**", por exemplo, para ver apenas a configuração da interface fast 0/0 utilizamos o "show running-config interface fast 0/0", conforme utilizamos nos exemplos anteriores para verificar as configurações.

Se você não estiver em modo privilegiado utilize a opção "**do**" para não precisar sair do modo de configuração e executar o comando show.

Também podemos utilizar o "show interfaces" e o "show ip interface brief", veja exemplo abaixo.

```
R1#sho ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
FastEthernet0/0    10.0.0.2        YES manual up       up
FastEthernet1/0    unassigned      YES unset administratively down down
FastEthernet1/1    unassigned      YES unset administratively down down
R1#
```

Com esse comando podemos verificar a interface, o endereço IP no campo (IP-Address), depois no OK se a interface está com problema, no campo Method temos a maneira que a configuração foi realizada, por exemplo, a interface fast 0/0 tem a configuração manual (IP estático) e por último temos os campos Status indicando se a camada física está up ou down e no campo Protocol temos o estado do protocolo de camada 2 se está up ou down.

Nesse comando não temos o detalhe da máscara de rede, para saber essa informação temos que utilizar o show interface ou show running-config.

Lembre-se que o status da Interface deve estar UP/UP, significando que tanto as camadas físicas como a de enlace estão funcionando perfeitamente. Os outros estados possíveis são:

- **UP/DOWN**: a camada física está OK, mas a de enlace está com problemas, por exemplo protocolo de camada 2 de um dos lados está configurado errado ou falta do comando clock rate em interfaces DCE.
- **DOWN/DOWN**: a camada física está com problemas, por exemplo, cabo rompido ou modelo errado.
- **Administratively Down**: falta o comando “no shutdown” na interface, ou seja, a interface está desabilitada.

Por último, sempre que configuramos e ativamos uma interface uma rota para a rede da interface configurada é inserida na tabela de roteamento, assim como uma rota local com máscara de host /32 para indicar o endereço configurado na própria Interface. Veja exemplo abaixo.

```
R1(config)#int f2/0
R1(config-if)#ip add 15.0.0.1 255.0.0.0
R1(config-if)#no shut
R1(config-if)#end
R1#sho
*Jul 11 22:49:37.215: %SYS-5-CONFIG_I: Configured from console by console
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
      ia - IS-IS inter area, * - candidate default, U - per-user static route
      o - ODR, P - periodic downloaded static route, H - NHRP, l - LISPs
      + - replicated route, % - next hop override

Gateway of last resort is not set

      15.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        15.0.0.0/8 is directly connected, FastEthernet2/0
L        15.0.0.1/32 is directly connected, FastEthernet2/0
R1#
```

A informação na tabela de roteamento destacada em amarelo e com o termo “**directly connected**” é uma rota diretamente conectada, ou seja, pertence ao próprio roteador local. Note que as rotas diretamente conectadas são marcadas com um “**C**” na frente.

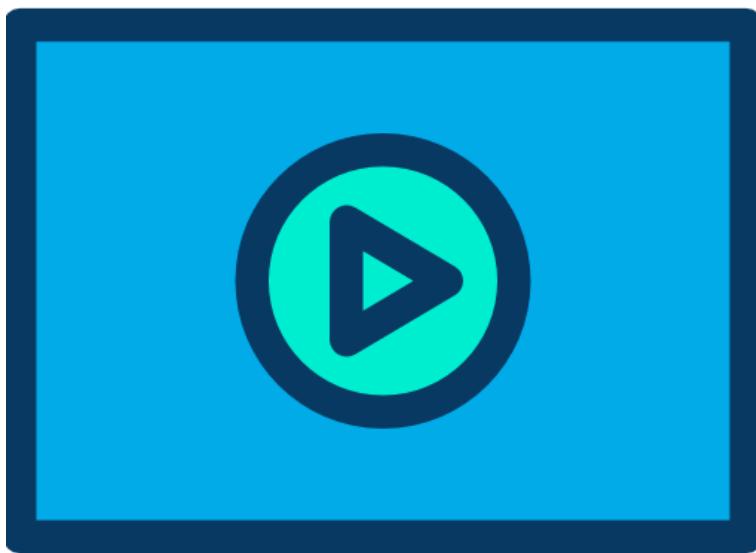
A rota local destacada em verde e marcada com o símbolo “**L**” no início foi inserida em IOSs versão 15, se você estiver realizando testes em IOSs mais antigos essa informação não é mostrada na saída desse comando. Ela indica o endereço IP configurado na interface, por isso a máscara inserida na tabela de roteamento é /32 ou 255.255.255.255.

Uma máscara 255.255.255.255 tem todos os IPs de rede, ou seja, indica um IP único, sem faixa de IPs válidos ou broadcast.

Resumo dos comandos:

- **Show interfaces [eth 0/0]**: verificar estado das interfaces (UP/DOWN), IP, contadores de pacotes, uso, erros, etc.
- **Show ip interface brief**: lista das interfaces, IP principal e estado (UP/DOWN).
- **Show interfaces status (switch)**: lista das interfaces e características físicas, além de indicar que portas estão configuradas como roteadas.
- **Show running-configuration [eth 0/0]**: configuração do roteador, inclusive das interfaces.
- **Show interfaces [eth 0/0] switchport (switch)**: verifica se a porta é L2 ou L3, além de diversos outros parâmetros de interfaces L2.
- **Show ip route [connected]**: mostra as rotas do roteador ou switch L3, lembrando que as interfaces configuradas e UP/UP tem suas redes e IP's locais mostrados nessa tabela de roteamento.

8.11.6 Testando as Interfaces com Ping, Traceroute e Telnet



O ping testa a conectividade fim a fim, ou seja, entre um host e outro, não especificando por onde esse pacote está passando.

Já o traceroute testa ponto a ponto com a opção TTL do cabeçalho do endereço IP, sendo utilizado para identificar o caminho do pacote ou em que ponto do caminho um ping que não foi completado parou.

Já o Telnet e SSH testa a conexão em camada-7, ou seja, a navegabilidade da Rede.

Para executar um teste simples de ping e traceroute basta digitar o comando e o IP.

Já o Telnet e SSH precisam ser configurados nos dispositivos, eles não funcionam por padrão. Essas configurações não fazem parte do escopo desse curso da trilha do CCNA em específico, serão estudadas em curso posterior.

Veja o exemplo de dois testes abaixo.

```
dltec#ping 192.168.1.1
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

Além disso, o ping no roteador pede ser executado de maneira estendida, inserindo apenas a palavra ping, sem o IP de destino. Veja um exemplo abaixo.

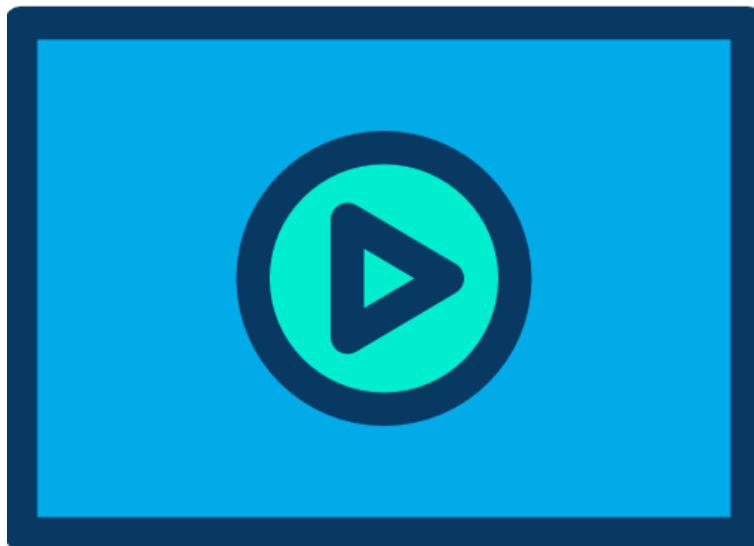
```
dltec#ping
Protocol [ip]:
Target IP address: 192.168.1.1
Repeat count [5]: 20
Datagram size [100]: 1000
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface:
Type of service [0]:
Set DF bit in IP header? [no]: y
Validate reply data? [no]:
Data pattern [0xABCD]: aaaaaaaa
Invalid pattern, try again.
Data pattern [0xABCD]: 0xaaaa
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 20, 1000-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
Packet sent with the DF bit set
Packet has data pattern 0xAAAA
!!!!!!!!!!!!!!!
Success rate is 100 percent (20/20), round-trip min/avg/max = 1/2/4 ms
dltec#
```

As mensagens que o ping e o traceroute podem fornecer nos roteadores da Cisco podemos encontrar estão na tabela abaixo.

!	Indica o recebimento do echo reply com sucesso.
.	Indica que o echo reply não foi recebido e o tempo de espera se esgotou.
U	Indica o recebimento de um destination unreachable.
Q	Indica o recebimento de uma mensagem de Source quench (destino muito ocupado).
M	Indica que precisa de fragmentação, mas o bit DF está setado.
?	Tipo de pacote desconhecido.
&	Tempo de vida do pacote excedido.

Lembre-se que não configuramos o roteamento IP ainda, portanto o ping deve ser dado para testar as interfaces locais e diretamente conectadas.

9 Endereçamento IPv6, Tipos e Configurações



A maior diferença entre o IPv4 e o IPv6 com certeza é o número de endereços IP disponíveis em cada um dos protocolos.

No IPv4 temos 4,294,967,296 endereços, enquanto no IPv6 temos um total de 340,282,366,920,938,463,463,374,607,431,768,211,456 endereços IP. Note abaixo como a diferença é gritante:

IPv4: **4,294,967,296**
IPv6: **340,282,366,920,938,463,463,374,607,431,768,211,456**

Esta diferença de valores entre o IPv4 e o IPv6 representa aproximadamente **79 octilhões de vezes** a quantidade de endereços IPv6 em relação a endereços IPv4, além disso, mais de **56 octilhões de endereços** por ser humano na Terra, considerando-se a população estimada em 6 bilhões de habitantes.

Tecnicamente as funcionalidades da Internet continuarão as mesmas com a introdução do IPv6 na rede e, com certeza, ambas versões do protocolo IP deverão funcionar ao mesmo tempo, tanto nas redes já implantadas em IPv4 como em novas redes que serão montadas.

Atualmente as redes que suportam IPv6 também suportam o IPv4 e ambos protocolos deverão ser utilizados por um bom tempo ainda.

Acompanhe na tabela onde mostramos uma comparação simples em termos somente do formato dos endereços e quantidades.

	Internet Protocol version 4 (IPv4)	Internet Protocol version 6 (IPv6)
Publicação	1981	1999
Tamanho do Endereço	32-bit	128-bit
Notação	Decimal: 192.149.252.76	Hexadecimal: 3FFE:F200:0234:AB00: 0123:4567:8901:ABCD
Notação em Prefixo	192.149.0.0/24	3FFE:F200:0234::/48
Quantidade de Endereços	$2^{32} = \sim 4,294,967,296$	$2^{128} = \sim 340,282,366,$ 920,938,463,463,374, 607,431,768,211,456

Outras diferenças importantes são:

- A introdução dos endereços de anycast e a retirada dos endereços de broadcast.
- O grande vilão do IPv4, o broadcast, no IPv6 não existe mais.
- Agora no IPv6 temos endereços de unicast, multicast e anycast.
- Caso seja necessário enviar uma mensagem a todos os hosts pode-se utilizar um pacote de multicast para o endereço de link-local de destino chamado de "all nodes address" (FF02::1).

Outro ponto importante é que no IPv6 ainda temos a parte de rede, subrede e host, como no IPv4, mas não utilizamos mais o termo **máscara** e sim somente **prefixo**.

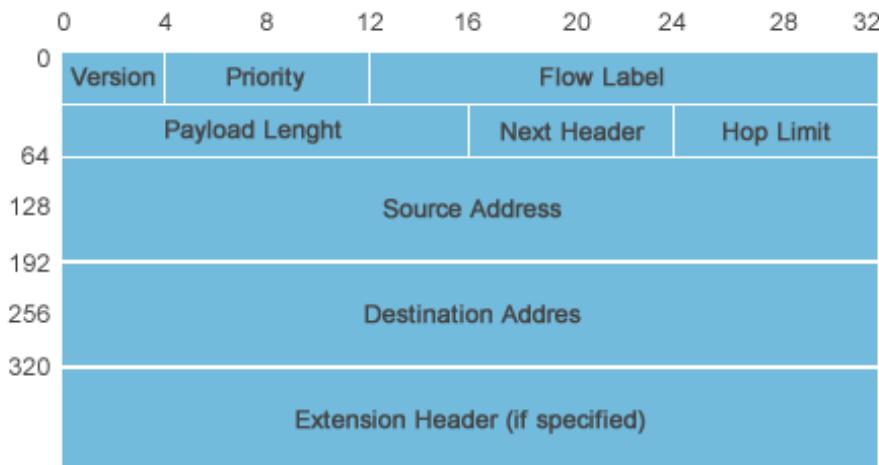
O prefixo do IPv6 tem a mesma funcionalidade do prefixo do CIDR e conta a quantidade de bits de rede ou subrede que a máscara tem, sendo que os bits 1 continuam indicando a porção de redes e os bits zero os hosts.

No exemplo dado na tabela anterior temos a rede 3FFE:F200:0234::/48 e o /48 representa o prefixo dessa rede, ou seja, os primeiros 48 bits do endereço são bits de rede e os demais 80 bits (128-48) são de host.

Isso mesmo, temos 80 bits para hosts nesse exemplo.

O cabeçalho do pacote IPv6 é bem mais simples que o do IPv4, contendo apenas 8 campos principais e caso serviços adicionais sejam necessários existem extensões de cabeçalho que podem ser utilizadas.

O cabeçalho (header) básico está na figura a seguir.



A descrição de cada campo segue abaixo:

- **Version (versão - 4 bits)**: Contém o valor para versão 6.
- **Priority ou Traffic Class (classe de tráfego - 8 bits)**: Um valor de DSCP para QoS (qualidade de serviços).
- **Flow Label (identificador de fluxo - 20 bits)**: Campo opcional que identifica fluxos individuais. Idealmente esse campo é configurado pelo endereço de destino para separar os fluxos de cada uma das aplicações e os nós intermediários de rede podem utilizá-lo de forma agregada com os endereços de origem e destino para realização de tratamento específico dos pacotes.
- **Payload Length (tamanho do payload - 16 bits)**: Tamanho do payload em bytes.
- **Next Header (próximo cabeçalho - 8 bits)**: Cabeçalho ou protocolo que virá a seguir. É utilizado para identificar que existem cabeçalhos de extensão após o principal.
- **Hop Limit (limite de saltos - 8 bits)**: Similar ao tempo de vida de um pacote IPv4 (TTL - time to live) utilizado no teste de traceroute.
- **Source Address (endereço IPv6 de origem - 128 bits)**: Endereço IP de quem está enviando os pacotes.
- **Destination Address (endereço IPv6 de destino - 128 bits)**: Endereço IP do host remoto que deve receber os pacotes.

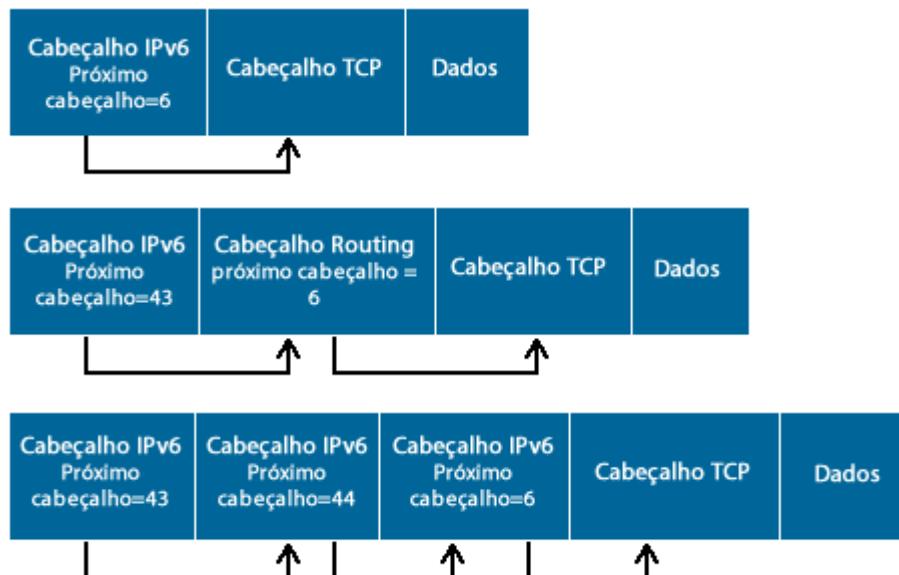
Aqui vem mais uma diferença do IPv6, pois no IPv4 o cabeçalho base continha todas as informações principais e opcionais (mesmo que não fossem utilizadas).

Já o IPv6 trata essas informações adicionais como cabeçalhos opcionais chamados de "**cabeçalhos de extensão**".

Os cabeçalhos de extensão são inseridos entre o cabeçalho base e o cabeçalho da camada imediatamente acima (payload), não tendo nem quantidade ou tamanho fixo.

Caso existam múltiplos cabeçalhos de extensão no mesmo pacote, eles serão encadeados em série formando uma "cadeia de cabeçalhos".

A figura a seguir mostra um exemplo dessa situação.



De uma maneira resumida seguem os cabeçalhos de extensão possíveis e seus identificadores:

- **Hop-by-hop Options (0)**: Transporta informações adicionais que devem ser examinadas por todos os roteadores de caminho, por isso o nome hop-by-hop que em português significa **salto a salto**.
- **Routing (43)**: Definido para ser utilizado como parte do mecanismo de suporte a mobilidade do IPv6.
- **Fragment (44)**: Indica se o pacote foi fragmentado na origem.
- **Encapsulating Security Payload (50) e Authentication Header (51)**: fazem parte do cabeçalho IPSec, utilizados para criptografia do payload.
- **Destination Options (60)**: Transporta informações que devem ser processadas apenas pelo computador de destino.

Portanto, o cabeçalho do IPv6 além de ser mais simples que o do IPv4, também trata de questões como QoS e segurança de maneira nativa, ou seja, dentro do próprio cabeçalho sem a necessidade de implementações e recursos adicionais como era necessário para o IPv4.

Teremos mais para frente um capítulo específico para tratar com mais detalhes do endereçamento IPv4 e IPv6.

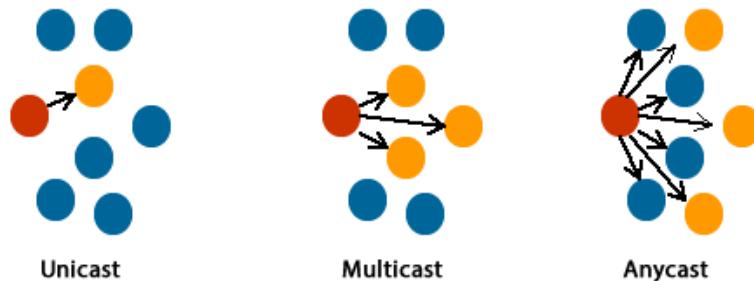
9.1 Tipos de Comunicação e Endereços em IPv6



Como já citado anteriormente, no IPv6 não temos mais os endereços e a comunicação via broadcast. Os endereços de unicast e multicast continuam existindo e com a mesma função em ambas versões de protocolo, porém foi criado um tipo a mais de endereçamento chamado de anycast. Veja abaixo a descrição resumida de cada um deles:

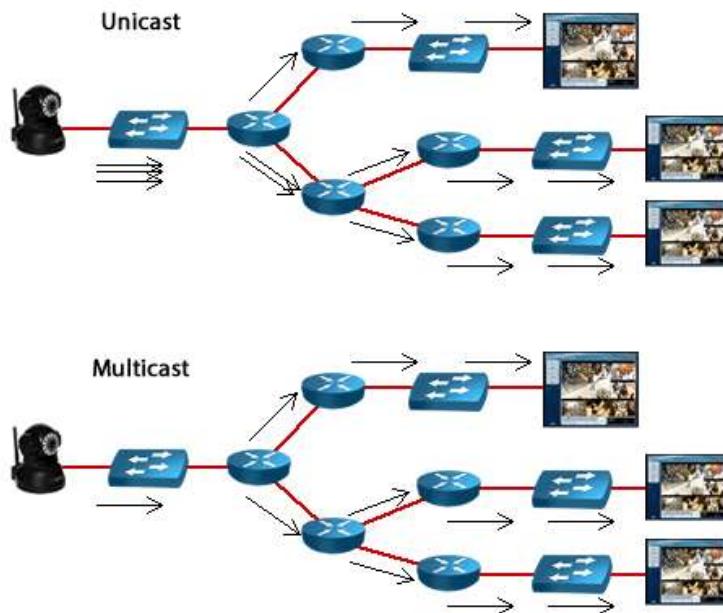
- **Unicast** → Comunicação um para um.
- **Multicast** → Comunicação um para muitos (grupo de dispositivos configurados com o mesmo endereço).
- **Anycast** → Endereço configurado em múltiplas interfaces.

Veja a figura a seguir com a representação de cada um dos três tipos de comunicação.



Para visualizar a diferença e aplicação do uso do unicast para multicast considere a figura abaixo, onde você tem um dispositivo de vídeo que irá transmitir o sinal para três hosts na rede.

Caso a transmissão seja feita utilizando unicast terão que ser criados três fluxos, um para cada host de destino, ocupando mais banda, pois a mesma informação é triplicada. Já no caso do uso do multicast o transmissor envia as informações para um único endereço que está configurado em todos os hosts que participam do mesmo “grupo de multicast” que ele, portanto a informação é transmitida utilizando apenas um fluxo até os hosts.



O endereço IP de anycast é um endereço que **podemos configurar em mais de um dispositivo**, portanto ele será anunciado em diferentes roteadores. Mas para que serve o anycast na prática? Uma das respostas e a mais utilizada é para redundância (apesar de que pode ser utilizado para balanceamento de carga).

Por exemplo, você tem três servidores DNS e configura o mesmo IP de anycast nos três, porém cada um está conectado por caminhos diferentes (roteadores distintos ou larguras de bandas diferentes). Quando o computador for realizar uma consulta ao DNS ele enviará o pacote para o IP de anycast (destino) configurado em sua placa de rede, porém quando a rede receber o pacote com o endereço de destino sendo um anycast os roteadores encaminharão esse pacote para o melhor destino em relação à origem. Ou seja, mesmo tendo três servidores com o mesmo IP de Anycast o que tiver melhor métrica em relação ao protocolo de roteamento utilizado é o que receberá a solicitação.

Por exemplo, você está utilizando OSPFv3, o qual utiliza um custo como métrica para encontrar o melhor caminho, se um dos servidores tem custo 25 (Server A), o segundo custo 40 (Server B) e o terceiro custo 20 (Server C) qual dos três irá receber a consulta enviada pelo cliente? Com certeza será o que possui menor custo (menor métrica), portanto o Server C receberá os pacotes referentes à consulta de nomes e deverá responder ao cliente.

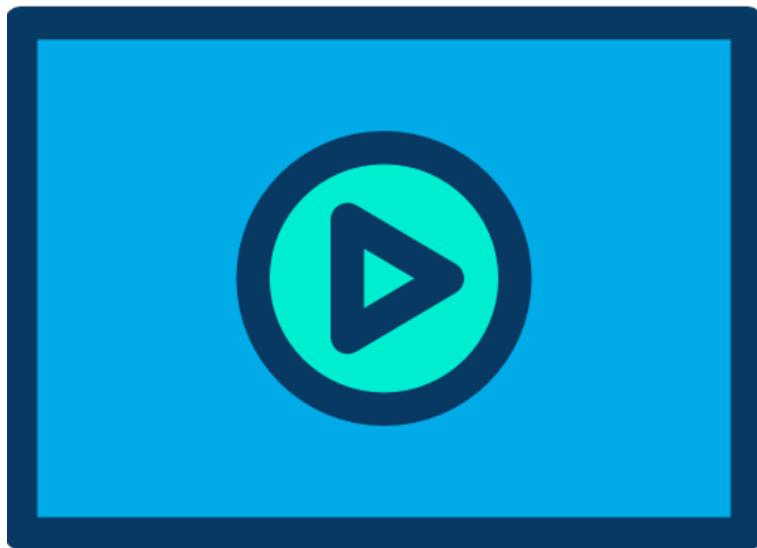


Duas dicas importantes, o IP de anycast não é utilizado como origem em um pacote IPv6, **somente como destino** e **precisa estar anunciado** entre os roteadores (através do protocolo de roteamento) para que possa ser encaminhado conforme exemplo anterior.

Portanto não é só configurar um IP, o uso do anycast exige configurações de roteamento na rede.

Normalmente ele é o primeiro IPv6 da rede ou sub-rede, o que contém todos os bits de host em zero. Isso mesmo, podemos utilizar um endereço que no IPv4 era reservado para rede ou sub-rede no IPv6 para endereçar hosts!

9.2 Escrevendo e Abreviando Endereços IPv6



Antes de falar de como o endereçamento é dividido vamos ver como podemos escrever um endereço IPv6 (notação em hexadecimal) e as partes que o compõe.

Como já visto em capítulos anteriores, o endereço IPv6 possui 128 bits e é escrito em hexadecimal, diferente do IPv4 que eram 32 bits (4 conjuntos de 8 bits escritos em decimal pontuado).

Portanto, agora cada algarismo de um IPv6 pode ter os números de 0 a 9, assim como as letras de A a F, totalizando 16 algarismos, por isso o nome hexadecimal. Além disso, cada Hexadecimal pode ser dividido em um conjunto de 4 bits e não mais 8 como no IPv4.

Veja quanto vale de A a F em decimal (*você pode escrever as letras do hexadecimal tanto em maiúsculo como em minúsculo, tanto faz!*):

- "A" vale 10 em decimal – em binário 1010
- "B" vale 11 em decimal – em binário 1011
- "C" vale 12 em decimal – em binário 1100
- "D" vale 13 em decimal – em binário 1101
- "E" vale 14 em decimal – em binário 1110
- "F" vale 15 em decimal – em binário 1111

Como cada algarismo em hexadecimal tem 4 bits, em 128 bits temos um total de 32 algarismos hexadecimais divididos de 4 em 4, ou seja, oito conjuntos de quatro algarismos em hexadecimal separados por dois pontos ":" (não mais pelo ponto "." como era no IPv4). Um exemplo de IPv6 é "**2000:1234:ade4:ffa0:2234:0000:0000:0012**".

Existem ainda três contrações (reduções) que podemos fazer nos endereços IPv6:

1. Zero a esquerda pode ser omitido: 2000:1234:ade4:ffa0:2234:0000:0000:**12**
2. Conjuntos de 4 zeros na mesma casa podem ser reduzidos para um zero: 2000:1234:ade4:ffa0:2234:**0:0**:12
3. Sequências de zeros podem ser substituídas por dois conjuntos de dois pontos: 2000:1234:ade4:ffa0:2234:**::**12

A única recomendação é que não haja **ambiguidade** para a terceira contração. Para entender vamos ver um exemplo com o IP 2000:1234:ade4:**0000:0000:2234:0000**:12. Se escrevermos ele com a contração 2000:1234:ade4::2234::12 nós sabemos, por visualizar o IP que deu origem, que existem dois conjuntos de 4 zeros à esquerda do 2234 e um só conjunto à direita.

No entanto, como um dispositivo (roteador ou computador) irá distinguir como ele deve completar isso na prática? Pois se pegarmos apenas o IP contraído 2000:1234:ade4:**::2234::12** ele pode ser tanto 2000:1234:ade4:**0000:2234:0000:0000:12** como 2000:1234:ade4:**0000:0000:2234:0000:12**.

Logo, essa notação é inválida, pois para o dispositivo ela é ambígua uma vez que ele não vai saber como preencher os espaços com os zeros. Portanto, o IP deveria ser escrito como "**2000:1234:ade4:0:0:2234::12**" ou "**2000:1234:ade4::2234:0:12**".

Outra representação importante, a qual já foi comentada anteriormente, é a dos **prefixos de rede**. No IPv6 continuamos escrevendo os endereços como no IPv4 utilizando a notação CIDR, ou seja, "**endereço-IPv6/tamanho do prefixo**", onde "**tamanho do prefixo**" é um valor decimal que especifica a **quantidade de bits contíguos à esquerda do endereço** que compreendem o prefixo, ou seja, a soma dos bits uns do prefixo.

Um endereço IPv6 pode ser dividido em um Prefixo Global (Global Prefix), Sub-rede (subnet ID) e endereço da Interface (Interface ID). O prefixo global normalmente é um /32, já o prefixo de sub-rede pode ser /48 (usuários corporativos) ou /56 a /64 (para usuários residenciais) dependendo do uso e recomendação de cada país. Já o endereço da interface utiliza os bits restantes do prefixo, ou seja, 128 bits menos o prefixo de sub-rede.



Vamos a um exemplo utilizando a rede **2001:db:3000:1::/64**, onde sabemos que temos 128 bits totais no endereço, porém 64 bits são utilizados para identificar a sub-rede, portanto termos:

- Prefixo 2001:db:3000:1::/64
- Prefixo global 2001:db::/32
- ID da sub-rede 3000:1
- ID de host: temos 64 bits (ou seja, $2^{64} = 18.446.744.073.709.551.616$ endereços IP)

Da mesma maneira que mostramos no IPv4 com o CIDR e a notação em prefixos, no IPv6 podemos fazer a agregação de várias sub-redes de maneira hierárquica para reduzir a quantidade de redes anunciadas pelos protocolos de roteamento, além de continuar valendo o conceito de sub-rede e a utilização de diferentes prefixos conforme a necessidade de cada rede IPv6, similar ao VLSM.

Com relação a representação dos endereços IPv6 em URLs (Uniform Resource Locators), eles agora passam a ser representados entre **colchetes**. Deste modo, não haverá ambiguidades caso seja necessário indicar o número de uma porta juntamente com a URL, por exemplo:

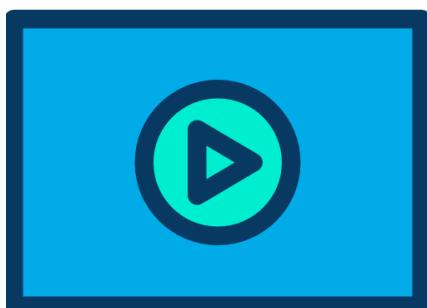
- [http://\[2001:db:3000:1::22\]/index.html](http://[2001:db:3000:1::22]/index.html)
- [http://\[2001:db:3000:1::22\]:8080](http://[2001:db:3000:1::22]:8080)

9.3 Tipos de Endereços IPv6

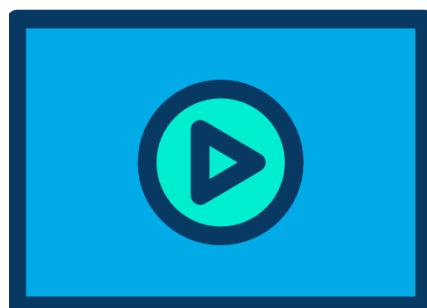
Se analisarmos a faixa total de endereços IPv6 vai de :: (0000:0000:0000:0000:0000:0000:0000) até ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff e assim como no IPv4 a IANA fez a alocação dos endereços entre os diversos tipos de endereçamento e faixas necessárias para serem distribuídas conforme explicado no capítulo sobre a Internet.

Portanto, vamos agora analisar a divisão dos endereços IPv6 e algumas faixas dedicadas a uso especial.

Na área do curso você vai encontrar dois vídeos iniciais falando sobre os tipos de endereços IPv4, com algumas novidades de interesse mais prático, assim como uma visão geral dos tipos de endereço IPv6 antes de estudarmos um a um.

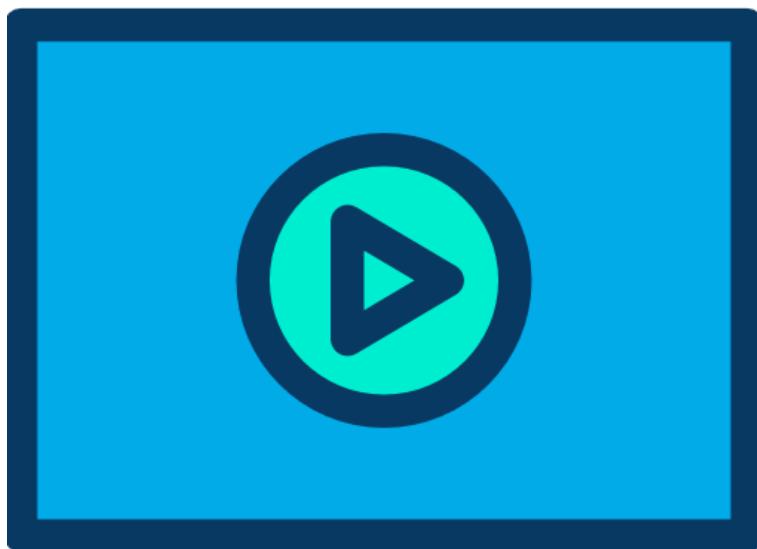


Tipos de Endereços IPv4



Tipos de Endereços IPv6

9.3.1 IEEE EUI-64 ou Modified EUI 64



O padrão EUI-64 é utilizado para formação do endereço de Link Local, no processo de autoconfiguração (SLAAC – Stateless Auto Configuration) e pode ser utilizado no DHCPv6. O objetivo básico é utilizar o endereço MAC da placa de rede do host para formar um Interface ID de 64 bits.

Sabemos que um endereço MAC tem 48 bits e já é escrito em Hexadecimal, portanto, para completar os 64 bits faltam apenas 16 bits, ou seja, quatro algarismos em Hexadecimal. Isto é feito com a inserção no meio do endereço MAC dos algarismos 0xffffe (FF-FE).

Além disso, o sétimo bit mais à esquerda (chamado de bit U/L – Universal/Local) do endereço MAC deve ser invertido, isto é, **se for 1 será alterado para 0 e se for 0 será alterado para 1.**

Veja a figura a seguir, no meio do endereço MAC foi inserida a palavra em hexadecimal 0xffffe e como os dois primeiros algarismos do MAC são 00, que em binário é 000000**00**, se trocarmos o sétimo bit ele fica 000000**10** ou 02 em hexadecimal (lembre-se que a cada 4 bits temos um algarismo em hexadecimal).

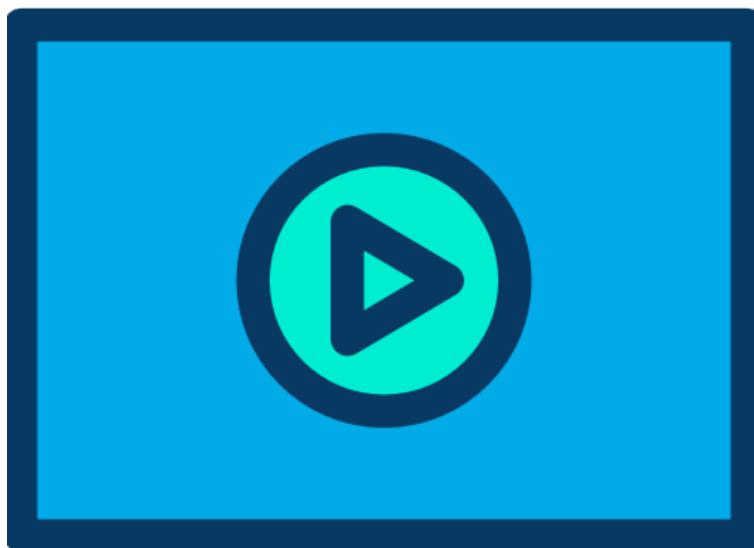
MAC	00 0A 27 5C 88 19
EUI-64	02 0A 27 FF FE 5C 88 19

Lembre-se que se recebermos um prefixo /64 podemos perfeitamente utilizar o EUI-64 para formar o Interface ID e assim termos o endereço global do computador (endereço de Internet), além do link local. Esse processo se chama autoconfiguração do IPv6.

Por exemplo, um computador que tem como endereço MAC 001e.130b.1aee e recebe um prefixo 2001::/64 do seu roteador terá os seguintes endereços de Link Local e Global Unicast:

- FE80::21E:13FF:FE0B:1AEE
- 2001::21E:13FF:FE0B:1AEE -> Prefixo 2001::/64

9.3.2 Link Local



- **FE80::/10** -> Link-local unicast.

Link-local unicast

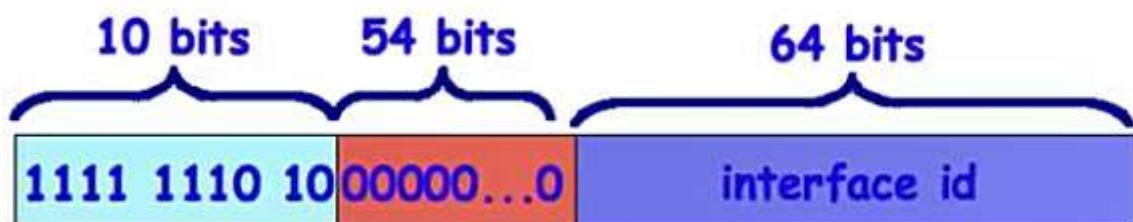


Este endereço é utilizado apenas na LAN onde a interface está conectada.

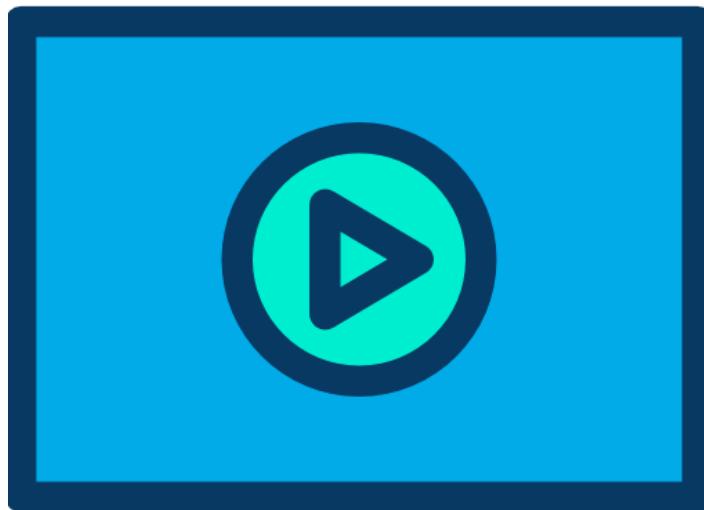
O endereço link local pode ser atribuído automaticamente utilizando o prefixo FE80::/64 e os outros 64 bits do ID da Interface são configurados utilizando o formato IEEE EUI-64, uma composição que utiliza o endereço MAC do host para formar o endereço da Interface.

Além disso, ele pode ser um endereço fixo, definido pelo administrador, ou utilizar a RFC 4941 (Privacy Extension) para definir o Interface-ID do cliente de forma randômica e “esconder” o endereço MAC do cliente.

Abaixo segue uma figura de um endereço de Link Local.



9.3.3 Unique Local Address

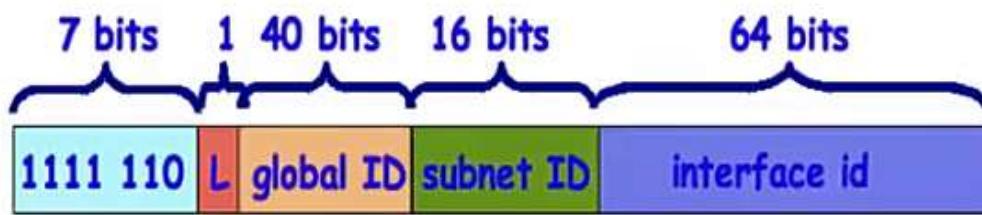


- **FC00::/7** -> Unique local (ULA). Este endereço será globalmente único, utilizado apenas para comunicações locais, geralmente dentro de um mesmo enlace ou conjunto de enlaces, portanto o endereço ULA não deve ser roteável na Internet.

Unique local



Similar ao endereço privativo (RFC1918) utilizado no IPv4, porém no IPv6 não está previsto o NAT de Ipv6 para IPv6, por isso ele a princípio não será roteado na Internet.

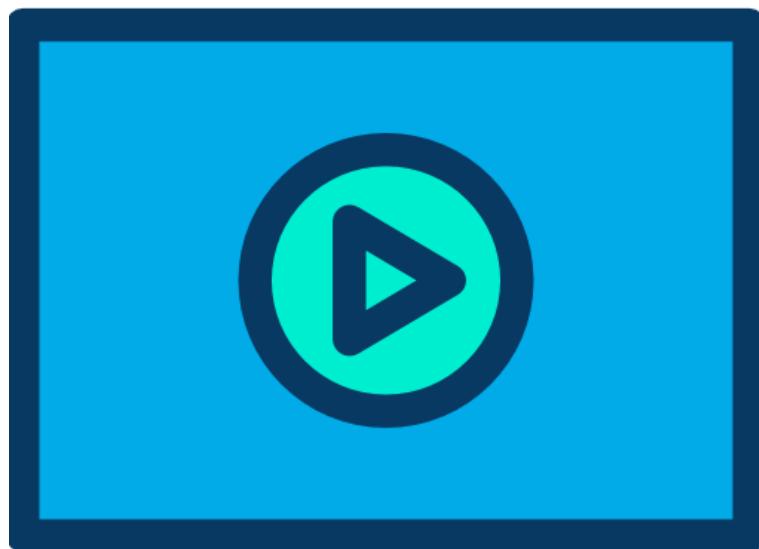


O endereço local único é dividido em:

- Prefixo: FC00::/7.
- Flag Local (L): apenas um bit, sendo que se o valor for 1 (FD) o prefixo é atribuído localmente. Se o valor for 0 (FC), o prefixo deve ser atribuído por uma organização central (ainda a definir).
- Identificador global: identificador de 40 bits usado para criar um prefixo globalmente único. Esse valor deve ser calculado conforme a RFC 4193 para garantir que esse valor seja único.
- Identificador da Interface: identificador da interface de 64 bits.

Dividido em dois grupos FC00::/8 e FD00::/8, sendo que a primeira sub-rede não é utilizada.

9.3.4 Global Unicast Address ou GUA



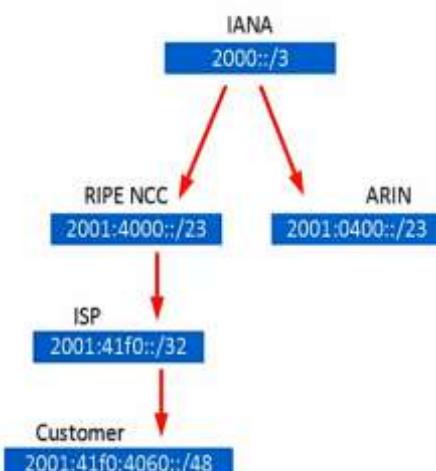
Para os endereços de Unicast (os roteáveis na Internet) está reservada para atribuição de endereços a faixa **2000::/3**, ou seja, dos endereços de 2000:: a 3fff:ffff:ffff:ffff:ffff:ffff:ffff:ffff. Isso representa **13% do total** de endereços possíveis com IPv6.

O nome dado aos endereços de Unicast é “**Global Unicast Address**” ou **GUA** ou endereço global unicast.

Global unicast



Esses endereços serão divididos conforme designação da IANA, sendo passados para os RIRs, entidades locais, provedores e sistemas autônomos seguindo regras e definições globais, ou seja, seguindo o mesmo padrão que estudamos para o IPv4.



A faixa 2800::/12 e 2001::1200::/23 foi destinada à LACNIC para alocação na América Latina. No Brasil o NIC.br possui três faixas de endereços que fazem parte deste /12 para distribuir entre as instituições e ISPs do nosso país.

/3 /12 /32 /48 /64					
3 bits	9 bits	20 bits	16 bits	16 bits	64 bits
001	IANA to RIR	RIR to ISP	ISP to End Site	Net	Interface ID
001	IANA to RIR	RIR to End Site	Net	Interface ID	
3 bits	9 bits	36 bits	16 bits	64 bits	



2000::/3

0010000000...000 > 2000::0

0011111111...111 > 3f:ffff:....:ffff

- LACNIC: 2800::/12 e 2001:1200::/23
- NIC.br: 2804::/16, 2801:0080::/26 e 2001:1280::/25

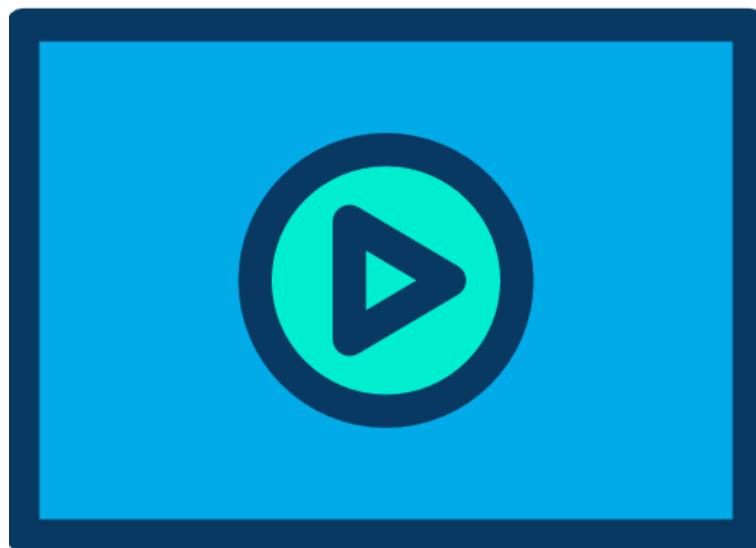
Note na figura anterior que prática um endereço Global ou de Internet em IPv6 pode ser subdividido em mais faixas que prevê a parte conceitual, pois a IANA definiu a faixa total, repassou blocos aos RIRs, os quais podem repassar para ISPs (provedores de Internet) ou então para Sistemas Autônomos (empresas com suas faixas próprias de endereçamento IPv6).

Os endereços de Anycast também são criados a partir da faixa de endereços unicast e não há diferenças de notação entre eles.

O que os diferencia é a configuração realizada nos roteadores e um anúncio explícito de que aquele IP é de Anycast.

Dessa maneira vai haver o roteamento e troca de informações sobre esses endereços de Anycast entre os roteadores, além disso, evita que os roteadores interpretem esse endereço como um IP duplicado e gere erros, pois o Anycast é um mesmo IP de Unicast configurado em vários hosts!

9.3.5 Multicast

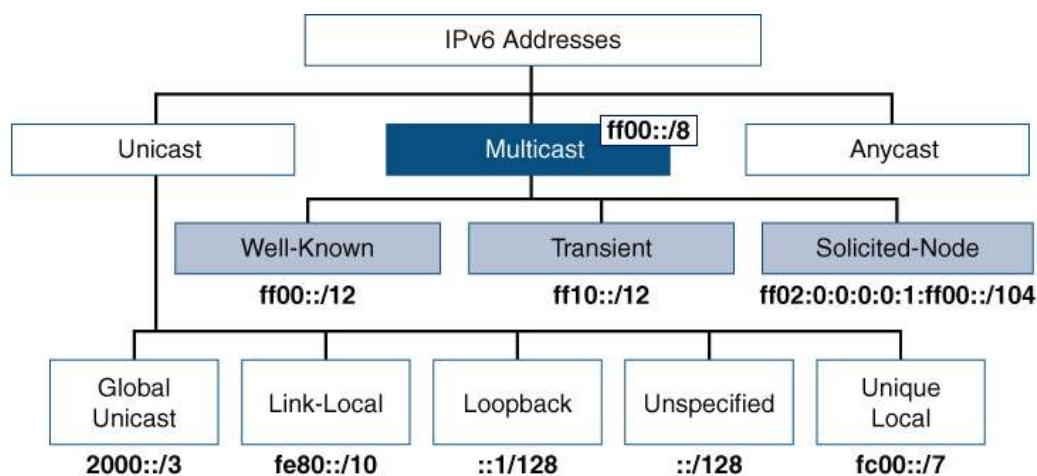


- **FF00::/8** → Faixa de endereços de multicast. Lembre-se que não existe mais broadcast no IPv6 e por isso o multicast tornou-se importante para esse protocolo.

Multicast



O multicast está dividido entre endereços bem conhecidos (Well-Known ff00::/12), transientes ou temporários (ff10::/12) e Solicited-Node (ff02:0:0:0:0:1:ff00::/104).



O endereço chamado solicited-node é utilizado na resolução de nomes via protocolo NDP (Neighbor Discovery Protocol), sendo criado automaticamente para cada endereço Unicast que um dispositivo tem configurado. Lembre-se que o IPv6 não tem mais broadcast, por isso mesmo não tem mais o ARP para mapear os endereços de camada-2 quando a origem de um pacote precisa montar um quadro de camada-2 e enviar mensagens em links Ethernet.

Os endereços de camada-2 ou MAC dos multicasts tem a faixa 33-33-00-00-00-00 até 33-33-FF-FF-FF-FF, sendo que normalmente os oito dígitos finais do MAC são os trinta e dois últimos bits do endereço de Multicast IPv6.

Abaixo seguem alguns outros endereços de grupos de multicast (endereços bem conhecidos – Well-Known) alocados pela IANA:

FF02::1 -> Todos os Hosts no Link (similar a um broadcast)

FF02::2 -> Todos os Roteadores no Link (utilizado para descobrir os roteadores)

FF02::5 -> Protocolo OSPFv3

FF02::6 -> Protocolo OSPFv3

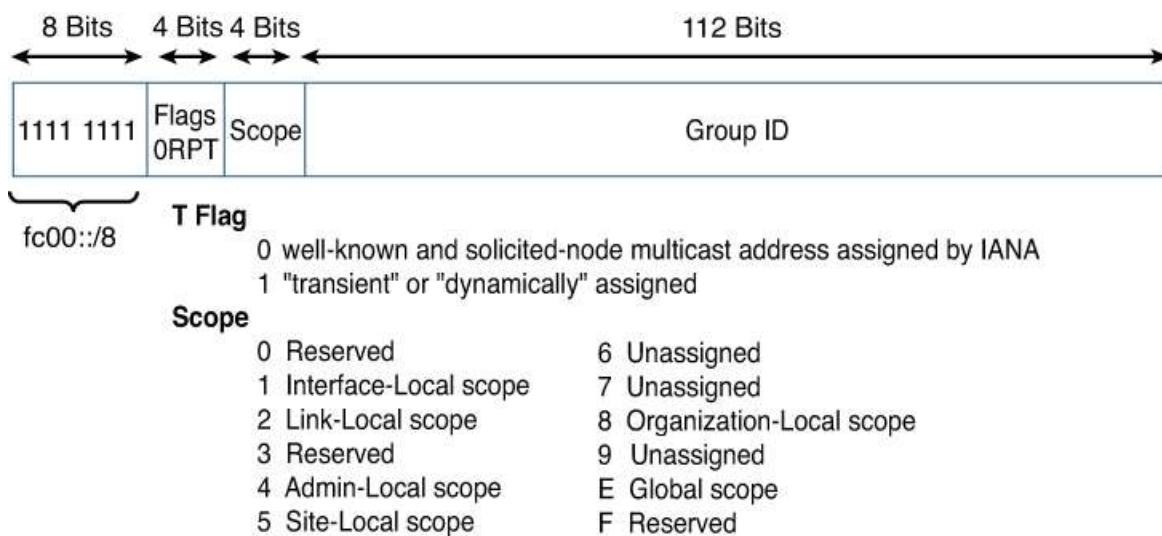
FF02::A -> Protocolo EIGRP/Cisco

FF02::1:2 -> Todos os Relay-Agents DHCP

FF05::1:3 -> Todos os Servidores DHCPv6 (utilizado para solicitar um endereço IPv6 dinâmico)

FF05::101 -> Todos os Servidores NTP

Informações Extras sobre Multicast:



Os flags são definidos da seguinte forma:

- **O primeiro bit** mais a esquerda é reservado e deve ser marcado com 0;
- **Flag R:** Se o valor for 1, indica que o endereço multicast "transporta" o endereço de um ponto de encontro (Rendezvous Point). Se o valor for 0, indica que não há um endereço de ponto de encontro embutido;
- **Flag P:** Se o valor for 1, indica que o endereço multicast é baseado em um prefixo de rede. Se o valor for 0, indica que o endereço não é baseado em um prefixo de rede;
- **Flag T:** Se o valor for 0, indica que o endereço multicast é permanente, ou seja, é atribuído pela IANA. Se o valor for 1, indica que o endereço multicast não é permanente, ou seja, é atribuído dinamicamente.

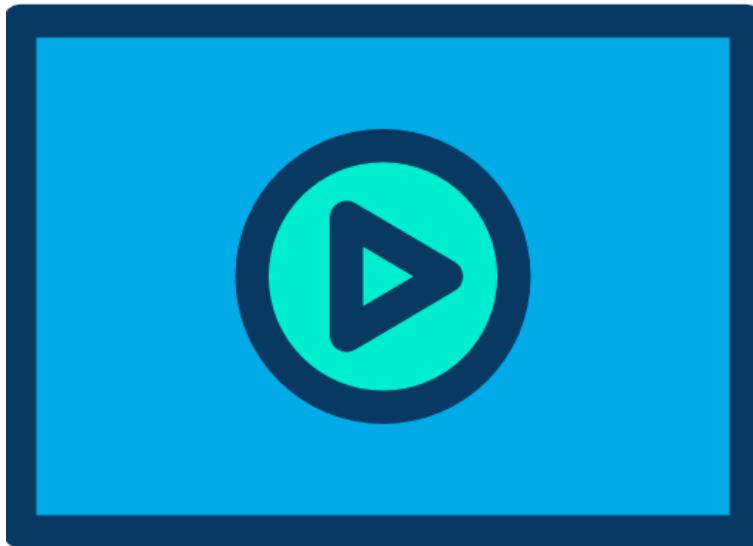
- **Os quatro bits** que representam **o escopo do endereço multicast (Scope)**, são utilizados para delimitar a **área de abrangência** de um grupo multicast. Os valores atribuídos a esse campo são o seguinte:
 - 1 – abrange apenas a interface local;
 - 2 – abrange os nós de um enlace (link local);
 - 4 – abrange a menor área que pode ser alocada pelo administrador;
 - 5 – abrange os nós de um site (site local);
 - 8 – abrange vários sites de uma mesma organização;
 - E – abrange toda a Internet;
 - 0, 3 e F – reservados;
 - 6, 7, 9, A, B, C e D – não estão alocados

9.3.6 Outros Tipos de Endereços IPv6

Abaixo segue uma lista de outros tipos endereços IPv6.

- **::/0** -> Rota padrão.
- **::/128** -> Endereço não especificado (Unspecified).
- **::1/128** -> Endereço de Loopback utilizados nos sistemas operacionais de servidores, computadores e laptops (no IPv4 é o 127.0.0.1).
- **::/96** -> Reservado para compatibilidade com IPv4, porém seu uso foi descontinuado. Seria um endereço como ::192.168.1.1, o motivo do /96 é que como temos 32 bits no IPv4 dá um total de "96+32=128 bits".
- **::FFFF:0:0/96** -> Endereço IPv4 mapeado como IPv6. É aplicado em técnicas de transição para que hosts IPv6 e IPv4 se comuniquem, por exemplo, ::FFFF:192.168.1.1.
- **2001::/32** → prefixo utilizado no mecanismo de transição Teredo. (mais para frente veremos o que é o Teredo).
- **2001:DB8::/32** -> prefixo utilizado para representar endereços IPv6 em textos e documentações.
- **2002::/16** -> Prefixo utilizado no mecanismo de transição 6to4.
- **FEC0::/10** → Site-local unicast, porém sua utilização foi substituída pelos endereços ULA e ele caiu em desuso.

9.4 Configurações e Verificações de Interfaces IPv6



Para configurar o IPv6 devemos começar habilitando o protocolo com o comando em modo de configuração global “**ipv6 unicast-routing**”.

```
R4#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R4(config)#ipv6 unicast-routing
R4(config)#
```

Você até consegue ativar um IPv6 em uma interface sem o comando acima, porém não haverá roteamento IPv6, os dispositivos camada-3 Cisco será um cliente de rede, parecido com o que ocorre com o IPv4 e os endereços de gerenciamento em switches. Veja exemplo abaixo.

```
DlteC-FW-GW#conf t
Enter configuration commands, one per line. End with CNTL/Z.
DlteC-FW-GW(config)#no ipv6 unicast-routing
DlteC-FW-GW(config)#int f0/0
DlteC-FW-GW(config-if)#ipv6 enable
DlteC-FW-GW(config-if)#do show ipv6 interface brief
FastEthernet0/0           [up/up]
  FE80::21E:13FF:FE0B:1AEE
FastEthernet0/1           [up/up]
  unassigned
DlteC-FW-GW(config-if)#

```

Na configuração mostrada no exemplo anterior utilizamos o comando “**ipv6 enable**” dentro da interface fast 0/0, o que faz com que o roteador crie um endereço IPv6 de Link Local mesmo que o comando “**no ipv6 unicast-routing**” esteja presente na configuração, pois o roteador não fará o roteamento com esse comando, mas nada impede que uma das suas interfaces responda através de IPv6, por exemplo, a um teste de ping.

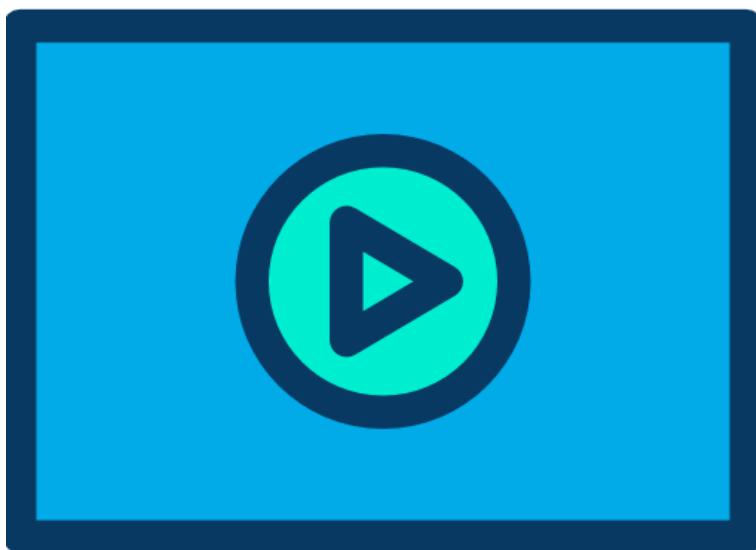
Note outro detalhe interessante que para verificar o IPv6 configurado utilizamos o comando **"show ipv6 interface brief"**, apenas trocamos o **ip** por **ipv6** e muitos dos comandos será assim, fica aqui essa dica!

Diferente do IPv4, o **roteamento IPv6 não vem habilitado por padrão** nos roteadores e switches L3 Cisco, por isso o comando acima ativa o roteamento IPv6 nos dispositivos camada-3.

Na maioria dos sistemas operacionais de clientes e servidores de rede essa realidade é bem diferente, sendo que o suporte nativo ao IPv6 é ativado.

Para verificar se o sistema operacional suporta IPv6 nativo basta dar um ping para a loopback "::1", se houver resposta o sistema operacional suporta IPv6. No Linux e MAC OS-X o comando é o **"ping6"** e no Windows e Cisco IOS continua com o "bom e velho **ping**".

9.4.1 Configurando Interfaces IPv6 no Cisco IOS



O próximo passo é configurar os endereços **Globais de Unicast**, pois os endereços **de link-local** são automaticamente configurados via EUI-64.

Para os endereços globais temos duas opções básicas de configuração:

1. Utilizar endereços de Internet da faixa **2000::/3**, porém para navegar com esses endereços é preciso que ele seja registrado, seja locado através de um provedor de serviços ou processos de Sistema Autônomo.
2. Utilizar a faixa dos endereços ULA (Unique Local Address) para criar uma rede privativa com endereços da faixa fc00::/7, sendo que para uso em redes corporativas normalmente utilizamos a faixa **fd00::/8** com sub-redes **/48**.

Para ambiente de laboratório mostramos um exemplo de projeto e alocação de endereços IP na parte I do capítulo de IPv6, basicamente o projeto é parecido com IPv4, onde temos que definir as redes, sub-redes, endereços de Interfaces e hosts da rede. A diferença é que os endereços de host utilizam identificadores (host-ID) de 64 bits.

Nos roteadores e switches Cisco podemos configurar os endereços globais das seguintes maneiras:

1. **Configuração estática:** "ipv6 address *end-ip6/tamanho-do-prefixo*"
2. **Configuração estática com EUI-64:** "ipv6 address *prefixo-de-rede/64 eui-64*"
3. **Autoconfiguração stateless:** "ipv6 address autoconfig [default]"
4. **DHCP statefull:** "ipv6 dhcp client"

Nas opções 1 e 2 o servidor DNS e roteador padrão deverão ser configurados manualmente. Na autoconfiguração é preciso um DHCP stateless ou configuração estática do DNS, pois o roteador padrão é passado via protocolo NDP (mensagens de RS e RA). Na opção DHCP statefull TODAS as opções são passadas pelo servidor DHCPv6, menos o roteador padrão, o qual é adquirido via NDP com a mensagem de RA (Router Advertisement).

Veja abaixo exemplos de configuração na sequência.

No primeiro exemplo vamos analisar a configuração a interface fast 0/0 com o IPv6 estático **2000:100::1/112**, já a interface fast 0/1 será configurada via **EUI-64** com o prefixo **2001:100::/64** e a interface fast 2/0 será configurada via **autoconfiguração**.

```
R1(config)#int f0/0
R1(config-if)#ipv6 address 2000:100::1/112 ?
  anycast Configure as an anycast
  eui-64 Use eui-64 interface identifier
<cr>
R1(config-if)#ipv6 address 2000:100::1/112
R1(config-if)#int f0/1
R1(config-if)#ipv6 address 2001:100::/64 eui-64
R1(config-if)#int f2/0
R1(config-if)#ipv6 address autoconfig
R1(config-if)#end
R1#
```

Com o comando "**show ipv6 interface brief**" temos um resumo das interfaces IPv6 e os endereços configurados, veja abaixo a saída para o R1 configurado anteriormente.

```
R1#sho ipv6 interface brief
FastEthernet0/0          [up/up]
  FE80::C001:33FF:FE7C:0      -> endereço de link-local via EUI-64
  2000:100::1                -> endereço global unicast estático
FastEthernet0/1          [up/up]
  FE80::C001:33FF:FE7C:1      -> link local e global usam EUI-64 e tem
  2001:100::C001:33FF:FE7C:1    -> mesmo interface ID "C001:33FF:FE7C:1"
FastEthernet2/0          [up/up]
  FE80::C001:33FF:FE7C:20     -> na autoconfig também é utilizado o
  2002:100::C001:33FF:FE7C:20   -> EUI-64 para definir a interface ID
```

Com o comando “**show ipv6 interface fast 0/0**”, por exemplo, você pode ver as opções completas referentes ao IPv6, veja exemplo abaixo da saída para as interfaces f0/0 e f2/0.

```
R1#sho ipv6 int f0/0 -> Interface usando configuração estática
FastEthernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::C001:33FF:FE7C:0 -> link local via
EUI-64 utilizando o MAC da interface
  No Virtual link-local address(es):
    Global unicast address(es):
      2000:100::1, subnet is 2000:100::/112 -> end global e subrede
  Joined group address(es): -> endereços de multicast
    FF02::1
    FF02::2
    FF02::1:FF00:1
    FF02::1:FF7C:0
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1 -> detecção de endereços
duplicados está habilitada e rodou uma vez (attempts)
  ND reachable time is 30000 milliseconds -> tempo de vida do protocolo de
descoberta de hosts vizinhos
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.

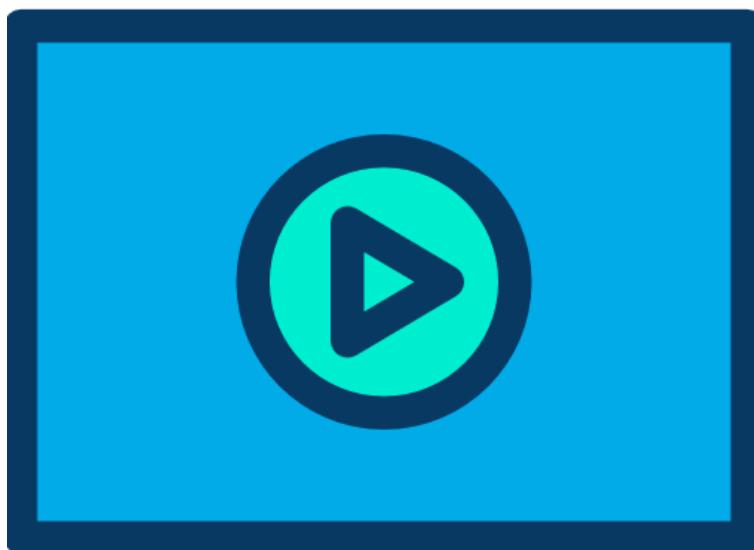
R1#
R1#sho ipv6 int fast 2/0 -> interface usando autoconfiguration
FastEthernet2/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::C001:33FF:FE7C:20
  No Virtual link-local address(es):
    Global unicast address(es):
      2002:100::C001:33FF:FE7C:20, subnet is 2002:100::/64 [EUI/CAL/PRE]
        valid lifetime 2591872 preferred lifetime 604672
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF7C:20
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
```

Quando utilizamos a autoconfiguração note na saída do comando “show ipv6 int f2/0” que embaixo do IPv6 global aparece uma linha destacada com um “lifetime” e “preferred lifetime” que são os timers do tempo de vida do prefixo recebido via NDP pelo roteador vizinho.

Como o IPv6 suporta a reconfiguração da rede (network renumbering), quando é preciso trocar um prefixo antigo por um novo é possível anunciar a rede antiga com um lifetime mais curto e a rede ou prefixo mais novo com um lifetime mais longo, para que haja a troca do antigo pelo novo. Outra opção é expirar um determinado prefixo em determinada data e hora. Isto é útil para a reconfiguração de prefixes em redes de grande porta com diversos hosts na mesma sub-rede.

O DAD (descoberta de IPs duplicados) é utilizado para verificar se não existe outro IP igual na rede. Note que na saída do comando show de ambas as interfaces têm a linha “*ND DAD is enabled, number of DAD attempts: 1*”, ou seja, o DAD está ativo e foi rodado 1 vez (number of DAD attempts: 1), ou seja, o IP configurado não deu nenhum conflito e foi ativado na interface. Se esse contador estiver diferente de 1 é sinal de que houve conflito de endereços.

9.4.2 Grupos de Multicast Padrões das Interfaces Cisco



Na saída do comando “show ipv6 interfaces” para ambas as interfaces mostradas anteriormente temos as informações sobre os grupos de multicast que elas por padrão pertencem. É importante saber essas informações porque agora não temos mais broadcast e muitas operações dependem do Multicast para funcionar.

Veja o detalhe apenas dos grupos de multicast retirados da interface fast 0/0.

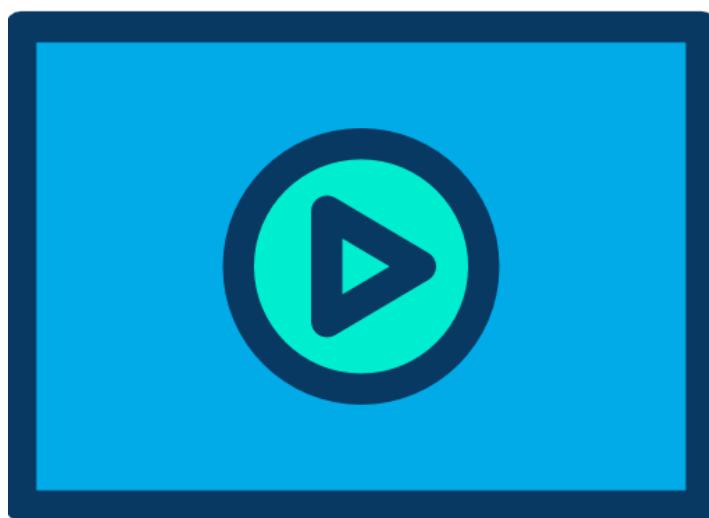
```
Joined group address(es): -> endereços de multicast
FF02::1
FF02::2
FF02::1:FF00:1
FF02::1:FF7C:0
```

Os dois primeiros grupos você deve saber, pois podem ser cobrados na prova, portanto que representam os endereços **FF02::1** e **FF02::2**?

A resposta é FF02::1 é o endereço de multicast de todos os Hosts da Rede e o FF02::2 representa todos os roteadores da rede.

O endereço **FF02::1:FF00:1** é o solicited-node do endereço global 2000:100:**::1** e o que vem logo abaixo **FF02::1:FF7C:0** é o endereço de solicited-node do endereço de link-local da interface FE80::C001:33FF:FE**7C:0**. Lembre-se que ele é formado pelo prefixo de multicast **FF02::1:FF** mais os últimos 24 bits do endereço local ou global configurado. Para cada endereço teremos um solicited-node.

9.4.3 Redes Locais e Diretamente Conectadas no IPv6



Quando configuramos interfaces no IPv6 e elas ficam UP/UP também são criadas rotas locais, apontando para a própria interface com uma máscara /128, e para a rede IPv6 que a interface pertence, conforme prefixo configurado.

Para verificar essas informações podemos utilizar o comando “**show ipv6 route**”, lembrando que para o IPv4 é “**show ip route**”. Veja exemplo da tabela de roteamento IPv6 abaixo.

```
R1#show ipv6 route
IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
      U - Per-user Static route, M - MIPv6
      I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
      O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
      ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
      D - EIGRP, EX - EIGRP external
C   2340:1111:AAAA:1::/64 [0/0]
    via ::, FastEthernet0/0
L   2340:1111:AAAA:1::1/128 [0/0]
    via ::, FastEthernet0/0
C   2340:1111:AAAA:2::/64 [0/0]
    via ::, Serial0/0
L   2340:1111:AAAA:2::1/128 [0/0]
    via ::, Serial0/0
L   FF00::/8 [0/0]
    via ::, Null0
```

Note na primeira linha em destaque temos a rede diretamente conectada à fast 0/0 2340:1111:AAAA:1::/64 (identificada com "C") e logo abaixo temos uma rota local para o endereço IP configurado nessa interface 2340:1111:AAAA:1::1/128 indicada com um "L" de Local na frente.

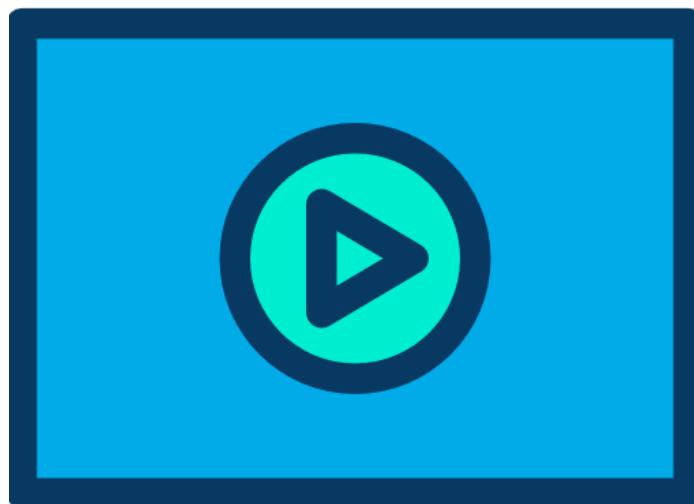
Após a rota, entre colchetes, temos as informações de distância administrativa e métrica, basicamente as mesmas informações que utilizamos no IPv4 para classificar as rotas entre diferentes protocolos de roteamento (distância administrativa) ou entre um mesmo protocolo (métrica). Para as rotas diretamente conectadas ambos os valores são zero e as regras são as mesmas que estudamos no IPv4. Por exemplo, rotas estáticas tem distância administrativa "1".

Quanto menor a distância administrativa e a métrica melhor é a rota, mesma regra de desempate que estudamos para o IPv4.

Você pode utilizar os comandos "**show ipv6 route connected**" e "**show ipv6 route local**" para verificar somente as rotas conectadas e locais respectivamente, veja exemplo abaixo.

```
R1#show ipv6 route connected
IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
C  2340:1111:AAAA:1::/64 [0/0]
  via ::, FastEthernet0/0
C  2340:1111:AAAA:2::/64 [0/0]
  via ::, Serial0/0
R1#show ipv6 route local
IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
L  2340:1111:AAAA:1::1/128 [0/0]
  via ::, FastEthernet0/0
L  2340:1111:AAAA:2::1/128 [0/0]
  via ::, Serial0/0
L  FF00::/8 [0/0]
  via ::, Null0
R1#
```

9.4.4 Testando a Conectividade das Interfaces IPv6



Como já citado, o ICMP do IPv4 foi trocado pelo protocolo ICMPv6 no IPv6, porém recursos como ping e trace continuam presentes para realizar os testes de conectividade entre hosts e interfaces IPv6. A diferença é que em determinadas versões de IOS será solicitada a interface de saída escrita de maneira completa e com o número da interface sem espaço, veja dois exemplos abaixo.

```
dltec#ping fe80::1
Output Interface: fastethernet0/0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FE80::1, timeout is 2 seconds:
Packet sent with a source address of FE80::1%FastEthernet0/0
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/4 ms
```

A justificativa do exemplo acima é simples, pois todas as interfaces têm endereços de link-local e eles iniciam com **FE80::/10**, portanto como saber para que interface encaminhar nesse caso? Somente identificando a interface de saída do ping ou traceroute.

Assim como para o IPv4 existem opções que você pode utilizar com o comando ping, veja um exemplo abaixo do ping com uma repetição de 100 vezes.

```
dltec#ping 2000:100::1 ?
  data      specify data pattern
  repeat    specify repeat count
  size      specify datagram size
  source    specify source address or name
  timeout   specify timeout interval
  verbose   verbose output
<cr>

dltec#ping fe80::1 repeat 100
Output Interface: fastethernet0/0
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to FE80::1, timeout is 2 seconds:
Packet sent with a source address of FE80::1%FastEthernet0/0
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 0/0/4 ms
```

Podemos também utilizar o ping estendido digitando apenas “ping”, dando um “enter” e no momento de escolher o protocolo digite “ipv6”, veja exemplo abaixo.

```
dltec#ping
Protocol [ip]: ipv6
Target IPv6 address: fe80::1
Repeat count [5]: 100
Datagram size [100]: 1000
Timeout in seconds [2]:
Extended commands? [no]: y
Source address or interface: fastethernet0/0
UDP protocol? [no]:
Verbose? [no]:
Precedence [0]:
DSCP [0]:
Include hop by hop option? [no]: y
Include destination option? [no]:
Sweep range of sizes? [no]:
Output Interface: fastethernet0/0
Type escape sequence to abort.
Sending 100, 1000-byte ICMP Echos to FE80::1, timeout is 2 seconds:
Packet sent with a source address of FE80::1%FastEthernet0/0
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 0/0/4 ms
```

Veja abaixo exemplo de traceroute no Cisco IOS. Os asteriscos representam que a partir do segundo salto não houve resposta, pois, a mesma simbologia de problemas que estudamos para o ping e trace no IPv4 continua a mesma no IPv6. Para cancelar os testes ainda podemos utilizar a sequência de saída “**ctrl+shift+6**”.

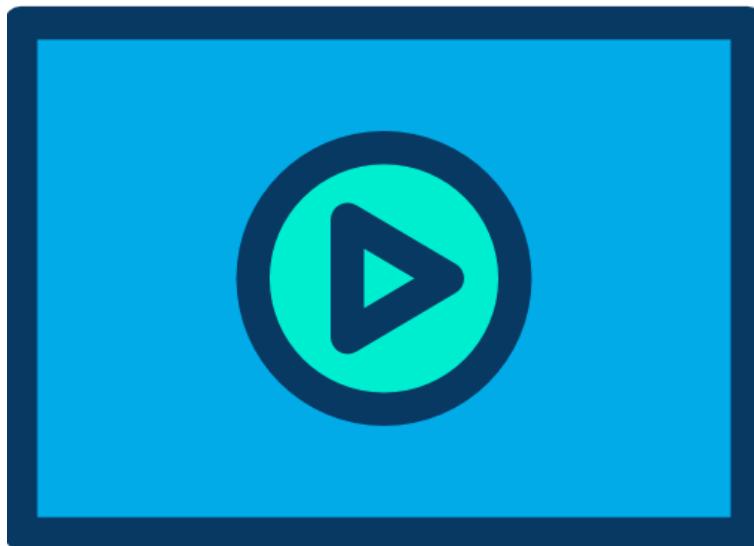
```
R1#traceroute 2340:1111:AAAA:3:C006:22FF:FEEC:0
Type escape sequence to abort.
Tracing the route to 2340:1111:AAAA:3:C006:22FF:FEEC:0

 1 2340:1111:AAAA:2::2 4 msec 8 msec 12 msec
 2 * * *
 3 * * *
R1#
```

Você pode também forçar que o ping e o traceroute seja através do IPv6 quando fizer um teste para um nome de domínio, por exemplo, “**ping ipv6 www.ietf.org**”.

Antes de iniciar a configuração de protocolo de roteamento ou recursos mais avançados em seus laboratórios lembre-se sempre de primeiro verificar a conectividade das interfaces através do ping. Teste tanto com os IPs globais como locais, iniciando sempre pelo de link-local, assim se houver um problema de camada 2 ou 3 simples você resolverá antes da ativação do roteamento e pode evitar tempo perdido tentando resolver um problema que não existe!

9.4.5 Verificando Vizinhos IPv6 – Protocolo NDP



Uma vez configuradas as interfaces você pode iniciar os testes de ping, traceroute, telnet para verificar a conectividade em camada 3 até a 7, porém lembre-se que para os vizinhos em uma LAN se comunicarem um protocolo novo entrou no lugar do ARP chamado NDP.

O NDP funciona automaticamente, sem necessidade de configurações, e a tabela de vizinhanças pode ser visualizada com o comando “**show ipv6 neighbors**”. Veja exemplo abaixo.

```
R2#ping ff02::1
Output Interface: fastethernet0/0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FF02::1, timeout is 2 seconds:
Packet sent with a source address of FE80::C005:22FF:FEEC:0

Reply to request 0 received from FE80::C006:22FF:FEEC:0, 32 ms
Reply to request 1 received from FE80::C006:22FF:FEEC:0, 24 ms
Reply to request 2 received from FE80::C006:22FF:FEEC:0, 16 ms
Reply to request 3 received from FE80::C006:22FF:FEEC:0, 20 ms
Reply to request 4 received from FE80::C006:22FF:FEEC:0, 20 ms
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/22/32 ms
5 multicast replies and 0 errors.

R2#show ipv6 neighbors
IPv6 Address          Age Link-layer Addr State Interface
FE80::C006:22FF:FEEC:0      0 c206.22ec.0000  REACH Fa0/0
2340:1111:AAAA:3:C006:22FF:FEEC:0      9 c206.22ec.0000  STALE Fa0/0
```

R2#

Note que iniciamos o teste pingando o endereço de multicast de todos os nós da rede, assim os clientes de rede que não tem bloqueio de segurança contra esse tipo de teste irão responder e teremos entradas na tabela de vizinhança do IPv6.

Os endereços descobertos têm o mesmo final C006:22FF:FEEC:0, por isso podemos concluir que é um endereço Global Unicast (faixa do 2000::/3) e seu link-local, ambos criados a partir do EUI-64. Note que ambos os endereços têm o mesmo endereço MAC.

Essa tabela é dinâmica e apagada de tempos em tempos, assim como uma entrada ARP que tem seu “aging-time” e é apagada após certo tempo sem atividade daquele endereço.

Podemos apagar a tabela de vizinhos com o comando “**clear ipv6 neighbors**”, veja exemplo abaixo:

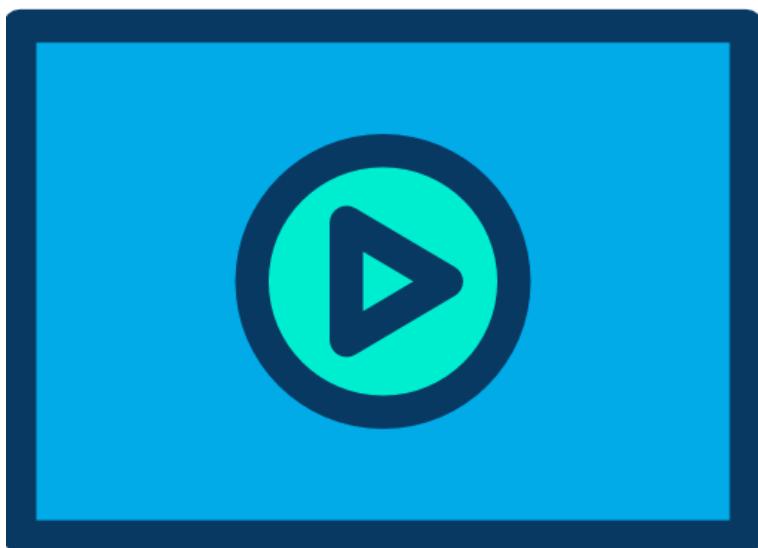
```
R2#clear ipv6 neighbors
R2#show ipv6 neighbors
R2#
```

Portanto, após o clear a tabela de vizinhos IPv6 está vazia e não mostra nenhuma entrada com o comando “show ipv6 neighbors”.

10 Clientes de Rede: MAC OS, Linux e Windows

Os clientes de rede conectam-se através de suas placas de rede e normalmente recebem as informações necessárias para acessar os serviços e aplicativos da rede de forma automática através de um servidor DHCP (para IPv4) ou DHCPv6 (para IPv6).

Existe uma infinidade de opções, modelos e marcas de interfaces ou placas de rede (NIC - Network Interface Cards), porém basicamente todas obedecem as normas definida pela IEEE (Institute of Electrical and Electronics Engineers - pronunciado "Eye-triple-E" em inglês ou "I-três-É" em português) relacionada às famílias Ethernet que elas conseguem suportar, por exemplo, Ethernet a 10Mbps ou Fastethernet a 100Mbps ou GigabitEthernet a 1000Mbps ou os três sendo 10/100/1000 Mbps.



10.1 Verificando Informações da Camada-2

Uma placa de rede é classificada na camada de enlace do Modelo OSI (camada-2 ou layer-2), pois ela toma suas decisões inicialmente através do endereço MAC que vem gravado em sua memória ROM de fábrica.

Portanto, basicamente quando sua placa de rede recebe um quadro de camada-2 ela verifica se aquele MAC de destino do quadro é igual ao gravado nela para saber se deve ou não processar aquela informação, se for igual ela vai processar, ou seja, remove as informações de camada-2 e passa as informações recebidas dentro do payload do quadro para a camada de Internet (protocolo IP).

Se o MAC de destino do quadro for diferente a placa de rede descarta as informações, pois não são para ela.

A exceção disso é quando no MAC de destino temos um broadcast (FFFF.FFFF.FFFF) ou um endereço de Multicast no qual a placa de rede faz parte daquele grupo, aí mesmo não sendo o MAC de destino igual ao gravado nela a informação é tratada.

Essa é a forma padrão de trabalho da placa de rede em camada-2, porém existe a possibilidade de colocar a placa de rede em modo "promiscuo" e passar a escutar ou "sniffar" a rede, ou seja, ela captura tudo o que vem e repassar para cima. Normalmente esse processo é feito para análise de rede com softwares como o Wireshark ou então para fins de espionagem mesmo (não aconselhado por ser crime!).

Sobre o endereço MAC ele é composto por 48 bits (escrito em 12 algarismos Hexadecimais) e dividido em duas partes: OUI (24 primeiros bits) + Serial (últimos 24 bits). O OUI é o fabricante da placa de rede e o serial é um número de série que garante que não existam duas placas de redes iguais no mundo, pelo menos não se ela for fabricada legalmente e não seja "pirata"...

Você pode ver o MAC da sua placa de rede no Windows com o comando "**ipconfig /all**" e no Linux/MAC com o comando "**ifconfig**".

Veja exemplo abaixo que tirei do meu computador que tem o Linux Mint, note que a interface se chama "eth0", no MAC normalmente ela vai se chamar "en0" e no Windows o nome é mais comprido como "Local area connection" ou "Conexão local de rede".

```
marcelo@marcelo-Vostro-3550 ~ $ ifconfig
eth0      Link encap:Ethernet HWaddr 24:b6:fd:06:dc:17
          inet addr:192.168.1.27 Bcast:192.168.1.255 Mask:255.255.255.0
          inet6 addr: fe80::26b6:fdff:fe06:dc17/64 Scope:Link
          inet6 addr: 2000::e0de:be9a:700c:5967/64 Scope:Global
          inet6 addr: 2000::26b6:fdff:fe06:dc17/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:681622 errors:0 dropped:0 overruns:0 frame:0
          TX packets:495930 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:885195955 (885.1 MB) TX bytes:58536729 (58.5 MB)
lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:65536 Metric:1
          RX packets:7041 errors:0 dropped:0 overruns:0 frame:0
          TX packets:7041 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:796613 (796.6 KB) TX bytes:796613 (796.6 KB)
marcelo@marcelo-Vostro-3550 ~ $
```

Com o OUI você consegue descobrir o fabricante da sua placa de rede em vários sites da Internet caso você precise da informação e não tenha. Um exemplo é o site <http://www.macvendorlookup.com/> basta copiar e colar o MAC que ele traz o fabricante.

Outra opção para o Linux é o comando “ip addr show [interface]”. Veja exemplo dado para verificar a interface ens33:

```
osboxes@osboxes:~$ ip addr show ens33
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN
group default qlen 1000
    link/ether 00:0c:29:64:16:33 brd ff:ff:ff:ff:ff:ff
        inet 192.168.112.129/24 brd 192.168.112.255 scope global dynamic
          noupdate
          valid_lft 1709sec preferred_lft 1709sec
        inet6 fe80::1974:92b3:41e7:dab2/64 scope link noupdate
          valid_lft forever preferred_lft forever
```

Veja a saída do ipconfig para uma máquina com Windows 10. Note que esse PC tem duas placas de rede, porém está utilizando a interface de rede sem fio no momento.

C:\>ipconfig /all

Configuração de IP do Windows

```
Nome do host. . . . . : LAPTOP-RNNLUMEM
Sufixo DNS primário . . . . . :
Tipo de nó. . . . . : híbrido
Roteamento de IP ativado. . . . . : não
Proxy WINS ativado. . . . . : não
```

Adaptador Ethernet Ethernet:

```
Estado da mídia. . . . . : mídia desconectada
Sufixo DNS específico de conexão. . . . . :
Descrição . . . . . : Realtek PCIe FE Family
Controller
Endereço Físico . . . . . : 98-83-89-F0-5A-59
DHCP Habilitado . . . . . : Sim
Configuração Automática Habilitada. . . . . : Sim
```

Adaptador de Rede sem Fio Wi-Fi:

```
Sufixo DNS específico de conexão. . . . . :
Descrição . . . . . : Qualcomm Atheros QCA9377
Wireless Network Adapter
Endereço Físico . . . . . : 98-83-89-E6-EE-82
DHCP Habilitado . . . . . : Sim
Configuração Automática Habilitada. . . . . : Sim
Endereço IPv6 . . . . . : 2804: . . . :34b0(Preferencial)
Endereço IPv6 Temporário. . . . . : 2804: . . . :666f(Preferencial)
Endereço IPv6 de link local . . . . . :
fe80::214b:a66f:5437:34b0%17(Preferencial)
Endereço IPv4. . . . . : 192.168.1.76(Preferencial)
Máscara de Sub-rede . . . . . : 255.255.255.0
Concessão Obtida. . . . . : quarta-feira, 25 de março de
2020 02:49:57
Concessão Expira. . . . . : quarta-feira, 25 de março de
2020 12:49:56
Gateway Padrão. . . . . : fe80::1%17
                                         192.168.1.254
Servidor DHCP . . . . . : 192.168.1.254
IAID de DHCPv6. . . . . : 110658441
```

```
DUID de Cliente DHCPv6. . . . . : 00-01-00-01-24-65-70-BA-98-83-  
89-F0-5A-59  
Servidores DNS. . . . . : fe80::1%17  
192.168.1.254  
fe80::1%17  
NetBIOS em Tcpip. . . . . : Habilitado
```

No MAC OS podemos também utilizar o comando ifconfig como do Linux ou o comando "networksetup -listallhardwarereports". Veja abaixo a saída do comando "ifconfig" com o MAC address das portas físicas destacadas.

```
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384  
      options=3<RXCSUM,TXCSUM>  
      inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1  
        inet 127.0.0.1 netmask 0xff000000  
          inet6 ::1 prefixlen 128  
  
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280  
  
stf0: flags=0<> mtu 1280  
  
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500  
      options=2b<RXCSUM,TXCSUM,VLAN_HWTAGGING,TSO4>  
      ether a8:20:66:16:95:59  
        inet6 fe80::aa20:66ff:fe16:9559%en0 prefixlen 64 scopeid 0x4  
          inet 172.16.21.88 netmask 0xfffffe00 broadcast 172.16.21.255  
            media: autoselect (1000baseT <full-duplex,energy-efficient-ethernet>)  
              status: active  
  
en1: flags=8823<UP,BROADCAST,SMART,SIMPLEX,MULTICAST> mtu 1500  
      ether 20:c9:d0:c9:18:1b  
      media: autoselect (<unknown type>)  
      status: inactive
```

10.2 Verificando Informações da Camada-3

Lembre-se que as placas de rede estão na camada-2 do modelo OSI e as propriedades de camada-3 estão no protocolo IP que faz parte da pilha do TCP/IP instalado no driver de rede dos computadores.

Por padrão uma placa de rede não precisa ser configurada, uma vez instalada corretamente ela ativa automaticamente o serviço de DHCP cliente para o IP versão 4 (IPv4) e para o IP versão 6 (IPv6) dependendo do sistema operacional (chamado DHCPv6).

O cliente DHCP (Dynamic Host Configuration Protocol) faz com que o computador envie uma solicitação para o servidor DHCP alocar um endereço da sua lista disponível de IPs, por isso nada precisa ser feito e desde que o serviço esteja presente na rede os computadores navegam pela Internet sem necessidade de configurações adicionais na rede.

No caso do IPv6 existem outras opções de alocação dinâmica de IPs como o SLAAC (Stateless Address Autoconfiguration) em conjunto com o DHCPv6 Stateless, porém isso normalmente é definido pelo administrador de redes e os clientes não precisam fazer nada em suas placas de rede, ou seja, isso tudo é transparente para os usuários finais da rede.

No caso de servidores ou se você necessitar definir de forma manual o endereço de camada-3 no seu computador isso é feito com a alocação de um "**IP Fixo**" no dispositivo. Para isso você precisa de alguns parâmetros mínimos para a configuração, segue a lista:

- Endereço IP a ser usado no computador
- Máscara de sub-rede
- Endereço do gateway (roteador padrão local)
- Pelo menos um endereço de servidor DNS

Esses parâmetros são necessários tanto para o IPv4 quanto para o IPv6 alocado manualmente, ou seja, IPv4 ou IPv6 fixo.

Os mesmos comandos utilizados para verificar as informações de camada-2 podem ser utilizados para verificar os parâmetros da camada de Rede ou Internet para os três sistemas operacionais, ou seja, **ipconfig /all** para o **Windows** e **ifconfig** para **Linux** e **MAC**.

Linux

```
marcelo@marcelo-Vostro-3550 ~ $ ifconfig
eth0      Link encap:Ethernet HWaddr 24:b6:fd:06:dc:17
          inet addr:192.168.1.27 Bcast:192.168.1.255 Mask:255.255.255.0
          inet6 addr: fe80::26b6:fdff:fe06:dc17/64 Scope:Link
          inet6 addr: 2000::e0de:be9a:700c:5967/64 Scope:Global
          inet6 addr: 2000::26b6:fdff:fe06:dc17/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:681622 errors:0 dropped:0 overruns:0 frame:0
          TX packets:495930 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:885195955 (885.1 MB) TX bytes:58536729 (58.5 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:65536 Metric:1
          RX packets:7041 errors:0 dropped:0 overruns:0 frame:0
          TX packets:7041 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:796613 (796.6 KB) TX bytes:796613 (796.6 KB)
```

Note que em interfaces Linux temos listados os endereços IPv4 como "inet addr" e IPv6 como "inet6 addr".

A interface Eth0 tem o endereço IPv4 192.168.1.27, com broadcast 192.168.1.255 e sua máscara de sub-rede 255.255.255.0.

Além disso ela possui um endereço IPv6 de Link Local (identificado como Scope:Link) e dois endereços GUA (endereços Globais de Unicast identificados com Scope:Global).

Os endereços IPv6 são:

1. **Link local:** fe80::26b6:fdff:fe06:dc17/64
2. **GUA1:** 2000::e0de:be9a:700c:5967/64
3. **GUA2:** 2000::26b6:fdff:fe06:dc17/64

Portanto os três endereços IPv6 estão utilizando prefixo "/64".

Já a interface Lo (loopback) utiliza os IPs 127.0.0.1 e ::1 que são padrões para o IPv4 e IPv6 respectivamente.

Outra opção para o Linux é o comando "ip addr show [interface]". Veja exemplo abaixo dado para verificar a interface ens33:

```
osboxes@osboxes:~$ ip addr show ens33
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN
group default qlen 1000
    link/ether 00:0c:29:64:16:33 brd ff:ff:ff:ff:ff:ff
    inet 192.168.112.129/24 brd 192.168.112.255 scope global dynamic
        noproxyroute ens33
            valid_lft 1709sec preferred_lft 1709sec
    inet6 fe80::1974:92b3:41e7:dab2/64 scope link noproxyroute
        valid_lft forever preferred_lft forever
```

Tanto o Linux como o MAC OS não mostram informações sobre os servidores DHCP e DNS nessa saída de comando.

Windows

```
C:\>ipconfig /all
```

Configuração de IP do Windows

```
Nome do host . . . . . : LAPTOP-RNNLUMEM
Sufixo DNS primário . . . . . :
Tipo de nó . . . . . : híbrido
Roteamento de IP ativado. . . . . : não
Proxy WINS ativado. . . . . : não
```

Adaptador Ethernet Ethernet:

```
Estado da mídia. . . . . : mídia desconectada
Sufixo DNS específico de conexão. . . . . :
Descrição . . . . . : Realtek PCIe FE Family
Controller
Endereço Físico . . . . . : 98-83-89-F0-5A-59
DHCP Habilitado . . . . . : Sim
Configuração Automática Habilitada. . . . . : Sim
```

Adaptador de Rede sem Fio Wi-Fi:

```
Sufixo DNS específico de conexão. . . . . :
Descrição . . . . . : Qualcomm Atheros QCA9377
Wireless Network Adapter
Endereço Físico . . . . . : 98-83-89-E6-EE-82
DHCP Habilitado . . . . . : Sim
Configuração Automática Habilitada. . . . . : Sim
Endereço IPv6 . . . . . : 2804: . . . :34b0(Preferencial)
Endereço IPv6 Temporário. . . . . : 2804: . . . :666f(Preferencial)
Endereço IPv6 de link local . . . . . :
fe80::214b:a66f:5437:34b0%17(Preferencial)
Endereço IPv4. . . . . : 192.168.1.76(Preferencial)
Máscara de Sub-rede . . . . . : 255.255.255.0
Concessão Obtida. . . . . : quarta-feira, 25 de março de
2020 02:49:57
Concessão Expira. . . . . : quarta-feira, 25 de março de
2020 12:49:56
Gateway Padrão. . . . . : fe80::1%17
192.168.1.254
Servidor DHCP . . . . . : 192.168.1.254
IAID de DHCPv6. . . . . : 110658441
DUID de Cliente DHCPv6. . . . . : 00-01-00-01-24-65-70-BA-98-83-
89-F0-5A-59
Servidores DNS. . . . . : fe80::1%17
192.168.1.254
fe80::1%17
NetBIOS em Tcpip. . . . . : Habilitado
```

No Windows, nesse exemplo especificamente, temos duas interfaces ou adaptadores, sendo que o primeiro que é da rede cabeada está desconectado, já o segundo da rede sem fio está conectado e configurado, por isso vamos analisar os parâmetros para essa interface.

Note que a saída traz primeiro os endereços IPv6, depois IPv4 e na sequência informação de gateway e DNS. Os endereços IPv6 foram suprimidos propositalmente.

- Endereço IPv6: 2804: ... :34b0
- Endereço IPv6 Temporário: 2804: ... :666f
- Endereço IPv6 de link local: fe80::214b:a66f:5437:34b0%17 (prefixo /17)
- Endereço IPv4: 192.168.1.76
- Máscara de Sub-rede: 255.255.255.0
- Gateway Padrão: fe80::1%17 (IPv6) e 192.168.1.254 (IPv4)
- Servidores DNS: fe80::1%17 (IPv6) e 192.168.1.254 (IPv4)

O Windows não mostrou o prefixo dos endereços IPv6 GUA (os dois primeiros) porque eles estão no padrão que é /64.

MAC OS

```
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
      options=3<RXCSUM,TXCSUM>
      inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
      inet 127.0.0.1 netmask 0xff000000
      inet6 ::1 prefixlen 128

en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
      options=2b<RXCSUM,TXCSUM,VLAN_HWTAGGING,TSO4>
      ether a8:20:66:16:95:59
      inet6 fe80::aa20:66ff:fe16:9559%en0 prefixlen 64 scopeid 0x4
      inet 172.16.21.88 netmask 0xfffffe00 broadcast 172.16.21.255
      media: autoselect (1000baseT <full-duplex,energy-efficient-ethernet>)
      status: active

en1: flags=8823<UP,BROADCAST,SMART,SIMPLEX,MULTICAST> mtu 1500
      ether 20:c9:d0:c9:18:1b
      media: autoselect (<unknown type>)
      status: inactive
```

Note que no MAC OS a saída é muito parecida com o Linux, até as nomenclaturas "inet" para IPv4 e "inet6" para IPv6 são as mesmas.

Portanto na Interface loopback (lo0) temos os endereços de loopback padrões para o IPV4 (127.0.0.1) e IPV6 (::1).

Na interface en0 (porta de rede ethernet 0) temos um endereço IPv6 de Link Local e um endereço IPv4, provavelmente nessa porta não foi configurado nenhum IPv6 Global ou GUA.

- IPv4 (inet): 172.16.21.88
- Máscara (netmask): 0xfffffe00
- Broadcast: 172.16.21.255
- IPv6 de Link Local (inet6): fe80::aa20:66ff:fe16:9559
- Prefixo (prefixlen): 64

10.2.1 Verificando DNS e Gateway no Linux e MAC OS

Para verificação do gateway no Linux podemos utilizar o comando “ip route”, veja abaixo:

```
osboxes@osboxes:~$ ip route
default via 192.168.112.2 dev ens33 proto dhcp metric 100
169.254.0.0/16 dev ens33 scope link metric 1000
192.168.112.0/24 dev ens33 proto kernel scope link src 192.168.112.129 metric 100
```

A informação do gateway vem com o nome “default via” e tem o endereço no exemplo acima 192.168.112.2.

Outra opção é o comando “netstat -rn”, o qual funciona tanto no Linux como no MAC OS. Veja saída abaixo.

```
osboxes@osboxes:~$ netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask        Flags   MSS Window irtt Iface
0.0.0.0         192.168.112.2  0.0.0.0        UG        0 0          0 ens33
... saídas omitidas
```

No Linux o gateway é representado pela rede 0.0.0.0 (rota para Internet) e no campo Gateway você tem o endereço dele, que no exemplo acima é 192.168.112.2.

No MAC OS fica um pouco diferente, a informação está no campo Destination e vem como o nome **default** e o IP está no campo Gateway, nesse exemplo o gateway é 192.168.20.1. Veja abaixo.

```
$ netstat -rn
Routing tables

Internet:
Destination     Gateway         Flags       Refs      Use     Netif Expire
default         192.168.20.1    UGSc        39          0     en0
127.0.0.1       127.0.0.1      UH          3     11132     lo0
... saídas omitidas
```

Para verificar o DNS no Linux você tem várias opções, mas vamos ensinar duas delas:

- Comando NSLookup
- Verificando o arquivo de configuração resolv.conf

Veja abaixo os dois exemplos de comando. Note que o endereço do DNS nesses exemplos é 127.0.0.53.

```
osboxes@osboxes:~$ nslookup dltec.com.br
Server:           127.0.0.53
Address:          127.0.0.53#53
```

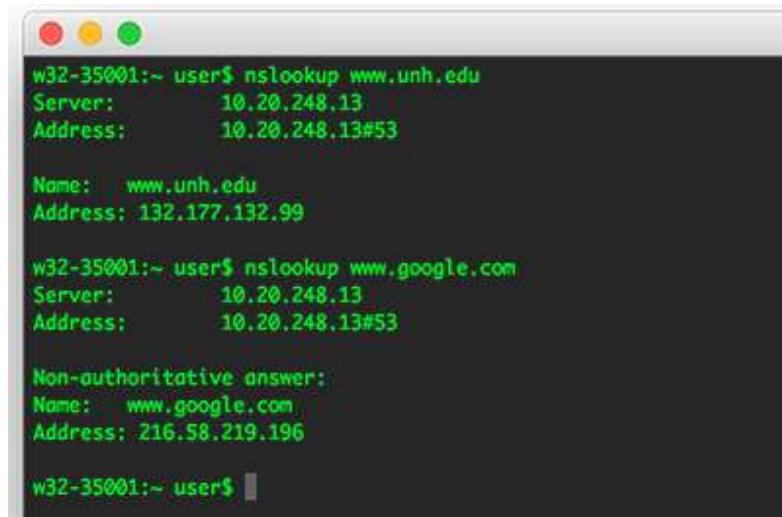
Non-authoritative answer:
Name: dltec.com.br
Address: 198.57.234.87

```
osboxes@osboxes:~$ cat /etc/resolv.conf
# ... saídas omitidas

nameserver 127.0.0.53
options edns0
```

search localdomain

No MAC OS você também tem diversas formas de encontrar seu DNS, seja de forma gráfica ou via comando. Veja abaixo como encontrar o servidor DNS via o comando **NSLookup**.



```
w32-35001:~ user$ nslookup www.unh.edu
Server:      10.20.248.13
Address:     10.20.248.13#53

Name:   www.unh.edu
Address: 132.177.132.99

w32-35001:~ user$ nslookup www.google.com
Server:      10.20.248.13
Address:     10.20.248.13#53

Non-authoritative answer:
Name:   www.google.com
Address: 216.58.219.196

w32-35001:~ user$
```

11 Conclusão e Certificado

Parabéns por ter chegado ao final do curso **Fundamentos de Redes Cisco!**

Tenha certeza de que compreendeu todos os conceitos aqui mostrados.

Não esqueça que você deve ler e assistir tudo para obter o seu certificado de conclusão do curso.

Ficamos por aqui e nos encontramos nos próximos cursos!!!!