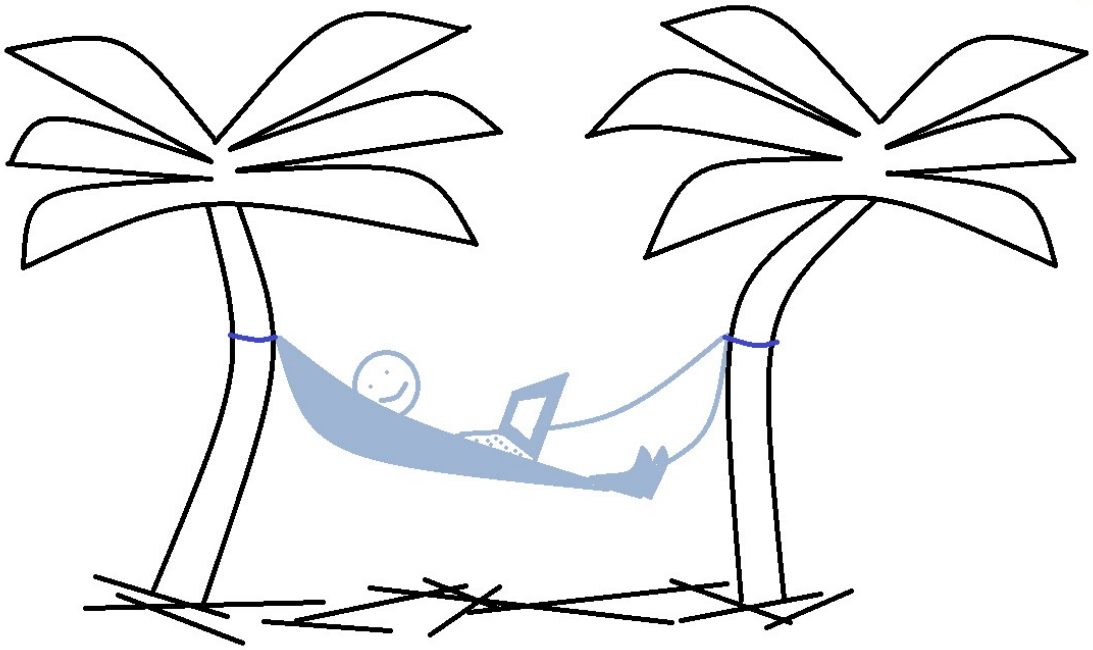
DESATANDO OS NÓS DA REDE

Conceitos básicos e configurações de *switch*

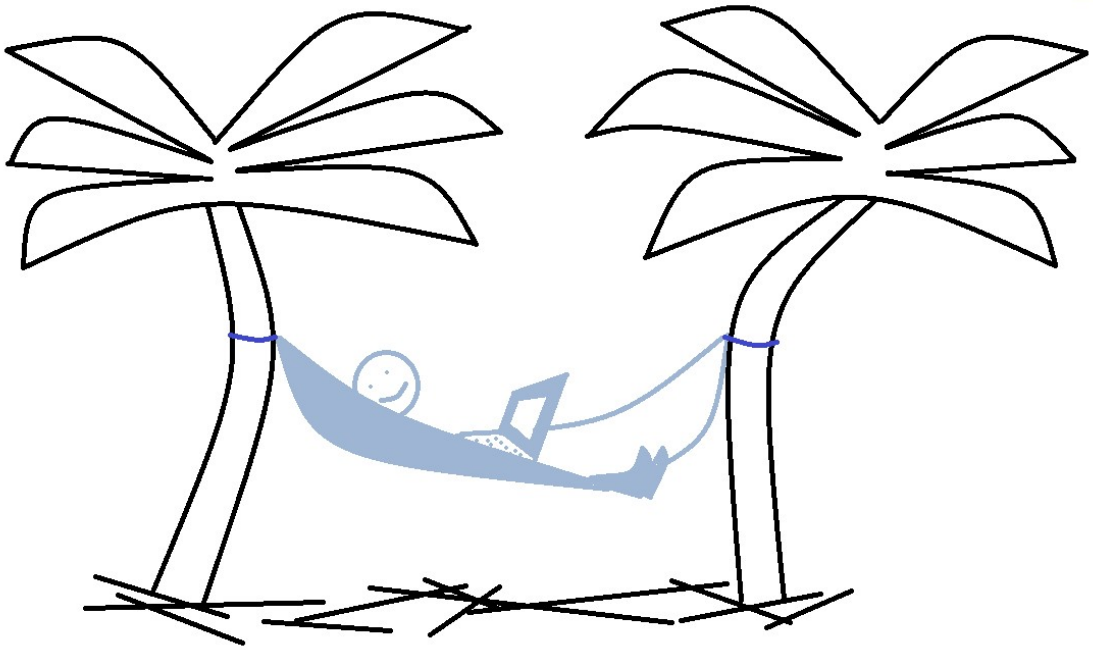


VITAL PEREIRA DOS SANTOS JUNIOR

editora IFC

DESATANDO OS NÓS DA REDE

Conceitos básicos e configurações de *switch*



editora IFC

EDITORA DO INSTITUTO FEDERAL CATARINENSE
Rua das Missões, 100 - Ponta Aguda
CEP: 89.051-000 – Blumenau/SC
www.editora.ifc.edu.br

Editora filiada a:
ASSOCIAÇÃO BRASILEIRA
DAS EDITORAS UNIVERSITÁRIAS

Obra
Desatando os nós da rede: conceitos básicos e configurações de *switch*

Autor
Vital Pereira dos Santos Junior

Capa
Vital Pereira dos Santos Junior

Projeto Gráfico e Diagramação
Vital Pereira dos Santos Junior

Dados Internacionais de Catalogação na Publicação (CIP)
Instituto Federal Catarinense – Biblioteca do Campus Blumenau

S237d

Santos Júnior, Vital Pereira dos
Desatando os nós da rede : conceitos básicos e configurações de switch [recursos eletrônico]. / Vital Pereira dos Santos Júnior. – Blumenau: Ed. IFC , 2021.

Inclui bibliografias.
Disponível somente na versão eletrônica.
ISBN 978-65-88089-08-8

1. Redes de computadores. 2. Rede de computador – Protocolo. 3. Jogos. I. Título.

CDD 004.6

Ficha catalográfica elaborada pela Bibliotecária Viviane da Rosa Matos (CRB 14/1185)

Sumário

1.Introdução

***Link* de Apresentação**: https://youtu.be/H0NN1OjhlTs

Esta obra tem como foco o estudo das redes de computadores, assunto fundamental e relevante, principalmente se levarmos em conta o volume de dados que trafegam em todo mundo através dos roteadores, *switches* e demais dispositivos de redes. A importância do tema se reflete no dia-a-dia da população mundial com uma abrangência sem precedentes, tornando tal tecnologia indispensável.

Percebe-se que, para viver de forma mais adequada no mundo de hoje, se faz necessário entender o mínimo de tecnologia. Assim como a palavra "analfabeto" serve para identificar o indivíduo que não sabe ler nem escrever, o termo "analfabeto tecnológico" ou "analfabeto digital" refere-se aqueles que não conseguem compreender o suficiente para usufruir deste mundo da tecnologia digital.

Observa-se também que a tecnologia trouxe uma velocidade espantosa nas mudanças, tornando a própria tecnologia sucessivamente obsoleta em um curto espaço de tempo, sendo complementada ou substituída por outras. As mudanças cada vez maiores nos mostram que precisamos constantemente nos aprofundar, pois o que aprendemos ontem talvez não se aplique de forma adequada no dia de hoje.

Portanto, este livro tem como objetivo apresentar de forma didática os fundamentos das redes de computadores. Se trata daquela base de conhecimento que tem poucas chances de mudar a curto prazo, contudo também serão apresentadas informações bem atuais sobre o tema, com conteúdo de ponta.

1.1. Como estudar com este e-book

Cada capítulo desse *e-book* tem disponível, além da parte textual, vários *links* de vídeos de aulas postadas no YouTube. Use este material da forma como seu cérebro melhor assimila as informações. Quero dizer com isso que, se desejar, pode ler todo o *e-book* e só depois assistir as videoaulas, pode ler e assistir os vídeos que encontrar na sequência da leitura, pode também ver primeiro todos os vídeos, de preferência com uma pipoca para acompanhar. Se você já conhece uma parte do assunto abordado aqui, então vá direto ao que lhe interessa. Parte do assunto é explicado com detalhes mais práticos e, em alguns momentos, são sugeridos exercícios de fixação para um aprendizado mais consistente. Os *links* das videoaulas e demais materiais necessários estarão disponíveis ao longo do *e-book*, algumas vezes no início dos capítulos, entretanto existem vários *links* distribuídos por serem pertinentes ao assunto naquele momento.

Por fim, acho muito interessante a ideia de imprimir este *e-book*, já que assim será aproveitado um potencial enorme de aprendizado, permitindo rabiscos e anotações diversas de forma fácil e intuitiva. Também compartilhe com quem quiser e se desejar faça contato comigo pelo canal do YouTube.

1.2. Material de apoio

Por meio de um canal do YouTube, conhecido como “Canal do Vital”, estão todos os vídeos necessários que darão apoio a este *e-book*, além de outras contribuições do autor. Por este canal você poderá ainda utilizar a opção de comentários, fazendo perguntas, dando suas opiniões, sugestões e contribuições em geral. Seus comentários são muito importantes, pois além de enriquecer o canal, as dúvidas ou sugestões poderão ajudar outras pessoas que tenham as mesmas indagações, bem como possibilitará melhorias nas novas edições do livro. Importante também contribuir com as tão conhecidas maneiras de tornar o canal mais difundido para o maior número de pessoas, que são as curtidas, compartilhamentos e inscrição no canal, além da ativação do sininho para notificação de novos vídeos.

***Link* do Canal do Vital**:

https://www.youtube.com/c/CanaldoVitalJr

1.3. Agradecimentos

Quero agradecer a inteligência suprema do Universo e causa primária de todas as coisas por me inspirar na elaboração desta obra. Como este material foi escrito com base na experiência adquirida na prática docente, agradeço imensamente a todos os alunos, professores, coordenadores e demais profissionais do ensino e da tecnologia que, de forma direta ou indireta, ajudaram a identificar maneiras mais adequadas de ensinar e/ou aprender o assunto. Um agradecimento especial ao professor Hylson Vescovi Netto pelo incentivo na publicação deste livro, principalmente por suas palavras durante nossas conversas ou mesmo por suas ações, sempre buscando formas de disseminar o conhecimento.

Não sei se seria exatamente um agradecimento nesse caso, mas a pandemia do Corona Vírus de 2020/2021 foi, sem dúvida alguma, um propulsor poderoso. Com o isolamento social comecei a gravar videoaulas e, depois de vários vídeos, surgiu a ideia de textualizar essas aulas. O resultado final é este *e-book* recheado de *links* de aulas gravadas, contribuindo assim para entender melhor o tema “Redes de Computadores”, ou seja, ajudando a desatar os nós da rede.

2.Entendendo o funcionamento das Redes

Durante a leitura da introdução deste livro você já deve ter percebido a importância do tema “Redes de Computadores”, e provavelmente está se perguntando: Como é possível a comunicação entre um computador e outro, mesmo estando do outro lado do mundo? Bem, para responder esta simples pergunta é necessária uma explicação de certa forma ampla, mas que pode ser respondida de maneira satisfatória lendo este *e-book*, assistindo todas as videoaulas e realizando os exercícios propostos.

De maneira sucinta e objetiva pode-se tentar iniciar a resposta com o que considero as três palavras-chave:

MATEMÁTICA BINÁRIA – DISPOSITIVOS DE REDE – MEIOS DE TRANSMISSÃO

A Figura 1 representa uma ilustração das palavras-chave, permitindo assim uma visão geral do que é uma rede de computadores.

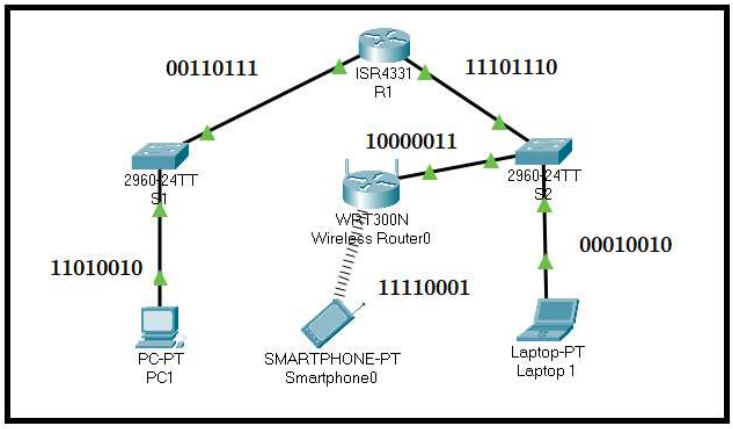


Figura 1: Exemplo de uma Rede de Computadores

Observe a matemática binária sendo representada pelos números 0 e 1, onde o “zero” consiste na não passagem de energia e o “um” na passagem de energia elétrica, tornando possível a representação de todos os caracteres utilizados na comunicação entre as pessoas. Além disso, esta forma binária de codificar as informações é adequada para serem processadas nos vários dispositivos, como computadores, *switches*, roteadores e *smartphones*. Temos também os meios de transmissão ou de comunicação, como os cabos de rede ou ainda sem fio.

2.1. Dispositivos de Rede

Na Figura 1 percebemos a representação de dois *switches* identificados como “S1” e “S2”, mais dois roteadores, sendo um que permite apenas a conexão de cabos, etiquetado com “R1” e outro sem fio, apresentado com o nome de “WRT 300N – Wireless Router0”. Tanto *switches* como roteadores são dispositivos que intermediam a conexão entre os dispositivos finais, entretanto tem funções distintas (ALECRIM, 2019).

Apesar de não estar sendo representado no nosso exemplo por se tratar de equipamento mais antigo, existe também um outro dispositivo intermediário chamado “hub”, como o da Figura 2. Sua função consiste em receber pacotes de dados em uma porta e encaminhá-los para todas as outras portas. O *switch* também recebe pacotes em uma porta, porém, ao invés de sempre enviar para todas as outras portas, envia apenas para uma porta específica, ou seja, aquela que realmente é o destino do pacote. Com isso o desempenho da rede melhora muito, tornando o *switch* o substituto natural do *hub* ao longo da história, ao ponto de raramente encontrarmos redes com este dispositivo atualmente.

Figura 2: Um antigo *hub*

O *switch* tem essa capacidade que o distingue do *hub* justamente porque ele é dotado de uma memória volátil que, a partir do momento que o dispositivo é ligado, ele começa a “aprender” qual é o endereço de cada dispositivo conectado a ele. Assim, em pouco tempo o *switch* terá registrado em sua memória que, por exemplo, na porta 1 existe uma conexão com o “Computador A”, na porta 2 com o “Computador B”, e assim sucessivamente. Na Figura 3 mostramos um *switch* Cisco de 48 portas.

Figura 3: *Switch* da Cisco

Já o roteador tem uma função diferente do *switch*, pois ele recebe e envia pacotes de dados entre redes diferentes. Justamente por fazer a interligação entre várias redes, podemos considerar o roteador um dispositivo mais avançado do que o *switch*, tendo ainda como diferencial a capacidade de determinar a melhor rota para os pacotes de dados. Na Figura 4 apresentamos um roteador da Cisco para redes corporativas. Note que ele não se parece com os roteadores residenciais, que normalmente são roteadores e *switches* ao mesmo tempo. Para

redes mais robustas é necessário um roteador com uma configuração mais avançada e com foco apenas na função específica de um roteador.

Figura 4: Roteador da Cisco

2.2. Meios de Transmissão

De acordo com Forouzan, 2008, os meios de transmissão são classificados em guiados (*wired*) e não guiados (*wireless*). Os não guiados usam o ar para a propagação dos dados, portanto os dispositivos de origem e destino precisam estar providos da tecnologia sem fio, conhecidos como dispositivos *wireless*. Já os guiados são os que utilizam os cabos para as conexões, sendo subdivididos em cabo coaxial (*coaxial cable*), cabo par trançado (*twisted-pair cable*) e cabo de fibra óptica (*fiber-optic cable*).

2.2.1. Cabo par trançado

São conhecidos também como cabos de rede, sendo bem comum encontrá-los na cor azul, porém existem em várias cores, como preto, amarelo, vermelho, etc. A diferenciação da cor em geral serve para organizar e documentar os cabos. Poderíamos definir que todos os cabos que vão do computador até o *switch* sejam de cor azul, e todos os cabos entre os *switches* e os roteadores sejam amarelos. Só essa definição facilita muito no momento de identificar os cabos e realizar alguma manutenção. A seguir a imagem mostra exemplos de rolos de cabos com variadas cores.

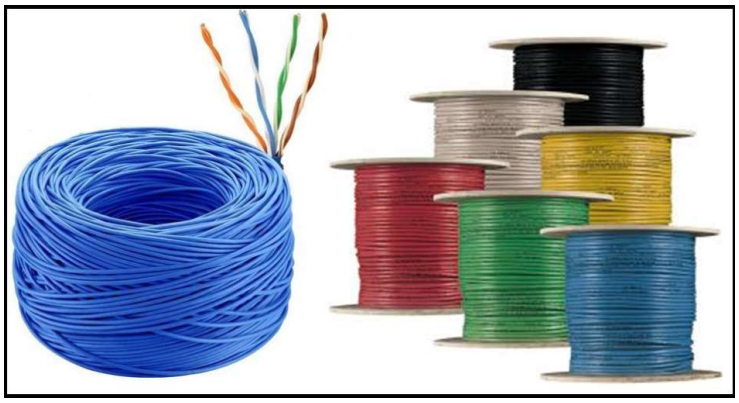


Figura 5: Cabo par trançado

O par trançado é um cabo metálico que tem em geral o elemento cobre ou alumínio como condutor no transporte de sinais. Os fios, normalmente quatro pares, são trançados justamente para evitar a interferência de ruídos externos, como barulho de motores e interferência eletromagnética de cabos de energia elétrica. É necessário ter alguns cuidados no manuseio desse tipo de cabo e evitar algumas ações como dobrar, fazer nós ou pisar neles, pois poderá mudar o trançado original dos fios e consequentemente reduzir o desempenho da rede, tornando-a mais lenta e em alguns casos nem mesmo funcionar.

Na maioria das vezes não é preciso utilizar uma blindagem a mais, pois o trançado dos fios já suporta os ruídos externos, porém, onde o ambiente é muito hostil, se faz necessário utilizar um tipo de cabo com blindagem. O cabo de rede sem blindagem é denominado cabo UTP (*Unshielded Twisted-Pair*) e o com blindagem chama-se cabo STP (*Shielded Twisted Pair*).

Os cabos UTP são os mais comuns, sendo que existem várias categorias definidas pela indústria de padrões. A categoria determina basicamente a capacidade de uma taxa de transferência maior ou menor, influenciando diretamente no desempenho da rede. As categorias mais utilizadas na atualidade são CAT5 (*Ethernet* a 10 Mbps), CAT5e (*Fast-Ethernet* a 100 Mbps) e CAT6 (*Gigabit-Ethernet* a 1 Gbps).

Nas pontas dos cabos são necessários conectores e no caso dos cabos UTP utiliza-se normalmente o RJ45 (*Registered Jack*). Naturalmente temos o conector RJ45 macho e fêmea, como observa-se na figura a seguir:

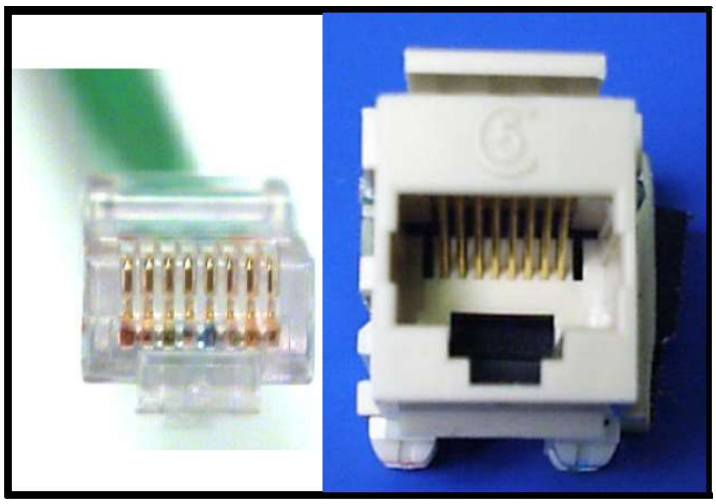


Figura 6: Conector RJ45 macho (esq.) e fêmea (dir.)

Quando os profissionais de rede vão executar um projeto onde é necessário o lançamento de cabos par trançado, a recomendação do fabricante é que seja no máximo 100 metros de distância. As pontas dos cabos precisam ser montadas, ou seja, é preciso fixar os conectores e posteriormente realizar a certificação dos cabos, objetivando a garantia da qualidade na entrega desse serviço especializado. Quando se trata do cabo que vai ligar seu computador ao PT (Ponto de Telecomunicação) ou tomada de rede, a recomendação é que seja comprado o cabo já com os conectores fixados de fábrica, para garantir a qualidade. No entanto, de forma emergencial, muitas empresas e organizações precisam que o técnico faça a montagem do cabo de rede, preferencialmente seguindo os padrões da EIA/TIA que define a sequência de cores dos 8 fios através do T568A e T568B. Veja na Figura 7 como se apresentam esses dois padrões.

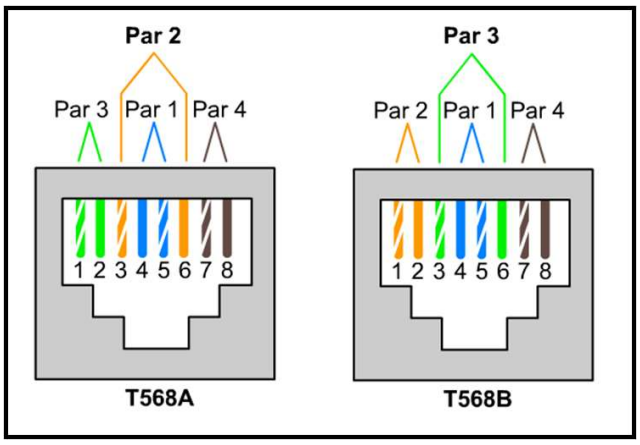


Figura 7: Padrão T568A e T568B

Mas qual o motivo para ter dois padrões de cores? Um só já não seria suficiente? Bem, na prática de hoje em dia você pode utilizar tanto um quanto outro para toda a sua rede. Ocorre que antigamente, para fazer a ligação de um cabo entre dois roteadores, dois *switches* ou dois computadores, obrigatoriamente precisava fazer numa ponta o T568A e na outra o T658B, conhecido por cabo cruzado (*crossover*), justamente pelo cruzamento dos 8 fios, organizando assim quais fios transmitem e quais fios recebem os dados na rede. Mas atualmente os próprios dispositivos já reconhecem os padrões e fazem os ajustes necessários internamente, permitindo então que nossos cabos tenham sempre o mesmo padrão nas duas pontas, por esse motivo são chamados de cabo direto.

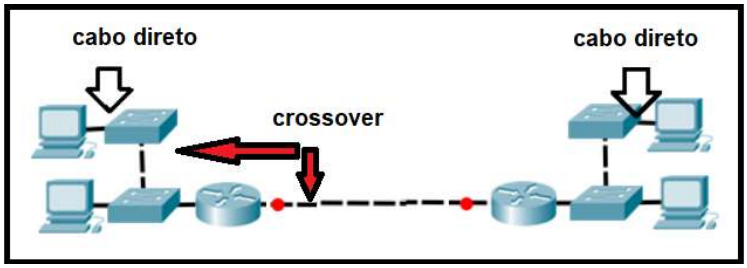


Figura 8: Cabo Direto e *Crossover*

Para fixar bem esses conhecimentos proponho um exercício prático de montagem de um cabo direto. É necessário assistir o vídeo a seguir, ter em mãos os itens da lista de material e usar a orientação do *check-list* mostrada no Exercício 1.

***Link* Montagem com Conector RJ45**: https://youtu.be/rHaVwVShTPk

Lista de material:

- 2 conectores RJ45 (comprar 6 para ter de reserva)
- 2 metros de cabo par trançado (pode ser maior se desejar)
- 1 alicate de crimpagem
- 1 testador de cabo

Os conectores, o cabo, a alicate e o testador podem ser comprados em lojas de componentes eletrônicos. Note que é importante comprar mais do que dois conectores, pois é normal nas primeiras tentativas errar a fixação do RJ5 no cabo, invalidando assim o conector. O alicate de crimpagem é uma ferramenta fundamental, porque com ela podemos cortar, descascar e crimpar os cabos.

Figura 9: Alicate de Crimpagem

Se preferir utilize um alicate de corte específico para esta função, assim como o da imagem abaixo:

Figura 10: Alicate de Corte

Temos ainda o testar de cabo, muito útil para ter certeza que você obteve sucesso na crimpagem mesmo antes de ligar nos dispositivos. A figura a seguir mostra um testador de cabo com suas várias portas de entrada.

Figura 11: Testador de Cabo

Exercício 1: *Check-List* para montagem de cabo

(marque com "X" os itens que conseguir executar)

ITEM	CHECK
1 – Desencapar capa externa do cabo (sem danificá-lo)	
2 – Destrançar/separar fios	
3 – Ordenar e alinhar os fios (Norma EIA/TIA 568A) Branco/Verde Verde Branco/Laranja Azul Branco/Azul Laranja Branco/Marrom Marrom	
4 – Cortar excesso dos fios (1,2 cm)	
5 – Encaixar o cabo no conector RJ45	
6 – Crimpar o cabo no conector	
7 – Testar usando o Testador de Cabos	

2.2.2. Cabo Coaxial

Esse tipo de cabo é similar aos utilizados pelas empresas de TV a cabo, mas ao invés de 8 fios trançados, tem apenas um fio, em geral também de cobre, com uma malha de blindagem externa. Também é classificado em categorias com a nomenclatura RG (*Radio Government*), o RG-59 aplicada para TV a cabo, o RG-58 e RG-11, com aplicação em redes de computadores *Ethernet*. O conector para montagem das pontas do cabo é chamado BNC (*Bayone-Neil-Concelman*), como pode ser visto na figura da sequência (FOROUZAN, 2008).

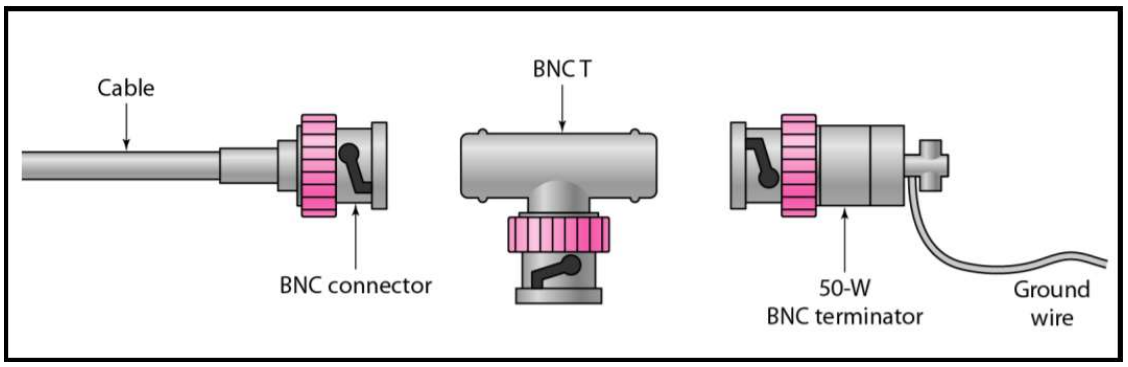


Figura 12: Conector BNC para cabo coaxial

No cabo coaxial também se faz necessário montar as pontas com os devidos conectores, porém não será abordado neste material. O testar de cabo da Figura 11 também pode ser utilizado para testar o cabo coaxial, já que ele possui uma entrada específico para essa função. Veja o vídeo a seguir para conhecer os passos para montagem do conector no cabo coaxial.

***Link* Montagem com Conector BNC**:

https://www.youtube.com/watch?v=DfdXuSBrUcM

2.2.3. Fibra Óptica

Os cabos de fibra transportam sinais por meio de pulsos de luz, podendo ser fabricada com vidro ou plástico, entretanto as de vidro tendem a ter um desempenho bem melhor. São classificadas em fibras multimodo e monomodo. Na multimodo o núcleo é maior e com isso tem maior dispersão de luz, permitindo lançamento de cabo até 2 km. A monomodo é constituía com núcleo mais estreito, permitindo menor dispersão e podendo alcançar até 40 km de distância sem a necessidade de um repetidor. A imagem da Figura 13 ilustra bem a passagem de luz pelo núcleo da fibra.

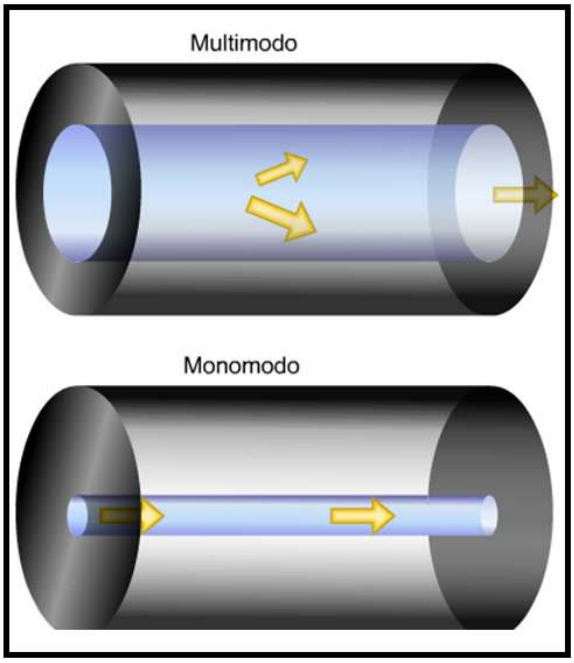


Figura 13: Fibra Óptica Multimodo e Monomodo

Os cabos de fibra óptica utilizam os conectores SC (*Subscriber Channel*) apropriado para TV a cabo, também o conector ST (*Straigh-Tip*), voltado para conectorização dos cabos de dispositivos de redes, sendo considerado mais confiável que o SC, e por fim o MT-RJ, com dimensões iguais ao do RJ45. Veja a diferença no formato dos conectores no desenho a seguir.

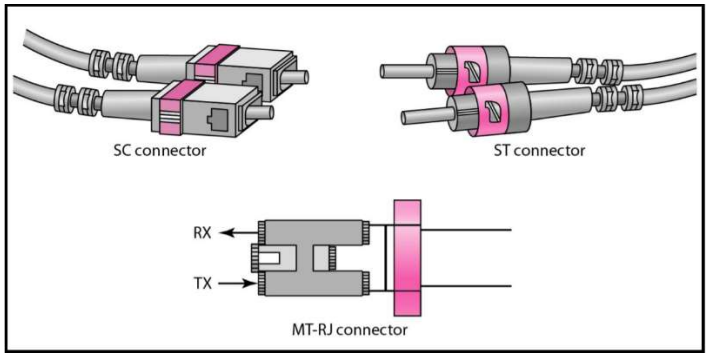


Figura 14: Conectores SC, ST e MT-RJ

Os cabos de fibra óptica tem muitas vantagens sobre os outros tipos de cabo, como:

- É totalmente imune a diafonia, interferência eletromagnética e de radiofreqüência
- Proporciona velocidade e distâncias maiores
- Os cabos de fibra não atraem raios, como os cabos de cobre

Assim como o cabo par trançado e o coaxial, a fibra óptica também precisa da afixação dos conectores e testagem de cabos. Apesar de não ser aprofundado esta prática aqui neste *e-book*, sugiro assistir o vídeo abaixo para entender melhor essa técnica.

***Link* Montagem com Conector SC**:

https://www.youtube.com/watch?v=mqn9ZhN4qAw

Na figura abaixo podemos visualizar um testador de cabo de fibra.

Figura 15: Testador de Cabo de Fibra

2.2.4. Sem Fio (*Wireless*)

Link* Rede *Wireless:

https://youtu.be/9l76yVbBUik

A transmissão sem fio se propaga pelas ondas eletromagnéticas sem utilizar cabos, viajando através do ar, acessível a quem tiver um dispositivo capaz de captar as ondas. O meio *wireless* é classificado em ondas de rádio, micro-ondas e infravermelho, dependendo do espectro eletromagnético que o dispositivo permite utilizar. De acordo com a classificação, a rede sem fio pode ser muito curta, curta, média ou longa distância.

O padrão de tecnologia *Bluetooth* é largamente utilizada para distâncias muito curtas (WPAN), usado para conectar uma grande variedade de dispositivos, como *mouse*, teclado, caixa de som, etc. Um tipo de rede local de curta distância (WLAN) bem disseminada é o WiFi (*Wireless Fidelity*), termo utilizado para identificar um padrão estabelecido pelas instituições de definição de padrões de redes. Atualmente está se difundindo muito a chamado WiFi 6, que se trata de uma versão melhorada desta tecnologia, além da das redes WiFi *Mash*, que proporciona velocidade e desempenho muito além do padrão original. O WiMAX (*Worldwide Interoperability for Microwave Access*) é similar ao WiFi, porém atesta maior velocidade e distância, classificando-se como uma rede WMAN. E finalmente um bom exemplo de tecnologia sem fio de longa distância é a telefonia móvel, conhecida como 3G, 4G e 5G, cada qual aponta novas gerações que permitem maior qualidade, desempenho e funcionalidades.

A rede sem fio é uma tecnologia extremamente útil e prática, por isso seu uso tem crescido muito nos últimos tempos. Na figura a seguir é possível visualizar os exemplos citados no parágrafo anterior de tecnologias utilizadas no mundo e uma noção de sua abrangência.

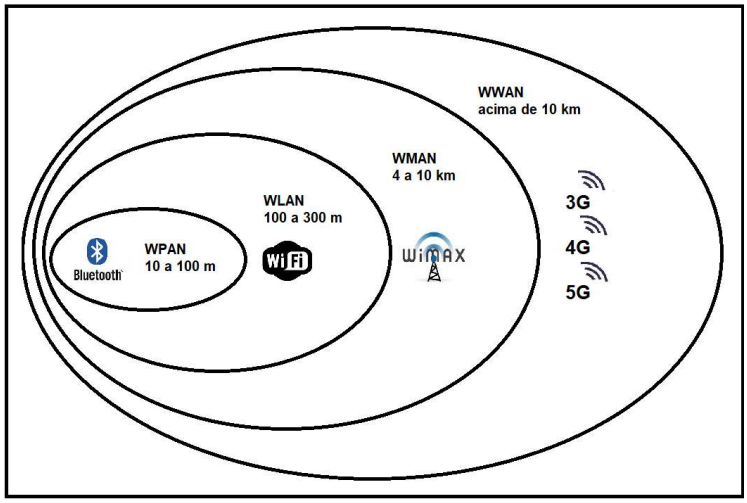


Figura 16: Tecnologias sem fio e abrangência

2.3. Componentes de Rede

***Link* Componentes de Rede**:

https://youtu.be/sJOc9xD1HFk

Agora vamos detalhar um pouco mais o nosso exemplo de rede de computadores, continuando com enfoque nos itens “dispositivos de rede” e “meios de transmissão”, que são os componentes efetivamente abordados neste e-*book*.

Uma palavra muito utilizada no jargão da área de redes de computadores é conhecida como “host”, termo em inglês que numa tradução livre significa hospedeiro. Na prática *host* corresponde a um computador, ou qualquer outro equipamento conectado à rede, tendo assim potencial para hospedar, por exemplo, páginas da *web*, levando-nos a associar de forma mais fácil o significado da tradução (*host* = hospedeiro). Aproveitando nosso exemplo de uma rede de computadores, observe na Figura 17 alguns *hosts* circulados para melhor entendimento.

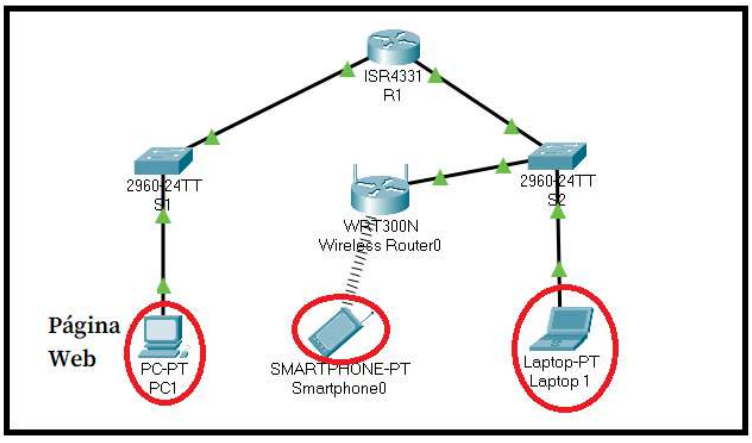


Figura 17: Exemplo de *Hosts*

Note que o “PC1” tem hospedado uma página *web* e, pelo fato de possuir conexão à rede física, pode permitir o acesso dos demais *hosts*, denominados “Smartphone0” e “Laptop 1”. Importante enfatizar que, além das conexões físicas, são necessários aspectos lógicos, como o uso do protocolo IP (*Internet Protocol*), ou Protocolo de Internet, sendo imprescindível a correta configuração em cada *host* da rede.

O computador “PC1”, que está disponibilizando a página *web*, é denominado como um computador “servidor”, pois está prestando um serviço aos demais *hosts* da rede, qualificados como computadores “clientes”, que neste caso o serviço é a hospedagem de um *site* ou página da Internet. Apesar de não haver nenhuma regra que determine qual imagem deve representar algum dispositivo de rede, em geral um servidor é apresentado com a figura de um gabinete de computador, como você pode observar na Figura 18, com destaque para o “Server0”.

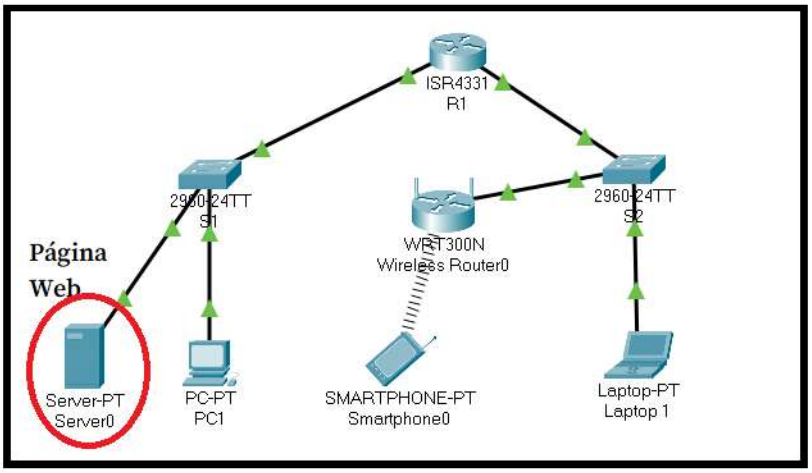


Figura 18: Representação de um servidor na rede

Muito bem, até aqui você já entendeu que existe o “Servidor” e o “Cliente”, o que faz lembrar um conhecido termo da área de informática, chamado “Cliente-Servidor”. Tal termo ratifica o que foi explicado anteriormente, consistindo assim a um modelo ou arquitetura de comunicação que, em primeira instância, faz a vinculação entre o “Host Servidor” e o “Host Cliente” através da rede de computadores.

Se você for chamado para montar uma rede de computadores, uma das primeiras questões que devem ser levantadas é: precisa ser uma rede “Cliente-Servidor”? Ou será que pode ser uma rede “Ponto a Ponto”?

Uma rede “Ponto a Ponto” é uma outra maneira de configurar a rede, utilizando um modelo em que não exista um servidor dedicado, centralizando as configurações desta rede. Nas redes domésticas é comum ter este tipo de arquitetura, onde normalmente tem um roteador sem fio instalado pela operadora de Internet, alguns computadores ligados via cabo e outros dispositivos, como *tablets* e *smartphones*, utilizando a rede sem fio, tudo funcionando sem a necessidade de um servidor específico.

Porém, em uma empresa, é relevante ter servidores por vários aspectos, seja pela quantidade de *hosts* que precisam acessar os serviços, pelas políticas de segurança, ou ainda para facilitar a mudança de alguma configuração na rede que tenha como escopo muitos computadores.

Verifique abaixo algumas vantagens e desvantagens de uma rede ponto a ponto, conhecida também como rede “peer-to-peer” (CISCO, 2021).

Vantagens de uma rede *peer-to-peer*:

- Fácil de configurar
- Menos complexo
- Menor custo porque os dispositivos de rede e os servidores dedicados podem não ser necessários
- Pode ser usada para tarefas simples como transferir arquivos e compartilhar impressoras

Desvantagens de uma rede *peer-to-peer*:

- Nenhuma administração centralizada
- Não é tão segura nem
- Não é escalável
- Todos os dispositivos podem atuar como clientes e servidores, podendo deixar seu desempenho lento.

Continuando com nosso exemplo de redes de computadores, vamos conhecer agora uma forma de classificar os dispositivos numa rede. Eles podem ser “dispositivos finais” ou “dispositivos intermediários”. Na Figura 19 é descrito quem é quem.

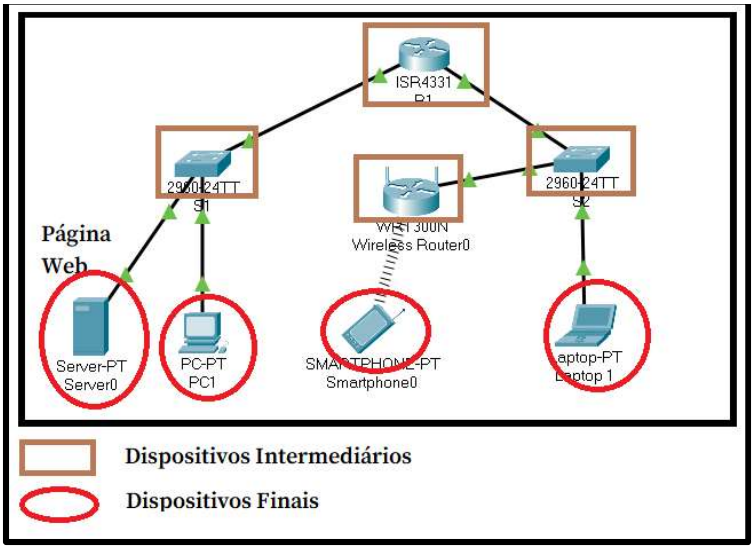


Figura 19: Dispositivos Finais e Intermediários

Com esta imagem ficou simples entender e identificar quando um dispositivo é final ou quando é intermediário, levando-nos a uma associação lógica das definições. Para finalizar a explanação desse conceito, abaixo são listadas as principais funções dos dispositivos intermediários (CISCO, 2021):

- Regenerar e retransmitir sinais de comunicação
- Manter informação sobre quais caminhos existem pela rede
- Notificar outros dispositivos sobre erros e falhas de comunicação
- Direcionar dados por caminhos alternativos quando houver falha em um link
- Classificar e direcionar mensagens de acordo com as prioridades
- Permitir ou negar o fluxo de dados, com base em configurações de segurança

Agora que você já tem mais esse conhecimento, vamos partir para a próxima etapa que é aprofundar um pouco mais sobre os “meios de rede”, ou para ficar mais claro podemos chamar de “meios de transmissão”, que foi uma das três palavras-chave mencionadas no início do capítulo. Alguns autores usam também o termo “meios de comunicação”, porém, mais importante do que a nomenclatura, é o entendimento do seu funcionamento.

Para compreender o que são meios de comunicação basta você se perguntar: Como vou interligar os dispositivos finais e intermediários? Então respondemos reiterando o que você já aprendeu no capítulo 2. Podemos utilizar os cabos, que são classificados em meios em cobre e meios em fibra. Os que utilizam o elemento cobre são cabos coaxiais (similares aos cabos de TV a cabo) e cabos par trançado (aqueles comumente ligados aos computadores para acesso à rede). Já as fibras são as conhecidas fibras ópticas tão populares por permitir alta taxa de transmissão de dados e em geral é conectada ao roteador residencial ou mesmo da empresa.

Outro meio de transmissão é pelo ar, muito conhecido como *wireless* ou “sem fio”, que utiliza frequência de rádio específica e dependendo do equipamento, pode servir para comunicação muito curta, curta, média ou longa distância.

Como técnico de redes você vai precisar saber decidir qual desses meios vai usar na sua rede, portanto, a seguir temos alguns critérios importantes para sua melhor decisão (CISCO, 2021):

- Qual é a distância máxima pela qual o meio físico consegue carregar um sinal com êxito?
- Qual é o ambiente em que a mídia será instalada?
- Qual é a quantidade de dados e a que velocidade deve ser transmitida?
- Qual é o custo do meio físico e da instalação?

2.4. Topologias e Tipos de Redes

***Link* Topologias e Tipos de Redes**:

https://youtu.be/WibMWOkRj_E

***Link* Redes Topologias**:

https://youtu.be/U2wwYU_3a0I

As topologias de redes podem ser divididas em duas partes, a topologia física e a topologia lógica, que iremos estudar a seguir, além é claro dos principais tipos de redes.

2.4.1. Topologia Física

A topologia física especifica a distribuição física ou *layout* dos dispositivos de rede e dos meios de transmissão. Tal estudo é muito importante e pode influenciar na velocidade, na segurança e na manutenção da rede. Quando um profissional de infraestrutura de redes é chamado para

planejar e executar a montagem de uma estrutura de rede, uma das primeiras providências é a elaboração de um projeto físico da rede, seja ela uma nova estrutura ou então a reorganização de uma rede já existente.

Assim como um engenheiro precisa elaborar uma planta baixa de uma nova construção, definindo as dimensões, por onde irá passar o encanamento de água com suas respectivas terminações, bem como a passagem de toda a parte elétrica e suas tomadas, assim também o técnico em redes vai precisar utilizar as ferramentas adequadas para definir por onde irão passar os cabos de rede, que tipos de cabos são esses, onde os dispositivos de rede ficarão acomodados, além de vários outros detalhes de infraestrutura necessários e fundamentais para uma topologia física de redes bem desenhada.

No material da Cisco, 2021 é mostrado uma imagem que resume muito bem esta representação física de redes, descrevendo de forma clara e objetiva os dispositivos de rede interligados por meios de comunicação. Observe e tente entender tudo o que aparece nesta imagem através da Figura 20 a seguir:

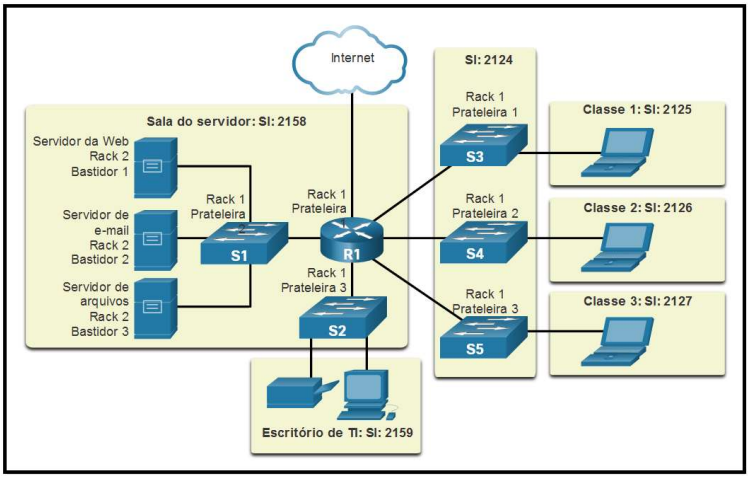


Figura 20: Topologia Física

Veja que a Figura 20 expõe de forma macro todos os principais dispositivos e meios que serão utilizados, devidamente identificados com uma nomenclatura definida, bem como a descrição apontando em que sala cada qual estará (sala do servidor 2158, escritório de TI 2159, sala para os *switches* 2124, salas 2125, 2126 e 2127 representando a área de trabalho propriamente dita). Agora, para que tenhamos maiores chances de aprovação deste projeto, é importante apresentar um detalhamento de cada sala. Como exemplo pegaremos a sala 2127 e vamos desenhar um diagrama similar ao da Figura 20, porém agora mostrando tudo que terá nesta sala, com todos os computadores e cabos devidamente distribuídos.

Se você quiser deixar a sua topologia física com cara de um projeto físico, facilitando ainda mais o entendimento daqueles que irão ou não financiar esta empreitada, pegue a planta baixa desta sala como pano de fundo e faça o seu *layout* com a distribuição de todos os equipamentos e meios de transmissão, como apresentado na Figura 21.

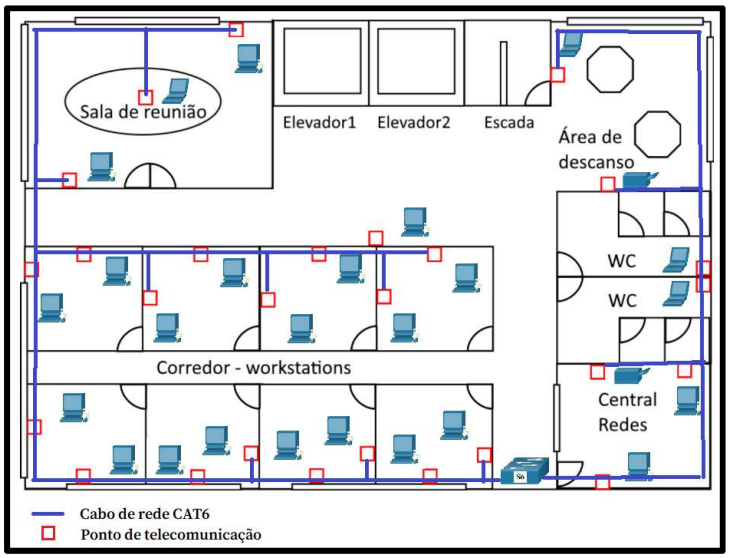


Figura 21: Projeto Físico da Sala 2127

Para conhecer um pouco mais com construir um projeto físico a partir de uma planta baixa, e de quebra ter uma noção básica de cabeamento estruturado, entre no link a seguir.

***Link* Projeto Físico**: https://youtu.be/SYce8pwKr_g

A topologia física mostrada na Figura 20 e desdobrada na Figura 21 é conhecida como "estrela estendida", tipo muito comum na atualidade, entretanto existem vários tipos de topologias físicas. Podemos conhecer as principais na Figura 22 abaixo.

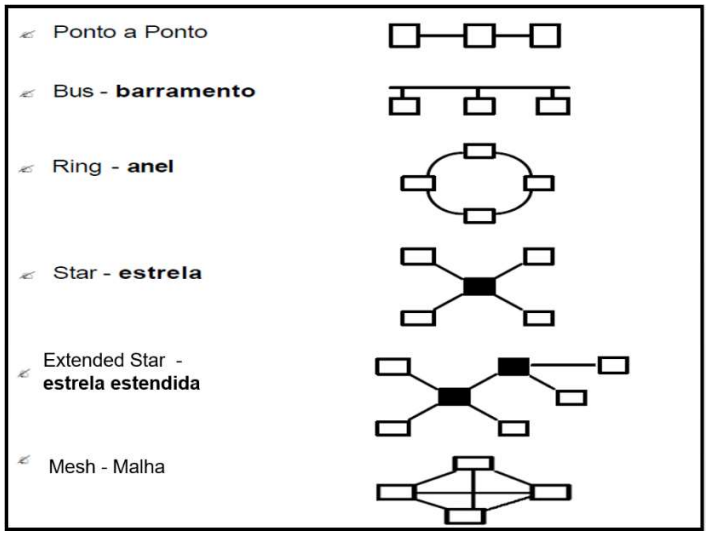


Figura 22: Tipos de topologias físicas

Ponto a Ponto: Fisicamente falando, esta topologia significa um computador ligado no outro e assim sucessivamente, sem nenhum dispositivo intermediário que faça a conexão entre eles, como um *hub*, *switch* ou roteador. Ou seja, em cada extremidade do cabo temos um *host*, que pode funcionar como um servidor com a capacidade de transferir informações solicitadas por outro *host*.

Nesse momento você deve estar se perguntando: Então a conexão ponto a ponto só existe quando um computador está ligado diretamente no outro? A resposta é não! Podemos ter sim uma topologia lógica ponto a ponto em qualquer topologia física. Um exemplo é a maioria das

redes domésticas onde logicamente a rede é ponto a ponto, porém fisicamente a rede é do tipo estrela ou estrela estendida.

Barramento: Perceba que a topologia barramento até parece com a topologia ponto a ponto apresentada na Figura 22. A principal diferença é que na topologia barramento existe um cabo central onde são ligados os cabos que vem dos *hosts*. Essa topologia foi muito utilizada nas primeiras redes implementadas no mundo todo, utilizando o cabo coaxial como meio de transmissão.

Anel: Ocorre uma topologia física anel quando um computador está interligado diretamente no outro, porém, diferente da topologia ponto a ponto, o último computador é conectado ao primeiro, formando assim um anel. A proposta desse tipo de topologia de rede é a não existência de colisões de dados, algo bastante comum nas demais topologias. Na prática esse tipo de rede é muito difícil de ser encontrada, principalmente pelo fato de exigir maior custo de implementação ou por ser lenta demais se comparada com outras topologias.

Estrela: Imagine um *switch* como sendo o centro de uma estrela e em cada ponta da estrela tem um computador. Como você pode observar na Figura 22, o retângulo escuro está representando o *switch* ligado aos computadores, formando então uma estrela. Tenho quase certeza que em nenhum momento você olhou para a sua rede de casa ou do trabalho e imaginou uma estrela, não é mesmo. Bem, fique tranquilo pois é apenas um conceito sem a necessidade estética de uma estrela.

Estrela estendida: Essa topologia é idêntica a estrela, porém um *switch*, ou qualquer outro dispositivo centralizador, está ligado a outros *switches*, formando uma extensão da estrela. Isso significa que se você olhar para a imagem da topologia estendida, necessariamente haverá também uma topologia estrela, dependendo apenas do escopo que for considerado.

Malha: Todos ligados com todos. Utilizada quando é imprescindível muita segurança na rede, principalmente quanto a tolerância a falhas de algum cabo, ou seja, se você perder a conexão por alguma das rotas de interligação, você terá outras rotas. No exemplo da Figura 22 cada *host* tem três rotas diferentes para comunicação. A Internet pode ser considerada uma grande malha semi-completa, já que não estamos todos diretamente ligados com todos, mas boa parte das pessoas ou empresas tem mais do que um *link* de comunicação para acessar a Internet. Se você tem um *smartphone* e está utilizando o WiFi juntamente com o roteador da sua casa, significa que você tem uma conexão com a grande rede, mas e se a sua conexão com WiFi cair? Bem, se você tiver sinal de telefonia móvel no seu celular, a conexão com a Internet continua, já que você possui esse segundo *link* de comunicação.

2.4.2. Topologia Lógica

Tão importante quanto a topologia física é a topologia lógica, que consiste na forma como os dados são transmitidos na rede. No nosso estudo vamos citar apenas as duas topologias lógicas mais conhecidas, que é a “Token Ring” e a “Ethernet”. A *Token Ring* foi projetada para funcionar na topologia física anel, onde o chamado “Token” faz o controle da transmissão dos dados, impedindo assim qualquer tipo de colisão, como se fosse um semáforo no trânsito evitando que os carros batam.

Já a mais conhecida e utilizada é a topologia lógica ou a tecnologia *Ethernet* que, ao contrário da *Token*, ocorrem naturalmente colisões de dados, principalmente com o disparo do chamado *broadcast* (envio de pacote de dados a todos os *hosts* da rede), fazendo com que esses mesmos dados tenham que ser retransmitidos na rede. Apesar desse "probleminha", a *Ethernet* foi a melhor solução de topologia lógica, pelo menos até a atualidade, principalmente porque podemos administrar muito bem as colisões utilizando de forma adequada os dispositivos e os meios, ou, falando de forma mais direta, o uso adequado de *switches*, roteadores e cabos de rede. Não poderia deixar de citar que, no gerenciamento dessas colisões, um outro elemento fundamental é o "endereçamento IP", que precisa ser corretamente configurado para um bom desempenho da rede, em especial as com muitos computadores. O estudo sobre endereço IP será aprofundando no capítulo 5.

Na Figura 23 temos um exemplo de topologia lógica, apresentando os endereços IP de cada segmento de rede, bem como a identificação das interfaces. O nível de detalhamento vai depender do técnico responsável, mas a próxima etapa naturalmente seria elaborar uma tabela com as seguintes informações: faixa ou *range* dos endereços IP da rede, primeiro *host*, último *host* e endereços de *broadcast*. Nesse *e-book* vamos chegar a elaborar uma tabela que contemple estes detalhes da rede.

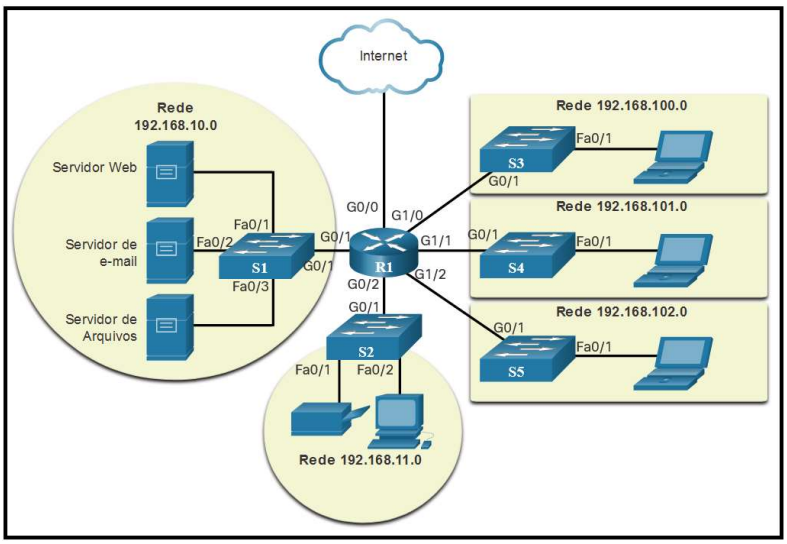


Figura 23: Topologia Lógica

2.4.3. Tipos de Redes

Vamos conhecer alguns tipos de redes existentes, lembrando que alguns autores chamam de "classificação de redes", que nada mais é do que uma forma de identificar a rede por sua escala, ou seja, seu tamanho e abrangência.

LAN: *Local Area Network* ou Área Local de Rede. São as redes que ocupam espaços restritos, geralmente pequenos, como uma sala ou um andar de um prédio. Suas características básicas são: altas taxas de transmissão, baixas taxas de erros, propriedade privada e geograficamente limitada.

MAN: *Metropolitan Area Network* ou Área Metropolitana de Rede. Esse tipo de rede já tem uma escala maior do que a LAN, como um conjunto de edifícios, condomínios ou *campi* universitários. Tem como características ser restrita a uma área metropolitana e a utilização de cabos de fibra óptica e rádio.

WAN: *Wide Area Network* ou Área Ampla de Rede. Maior que a MAN e a LAN e tem uma escala global. A Internet pode ser classificada como uma WAN. Suas características permitem conectar redes locais geograficamente distantes com utilização de satélites, linhas telefônicas, micro-ondas e fibras ópticas como meios de transmissão. Geralmente são redes públicas.

PAN: *Personal Area Network* ou Área Pessoal de Rede. É menor que uma LAN abrangendo os dispositivos de uso mais pessoal ou doméstica. O meio de comunicação muito utilizado é o sem fio, principalmente pelo protocolo de comunicação *bluetooth*.

RAN: *Regional Area Nework* ou Área Regional de Rede. É menor que a WAN e maior que a MAN, sendo definida em uma região geograficamente específica. Possui como característica conexões de alta velocidade.

SAN: *Store Area Network* ou Área de Armazenamento de Rede. É basicamente uma rede de armazenamento de dados, agrupando vários dispositivos na rede. Muito comum em armazenamentos de grande porte e possui transferência de dados robusta e segura.

A Figura 24 nos mostra imagens dos tipos de redes para facilitar a compreensão.

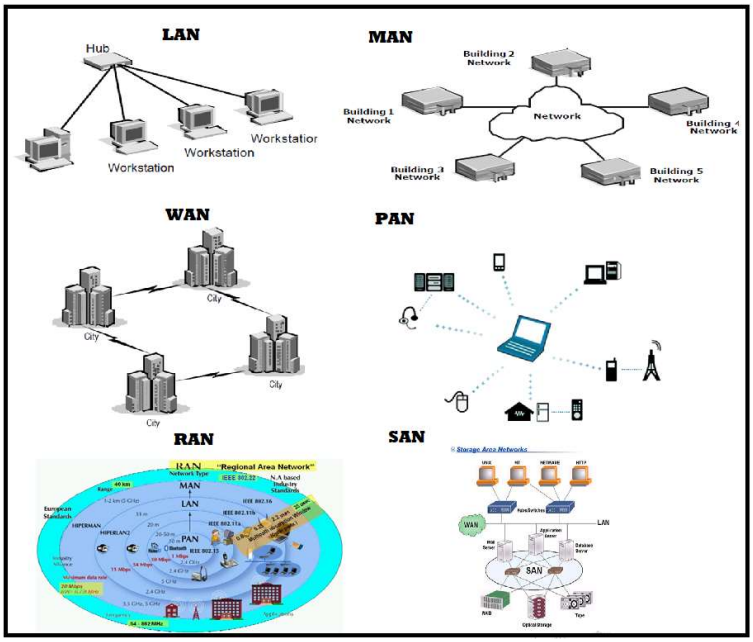


Figura 24: Tipos de Redes

Não poderia deixar de, através de mais algumas palavras-chave, consolidar suas definições, objetivando aprimorar seu conhecimento de redes de computadores:

Internet: Em 1995 a *Federal Networking Council* norte-americana aprovou uma resolução definindo o termo “Internet” que, através de reunião com membros especialistas no assunto e comunidades de direitos da propriedade intelectual, definiu a Internet como sendo:

1) Logicamente um endereço único global baseado no Internet Protocol (IP) ou suas subsequentes extensões
2) É capaz de suportar comunicações usando o Transmission Control Protocol/Internet Protocol (TCP/IP) ou suas subsequentes extensões e/ou outros protocolos compatíveis ao IP
3) Provê, usa ou torna acessível, tanto publicamente como privadamente, serviços de mais alto nível, produzidos na infraestrutura descrita

Intranet: Forma de permitir a comunicação interna e a coerência das informações, com velocidade e segurança dentro da empresa ou entidade, evitando o risco de violação.

Extranet: Evolução da *intranet* que permite que seu acesso seja possível fora da sua rede local, tornando seus pares, como funcionários e fornecedores, usuários da *intranet* usando a estrutura da Internet.

Ethernet: Tecnologia de interconexão para redes locais (LANs) baseada no envio de pacotes de dados. Abrange o cabeamento e os sinais elétricos para a camada física, bem como o formato de pacotes. A *ethernet* foi padronizada pela IEEE como 802.3 e seu uso se estende desde os anos 90.

2.5. Conexões com a Internet

***Link* Conexões com a Internet**: https://youtu.be/p-oYmVpZi7o

***Link* Redes Download Packet Tracer**: https://youtu.be/QkdJIl2oJdE

***Link* Resolução Exercício 6318 no Packet Tracer**: https://youtu.be/lifXkkJmPDU

***Link* Download Packet Tracer**: https://www.netacad.com/pt-br/courses/packet-tracer

Um dos focos desse capítulo é a maneira como acessamos a Internet. Serão feitos ainda alguns comentários sobre as conhecidas “Redes Convergentes”, assunto que traz muitos benefícios e que vale a pena um aprofundamento. Observe que foi disponibilizado, além dos *links* das videoaulas, o *link* para *download* do simulador de redes, justamente porque neste capítulo você terá oportunidade de praticar. Numa das videoaulas apresento a resolução de um desafio utilizando o simulador de redes *Packet Tracer* da Cisco.

Existem muitas formas de ter conexão com a Internet, porém neste capítulo vamos apresentar as mais difundidas que são: DSL, Cabo, Celular, Satélite, *dial-up*, *Metro-Ethernet* e Linha dedicada privada. Para facilitar o entendimento vamos dividir em dois grupos, o de residências/pequenos negócios e os corporativos (CISCO, 2021).

2.5.1. Conexões para residências

Cabo: é aquele cabo que você utilizada para assistir TV a cabo, podendo prover também acesso à Internet com largura de banda e disponibilidade muito boa.

DSL (*Digital Subscriber Line*): essa forma de conexão à Internet funciona através da linha telefônica, tendo alta largura de banda e alta disponibilidade. Geralmente quando o usuário é residencial ou de pequenos escritórios, usa-se a chamada ADSL ou DLS Assíncrona, que na prática significa que a velocidade de *download* é maior do que a de *upload*.

Celular: Se estiver dentro de uma área coberta por uma torre de celular, recebendo sinal suficiente, você terá acesso à Internet, sempre com as limitações da torre e dos recursos do próprio celular. A tecnologia mais utilizada atualmente é conhecida como 4G (4ª Geração de telefonia móvel), porém a 5G já está sendo regularizada em várias partes do mundo e será a sua substituta natural. Para um futuro não tão distante já se deslumbra a 6G.

Satélite: é uma solução para os locais mais remotos, como áreas rurais, que ficam distantes da infraestrutura de redes existente nas cidades. São instaladas antenas parabólicas direcionadas para o satélite objetivando enviar e receber dados.

Conexão Discada (*Dial-up*): é uma antiga forma de se conectar à Internet, mas pode ser utilizada em caso de necessidade. Basta conectar seu computador a um *modem* que esteja ligado na tomada de linha telefônica da casa, fazer as configurações necessárias e então realizar o acesso que, infelizmente, tem grande limitação de velocidade, mas foi maciçamente usufruída na década de 90.

2.5.2. Conexões Corporativas

Linha Dedicada: o provedor de Internet aluga uma linha privada e dedicada que fornece, além do acesso à Internet, a conexão entre escritórios geograficamente separados.

Metro Ethernet: a *Ethernet* é originalmente para redes locais (LAN), entretanto a *Metro Ethernet* ou *Ethernet* WAN permite aproveitar tal tecnologia na WAN.

DSL de negócios: Semelhante a DSL e disponibilizada em vários formatos como o SDSL (*Symmetric Digital Subscriber Line*), que permite mesma velocidade de *download* e *upload*.

Satélite: Funciona como a já citada nas conexões residenciais e busca atender também o público corporativo com empreendimentos em locais remotos.

2.5.3. Redes Convergentes

Segundo Alctel, 2020, as redes convergentes vieram para unir a transmissão de imagens, voz e dados em uma única rede digital. Pode ser definida como sendo uma forma de garantir altos níveis de serviço e escalabilidade para as aplicações, além de redução de custos e maior controle sobre as atividades nos canais de comunicação.

Para que a rede seja definida como convergente é necessário um padrão, ou seja, o mesmo conjunto de regras para que as mídias trabalhem de forma integrada, independentemente do tipo de dispositivo utilizado nessa infraestrutura.

A Figura 25 a seguir retrata bem o uso integrado do computador, da telefonia, da *smart* TV ou qualquer outro dispositivo em uma única infraestrutura, representando assim uma nova realidade multimídia (CISCO, 2021).

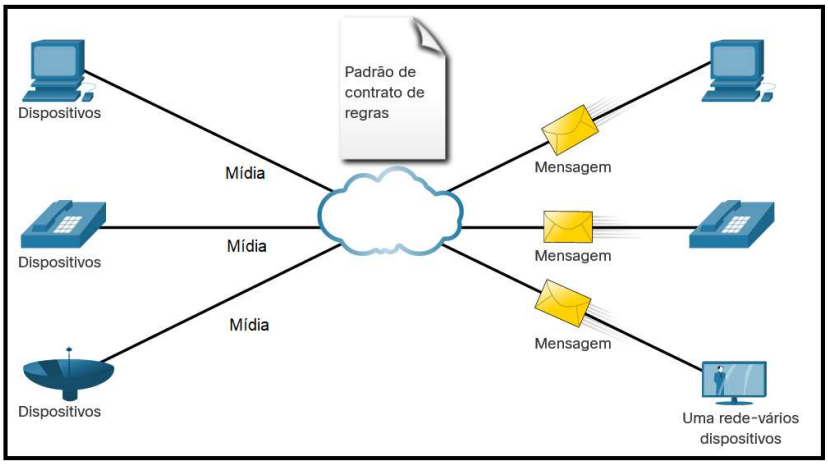


Figura 25: Redes Convergentes

3.As Redes são seguras?

***Link* Redes Confiáveis**: https://youtu.be/WNdJH5zf-7k

***Link* Tendência de Redes**: https://youtu.be/oOaPkgTxDpA

***Link* Segurança de Redes**: https://youtu.be/SsxgJhJ5ggM

Quando pensamos em segurança nas redes logo imaginamos algum invasor querendo acessar nossos dados, furtar nossas senhas e apagar os arquivos. Entretanto, o tema segurança de rede é muito mais amplo, pois passa por outras situações intrigantes, como por exemplo a disponibilidade da rede. O que acontece quando você fica sem Internet na sua casa ou trabalho? Acredito que você já passou por isso e, se a solução do problema não ocorrer logo, você fica sem conseguir trabalhar, estudar ou mesmo se divertir. Bem, é claro que usando a criatividade você pode sim se divertir sem a Internet, mas a nossa dependência das redes nos dias atuais é tão grande que, por algum momento que seja, acreditamos que não tenha outro jeito.

3.1. Redes Confiáveis

Para ter uma rede confiável existem quatro características básicas que devem ser atendidas. Você como estudante de redes de computadores precisa realmente conhecê-las e posteriormente, aplicá-las no seu dia-a-dia profissional. Na sequência são apresentadas as características com as devidas definições.

Tolerância a falhas: anteriormente você estudou sobre topologias, uma delas era a topologia em malha, em que todos os *hosts* estavam ligados entre si, lembra? Este tipo de estrutura física permite redundância, ou seja, temos mais do que um caminho para enviar os pacotes de dados. Claro que você não precisa ligar todos os *hosts* entre si, pois seria inviável, porém, se você fizer uma redundância de roteadores, de tal forma que quando falhar um deles o outro assume a função de forma automática, então já vai fazer muita diferença. Essa mesma ideia se aplica para redundância de servidores, *links* de internet e até mesmo de fonte de alimentação (energia elétrica).

Escalabilidade: a recomendação básica para se ter escalabilidade é sempre pensar no crescimento do número de *hosts* do ambiente. Para tanto, devemos planejar os dispositivos (roteadores, *switches* e computadores), e os meios de comunicação (cabeamento ou rede sem fio), tendo como referência o tamanho da sala. Por exemplo, se temos uma sala de 100 m^2, então vamos precisar ter no mínimo 8 pontos de rede, ou seja, 2 pontos de rede a cada 10 m^2 segundo as normas de cabeamento estruturado NBR-14565, EIA/TIA-568 e ANSI/EIA/TIA 606 (ABNT, 2013)

Qualidade de serviço (QoS): é uma maneira relevante para gerenciar os congestionamentos e garantir entregas confiáveis de conteúdo aos usuários da rede. Podemos configurar nos roteadores prioridade de voz e de dados, ou seja, se alguns usuários estiverem acessando páginas *web* e outros estiverem em ligações telefônicas (utilizando VoIP), é possível dar prioridade para a telefonia, objetivando o entendimento e a clareza da fala das pessoas. Os

usuários das páginas *web* não terão problemas se o acesso demorar, por exemplo, um segundo a mais do esperado.

Segurança: aqui devemos pensar na segurança de infraestrutura e de segurança da informação. Na de infraestrutura de rede consideramos a proteção física dos dispositivos, impedindo acesso não autorizado ao *software* de gerenciamento que reside nesses dispositivos de rede. Já quando falamos em segurança da informação, devemos imaginar a proteção necessária dos pacotes transmitidos pela rede, além das informações armazenadas nos dispositivos. Com isso são considerados três pilares para atingir os objetivos de segurança da informação. Vamos entender com exemplos (TERRA, 2005):

> **Confidencialidade**: apenas destinatários autorizados podem acessar e ler os dados.
> **Ex.:** Alguém obtém acesso não autorizado ao seu computador e lê todas as informações contidas na sua declaração de imposto de renda.
> **Solução:** *logins*, senhas, *tokens*, criptografias, entre outros.

> **Integridade**: garante que as informações não foram alteradas na transmissão.
> **Ex.:** Alguém obtém acesso não autorizado ao seu computador e altera informações da sua declaração de imposto de renda, momentos antes de você enviar para a Receita Federal.
> **Solução:** criptografia, *hashing* e assinaturas digitais.

> **Disponibilidade**: garante acesso oportuno e confiável aos usuários autorizados.
> **Ex.:** O seu provedor sofre uma grande sobrecarga de dados ou um ataque de negação de serviço. Por este motivo você fica impossibilitado de enviar sua declaração de imposto de renda a Receita Federal.
> **Solução:** *backups* locais ou em nuvem, atualizações dos sistemas e uso de banda compatível a fim de evitar quedas na rede.

3.2. Tendências de Redes

Este *e-book* corre o grande risco de já estar desatualizado no momento da sua leitura, visto que as transformações tecnológicas em todas as áreas do conhecimento estão em um crescimento exponencial, entretanto vamos listar aqui algumas dessas mudanças mais marcantes na atualidade:

BYOD (*Bring Your Own Device*): Levar seu próprio dispositivo, seja um *notebook*, *tablet* ou *smartphone*, é uma tendência cada vez mais flagrante. Você precisa mesmo utilizar o computador do ambiente de trabalho ou do ambiente escolar?

Colaboração *on-line*: O trabalho, o estudo e o lazer a distância fortaleceu o uso de ferramentas colaborativas e compartilhadas. As conferências *on-line*, vídeo chamadas, as planilhas e editores de texto compartilhados, fotos e vídeos na nuvem dentre outras formas de interação são algumas características dessa tendência a colaboração remota.

Comunicação por vídeo: A maioria das reuniões não precisam ser mais presenciais, pois agora temos este recurso cada vez mais difundido no mundo. A economia de tempo de deslocamento e recursos para encontros presenciais tornaram esta tendência potencializada.

Computação em nuvem: Esta tendência trouxe a facilidade de acesso a arquivos, imagens, fotos, vídeos, filmes e demais dados de forma fácil e confortável, independentemente do dispositivo utilizado, podendo ser um *smartphone*, *tablet*, computador, *smart* TV, etc.

Além de toda transformação na forma como nos comunicamos, estudamos, trabalhamos e nos divertimos, as redes também tendem a modificar as casas, edifícios e demais ambientes físicos que normalmente convivemos. Entra aqui o conceito de casa ou edifício inteligente, impulsionado pelos vários conceitos e/ou tecnologias como: Internet das coisas (IoT), RFID (IDentificação por Rádio Frequência), inteligência artificial (IA), computação em nuvem, mobilidade (mobile), virtualização (VLANs e SDNs), *big data*, realidade aumentada, geolocalização, banda larga sem fio, Li-Fi (*Light Fidelity*), rede *powerline*, etc.

Com tantos novos equipamentos e grande volume de tráfego de dados se tornando natural, surge a preocupação com a eficiência energética. A casa eficiente é um conceito que contempla tal impacto, maximizando a eficiência energética, bem como ampliando o conforto e segurança através das redes, representado pela Figura 26 a seguir (CASA EFICIENTE, 2020).

Figura 26: Casa eficiente

3.3. Segurança de Redes

Já falamos um pouco sobre segurança de redes no início deste capítulo, porém esse tema sempre será prioridade máxima dos envolvidos na administração das redes, justamente por ser parte integrante da rede de computadores. Os dados devem ser protegidos, ao mesmo tempo que a qualidade do serviço seja mantida. Existem várias técnicas, ferramentas, dispositivos e tecnologias para proteger e mitigar ameaças, portanto vamos conhecer as principais ameaças externas que devemos ficar atentos (CISCO, 2020):

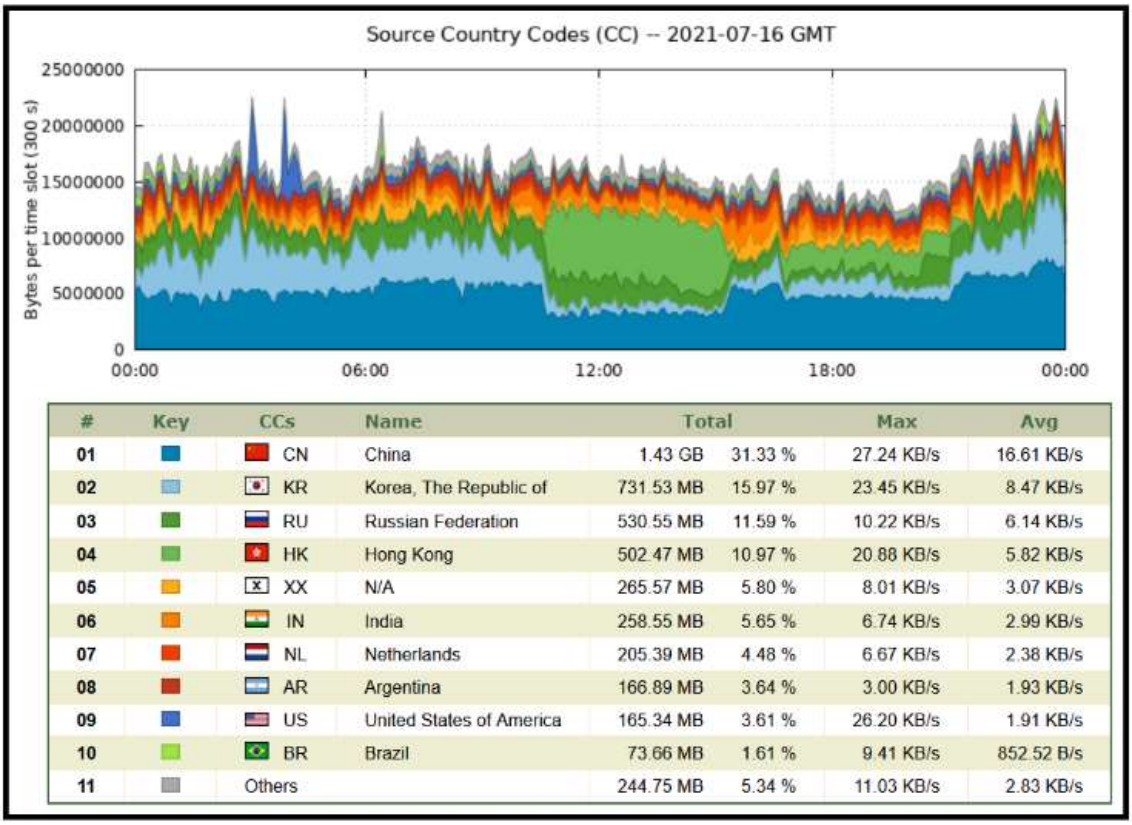
- **Vírus, *worms* e cavalos de Tróia** - Eles contêm software ou código malicioso em execução no dispositivo do usuário.
- **Spyware e adware** - Estes são tipos de softwares instalados no dispositivo de um usuário. O software, em seguida, coleta secretamente informações sobre o usuário.
- **Ataques de dia zero** - Também chamados de ataques de hora zero, ocorrem no primeiro dia em que uma vulnerabilidade se torna conhecida.
- **Ataques de ator de ameaça** - Uma pessoa mal-intencionada ataca dispositivos de usuário ou recursos de rede.
- **Ataques de negação de serviço (DDoS)** - Esses ataques atrasam ou travam aplicativos e processos em um dispositivo de rede.
- **Interceptação de dados e roubo** - Esse ataque captura informações privadas da rede de uma organização.
- **Roubo de identidade** - Esse ataque rouba as credenciais de login de um usuário para acessar informações privadas.

Além das ameaças externas citadas acima, temos as ameaças internas que são tão perigosas e danosas quanto as externas. O usuário interno da rede, muitas vezes podendo ser o próprio colaborador ou funcionário da empresa, se aproveita do acesso mais fácil ao ambiente e elabora estratégias ilícitas para conseguir o que quer. É possível que seja apenas mau uso acidental, mas também que sejam subtraídos dispositivos da rede por funcionários mal-intencionados, além do uso da conhecida engenharia social, onde o invasor do sistema se aproveita da parte sentimental e psicológica das pessoas, conseguindo senhas de acesso e entradas em locais restritos.

Em ambientes residenciais normalmente o uso de antivírus e *antispywares*, que são aplicativos que protegem os dispositivos finais, já são suficientes para uma proteção básica. Mas, para ser ainda mais seguro pode-se utilizar a filtragem por *firewall*, que consiste em bloquear acesso externo, tanto nos dispositivos finais quanto intermediários.

Já nos ambientes corporativos existem mais opções como: sistema de *firewall* dedicado (recursos mais avançados de filtragem), lista de controle de acesso ou ACL (configurado nos dispositivos intermediários tendo como base os endereços IP para filtragem do tráfego), sistema de prevenção de intrusões ou IP (identificam ameaças de rápida disseminação) e redes privadas virtuais ou VPN (acesso seguro para trabalho remoto).

A CERT.BR, 2019, mantém um projeto com o objetivo de aumentar a capacidade de detecção de incidentes e tendências de ataques na Internet brasileira. Uma das atividades é a estatística pública diária do fluxo de tráfego na Internet, conforme apresentado na Figura 27.



#	Key	CCs	Name	Total		Max	Avg
01		CN	China	1.43 GB	31.33 %	27.24 KB/s	16.61 KB/s
02		KR	Korea, The Republic of	731.53 MB	15.97 %	23.45 KB/s	8.47 KB/s
03		RU	Russian Federation	530.55 MB	11.59 %	10.22 KB/s	6.14 KB/s
04		HK	Hong Kong	502.47 MB	10.97 %	20.88 KB/s	5.82 KB/s
05		XX	N/A	265.57 MB	5.80 %	8.01 KB/s	3.07 KB/s
06		IN	India	258.55 MB	5.65 %	6.74 KB/s	2.99 KB/s
07		NL	Netherlands	205.39 MB	4.48 %	6.67 KB/s	2.38 KB/s
08		AR	Argentina	166.89 MB	3.64 %	3.00 KB/s	1.93 KB/s
09		US	United States of America	165.34 MB	3.61 %	26.20 KB/s	1.91 KB/s
10		BR	Brazil	73.66 MB	1.61 %	9.41 KB/s	852.52 B/s
11		Others		244.75 MB	5.34 %	11.03 KB/s	2.83 KB/s

Figura 27: Tráfego direcionado aos *honeypots* nas últimas 24 horas

4.Configurando um Switch

***Link* Curso sobre Packet Tracer**:

https://www.netacad.com/pt-br/courses/packet-tracer/introduction-packet-tracer

Chegou o momento de colocar a mão na massa, ou seja, fazer as configurações do *switch* através de comandos específicos. Caso você não tenha acesso a *switches* ou roteadores, será fundamental fazer o *download* do simulador de redes *Packet Tracer*, lembrando que este programa é gratuito e você pode baixar agora usando o *link* do início do capítulo 4 acima.

Vamos utilizar o Cisco IOS (*Internetwork Operation System*), ou seja, o sistema operacional existente nos *switches* e roteadores da Cisco que está sendo simulado dentro do *Packet Tracer*. Por meio do desenho de uma topologia com os dispositivos e meios de comunicação, daremos início as configurações básicas via linha de comando, conhecido também como CLI (*Command Line Interface*). Porém, antes é importante conhecer os métodos de acesso ao *switch* ou roteador, conforme material da Cisco (CISCO, 2020):

Console: Esta é uma porta de gerenciamento físico que fornece acesso fora de banda a um dispositivo Cisco. O acesso *out-of-band* refere-se ao acesso por meio de um canal dedicado de gerenciamento que é utilizado somente para fins de manutenção do dispositivo. A vantagem de usar uma porta do console é que o dispositivo está acessível mesmo que nenhum serviço de rede esteja configurado, como a configuração inicial. Um computador executando um software de emulação de terminal e um cabo de console especial para se conectar ao dispositivo são necessários para uma conexão de console.

***Secure Shell* (SSH):** O SSH é um método dentro da banda e recomendado para estabelecer remotamente uma conexão CLI segura, através de uma interface virtual, através de uma rede. Ao contrário de uma conexão de console, as conexões SSH requerem serviços de rede ativos no dispositivo, incluindo uma interface ativa configurada com um endereço. A maioria das versões do Cisco IOS inclui um servidor SSH e um cliente SSH que podem ser usados para estabelecer sessões de SSH com outros dispositivos. https://youtu.be/ptQuntLZgSI

Telnet: O Telnet é um método inseguro em banda para estabelecer remotamente uma sessão de CLI, por meio de uma interface virtual, por uma rede. Ao contrário do SSH, o Telnet não fornece uma conexão segura e criptografada e só deve ser usado em um ambiente de laboratório. A autenticação de usuário, as senhas e os comandos são enviados pela rede como texto simples. A melhor prática é usar SSH em vez de Telnet. O Cisco IOS inclui um servidor Telnet e um cliente Telnet. https://youtu.be/eGO0QYtRYpI

Observação: Alguns dispositivos, como roteadores, também podem suportar uma porta auxiliar herdada e usada para estabelecer uma sessão CLI remotamente por uma conexão telefônica usando um modem. De modo semelhante a uma conexão de console, a porta AUX é do tipo fora de banda e não requer serviços de rede para ser configurada ou estar disponível.

4.1. Switch Básico (parte 1)

***Link* Switch Básico Parte 1**: https://youtu.be/3MdGL0wc3AE

Para iniciar iremos aprender a navegar pelo IOS, que é um processo similar a entrar e sair de diretórios ou pastas, porém utilizando comandos específicos na CLI do *switch*. Os dois modos de acesso são:

Modo EXEC usuário: assim que você entra no IOS o modo é EXEC usuário, que permite a execução de comandos básicos de monitoramento, não influenciando nas configurações do equipamento. Apenas depois de executar o comando "enable" será possível acessar o próximo modo, ou seja, o modo EXEC privilegiado. Sabemos que estamos no EXEC usuário se o *prompt* de comando for o seguinte:

```
Switch>
```

Modo EXEC privilegiado: neste modo existem comando que permitem a alteração na configuração do dispositivo, sendo que você consegue chegar aqui depois de entrar no EXEC usuário e digitar o comando "enable". A partir daqui é possível acessar outros modos, como o de configuração global, pelo comando "configure terminal". Sabemos que estamos no EXEC privilegiado se o *prompt* de comando for o seguinte:

```
Switch#
```

Agora que conhecemos os modos de acesso, vamos conhecer os modos de configuração e subconfiguração.

Modo de configuração global: estando no modo EXEC privilegiado e digitando "configure terminal" você estará automaticamente no modo de configuração global. Percebe-se isso se o seu *prompt* de comando estiver assim:

```
Switch(config)#
```

Modo de configuração de linha: se você estiver no modo de configuração global e digitar "line console 0" então você irá pular para o modo de configuração de linha, que pode ser notado pelo seguinte *prompt*:

```
Switch(config-line)#
```

Modo de configuração da interface: depois que você entrou no modo de configuração de linha digite o comando "interface fastethernet 0/1" para entrar especificamente no local onde, com outros comandos específicos, você poderá alterar configurações da porta do *switch*. O *prompt* que identifica essa mudança de modo é:

```
Switch(config-if)#
```

A Figura 28 resume bem a hierarquia existente na CLI do IOS (XAVIER, 2011):

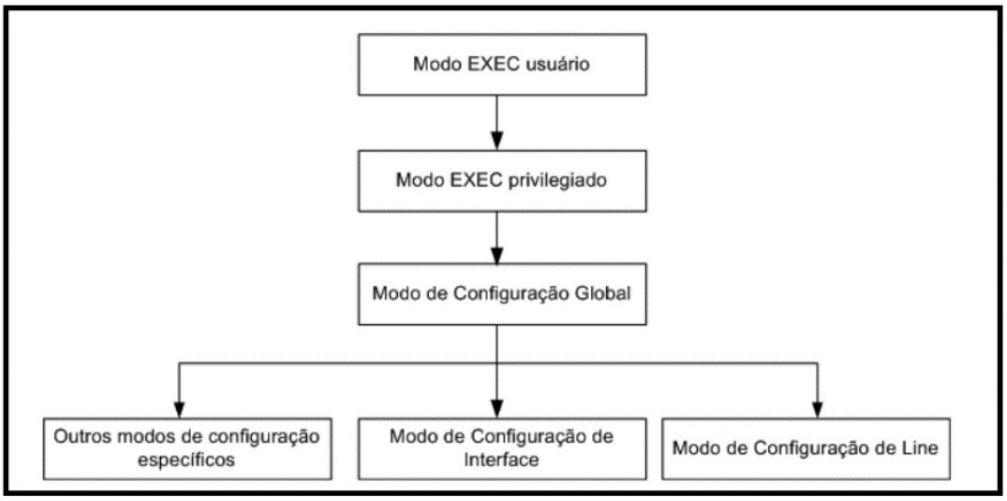


Figura 28: Hierarquia de modos na CLI

Então, antes de praticar, deixo registrado aqui os comandos básicos que vamos utilizar: ***enable***, ***configure terminal***, ***line console 0***, ***interface fastethernet 0/1***. Além desses é importante conhecer os comandos ***exit*** e ***end*** utilizados para voltar um nível ou vários níveis na hierarquia em árvore de modos na CLI. Na sequência será explicado o passo a passo de duas formas, uma usando o simulador *Packet Tracer*, e a outra com o emulador de terminal Minicom.

4.1.1. Simulador Packet Tracer

A topologia que vamos utilizar vai ser a apresentada na Figura 29, através de um cabo console ligando a entrada RS232 ou USB do computador até a saída "console" do *switch*.

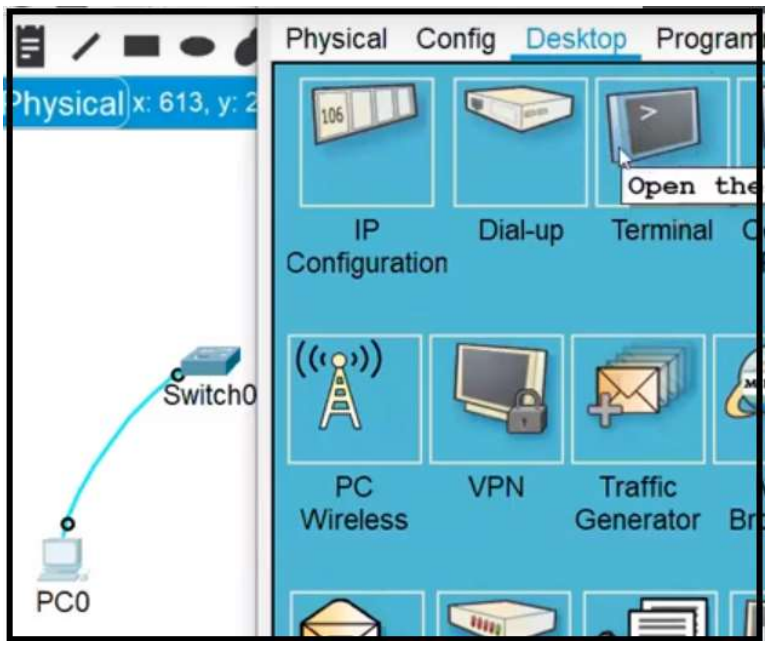


Figura 29: Acesso via cabo console

Após clicar no “PC0” deve-se abrir a aba “Desktop” e clicar no ícone que representa o terminal, local onde poderemos digitar os comandos aprendidos e fazer a navegação pelo IOS, como mostra a Figura 30:

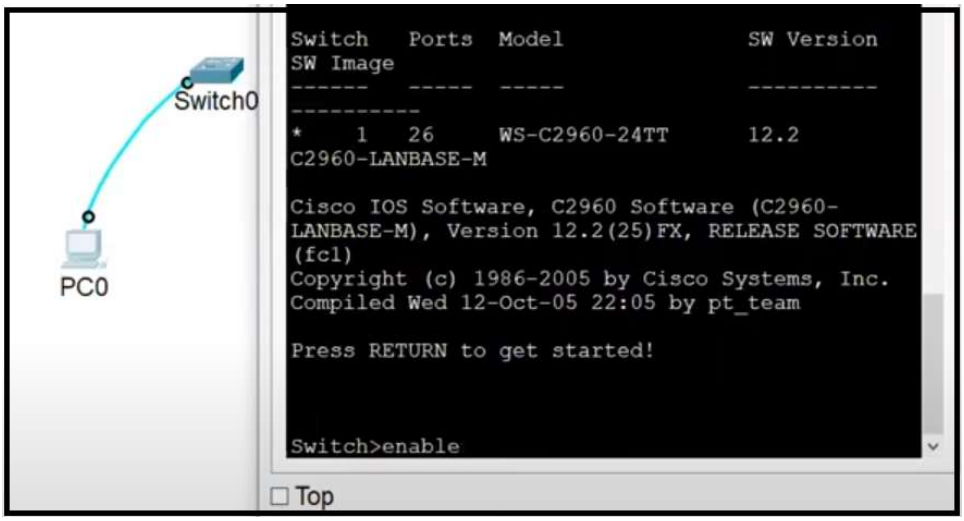


Figura 30: Comando “enable” na CLI

Para que você possa exercitar de forma prática e direta, abaixo listei uma sequência de comandos com um breve comentário, bastando digitar na linha de comando juntamente com o <*enter*>. Note as mudanças no *prompt* de comando e repita este *script* várias vezes, até conseguir memorizar e entender a dinâmica de navegação no IOS.

```
Switch>enable                                   //entra no modo EXEC privilegiado
Switch#configure terminal                       //entra no modo configuração global
Switch(config)#line console 0                   //entra no modo configuração de linha
Switch(config-line)#exit                        //volta um nível
Switch(config)#interface fastethernet 0/1       //entra no modo configuração da interface F0/1
Switch(config-if)#interface fastethernet 0/2    //entra no modo configuração da interface F0/2
Switch(config-if)#exit                          //volta um nível
Switch(config)#exit                             //volta um nível
Switch#exit                                     //volta um nível
Switch>enable                                   //entra no modo EXEC privilegiado
Switch#configure terminal                       //entra no modo configuração global
Switch(config)#line console 0                   //entra no modo configuração de linha
Switch(config-line)#exit                        //volta um nível
Switch(config)#live vty 0 15                    //entra no modo configuração de linha (telnet)
Switch(config-line)#exit                        //volta um nível
Switch(config)#interface vlan 1                 //entra no modo configuração da interface (VLAN)
Switch(config-if)#line console 0                //entra no modo configuração de linha
Switch(config-line)#end                         //volta todos os níveis
```

4.1.2. Emulador Minicom

Vamos aproveitar a topologia apresentada na Figura 29 com um cabo console ligando a entrada RS232 do computador até a saída “console” do *switch*, mas dessa vez em equipamentos reais que vão precisar de um emulador de terminal, como é mostrado abaixo (EDGE-CORE, 2017).

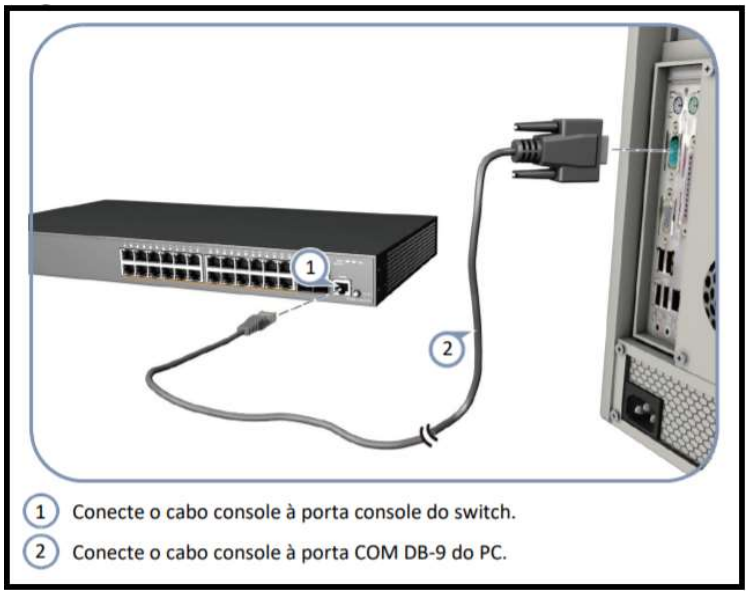


Figura 31: Conexão vai cabo console

Os emuladores de terminal são necessários para acessar e configurar o *switch* ou roteador por meio do computador. Nesse exemplo prático vamos ligar através da porta serial, depois usar o Minicom, que é um *software* livre para o sistema operacional Linux (RUFINO, 2009). Depois de devidamente instalado, acompanhe os passos para as configurações iniciais, começando pela linha de comando do Linux.

Considere que estamos num ambiente de laboratório de informática de uma escola, portanto existe uma segurança de acesso para que os alunos, para o caso de, por algum descuido, façam alterações na configuração do computador que interfira no uso da máquina dos próximos alunos. Por ser um ambiente seguro, todos os alunos precisam entrar com seu *login* e senha, tendo assim acesso limitado evitando problemas nas configurações.

Vamos admitir que neste laboratório o serviço DHCP (*Dynamic Host Configuration Protocol*), usado para obter o endereço IP de um servidor, está ativado. Entretanto, para essa atividade, vamos adicionar o IP de forma manual no nosso computador, seguindo os passos abaixo:

```
# ip link                                          // Ver nome da interface
# sudo ip addr add <ip>/<masc> dev <interface>     // Adiciona IP e máscara na interface
# ip addr                                          // Ver IP adicionado
# sudo ip link set <interface> up                  // Habilita a interface
```

Com o endereço IP da máquina devidamente adicionado, basta digitar o comando para executar o emulador de terminal.

```
# sudo minicom –s –c on                    // Executando o software minicom
```

Após executar o comando acima deverá aparecer as seguintes opções.

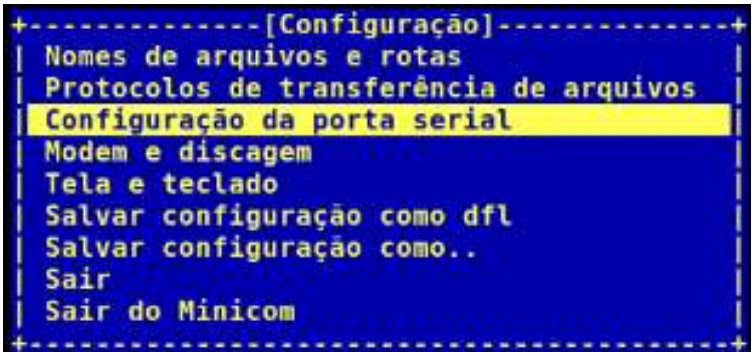


Figura 32: Configuração da porta serial

O próximo passo depois que você escolheu a opção “Configuração da porta serial” é alterar as configurações dos itens A, E e F que estão circulados, de tal forma que fique exatamente como aparece na Figura 33. Tecle a letra “A”, digite a sequência de caracteres e depois tecle um <*enter*>. Da mesma forma faça com a letra “E” e “F”.

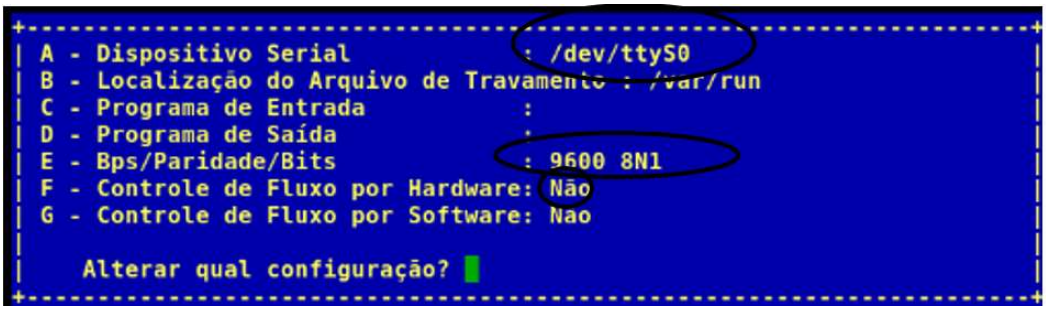


Figura 33: Configuração final da porta serial

Por fim salve as configurações escolhendo a opção “Salvar configuração como dfl” e em seguida a opção “Sair”. Se tudo estiver correto você estará acessando o *prompt* de comando do *switch*.

```
Switch>                                    //Acesso ao switch
```

Abaixo um pequeno resumo dos passos aprendidos:

- Sudo minicom -s -c on
- Configuração da porta serial
- A - /dev/ttyS0
- E - 9600 8N1
- F - Não
- ENTER
- Salvar configuração com dfl

4.2. Switch Básico (parte 2)

***Link* Switch Básico Parte 2**: https://youtu.be/kCeKngFI5T4

Um comando muito útil é o "?" (ponto de enterrogação) que funciona como um *help* ou ajuda. Ao digitá-lo será apresentado a lista de comandos possíveis naquele modo em que você se encontra no momento, juntamente com sua respectiva descrição. No exemplo a seguir o "?" é acionado no modo EXEC usuário.

```
Switch>?
Exec commands:
  connect     Open a terminal connection
  disable     Turn off privileged commands
  disconnect  Disconnect an existing network connection
  enable      Turn on privileged commands
  exit        Exit from the EXEC
  logout      Exit from the EXEC
  ping        Send echo messages
  resume      Resume an active network connection
  show        Show running system information
  ssh         Open a secure shell client connection
  telnet      Open a telnet connection
  terminal    Set terminal line parameters
  traceroute  Trace route to destination
Switch>
```

Observe que na lista acima aparece o comando "enable", confirmando assim que podemos digitar esse comando e acessar uma nova gama de comandos no EXEC privilegiado, como será feito a seguir. E para ver todos os comandos nesse modo, digitamos novamente o comando "?".

```
Switch#?
Exec commands:
  clear       Reset functions
  clock       Manage the system clock
  configure   Enter configuration mode
  connect     Open a terminal connection
  copy        Copy from one file to another
  debug       Debugging functions (see also 'undebug')
  delete      Delete a file
  dir         List files on a filesystem
  disable     Turn off privileged commands
  disconnect  Disconnect an existing network connection
  enable      Turn on privileged commands
  erase       Erase a filesystem
  exit        Exit from the EXEC
  logout      Exit from the EXEC
  more        Display the contents of a file
  no          Disable debugging informations
  ping        Send echo messages
  reload      Halt and perform a cold restart
  resume      Resume an active network connection
  setup       Run the SETUP command facility
  show        Show running system information
  ssh         Open a secure shell client connection
  telnet      Open a telnet connection
  terminal    Set terminal line parameters
  traceroute  Trace route to destination
  undebug     Disable debugging functions (see also 'debug')
  write       Write running configuration to memory, network, or terminal
Switch#
```

Perceba que a quantidade de comandos dentro do EXEC privilegiado é bem maior, sinalizando o leque de possibilidades de interação com o *switch*. A partir daqui podemos entrar em subconfigurações ou subcomandos, objetivando fazer intervenções em pontos específicos.

Então vamos executar um comando já exercitado anteriormente que permite a entrada no modo de configuração global.

```
Switch#confire terminal
              ^
% Invalid input detected at '^' marker.

Switch#
```

Ops...! Digitei o comando de forma errada, pois troquei a palavra “configure” por “confire”. Veja que o IOS aponta para a letra “t” de *terminal*, pois durante a interpretação o comando não foi reconhecido pelo algoritmo. Vamos imaginar que, mesmo com a mensagem de erro de sintaxe do interpretador, ainda não conseguimos lembrar como se escreve exatamente o comando. Nesse caso vamos usar novamente o recurso do “?”, da seguinte forma:

```
Switch#conf?
configure
Switch#conf
```

O interpretador vai listar todos os comandos que iniciam com a palavra “conf” possíveis de serem executados no modo EXEC privilegiado. Desta vez então vamos digitar o comando de tal forma que o interpretador entenda.

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
```

Vamos continuar com o nosso *help* inteligente, agora estando no modo de configuração global. Quais são os comandos possíveis aqui?

```
Switch(config)#?
Configure commands:
  aaa                 Authentication, Authorization and Accounting.
  access-list         Add an access list entry
  banner              Define a login banner
  boot                Boot Commands
  cdp                 Global CDP configuration subcommands
  clock               Configure time-of-day clock
  crypto              Encryption module
  default             Set a command to its defaults
  do-exec             To run exec commands in config mode
  dot1x               IEEE 802.1X Global Configuration Commands
  enable              Modify enable password parameters
  end                 Exit from configure mode
  exit                Exit from configure mode
  hostname            Set system's network name
  interface           Select an interface to configure
  ip                  Global IP configuration subcommands
  line                Configure a terminal line
  lldp                Global LLDP configuration subcommands
  logging             Modify message logging facilities
  mac                 MAC configuration
  mls                 mls global commands
  monitor             SPAN information and configuration
  no                  Negate a command or set its defaults
  ntp                 Configure NTP
  port-channel        EtherChannel configuration
  privilege           Command privilege parameters
  radius-server       Modify Radius query parameters
  sdm                 Switch database management
  service             Modify use of network based services
  snmp-server         Modify SNMP engine parameters
  spanning-tree       Spanning Tree Subsystem
  tacacs-server       Modify TACACS query parameters
  username            Establish User Name Authentication
  vlan                Vlan commands
  vtp                 Configure global VTP state
Switch(config)#
```

Uma lista razoável de comandos aparece nos indicando todas as possibilidades de configurações no *switch*. Tente entender o que foi feito na listagem a seguir.

```
Switch(config)#line console 0
Switch(config-line)#exit
Switch(config)#line vty 0 15
Switch(config-line)#exit
Switch(config)#interface ?
  Ethernet         IEEE 802.3
  FastEthernet     FastEthernet IEEE 802.3
  GigabitEthernet  GigabitEthernet IEEE 802.3z
  Port-channel     Ethernet Channel of interfaces
  Vlan             Catalyst Vlans
  range            interface range command
Switch(config)#interface fastethernet ?
  <0-9>  FastEthernet interface number
Switch(config)#interface fastethernet 0/1
Switch(config-if)#
```

Primeiramente digitamos o comando ***line console 0*** para entrar no modo de configuração de linha. Posteriormente entramos no ***line vty 0 15*** e na sequência tivemos a intensão de digitar o comando ***interface fastethernet 0/1***, entretanto não lembramos o restante do comando. Podemos então utilizar o "?" aqui também, onde o IOS nos mostrará o que ele aceitará para completar o comando. No nosso exemplo será "fastethernet", porém, mais uma vez ficamos indecisos na continuação do comando. Basta então novamente digitar o "?" que o IOS nos dará as possibilidades possíveis. Por fim então digitamos o número da porta do *switch* que queremos acessar e entramos na interface requerida.

Muito bem pessoal, até aqui foi possível entender o funcionamento do comando "?" e de quebra exercitar um pouco mais os comandos básicos para navegação no CLI do *switch*. A partir de agora vamos conhecer mais possibilidades e aprofundar no assunto.

4.2.1. Ping

Comando utilizado para testar conectividade entre os dispositivos. Basicamente são disparados pacotes de dados entre o dispositivo origem e destino. Assim que o dispositivo destino identifica a requisição, envia um eco ou resposta para o dispositivo origem, confirmando assim a conectividade, ou seja, o funcionamento correto entre os dois nós da rede.

Para executar o "ping" vamos utilizar aquela topologia inicial com o "PC0" e o *switch*, porém faremos dois ajustes antes. O primeiro é a atribuição de um endereço IP no "PC0" e o segundo é a inclusão de dois cabos par trançado e um outro computador, conectando o "PC0" e o novo "PC1" ao *switch*, já que o cabo que foi colocado anteriormente é um cabo de console, específico para acesso as configurações do *switch*. A comunicação e troca de dados propriamente dita, usada no dia-a-dia pelos usuários comuns, é feita via cabo par trançado.

Vamos inserir o endereço IP clicando no "PC0", entrando na aba "Desktop" e clicando na opção "IP Configuration". Nesse momento abrem-se os campos para preenchimento, conforme a Figura 34. Iremos configurar um endereço IP "Static", ou seja, será incluído manualmente e permanecerá sempre o mesmo IP. Na verdade, são duas informações que devem ser digitadas, uma é o endereço IP propriamente dito e a outra a máscara de sub-rede. Vamos aprofundar o assunto sobre endereçamento IP no próximo capítulo, portanto, nesse momento, vamos nos

limitar a digitar essas duas informações, sendo o IP “192.168.10.1” e a máscara de sub-rede “255.255.255.0”.

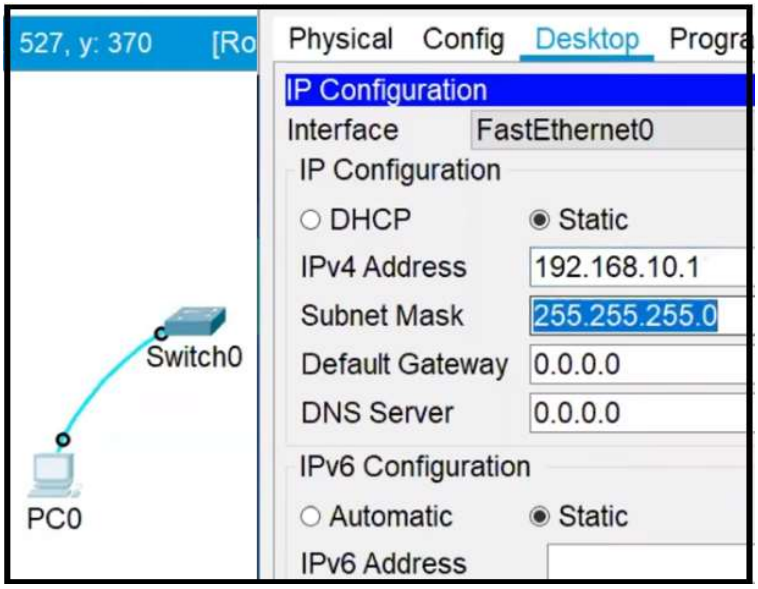


Figura 34: Configuração de endereço IP e máscara de sub-rede

Depois de finalizada a parte lógica de configuração, passaremos para a parte física, ou seja, a colocação dos cabos par trançado e o novo computador. Podemos deixar o cabo console ali onde está, ocupando as portas RS232 do computador e a porta console do *switch*, para caso for preciso fazer mais alguma configuração no *switch*.

Vamos ligar a porta *fastethernet* do “PC0” em uma das pontas do cabo, e numa das portas *fastethernet* do *switch* a outra ponta do cabo. Depois, basta acrescentar o “PC1” e repetir o procedimento para inclusão do segundo cabo de rede, ligando o “PC1” no *switch*.

Para finalizar, devemos ainda lembrar de configurar o endereço IP do novo computador. O “PC1” receberá então o IP “192.168.10.5” e máscara de sub-rede “255.255.255.0”. Note que o final do IP do “PC1” é diferente do “PC0”, justamente porque cada IP deve ser único na mesma rede. Já a máscara é exatamente a mesma, indicando que os dois PCs estão na mesma rede. Observe na Figura 35 como ficará no final.

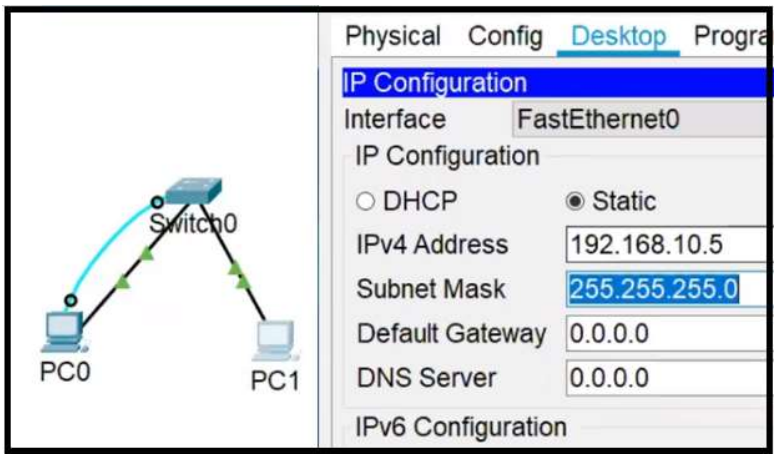


Figura 35 – Inclusão de cabo, computador, endereço IP e máscara de sub-rede

Agora vamos partir para o nosso objetivo que é a execução do comando “ping”. Iremos fazer o *ping* entre o “PC0”, que será a origem, e o “PC1”, que será o destino dos pacotes de dados. Para tanto, clique no “PC0”, selecione a aba “Desktop” e em seguida clique em “Command Prompt”, local onde você deverá digitar o comando, como mostrado abaixo:

```
C:\>ping 192.168.10.5

Pinging 192.168.10.5 with 32 bytes of data:

Reply from 192.168.10.5: bytes=32 time=1ms TTL=128
Reply from 192.168.10.5: bytes=32 time<1ms TTL=128
Reply from 192.168.10.5: bytes=32 time<1ms TTL=128
Reply from 192.168.10.5: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

A execução do “ping”, tendo como destino o endereço “192.168.10.5”, retorna quatro tentativas de respostas bem-sucedidas, cada uma com pacote de dados de 32 bytes e TTL (tempo de vida do pacote) de 128. Outra informação importante nesse relatório do comando *ping* é a que aparece na penúltima linha entre parênteses, que é “(0% loss)”, nos indicando que a conectividade está funcionando perfeitamente.

4.2.2. Hostname

Este comando serve para modificar o nome do dispositivo que no nosso exemplo chama-se “Switch0”. Importante ressaltar que esse comando só funcionará no EXEC privilegiado, dentro do modo de configuração global. Vamos então mudar o nome do *host* atual para “Sw-Floor-1”.

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname Sw-Floor-1
Sw-Floor-1(config)#
```

Observe que dessa vez, ao invés de digitar “configure terminal”, foi digitado apenas “conf t”, porque o IOS da Cisco entende o comando em formatos abreviados também, agilizando a sua digitação. E sobre o comando “hostname” veja como o *prompt* de comando se alterou, indicando a mudança de nome do *switch*. Este recurso, apesar de simples, é relevante para organização e documentação dos dispositivos, conforme a Figura 36 revela.

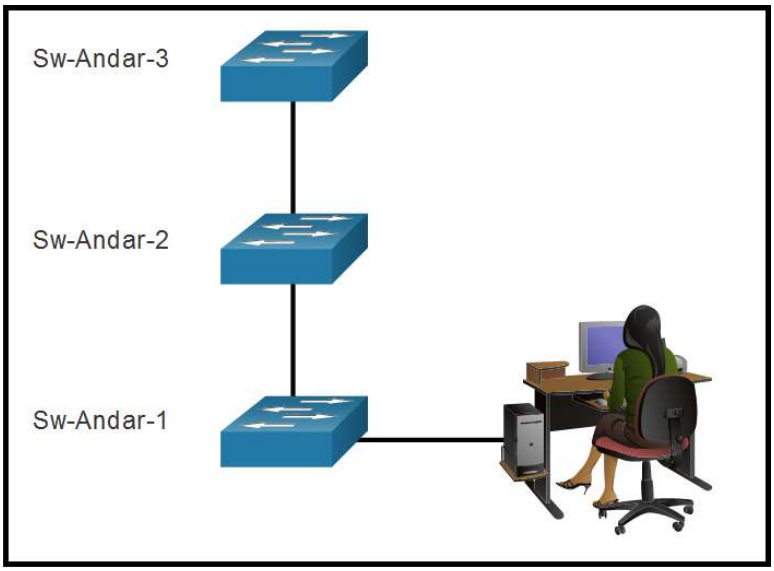


Figura 36 – Organizando com *hostname*

4.2.3. Configuração de Senha

Como você já sabe, a segurança deve ser uma preocupação constante para o profissional de redes, portanto iremos aprender a bloquear acessos não autorizados através de inclusão de senhas. Primeiramente vamos aprender a colocar senha para o EXE Usuário, que seria o *hall* de entrada de configurações do dispositivo, ou seja, para entrar no *switch* tem que passar por ali.

Senha no EXCE usuário:

```
Sw-Floor-1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Sw-Floor-1(config)#line console 0
Sw-Floor-1(config-line)#password cisco
Sw-Floor-1(config-line)#login
Sw-Floor-1(config-line)#end
Sw-Floor-1#
```

Nessa altura dos nossos estudos a novidade aqui é o comando “password” seguido da senha em si, nesse caso “cisco”. Na linha seguinte é necessário colocar também o comando “login”, para completar este processo de inclusão de senha. Opcionalmente é digitado o comando “end” só para voltar todos os níveis do EXEC privilegiado.

Bem, para testar se realmente a senha foi adicionada, vamos digitar o comando “exit” que o *switch* será reiniciado, forçando o pedido da *password*. Após digitar a senha, que permanece oculta durante a digitação, você terá acesso novamente ao *switch* pelo nosso *hall* de entrada, ou seja, pelo EXEC usuário.

```
Sw-Floor-1#exit


Sw-Floor-1 con0 is now available


Press RETURN to get started.



User Access Verification

Password:

Sw-Floor-1>
```

Vamos agora incluir senha no EXEC privilegiado, pois é um local de extremo risco caso um invasor consiga acessar.

Senha no EXEC privilegiado:

```
Sw-Floor-1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Sw-Floor-1(config)#enable password class
Sw-Floor-1(config)#end
Sw-Floor-1#
```

O comando “enable password” é utilizado para incluir a senha “class” no EXEC privilegiado. Novamente temos o comando “end” sendo usado opcionalmente, apenas para voltar ao nível inicial do modo. Digitamos o comando “exit” para sair efetivamente do EXEC privilegiado e na sequência tentar acessar, dessa vez com a senha.

```
Sw-Floor-1>enable
Password:
Sw-Floor-1#
```

Existe outro comando para colocar senha no EXEC privilegiado, porém de forma mais segura usando criptografia. Com o comando anterior a senha fica fácil para ser lida caso algum invasor consiga interceptar tal informação. A seguir vou mostrar o comando “show running-config” que permite visualizar as configurações já feitas no *switch*, inclusive a senha.

```
Sw-Floor-1#show running-config
Building configuration...

Current configuration : 1178 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Sw-Floor-1
!
enable password class
!
!
!
line con 0
 password cisco
 login
!
```

Vamos aproveitar essa imagem para destacar três configurações que já fizemos. A primeira foi o nome do *hostname*, que alteramos para “Sw-Floor-1”, a segunda e terceira foram as senhas do EXEC usuário, que aparece mais abaixo com o nome de “cisco”, e a do EXEC privilegiado com

a palavra “class”. Você já percebeu a vulnerabilidade de vazamento das senhas, por isso o próximo comando será para colocar senha criptografada no EXEC privilegiado.

```
Sw-Floor-1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Sw-Floor-1(config)#enable secret class
Sw-Floor-1(config)#end
Sw-Floor-1#
```

Se executarmos o “show running-config” novamente, o resultado será o seguinte.

```
Sw-Floor-1#show running-config
Building configuration...

Current configuration : 1178 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Sw-Floor-1
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
!
line con 0
 password cisco
 login
!
```

Agora sim conseguimos dificultar o trabalho do invasor, já que a senha está difícil de decifrar, entretanto a senha do EXEC usuário continua exposta. Para termos maior segurança vamos consertar isso utilizando o comando “service password-encryptions”, que transforma todas as senhas do tipo texto em senhas criptografadas, inclusive aquelas que serão configuradas em momentos futuros.

```
Sw-Floor-1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Sw-Floor-1(config)#service password-encryption
Sw-Floor-1(config)#end
Sw-Floor-1#
```

Basta agora executar o comando “show running-config” e verificar se a alteração funcionou.

```
line con 0
 password 7 0822455D0A16
 login
!
line vty 0 4
 login
line vty 5 15
```

Percebe-se então a que a senha do “line console 0” está também criptografada, evitando assim acesso de pessoal não autorizado. Aproveitando essa listagem, observe que temos também o “line vty 0 4” e “line vty 5 15”, que são usados para acesso remoto via terminal virtual, utilizando comandos como “telnet” ou “SSH”. Por hora vamos nos limitar a incluir uma senha também nesse modo de configuração de linha. Utilizaremos a senha “cisco” novamente, porém poderia ser qualquer outra.

Senha no VTY 0 15:

```
Sw-Floor-1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Sw-Floor-1(config)#line vty 0 15
Sw-Floor-1(config-line)#password cisco
Sw-Floor-1(config-line)#end
Sw-Floor-1#
```

Note que os números 0 a 15 representam o número de conexões possível, ou seja, 16 no total. Como desejamos bloquear com senha todas as conexões então digitamos o comando dessa forma.

```
line con 0
 password 7 0822455D0A16
 login
!
line vty 0 4
 password 7 0822455D0A16
 login
line vty 5 15
 password 7 0822455D0A16
 login
!
```

Após o comando “show running-config” ser executado veja que a senha ficou criptografada também para “vty”. Isso ocorreu por causa do comando “service password-encryptions” executado anteriormente. Na listagem apresentada o “vty” aparece em duas partes, a primeira de 0 a 4 e a outra de 5 a 15, entretanto o efeito do comando de configuração de senha utilizado aplicou-se para todas as 16 conexões.

4.2.4. Banner MOTD

Quando falamos em segurança, devemos mencionar também o comando “banner motd” que, apesar de ser um comando incrivelmente simples, funciona como argumento jurídico em vários países contra o ataque de invasores. Este comando simplesmente insere uma mensagem que vai aparecer no momento de entrada no EXEC usuário, o nosso *hall* de entrada do dispositivo, lembra? Essa mensagem pode ser algo como “Somente pessoal autorizado”, fazendo com que muitos invasores reflitam se vale a pena continuar com a invasão ou não. Vamos então executar o comando.

```
Sw-Floor-1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Sw-Floor-1(config)#banner motd #Somente pessoal autorizado#
Sw-Floor-1(config)#end
Sw-Floor-1#
```

A mensagem deve estar entre dois caracteres que não serão usados dentro da mensagem propriamente dita, que no nosso caso foi o símbolo “#”, mas que poderia ser qualquer outro. Vamos ver se realmente aparece a mensagem.

```
Sw-Floor-1#exit

Sw-Floor-1 con0 is now available



Press RETURN to get started.




Somente pessoal autorizado
User Access Verification

Password:
```

Veja que após a reentrada no EXEC usuário aparece a mensagem “Somente pessoal autorizado” enquanto o IOS aguarda a digitação da senha.

4.2.5. Salvando as configurações

Tudo que foi configurado até agora corre o risco de ser perdido se desligar o *switch* porque está ainda somente na memória RAM. Sendo assim, vamos copiar da memória RAM para a memória NVRAM que está dentro do *switch*. Tudo que está na memória RAM, ou seja, o que está sendo executado, usamos o termo “running-config”. Já tudo que está na memória NVRAM, ou seja, o que está salvo, usamos o termo “startup-config”. Utilizaremos o comando “copy” para realizar essa tarefa de salvamento das configurações atuais.

```
Sw-Floor-1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Sw-Floor-1#
```

Após digitar o comando e confirmar a cópia o IOS responde com “OK”, ratificando então sucesso no procedimento. Para testar você precisará desligar e ligar o *switch*, ou então, via linha de comando digitar “reload”, onde o equipamento irá reiniciar, copiando tudo que estiver na memória NVRAM para a memória RAM.

Depois de uma série de informações listadas na tela durante o “reload”, o interpretador fica aguardando a entrada da senha do usuário.

```
Sw-Floor-1#reload
Proceed with reload? [confirm]
C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE SOFTWARE (fc4)
Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of
memory.
2960-24TT starting...
Boot Sector Filesystem (bs:) installed, fsid: 3
Parameter Block Filesystem (pb:) installed, fsid: 4


Loading "flash:/2960-lanbasek9-mz.150-2.SE4.bin"...
#########################
Press RETURN to get started!

Somente pessoal autorizado

User Access Verification

Password:
```

4.2.6. VLANs

É possível configurar redes locais virtuais ou VLANs, abrindo-se a possibilidade de criação de sub-redes. Isso significa que não precisamos ficar totalmente amarrado a estrutura física em si. Fisicamente falando, você tem duas redes quando, usando um roteador, liga um cabo em uma porta LAN e o outro cabo na outra porta LAN. Essa segmentação da rede em duas sub-redes faz com que o desempenho da rede como um todo seja melhor. Mas imagine que você tenha 1.000 computadores em uma empresa e, para melhorar o desempenho precisasse dividir em 10 sub-redes. Bem, o preço de um roteador em geral é bem maior do que um *switch*, portanto ficaria bem caro fazer isso só na base de roteadores. Outra solução é, usar *switches* gerenciáveis, que permitam a criação de VLANs. O *switch* por si só não faz a segmentação de rede como é o caso do roteador, então é necessário usar o recurso de configuração de VLANs para isso. Além do mais, outra vantagem é que não ficamos dependentes da estrutura física dos *switches* também, pois podemos a qualquer momento determinar que porta do *switch* pertence a qual VLAN.

Podemos entender uma VLAN como sendo uma “ilha”, que fica isolada do *broadcast* da rede, e não conversa diretamente com outras VLANs. Existe uma VLAN que vem como padrão nos *switches*, que é chamada VLAN 1. Vamos utilizar ela como exemplo e fazer a atribuição de endereço IP nessa interface virtual.

```
Sw-Floor-1(config)#interface vlan 1
Sw-Floor-1(config-if)#ip add 192.168.10.254 255.255.255.0
Sw-Floor-1(config-if)#no shutdown

Sw-Floor-1(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

Sw-Floor-1(config-if)#end
Sw-Floor-1#
%SYS-5-CONFIG_I: Configured from console by console

Sw-Floor-1#
```

Acessamos a VLAN pelo comando “interface vlan 1” e depois adicionamos o endereço IP pelo comando “ip add”. É necessário também o comando “no shutdown”, que faz com que a porta lógica fique “up” ou ativa para uso.

Vamos confirmar a atribuição feita através do comando “show running-config”:

```
!
interface Vlan1
 ip address 192.168.10.254 255.255.255.0
!
```

Para finalizar faremos um teste efetivo, usando o comando “ping” entre o computador e a VLAN do *switch*. Lembre-se que, após todas as alterações que já fizemos, nossa topologia está como apresentada na Figura 37.

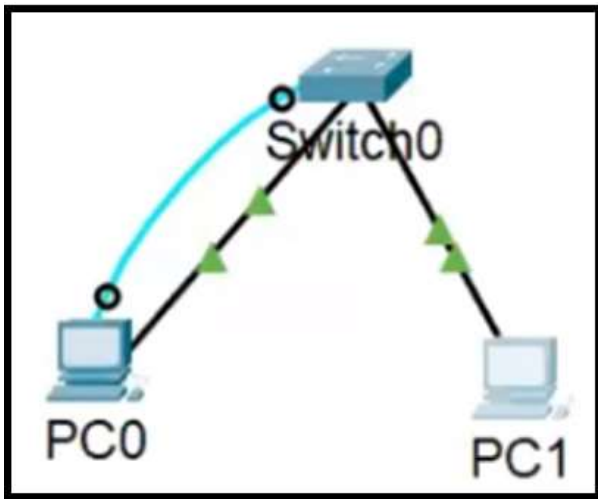


Figura 37 – Topologia com 1 switch e 2 computadores

Seguindo os passos já aprendidos anteriormente, vamos clicar no “PC0”, escolher a aba “Desktop” e clicar na opção “Command Prompt”. Com o cursor piscando no *prompt* de comando, basta digitar “ping 192.168.10.254” que corresponde ao endereço destino, ou seja, o endereço da VLAN do *switch*.

```
C:\>ping 192.168.10.254

Pinging 192.168.10.254 with 32 bytes of data:

Reply from 192.168.10.254: bytes=32 time<1ms TTL=255
Reply from 192.168.10.254: bytes=32 time<1ms TTL=255
Reply from 192.168.10.254: bytes=32 time<1ms TTL=255
Reply from 192.168.10.254: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.10.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Observe que o teste de conectividade foi bem-sucedido, onde tivemos 0% de perda de dados, confirmando então a atribuição efetiva do endereço IP. Para exercitar faça o ping do “PC1” para o *switch* e depois do *switch* para os computadores, executando assim um teste completo de conectividade.

Nesse *e-book* não será aprofundado o assunto de VLANs, nos limitando apenas com a visão geral do seu funcionamento.

5.Protocolos e Modelos

***Link* Protocolos e Modelos**: https://youtu.be/TxyqdvRRYB8

Neste material não aprofundaremos esse assunto, entretanto, nos vídeos deste *e-book* vamos trabalhar com enfoque na parte prática sobre protocolos e modelos, já que se encontra em abundância em livros, outros materiais impressos e na Internet. Sendo assim, vou dar uma explanação básica de algumas palavras-chave importantes nesse contexto.

Regras: assim como os idiomas necessitam de regras estruturadas, como a gramática e a pontuação, também os dispositivos de rede precisam de regras bem definidas, para que exista uma comunicação eficiente. Uma empresa que decida começar a fabricar roteadores ou *switches*, deve seguir as regras estabelecida pelas instituições que definem os padrões de comunicação, caso contrário este novo equipamento não conseguirá estabelecer comunicação com os equipamentos de outros fabricantes.

Protocolos: os protocolos são definidos usando regras, permitindo assim a comunicação. Para escrever um programa de computador que faça, por exemplo, o tratamento de colisões na rede de computadores, é necessário que seja baseado nos protocolos de rede que abrangem as seguintes características: codificação da mensagem, formatação e encapsulamento de mensagens, tamanho da mensagem, tempo da mensagem e opções de envio de mensagem.

Conjunto de protocolos: a comunicação nas redes de computadores se baseiam em um conjunto de protocolos, uma verdadeira sopa de letrinhas (HTTP, TCP, IP, ARP, ICMP, etc.), onde cada protocolo tem uma função específica. Os protocolos foram organizados de tal forma que funcionam em determinadas camadas dos modelos criados. O modelo TCP/IP é dividido em 4 camadas, enquanto que o modelo OSI em 7 camadas. Na Figura 38 podemos ver a pilha de protocolos TCP/IP, cada um em suas devidas camadas. Na realidade existem mais protocolos do que esses da imagem, porém aqui retratamos os principais (CISCO, 2020):

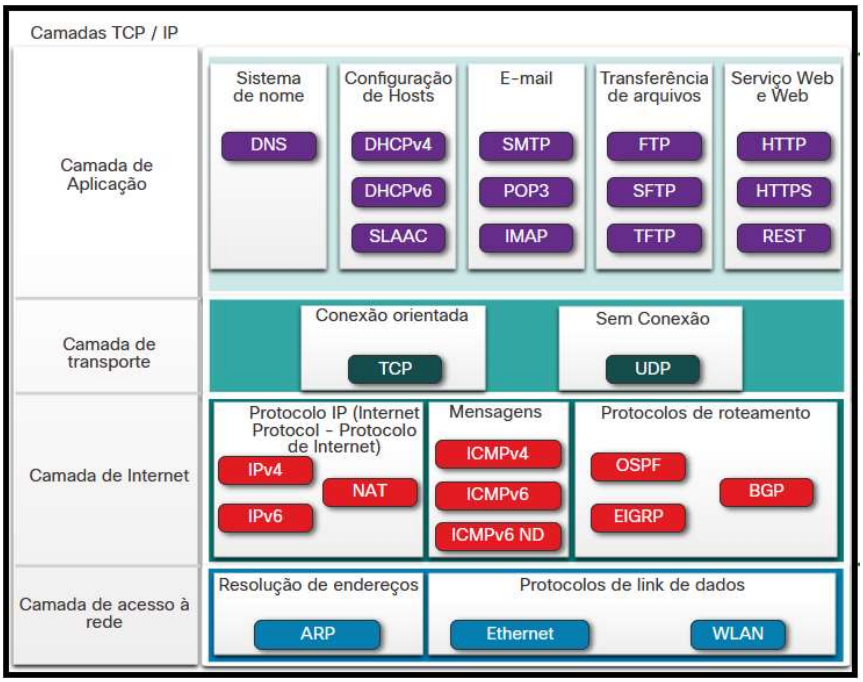


Figura 38 – Protocolos TCP/IP

Empresas de padrões: o protocolo TCP/IP é um padrão aberto, ou seja, são livres para serem utilizados. As instituições internacionais que são responsáveis por organizar e definir os padrões de protocolos de redes são: IEEE, IANA, ICANN, IETF, ITU e TIA. Aquelas mais voltadas para os padrões da Internet propriamente dita são: ISOC, IAB, IETF e IRTF.

Modelos de referência: o modelo em camadas foi adotado para facilitar o entendimento do funcionamento da rede, justamente por se tratar de um conceito complexo. Como dizem, se o problema é grande demais, então você precisa dividir ele em várias partes e ir resolvendo cada uma delas. Tanto o modelo TCP/IP quanto o modelo OSI utilizam o modelo em camadas, pois assim conseguem gerenciar melhor cada protocolo que atua somente em uma camada específica.

Encapsulamento de dados: a técnica de encapsular dados surgiu com a necessidade de aumentar a velocidade e eficiência na transmissão. Antes disso as mensagens eram enviadas da origem ao destino num fluxo contínuo e sem interrupção, entretanto, isso criava problemas para outros dispositivos que precisassem do mesmo dispositivo ou meio, resultando em atrasos consideráveis. Outro problema é que, caso houvesse uma falha durante a transmissão, toda a mensagem teria que ser retransmitida. Imagine você fazendo um *download* de um filme e, quando estivesse bem no final, por algum motivo, houvesse uma interrupção de transmissão. Pois fique sabendo que essa interrupção ocorre muitas vezes na rede e nós nem ficamos sabendo. Mas, com essa técnica de encapsulamento, apenas o que faltou no *download* é que será reenviado, tornando o processo muito mais rápido. Então, se você enviar um *e-mail* para alguém, saiba que o texto da mensagem vai fatiado em pacotes. Durante a transmissão cada pacote pode percorrer caminhos diferentes na rede até o destino. No destino os pacotes são reorganizados e desencapsulados, resultando em uma mensagem legível para o leitor.

Acesso a dados: o esquema de endereçamento é o fundamento para o acesso a dados, tanto nas redes locais como remotas. Para a comunicação na rede local utiliza-se o endereço físico, também conhecido como endereço MAC (*Media Access Control*), que já vem definido junto com a placa de rede do dispositivo. E para a comunicação remota utiliza-se o endereço lógico, também conhecido como endereço IP (*Internet Protocol*), que é configurado no equipamento, podendo ser estático ou dinâmico.

PDU (*Protocol Data Unit*): A Unidade de Dados de Protocolo nada mais é do que aquela fatia ou parte da mensagem a ser transmitida, como o exemplo da Figura 39. O PDU contém, além do dado que é parte da mensagem que será transmitida, também os metadados que tem várias funções, como armazenar o endereço de origem e de destino da mensagem. Quando o PDU é encapsulado ou desencapsulado, recebe um nome específico dependendo da camada que se encontra, que são:

Camada física:	*BIT*
Camada de enlace:	QUADRO ou *FRAME*
Camada de rede:	PACOTE
Camada de transporte:	SEGMENTO ou DATAGRAMA
Camada de aplicação:	DADOS

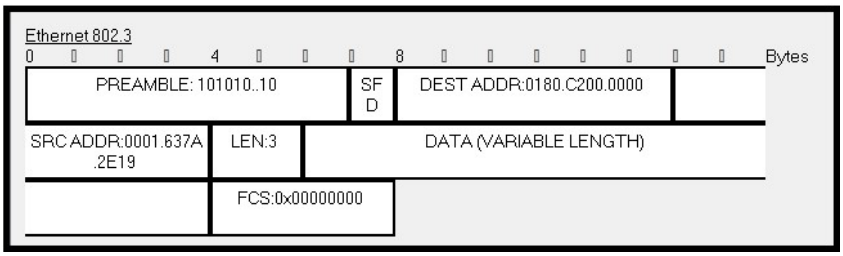


Figura 39: PDU Ethernet 802.3

Protocolo ARP (*Address Resolution Protocol*): O Protocolo de Resolução de Endereço faz o mapeamento dinâmico entre endereço lógico IP e endereços físico MAC, baseando-se no disparo de *broadcast*. Esse mapeamento é necessário porque a comunicação na rede local utiliza o endereço MAC, entretanto em geral se conhece apenas o endereço IP destino, então, através da tabela ARP é possível saber qual é o endereço MAC destino. Na sequência observamos a execução do comando "arp –a" que mostra o status atual da tabela ARP em um computador.

```
C:\>arp -a
  Internet Address      Physical Address      Type
  192.168.10.5          0002.1740.9734        dynamic
  192.168.10.254        0090.0cba.9dd1        dynamic

C:\>
```

Protocolo ICMP (*Internet Control Message Protocol*): Basicamente esse protocolo faz a notificação de erros de conectividade na rede, porém tem outras funções. No vídeo deste *e-book* é mostrado a utilização do ICMP atuando na resposta de eco da mensagem, utilizando-se o comando "ping". Essa prática será realizada através do simulador de redes *Packet Tracer*, enviando pacotes de dados entre os computadores, como ilustra a Figura 40.

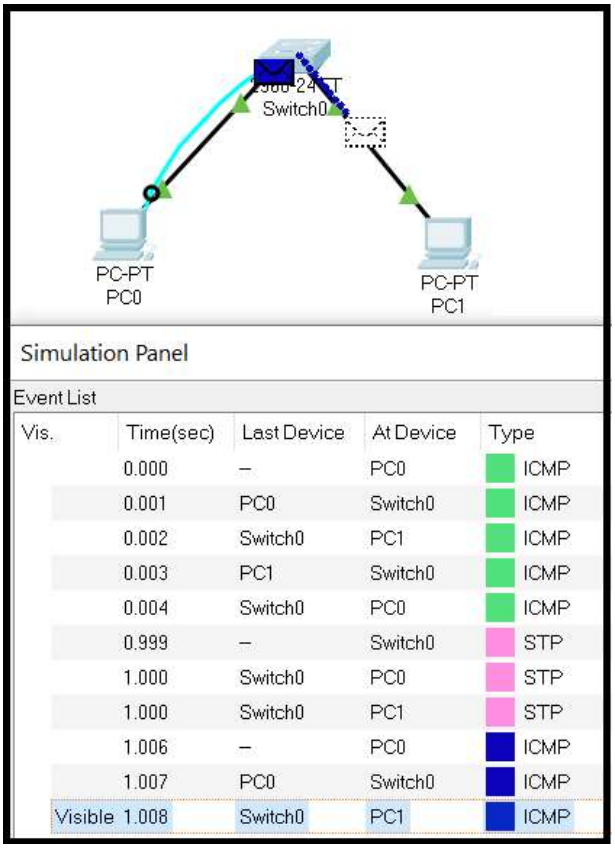


Figura 40: Protocolo ICMP

Comutação de pacotes: permite a otimização da largura de banda da rede. A comutação de pacotes difere da comutação de circuito, que estabelece uma ligação virtual de uso dedicado entre os nós da rede. A comutação de pacotes utiliza melhor os recursos da rede, visto que partilha o meio de transmissão com outros nós da rede, utilizando para isso técnicas de multiplexação temporal estatística.

Unicast: quando um quadro é enviado de um *host* endereçado a outro *host* específico, ou seja, uma entrega simples ponto a ponto. Exemplo de protocolos: HTTP, SMTP, FTP, Telnet e ICMP.

Multicast: quando um quadro é enviado de um *host* endereçado a vários outros *hosts*. Exemplo de protocolos: RTP e ATM.

Broadcast: quando um quadro é enviado de um *host* endereçado para todos os *hosts* da rede. Exemplo de protocolos: ARP e DHCP.

***Link* LAN com DHCP**: *https://youtu.be/T0Jv9eWUjTg*

***Link* Projeto de Rede com DHCP**: https://youtu.be/rdW2pXDFM-4

***Link* Configuração DHCP**: https://youtu.be/Hwht-_ZFqcY

5.1. Endereçamento IP

Chegamos em um momento valioso do *e-book*, pois o IP (*Internet Protocol*) é um dos protocolos mais importantes para o funcionamento da rede como a conhecemos. Eu diria até mesmo o mais importante, porque se o aprendizado deste assunto não for compreendido o suficiente, haverá grandes dificuldades em entender elementos mais avançados sobre redes de computadores. Por isso mesmo vou procurar ser o mais didático possível, mas o seu esforço precisa acontecer, principalmente fazendo os exercícios propostos. O assunto abrange a parte matemática, então a execução e repetição de exercícios, errando e acertando, é o pulo do gato para você se apropriar desse conhecimento.

Temos duas versões de endereço IP sendo utilizado, o IPv4 e o IPv6, ambos são incompatíveis entre si, mas com o mesmo objetivo de identificar um ponto da rede. O IPv4, ou versão 4 de endereço IP, é aquele que nos serviu e ainda serve muito bem, porém precisou ser redesenhado principalmente pela previsão de esgotamento da quantidade de endereços IP utilizados no mundo. O IPv6, ou versão 6 de endereço IP, é o substituto que já existe em muitas redes e a cada dia ocupa mais e mais o lugar do antigo. Na sequência aprenderemos primeiro sobre o IPv4 e depois sobre o IPv6.

5.1.1. Endereço IPv4

Antes de conhecer detalhadamente o IPv4 precisamos saber fazer conversão de base binária para base decimal e vice-versa. Aqui vou fazer apenas uma pequena revisão usando um método de conversão rápida, porque será necessário durante os exercícios sobre IPv4, entretanto, caso você não conheça sobre conversão de base ou queira fazer uma recapitulação mais aprofundada, sugiro acessar os *links* abaixo:

***Link* Fund Bin para Dec**: https://youtu.be/tbTdVr9KrwE

***Link* Fund Decimal para Binário**: https://youtu.be/QIJ1beTW9QE

5.1.1.1. Conversão de base binária

Vamos observar a Tabela 1 porque ela nos permitirá fazer a conversão de base de forma rápida. No IPv4 vamos utilizar no máximo 8 *bits*, ou seja, 8 números binários na mesma sequência, por esse motivo a tabela tem 8 colunas.

Tabela 1: Conversão de base

128	64	32	16	8	4	2	1

Na primeira linha, na célula de cada coluna, temos números múltiplos de 2 (1 até 128), que estão posicionados estrategicamente para receber nas células da segunda linha os números em binário. Vamos usar como exemplo o número binário “00001010” para convertê-lo em decimal, para isso basta colocar cada dígito ou *bit* nas células da segunda linha.

128	64	32	16	**8**	4	**2**	1
0	**0**	**0**	**0**	**1**	**0**	**1**	**0**

O próximo passo é simplesmente somar os números da primeira linha que tenham o dígito “1” na segunda linha. Ao somar “8 + 2”, que é igual a 10, percebemos que o número em binário “00001010” equivale ao número decimal “10”.

Se quisermos fazer o inverso, ou seja, converter o número decimal “10” para binário, basta utilizar a mesma tabela, mas desta vez vamos procurar nas colunas com os múltiplos de 2 (primeira linha), cuja soma tenha como resultado o número 10 e então inserir o “1”, ficando desta forma exposto na segunda linha o número em binário que estávamos buscando.

Apenas para ilustrar mais um pouco, abaixo temos mais dois exemplos de números convertidos de binário para decimal ou de decimal para binário. Na segunda linha temos o binário “11000000” cujo resultado em decimal é “128 + 64” totalizando “192”. Na terceira linha temos tudo preenchido com o número “1”, sendo que a soma é igual a “255”.

128	64	32	16	8	4	2	1
1	1	0	0	0	0	0	0
1	1	1	1	1	1	1	1

Coloquei estes dois exemplos de propósito para que você já comece a perceber alguma ligação desses números com o endereço IPv4. Observe que o número “192” é justamente uma identificação do primeiro valor do famoso endereço IP “**192**.168.10.1”. Já o “255” nos mostra claramente o maior número possível a ser representado, ou seja, não podemos ter um IP do tipo “**256**.168.10.1” simplesmente por ser impossível.

Agora, para ratificar seu aprendizado, resolva o exercício a seguir preenchendo a última coluna da tabela com o valor em decimal de cada linha.

Exercício 2: Conversão de binário para decimal

128	64	32	16	8	4	2	1	Decimal
1	1	0	0	0	1	1	1	
0	1	0	0	0	0	0	1	
0	0	1	0	0	0	0	0	
1	0	0	0	0	1	1	1	
0	1	1	1	1	1	1	1	
1	1	1	1	1	1	1	1	

Veja o gabarito deste exercício no *link* abaixo:

https://youtu.be/Wtq73RMyEKE?list=PL0_AXsBfViL8VF1S79OAlZmRSEEFhjGGE&t=329

5.1.1.2. Partes do IPv4

***Link* Endereço IPv4**: https://youtu.be/C2U7VoDAvlc

Tente responder as seguintes perguntas:

1) Em quantas partes se divido o endereço IPv4?
2) O que significam as classes de endereço IP (A, B, C)?
3) O que é máscara de sub-rede?

Prefiro iniciar a resposta com uma imagem de Silva, 2016:

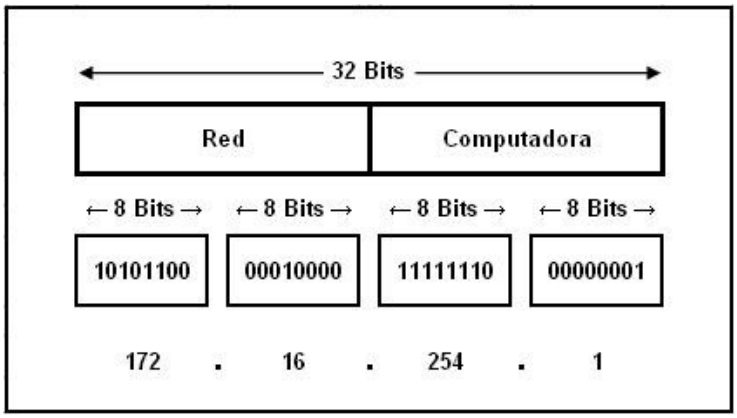


Figura 41: Partes do IPv4

Na imagem notamos que o IPv4 se divido em **32**, **4** ou **2** partes, dependendo do que exatamente queremos saber. Será em **32** partes quando contamos o número de *bits* máximo que compõe o endereço. São **4** conjuntos de 8 *bits*, também chamados de octetos, distribuídos em uma sequência numérica binária. Quando convertidos para decimal, revela-se o endereço "172.16.254.1", conforme exemplificado na Figura 41.

Mas ainda falta explicar por que o IPv4, sob outro ponto de vista, se divide em **2** partes. Só é possível responder isso se entendermos o que são as classes A, B e C, bem como o que é máscara de sub-rede. Existem ainda as classes D e E, porém não será abordado nesse material.

Você já sabe que o endereço IP é um número para identificar um dispositivo na rede, e além disso tem que ser único nesta mesma rede. Entenda que, quando temos um endereço como "172.16.254.1", uma parte dele é o número da rede e a outra parte é o número que identifica o computador propriamente dito. Para facilitar a compreensão observe a imagem a seguir que resume bem esse parágrafo.

End. IPv4 = [nº REDE LOCAL] + [nº HOST]

A dúvida que fica no ar agora é, que parte do endereço é rede local e que parte é *host*? Bem, sempre o início do endereço é da rede e o fim do endereço é do *host*. Para saber exatamente o limite entre as duas partes é necessário saber de qual classe o endereço pertence e sua máscara de sub-rede padrão, conforme mostra a Figura 42:

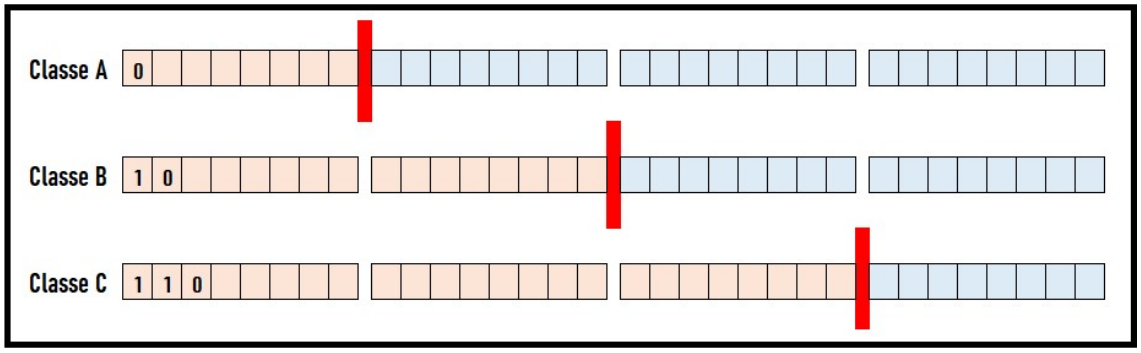


Figura 42 – Classes de Endereço IPv4

Note que um endereço de classe A é aquele em que o primeiro octeto identifica a rede, consequentemente os outros três octetos identificam o *host*. A classe B são os dois primeiros octetos para rede e os dois seguintes para *host*. Por fim a classe C tem os três primeiros octetos para rede e o último para *host*.

A máscara de sub-rede padrão nada mais é do que uma maneira de informar ao algoritmo que classe o IP pertence. A classe A tem a máscara padrão como "255.0.0.0", classe B como "255.255.0.0" e classe C como "255.255.255.0". Onde tem "255" corresponde ao octeto que é rede e onde tem "0" correspondo ao octeto que é *host*.

Uma outra notação, ou seja, outra forma de escrever a máscara de sub-rede é utilizando o símbolo "/" depois do endereço IP. Por exemplo, podemos dizer que temos o endereço IP 172.16.254.1 com a máscara 255.255.0.0 ou então simplesmente 172.16.254.1/16. O complemento "/16" significa que contamos 16 bits a partir do 1º octeto (da esquerda para direita) no endereço IP, definindo assim a máscara de sub-rede. Dependendo do sistema operacional que está sendo usado, configura-se os equipamentos com uma dessas notações.

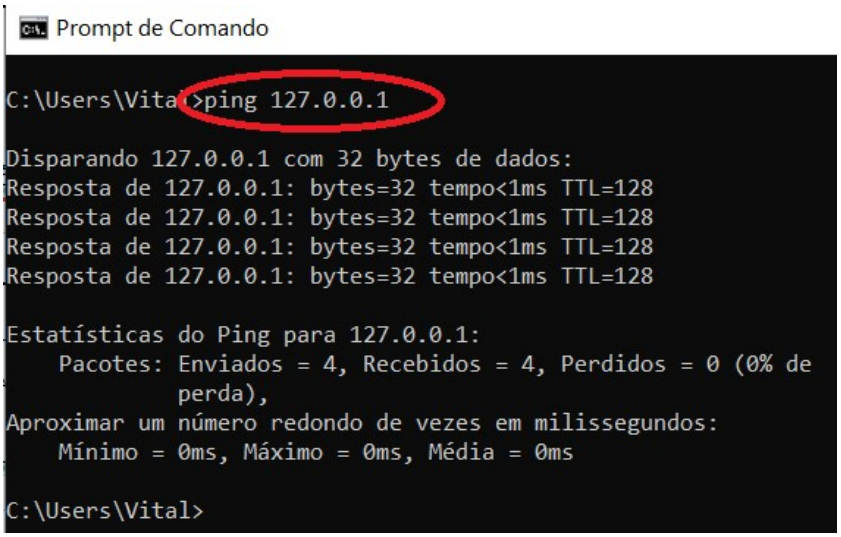
Atenção para os *bits* que aparecem no início de cada classe. Na classe A temos o *bit* "0" fixo, ou seja, todo endereço de classe A tem que ter o primeiro *bit* do primeiro octeto fixado em zero. Ficou fácil de entender que conseguimos saber qual é a classe do endereço pelo primeiro octeto, certo? Então...

1) **Qual seria a faixa de números que representa a classe A?**

Resposta: de "**0**0000001" a "**0**1111111", ou seja, qualquer IPv4 que inicia com **1**.0.0.0 a **127**.255.255.255 é um endereço de classe A.

Classe A	**0**	0	0	0	0	0	0	1	= **1**
	0	1	1	1	1	1	1	1	= **127**

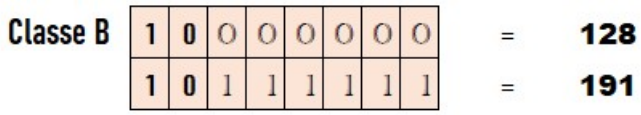
Na classe A existe uma exceção com o 127, pois ele é reservado para o chamado *loopback*, termo utilizado para fazer teste de conectividade no próprio ponto de rede. Experimento o comando "ping 127.0.0.1" no seu computador e veja que, se a conectividade de rede estiver correta, o *ping* será bem-sucedido conforme o teste a seguir:



- Máscara de sub-rede padrão: “255.0.0.0” ou sob a notação “/8”
- Número de redes: 27=128 - 2 (“0” e “127”) = 126
- Número de hosts: 224=16.777.216 – 2 (rede e broadcast) = 16.777.214

2) Qual seria a faixa de números que representa a classe B?

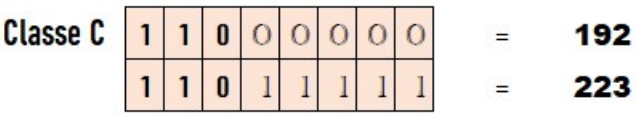
Resposta: de “**10**000000” a “**10**111111”, ou seja, qualquer IPv4 que inicia com **128**.0.0.0 a **191**.255.255.255.



- Máscara de sub-rede padrão: “255.255.0.0” ou sob a notação “/16”
- Número de redes: 214=16.384
- Número de hosts: 216=65.536 - 2 (rede e broadcast) = 65.534

3) Qual seria a faixa de números que representa a classe C?

Resposta: de “**110**00000” a “**110**11111”, ou seja, qualquer IPv4 que inicia com **192**.0.0.0 a **223**.255.255.255.



- Máscara de sub-rede padrão: “255.255.255.0” ou sob a notação “/24”
- Número de redes: 221=2.097.152
- Número de hosts: 28=256 - 2 (rede e broadcast) = 254

Com todo esse conceito em mãos você já tem condições de saber que o endereço IP “172.16.254.1” da Figura 41, é de classe “B” e por isso “172.16” é a rede do IP, e o “254.1” é o *host* propriamente dito.

Alguns endereços IP são reservados para uso interno (rede local), sem conectividade direta com a Internet global, com o objetivo de padronização da configuração das redes. São eles: “10.0.0.0 a 10.255.255.255”, “172.16.0.0 a 172.31.255.255” e “192.168.0.0 a 192.168.255.255”.

Finalizamos os estudos iniciais sobre IPv4 com um exercício. Preencha as lacunas em branco com a classe e máscara de sub-rede correta:

Exercício 3: Classe e Máscara

IP	Classe	Máscara sub-rede
192.168.10.5	_____	_____
30.10.55.10	_____	_____
129.0.0.0	_____	_____
1.1.1.1		

Veja o gabarito deste exercício no *link* abaixo:

https://youtu.be/C2U7VoDAvlc?list=PL0_AXsBfViL9Ruv1etO6Z_nXxhpMIRpFn&t=1936

***Link* Resulução Atividade:** https://youtu.be/0GoP_wndGxQ

5.1.1.3. Máscara de tamanho variável

Nesse ponto dos estudos já entendemos que a máscara de sub-rede serve para identificar a parte de rede e a parte de *host* do endereço IP, ou seja, o IP é dividido em duas partes por causa da máscara. A partir de agora vamos dividir o nosso IP em três partes: **rede**, **sub-rede** e ***host***, e isso é possível apenas alterando a máscara. Mas para que fazer isso?

Resposta: Utilizando-se máscara de sub-rede padrão (classes A, B e C) ocorre muito desperdício de endereços IP. Imagine que um ISP (*Internet Service Provider*), conhecido popularmente como provedor de acesso, precisasse disponibilizar para uma empresa ou organização 10.000 endereços IP. Para isso iria utilizar um IP de classe B que daria até 65 mil endereços. Perceba que são 55 mil endereços IP não aproveitados, simplesmente por usar uma classe padrão que engessa muito a otimização dos endereços. Poderia ainda utilizar 40 faixas de endereços de classe C separadas (40 x 254 *hosts* = 10.160), o que complicaria a configuração. Além do mais temos o gigantesco desperdício com as faixas de endereços de classe A, já que nenhuma empresa ou organização sozinha chega a utilizar 16 milhões de endereços IP.

Resolveu-se o problema com a implantação do sistema CIDR (*Classless Inter-Domain Routing*), que pronuncia-se como “cider”, desde 1993, onde são utilizadas máscaras de tamanho variável, conhecido como VLSM (*Variable-Length Subnet Mask*), permitindo a flexibilidade necessária para os projetos lógicos de rede. Se caso forem necessários 1000 endereços, poderia ser usado a máscara “/22”, que permitiria até 1022 endereços, ao invés de uma faixa inteira de classe B com 65 mil endereços (MONQUEIRO, 2010).

Objetivando deixar bem visível o funcionamento das máscaras de tamanho variável, apresentamos abaixo a tabela CIDR (BEIJER, 2012).

Tabela 2: Tabela CIDR

Pre-fixo CIDR	Máscara em Decimal	Número de 0s	Nº Redes Classful	Nº de Hosts
/1	128.0.0.0	32	128 As	2.147.483.646
/2	192.0.0.0	31	64 As	1.073.741.822
/3	224.0.0.0	30	32 As	536.870.910
/4	240.0.0.0	29	16 As	268.435.424
/5	248.0.0.0	28	8 As	134.217.726
/6	252.0.0.0	27	4 As	67.108.862
/7	254.0.0.0	26	2 As	33.554.430
/8	**255.0.0.0**	**25**	**1 A ou 256 Bs**	**16.777.214**
/9	255.128.0.0	24	128 Bs	8.388.606
/10	255.192.0.0	23	64 Bs	4.194.302
/11	255.224.0.0	22	32 Bs	2.097.150
/12	255.240.0.0	21	16 Bs	1.048.574
/13	255.248.0.0	20	8 Bs	524.286
/14	255.252.0.0	19	4 Bs	262.142
/15	255.254.0.0	18	2 Bs	131.070
/16	**255.255.0.0**	**17**	**1 B ou 256 Cs**	**65.534**
/17	255.255.128.0	16	128 Cs	32.766
/18	255.255.192.0	15	64 Cs	16.382
/19	255.255.224.0	14	32 Cs	8.190
/20	255.255.240.0	13	16 Cs	4.094
/21	255.255.248.0	12	8 Cs	2.046
/22	255.255.252.0	11	4 Cs	1.022
/23	255.255.254.0	10	2 Cs	510
/24	**255.255.255.0**	**9**	**1 C**	**254**
/25	255.255.255.128	8	1/2 C	126
/26	255.255.255.192	7	1/8 C	62
/27	255.255.255.224	6	1/4 C	30
/28	255.255.255.240	5	1/16 C	14
/29	255.255.255.248	4	1/32 C	6
/30	255.255.255.252	3	1/64 C	2
/31	255.255.255.254	2	1/128 C	0
/32	255.255.255.255	1	1/256 C	1

Vamos pegar como exemplo o seguinte endereço.

Endereço IP: 192.168.10.1/24
Classe: C
Máscara: 255.255.255.0

Observe que tem a notação "/24" atrás do IP, apontando que a máscara atual é 255.255.255.0. Isso significa dizer que "192.168.10" é rede e "1" é *host*. Agora vamos alterar a máscara para que possamos ter também alguns *bits* para sub-rede.

Endereço IP: 192.168.10.1/27
Classe: C
Máscara: 255.255.255.224

Através da Figura 43 fica fácil para perceber a alteração da máscara, contando mais 3 *bits* e avançado sobre o *host*. Na prática ocorre a liberação de alguns *bits* do *host* para que possa ser usado pela sub-rede. É claro que com isso haverá menos *hosts* por sub-rede, entretanto o uso de sub-redes é relevante principalmente em redes com mais de 50 computadores, visto que o compartilhamento de uma mesma sub-rede por vários pontos acarreta o chamado *broadcast*, ou seja, lentidão pela redução na taxa de transmissão de dados.

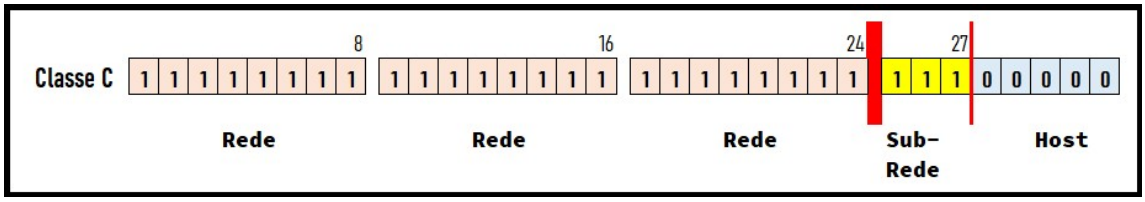


Figura 43 – Máscara de sub-rede alterada

Veja que os 3 *bits* da sub-rede não podem ser representados separadamente em decimal, por isso mesmo que o último octeto ficou em "224", que é a conversão do binário "1110000" para decimal. Tudo isso vai ficar mais claro assistindo ao vídeo e fazendo os exercícios.

***Link* Máscara Sub-Rede**: https://youtu.be/D0iShYtT3dQ

Tabela 3: *Range* de endereços IP

Número de Sub-Redes: $2^3 = 8$ Número de Hosts: $2^5 = 32-2= 30$

IP	**192**	**168**	**0**	**0**	192.168.0.0/27	
Másc	255	255	255	224		
	1º octeto	2º octeto	3º octeto	4º octeto	IP	
1ª sub rede				000 00000	192.168.0.0	**sub-rede**
				000 00001	192.168.0.1	**1º host**
				000 11110	192.168.0.30	**último host**
				000 11111	192.168.0.31	**Broadcast**
2ª sub rede				001 00000	192.168.0.32	**sub-rede**
				001 00001	192.168.0.33	**1º host**
				001 11110	192.168.0.62	**último host**
				001 11111	192.168.0.63	**Broadcast**

A Tabela 3 nos mostra logo no início o cálculo da quantidade de sub-redes possíveis com este endereço IP e máscara, juntamente com a quantidade de *hosts*. Na primeira e segunda linhas da tabela temos as informações básica para conseguirmos destrinchar cada *bit*, e assim entender o que acontece.

Note que existem as colunas de 1º, 2º, 3º e 4º octetos, onde trabalharemos os detalhes apenas do 4º octeto, pois é ali que está a sub-rede. A primeira informação importante é o preenchimento do primeiro IP possível, ou seja, a sequência de *bits* "**000**00000". Sabemos que esse IP é da sub-rede "000" e host "00000". O primeiro endereço de *host* possível sempre é reservado para identificação da sub-rede, então não podemos utilizá-lo como o IP de um computador. Portanto, convertendo de binário para decimal teremos o endereço IP "192.168.0.0", correspondente ao endereço de sub-rede.

Continuando a contagem, na linha seguinte temos os *bits* "**000**00001", ainda na sub-rede zero, porém com um endereço IP válido para ser atribuído em algum dispositivo da rede. Convertendo de binário para decimal temos o IP "192.168.0.1".

Para a nossa tabela não ficar muito grande, vamos pular dos dois primeiros IP´s para os dois últimos da mesma sub-rede. Fica então "**000**11110" para o penúltimo IP da sub-rede zero. Com a conversão ficamos com o IP "192.168.0.30". E por fim o último IP que sempre é reservado para endereço de *broacast*, que é uma maneira de enviar pacotes para todos da mesma sub-rede. Fica então o IP "192.168.0.31".

Assim, qualquer endereço entre "192.168.0.1" até "192.168.0.30", podem ser atribuídos aos dispositivos. Esse *range* de endereços pertence a sub-rede "000".

A história se repete exatamente da mesma forma, só que agora para a sub-rede "001". São quatro endereços que precisamos (sub-rede, primeiro *host*, último *host* e *broadcast*). Com essas informações temos o *range* ou faixa de endereços dessa segunda sub-rede.

Perceba que a Tabela 3 está incompleta, visto que podemos ter até 8 sub-redes. Então agora é sua vez! Através do Exercício 4 você irá preencher os campos vazios da tabela.

Observação:

Todo esse cálculo pode ser realizado utilizando-se uma calculadora IP, bastando simplesmente você colocar os parâmetros iniciais, como o endereço IP e a máscara de sub-rede desejada. Para conhecer esse tipo de calculadora, assista o vídeo a seguir.

***Link* Calculadora IP**: https://youtu.be/XU27eXydaUk

Exercício 4: Praticando o *range* de endereços IPv4

	1º octeto	2º octeto	3º octeto	4º octeto	IP	
3ª sub rede				010		**sub-rede**
						1º host
						último host
						Broadcast
4ª sub rede						**sub-rede**
						1º host
						último host
						Broadcast
5ª sub rede						**sub-rede**
						1º host
						último host
						Broadcast
6ª sub rede						**sub-rede**
						1º host
						último host
						Broadcast
7ª sub rede						**sub-rede**
						1º host
						último host
						Broadcast
8ª sub rede						**sub-rede**
						1º host
						último host
						Broadcast

Tabela 4: Gabarito do Exercício 4

	SUB-REDE	1º HOST	ÚLTIMO HOST	BROADCAST
1º	**0**	**1**	**30**	**31**
2º	32	33	62	63
3º	64	65	94	95
4º	**96**	**97**	**126**	**127**
5º	128	129	158	159
6º	160	161	190	191
7º	192	193	222	223
8º	**224**	**225**	**254**	**255**

5.1.2. Endereço IPv6

***Link* IPv6**: https://youtu.be/HM-N2YNwglU

Seguindo a mesma linha de raciocínio nos estudos sobre IPv4, aqui também podemos nos perguntar:

1. Em quantas partes se divide o IPv6?
2. Existem classes de endereços (A, B e C) como no IPv4?
3. Existe máscara de sub-rede também no IPv6?

A Figura 44 de SILVA, 2016, nos ajuda na busca das respostas.

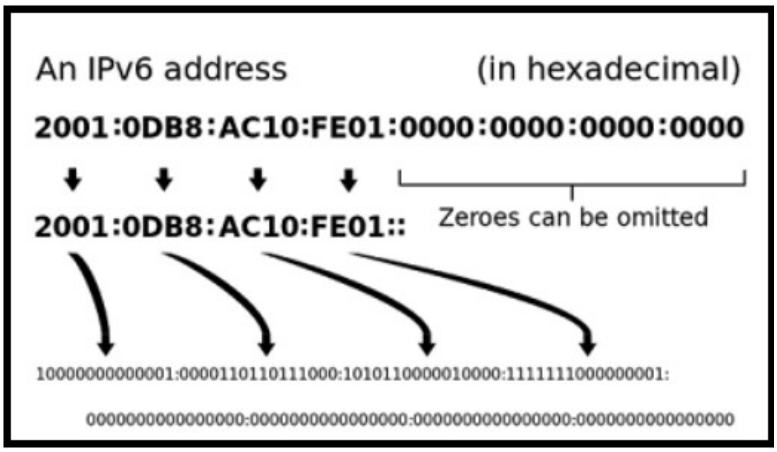


Figura 44: Partes do IPv6

O IPv6 se divide em **128**, **8** e **2** partes, dependendo do ponto de vista. Em número de *bits* são 128, ou seja, 4 vezes mais do que o IPv4. São 8 conjuntos de 16 *bits*, comumente chamados de hextetos, distribuídos em uma sequência numérica binária. Quando convertidos para hexadecimal, revela-se o endereço "2001:0DB8:AC10:FE01:0000:0000:0000:0000", conforme exemplificado na Figura 44. Se desejar entender melhor como funcionam os números hexadecimais, então assista o vídeo a seguir:

***Link* Hexadecimal**: https://youtu.be/dKFXTGDdA4I

Só pra ter uma ideia em termos de quantidade de *hosts* que poderíamos ter com apenas um hexteto, vamos pegar como exemplo o último bloco de hexteto que inicia em "0000". O maior valor que podemos representar é "FFFF", ou seja, "1111 1111 1111 1111" em binário. Isso quer dizer que apenas nesse hexteto podemos ter até 65.536 *hosts*, tornando assim o gerenciamento de endereços muito mais simples do que no IPv4.

A divisão em **2** partes ocorre pela mesma razão que vimos no IPv4, ou seja, o início do endereço IPv6 é para identificar a rede e o final para identificar o *host*. Mas será que existem classes de endereços (A, B e C) no IPv6? E será que podemos também criar sub-redes com o IPv6?

No IPv6 não existem classes de endereços, liberando assim a antiga forma engessada de dividir o endereço em parte de rede e parte de *host*. O que existe é o prefixo (rede) e o sufixo (*host*), cuja divisão entre rede e *host* pode ser em qualquer parte do endereço. Para as sub-redes utilizamos uma parte do endereço IP, como já fazíamos no IPv4, entretanto com uma quantidade

de combinações absurdamente maior. Por padrão a divisão do IPv6 em rede, sub-rede e *host* é feita como mostra a Figura 45 (CISCO, 2021):

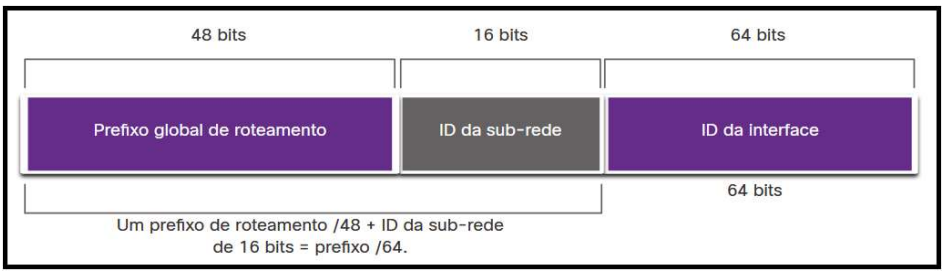


Figura 45: IPv6 em rede, sub-rede e *host*

Os primeiros 48 *bits* são para roteamento global, conhecido como prefixo de rede. Os demais 16 *bits* servem para usar como sub-rede, onde espera-se que seja suficiente para suprir a necessidade de todos, afinal de contas é possível ter até 65.536 sub-redes para cada rede local. Os outros 64 *bits* são para o *host*, lembrando que o termo correto para *host* quando estamos falando sobre IPv6 é "ID da interface".

Vamos finalizar os estudos iniciais sobre IPv6 mostrando algumas regras básicas que podemos usar para abreviar o tamanho do número, pois como você percebeu, mesmo em hexadecimal, ele se torna um número um tanto extenso. Vamos continuar com o exemplo da Figura 45, ou seja, o "2001:0DB8:AC10:FE01:0000:0000:0000:0000"

Existem duas regras ou etapas para compactar a representação numérica do IPv6, que são:

Regra 1: Omitir zero à esquerda

TIPO	FORMATO
Preferencial	2001:0DB8:AC10:FE01:0000:0000:0000:0000
Nenhum zero à esquerda	2001:**DB8**:AC10:FE01:**0**:**0**:**0**:**0**

Observe que todos os zeros à esquerda de cada hexteto foram eliminados do formato preferencial, reduzindo de forma considerável o tamanho de sua representação.

Regra 2: Dois pontos duplos

TIPO	FORMATO
Preferencial	2001:0DB8:AC10:FE01:0000:0000:0000:0000
Nenhum zero à esquerda	2001:**DB8**:AC10:FE01:**0**:**0**:**0**:**0**
Compactado	2001:DB8:AC10:FE01**::**

Veja que no formato compactado trocamos o "0:0:0:0" por "::", tornando muito mais simples a visualização e, consequentemente, facilitando o estudo, análise e documentação do mesmo.

O Exercício 5 da Cisco, 2021 a seguir irá ajudar na absorção dessas duas regras exemplificadas. Faça cuidadosamente e depois confira o gabarito para avaliar seu aprendizado.

Exercício 5: Praticando tipos de formatos do IPv6

a) TIPO	FORMATO
Preferencial	2001 : 0db8 : 0000 : 1111 : 0000 : 0000 : 0000 : 0200
Nenhum 0 à esq.	
Compacto	

b) TIPO	FORMATO
Preferencial	2001 : 0db8 : 0000 : 0000 : ab00 : 0000 : 0000 : 0000
Nenhum 0 à esq.	
Compacto	

c) TIPO	FORMATO
Preferencial	2001 : 0db8 : aaaa : 0001 : 0000 : 0000 : 0000 : 0000
Nenhum 0 à esq.	
Compacto	

d) TIPO	FORMATO
Preferencial	fe80 : 0000 : 0000 : 0000 : 0123 : 4567 : 89ab : cdef
Nenhum 0 à esq.	
Compacto	

e) TIPO	FORMATO
Preferencial	fe80 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0001
Nenhum 0 à esq.	
Compacto	

f) TIPO	FORMATO
Preferencial	0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0001
Nenhum 0 à esq.	
Compacto	

g) TIPO	FORMATO
Preferencial	0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000
Nenhum 0 à esq.	
Compacto	

Tabela 5: Gabarito do Exercício 5

Tipo	Formato
Preferêncial	2001 : 0db8 : 0000 : 1111 : 0000 : 0000 : 0000 : 0200
Compressados/espaços	2001 : db8 : 0 : 1111 : : 200
Compactado	2001:db8:0:1111::200
Preferencial	2001 : 0db8 : 0000 : 0000 : ab00 : 0000 : 0000 : 0000
Compressados/espaços	2001 : db8 : 0 : 0 : ab00 ::
Compactado	2001:db8:0:0:ab00::
Preferencial	2001 : 0db8 : aaaa : 0001 : 0000 : 0000 : 0000 : 0000
Compressados/espaços	2001 : db8 : aaaa : 1 ::
Compactado	2001:db8:aaaa:1::
Preferencial	fe80 : 0000 : 0000 : 0000 : 0123 : 4567 : 89ab : cdef
Compressados/espaços	fe80 : : 123 : 4567 : 89ab : cdef
Compactado	fe80::123:4567:89ab:cdef
Preferencial	fe80 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0001
Compressados/espaços	fe80 : : 1
Compactado	fe80::1
Preferencial	0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0001
Compressados/espaços	:: 1
Compactado	::1
Preferencial	0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000
Compressados/espaços	::
Compactado	::

5.2. Game

Game Aspire CCNA: https://youtu.be/7bZR1pqRzK4

Dicas e Desafios: https://youtu.be/CzT1cTqZ8m8

Se você gosta de *games* e também de tecnologia então chegou aquele momento de, além de brincar, também fixar ainda mais os conhecimentos deste *e-book*. Estou falando de um jogo da Cisco chama Aspire CCNA, no estilo dos jogos de RPG, projetado para aqueles que desejam se preparar para as provas de certificação da Cisco ou simplesmente se divertir.

O *download* do *game* está na descrição do vídeo onde é apresentado uma visão geral, como se fosse um pequeno tutorial. Tem ainda um segundo vídeo onde revelo algumas dicas para conseguir vencer certos desafios do jogo. Bom divertimento!

Figura 46: Casa do seu avatar

Figura 47: Cidade do seu avatar

6.Acrônimos

ACL	Access Control List
ADSL	Assymetrical Digital Subscriber Line
ANSI	American National Standards Institute
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
BNC	Bayone Neil Concelman
BYOD	Bring Your Own Device
CCNA	Cisco Certified Network Associate
CLI	Command Line Interface
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DSL	Digital Subscriber Line
EIA	Electronic Industries Association/
FTP	File Transfer Protocol
HTTP	HyperText Transfer Protocol
IA	Inteligência Artificial
IAB	Internet Architecture Board
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IOS	Internetwork Operation System
IoT	Internet of Things
IP	Internet Protocol
IP	Intrusion Prevention System
IRTF	Internet Research Task Force
ISOC	Internet Society
ITU	International Telecommunication Union
LAN	Local Area Network
Li-Fi	Light Fidelity
MAC	Media Access Control
MAN	Metropolitan Area Network
MT-RJ	Mechanical Register-Registered Jack
NBR	Normas Brasileiras
OSI	Open System Interconnection
PAN	Personal Area Network
PDU	Protocol Data Unit
PT	Ponto de Telecomunicação
QoS	Quality of Service
RAN	Regional Area Nework
RFID	Radio-Frequency Identification
RG	Radio Government
RJ45	Registered Jack
RPG	RolePlaying Game
RTP	Real-time Transport Protocol
SAN	Store Area Network
SC	Subscriber Channel
SDN	Software Defined Networking
SDSL	Symmetric Digital Subscriber Line
SMTP	Simple Mail Transfer Protocol
ST	Straigh-Tip
STP	Shielded Twisted Pair
TCP	Transmission Control Protocol/
TIA	Telecommunications Industry Association
UTP	Unshielded Twisted-Pair
VLAN	Virtual Local Area Network
VoIP	Voice of Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
WiFi	Wireless Fidelity
Wi-MAX	Worldwide Interoperability for Microwave Access

Referências Bibliográficas

ABNT. Cabeamento estruturado para edifícios comerciais e data centers. 2013. Acessado em 07/08/2021. Disponível em: < https://www.abntcatalogo.com.br/norma.aspx?ID=307178>. Citado na página 31.

ALCTEL. Redes Convergentes: conheça as suas principais vantagens. 2020. Acessado em 16/07/2021. Disponível em: <https://novosite.alctel.com.br/redes-convergentes-conheca-as-suas-principais-vantagens/>. Citado na página 30.

ALECRIM, Emerson. Diferenças entre roteador, switch, modem e hub. 2019. Acessado em 22/09/2021. Disponível em: <https://www.infowester.com/hubswitchrouter.php>. Citado na página 9.

BEIJER, Jaques de. Tabela de SubNets IPv4. 2012. Acessado em 23/09/2021. Disponível em: <https://linuxrede.wordpress.com/?s=cidr>. Citado na página 63.

CASA EFICIENTE. Eficiência, controle e segurança: os eixos que comandam a domótica. 2020. Acessado em 17/07/2021 em: < https://casaeficiente.com/eficiencia-controlo-e-seguranca-os-eixos-que-comandam-a-domotica/>. Citado na página 32.

CERT.BR. Honeypots Distribuídos. 2019. Acessado em 17/07/2021. Disponível em: < https://www.cert.br/projetos/>. Citado na página 34.

CISCO. Introduction to Networks. 2021. Acessado em 14/07/2021. Disponível em: <https://www.netacad.com/courses/networking/ccna-introduction-networks>. Citado nas páginas 20, 21, 22, 23, 28, 30, 33, 35, 53, 68.

EDGE-CORE. Guia de Instalação. 2017. Acessado em 28/09/2021 em: < https://www.edge-core.com/_upload/images/ECS2100_series_8_models_IG_R03_20181019-Portuguese.pdf>. Citado na página 39.

FOROUZAN, Behrouz A. Comunicação de Dados e Redes de Computadores, 4a ed. - Editora Bookman, 2008. Citado nas páginas 11 e 16.

MONQUEIRO, Julio Cesar Bessa. Entendendo o CIDR (máscaras de tamanho variável). 2010. Acessado em 23/09/2021. Disponível em: <https://www.hardware.com.br/dicas/entendendo-cidr.html>. Citado na página 63.

RUFINO, Antonio Carlos dos Santos. Minicom em notebooks. 2009. Acessado em 28/09/2021. Disponível em: < https://www.vivaolinux.com.br/dica/Minicom-em-notebooks>. Citado na página 39.

SILVA, Gabriel. As diferenças entre IPv4 e IPv6. 2016. Acessado em 29/07/2021. Disponível em: <http://1430831612010-gabriel-silva.blogspot.com/2016/05/as-diferencas-entre-ipv4-e-ipv6.html>. Citado nas páginas 59 e 67.

TERRA, Portal. Cartilha de Segurança para Internet. 2005. Acessado em 20/08/2021. Disponível em: <https://www.terra.com.br/informatica/especial/cartilha>. Citado na página 99.

XAVIER, Fábio Correa. Roteadores Cisco: Guia Básico de Configuração e Operação. 2011. Acessado em 17/07/2021. Disponível em: < https://s3.novatec.com.br/capitulos/capitulo-9788575222096.pdf>. Citado na página 37.