Componentes de uma Rede, LAN, WAN

Uma rede é um conjunto de dispositivos ligados que podem trocar informações entre si (não apenas computadores, mas também impressoras, servidores, câmeras de vigilância, smartphones, etc.), além de compartilhar recursos e aplicativos.

Um exemplo é um compartilhamento de impressora, que pode ser acessada diretamente pelos computadores, ou pode ter um computador na rede que vai ser o servidor de impressão. Isso vale pra outras coisas como banco de dados e aplicativos.

Essas são as partes que compõem uma rede:

- **Computadores Cliente:** Também chamados de estações de trabalho. É o computador do usuário final.
- **Servidores:** São os computadores que compartilham algum recurso como discos para armazenamentos de dados ou impressoras. Em um servidor normalmente roda um sistema operacional de rede como o Windows Server 2008 ou uma versão de Linux como o Red Hat ou o Ubuntu Enterprise.
- **Interfaces de Rede:** Hoje computadores como desktop e notebook vêm de fábrica com uma "placa de rede" incorporada.
- **Cabos:** A maior parte das redes hoje utilizam um tipo de cabo de rede do tipo UTP, outras opções como cabo coaxial e fibra óptica são encontradas de acordo com a necessidade da rede.
- **Switches e Roteadores:** Switches ligam dispositivos entre si e roteadores conectam redes diferentes. Falaremos sobre eles mais pra frente.
- **Redes sem Fio:** Antenas, placas de rede para redes sem fio, pontos de acesso e outros dispositivos são encontrados facilmente hoje em dia.

PS: Nesses servidores ficam também programas como o Apache Web Server e o Microsoft Exchange.

Quando usamos o conceito de LAN e WAN, não exatamente falamos do tamanho da rede.

Quando falamos de LAN, estamos falando de uma rede de área local, mas não necessariamente uma rede pequena, mas sim uma rede interna (como por exemplo, os computadores que estão numa mesma rede, o roteador e o modem).

Já a WAN, é uma rede interligada de lugares distantes (por exemplo, uma rede LAN em São Paulo ligada numa rede em Recife), o que permite controlar computadores mesmo por essa distância (como um acesso remoto). A WAN também inclui o acesso à internet à qualquer site (como o seu computador e o servidor do Google, por exemplo).

Topologias

Topologia basicamente é a forma de como os dispositivos ficam dispostos na rede, como se fosse o "desenho" da rede:

As topologias mais comuns são:

- **Barramento:** Todos os dispositivos são ligados no mesmo cabo, que precisa de uma terminação em cada uma das pontas (onde não tem dispositivo, tem um terminador para não dar interferência).
- **Anel:** Um dispositivo é ligado um ao outro sem terminação, como um “anel” mesmo.
- **Estrela:** Os dispositivos são conectados através de um dispositivo concentrador (muitas vezes um roteador ou switch). O mais comum.
- **Malha:** Não é muito usada em redes pequenas, os nós nela tem mais de uma conexão.
- **Híbrida:** Quando usamos mais de uma topologia juntas (tipo por exemplo, barramento estrela.

Modelo OSI

O modelo OSI descreve as regras que padronizam os diversos componentes em uma rede para que os dispositivos consigam se comunicar. O modelo OSI é dividido em sete camadas:

- **Aplicação:** Interfaces com aplicativos (tudo que o usuário mexe no computador que acessa a rede, como navegadores, através de regras de protocolos).
- **Apresentação:** Formatos e criptografia (quando vemos por exemplo, uma foto que é transmitida na rede e é interpretada por um formato, como JPG ou PNG. Criptografia já é algo mais a segurança).
- **Sessão:** Controle de sessões entre aplicativos (quando acessamos um outro computador remotamente, quando começa e termina a sessão, etc.).
- **Transporte:** Conexão entre hosts/portas (dessas conexões define se estas serão confiáveis, e se usará TCP ou UDP), Já sobre as portas, é o identificador do host do computador ou servidor.
- **Rede:** Endereço lógico e roteamento (endereço lógico nada mais é que o IP, que toda máquina tem). Roteamento é quando acessamos um servidor através de roteadores, não os da nossa LAN.
- **Enlace:** Endereço físico (isso é referente ao endereço MAC) e verificação de erros.
- **Física:** Hardware e sinal elétrico (hardware é a placa de rede e os conectores. O sinal elétrico é nada mais que a tensão da rede telefônica).

PS: As camadas são contadas de baixo pra cima nesse caso, a primeira é a Física, a segunda é a Enlace e assim por diante.

Introdução ao TCP/IP

TCP/IP é um conjunto de protocolos de comunicação e começou a ser desenvolvido pelo departamento de defesa americano de onde vem o termo DoD.

O TCP/IP é dividido em quatro camadas:

TCP/IP	Referente ao Modelo OSI
Aplicação	Aplicação
	Apresentação
	Sessão
Transporte (Host-to-Host)	Transporte
Rede (Internet)	Rede

Física (Acesso à Rede)	Enlace
	Física

Veja alguns exemplos dos protocolos em pilhas de TCP/IP:

Camadas	Protocolos
Aplicação	HTTP, SMTP, IMAP, FTP, SIP, SSH, Telnet
Transporte (Host-to-Host)	TCP, UDP
Rede (Internet)	IPv4, IPv6
Física (Acesso à Rede)	ARP, Ethernet, FDDI

PS: A camada física no TCP/IP engloba as camadas 1 e 2 do OSI, mas elas tratam de coisas diferentes.

Enquanto o TCP (Transmission Control Protocol) organiza os pacotes, ele também utiliza o sistema de reconhecimento da informação para verificar se os dados estão íntegros. Outro protocolo presente nesta camada é o UDP (User Datagram Protocol) que é utilizado quando dados menos importantes são transmitidos, tipicamente em requisições DNS. Isto porque o UDP não possui as funcionalidades de reorganização das informações nem de verificação da integridade dos dados. No entanto, ele é bem mais rápido que o TCP.

Definições do Protocolo TCP/IP

Para isso, podemos definir a função de cada uma das camadas do protocolo TCP/IP como:

- **Aplicação:** Nesta camada define-se como os programas vão se comunicar com as diversas aplicações disponíveis nas redes. Ainda é de responsabilidade desta camada efetuar o gerenciamento da interface pela qual o usuário vai interagir com a aplicação.
- **Transporte (Host-to-Host):** É idêntica à camada de transporte do modelo de referência OSI, ou seja, responsável por prover, gerenciar e encerrar uma conexão ponto a ponto. Ao efetuar o gerenciamento da conexão, visa-se garantir a integridade dos dados pelo sequenciamento dos pacotes segmentados para efetuar o envio/recebimento das mensagens.
- **Rede (Internet):** Tem o mesmo objetivo da camada de rede do modelo de referência OSI, sendo responsável por definir o endereçamento dos dispositivos por meio do IP e garantir o roteamento dos pacotes nas redes.
- **Física (Acesso à Rede):** Desempenha a mesma função das camadas de enlace e física do modelo de referência OSI. Efetua o monitoramento do tráfego e analisa o endereçamento de hardware antes da transmissão pelo meio físico.

Podemos destacar algumas semelhanças entre o modelo OSI e o protocolo TCP/IP:

- Divisão em camadas.
- As camadas de transporte e rede são equivalentes.
- A comutação de pacotes é definida no modelo e efetuada no protocolo.
- Os profissionais de redes necessitam conhecer ambos.

Endereço IP

O endereço IP é o endereço lógico que cada dispositivo na rede deverá ter, por exemplo, computadores, roteadores, tablets, smartphones, etc.

Existem duas formas de colocar o endereço IP na máquina, uma é manualmente, onde entramos na configuração do dispositivo e colocamos o endereço IP, e a outra é através de um servidor DHCP (pode ser uma máquina ou servidor com Windows, Linux, roteador, etc.), que vai atribuir um IP a cada dispositivo que entrar na rede.

Um endereço de IP é formado por quatro números, cada um passando de 001 a 255, como por exemplo *192.168.0.2*.

Um IP necessita de uma máscara de subrede, como 255.255.255.0, no caso, a máscara, os números 255 indica que o número corresponde ao IP no mesmo ponto (com o exemplo acima seria *192.168.0* no primeiro) seria de endereço de rede, já os últimos números são referentes ao host (dispositivos). Por exemplo, um computador teria o IP *192.168.0.2*, seria o computador 2 na rede *192.168.0*, e o três seria *192.168.0.3*, e assim por diante, se alterar um deles para, por exemplo, *192.168.1.2*, ele já faria parte de outra rede. Todos usariam a mesma máscara *255.255.255.0*.

Pra facilitar a criação de redes, foram estabelecidos alguns padrões, por exemplo, quando tivermos uma rede, ela terá uma classe padrão. Veja as classes logo abaixo:

- **Classe A:** Primeiro octeto entre 1 e 126.
- Em binário, o primeiro bit do primeiro octeto é 0.
- A máscara padrão é *255.0.0.0*.
- Um exemplo é *10.0.0.2*.

- **Classe B:** Primeiro octeto entre 128 e 191.
- Em binário, o primeiro bit do primeiro octeto é 1 e o segundo é 0.
- A máscara padrão é *255.255.0.0*.
- Um exemplo é *172.16.0.13*.

- **Classe C:** Primeiro octeto entre 192 e 223.
- Em binário, os primeiros dois bits do primeiro octeto é 1 e o terceiro é 0.
- A máscara padrão é *255.255.255.0*.
- Um exemplo é *192.168.0.3*.

PS: Note que faltou o 127, ele é usado para loopback, que explicaremos logo abaixo.

Temos também os vários tipos de endereços à serem usados pelo IP:

- **Endereço Público:** Endereço IP fornecido pelas operadoras para acesso à internet.
- **Endereço Privado:** Usados em redes internas, com os padrões de classes acima (classe A de *10.0.0.0* a *10.255.255.255*, classe B de *172.16.0.0* a *172.31.255.255* e classe C de *192.168.0.0* a *192.168.255.255*). Tipo um ramal de telefone.
- **Endereço Loopback:** Usado para testes de diagnóstico no próprio dispositivo, usando o *127.x.x.x* (sua máscara é da classe A, *255.0.0.0*).
- **Endereço de Autoconfiguração (APIPA):** Ele é usado quando o computador não consegue pegar um endereço IP, por exemplo, ao usar um DHCP. Ele usa o *169.254.x.x* (sua máscara é da classe B, *255.255.0.0*).

Portas TCP e UDP

Em redes de computadores, uma porta é um software de aplicação específica ou processo específico servindo de ponto final de comunicações em um sistema operacional hospedeiro de um computador. Uma porta tem associação com o endereço de IP do hospedeiro, assim como o tipo de protocolo usado para comunicação. O propósito das portas é para singularmente identificar aplicações e processos de um único computador e assim possibilitá-los a compartilhar uma única conexão física com uma rede de comutação de pacotes, como a internet.

Imagine que as duas partes do endereço IP (a parte referente à rede e a parte referente ao host) correspondam ao CEP da rua e ao número do prédio. Um carteiro só precisa destas duas informações para entregar uma carta. Mas, dentro do prédio moram várias pessoas. O CEP e o número do prédio só vão fazer a carta chegar até a portaria. Daí em diante é preciso saber o número do apartamento. É aqui que entrem as famosas portas TCP.

Ao todo, é possível usar 65536 portas TCP e UDP, começando em 1. Tanto no protocolo TCP como no UDP, é comum o uso das portas de 1 a 1024, já que a aplicação destas é padronizada pela IANA (Internet Assigned Numbers Authority).

Essas são algumas das portas mais usadas:

Protocolo	Porta Padrão	Serviço	Protocolo de Comunicaçã o
HTTP	80 8080	Navegação web (processamento de HTML)	TCP
HTTPS	443	Navegação web (processamento de HTML) com criptografia	TCP
SMTP	25 587	Envio de e-mails	TCP/UDP
	465	Envio de e-mails com criptografia	TCP
IMAP	143	Recebimento de e-mails	TCP/UDP
	993	Recebimento de e-mails com criptografia	TCP
POP	110	Recebimento de e-mails	TCP
	995	Recebimento de e-mails com criptografia	TCP
MSSQL	1039 433 1040	Banco de dados SQL Server	TCP/UDP
MYSQL	3306	Banco de dados MySQL	TCP/UDP
PGSQL	5432	Banco de dados Postgre	TCP
FIREBIRD	3050	Banco de dados Firebird	TCP/UDP
DNS	53	Consulta de DNS	TCP/UDP
WHOIS	43	Consulta de Whois	TCP
FTP	21	Comandos FTP	TCP

	20	Transmissão de arquivos FTP	TCP
SSH	22	Acesso SSH	TCP/UDP
SFTP		FTP com criptografia	
TELNET	23	Acesso remoto Telnet	TCP/UDP
SVN	3690	Controle de versões subversion	TCP
DHCP	67	Envio de dados do cliente ao servidor	UDP
	68	Recebimento de dados do servidor ao cliente	
SNMP	161 162	Gerenciamento de redes	TCP/UDP
RIP	520 521	Roteamento que não requer conexões	UDP
RDP	3389	Acesso remoto do Windows	TCP
SKYPE	81	Protocolo Skype	TCP
VNC	5900	Acesso remoto VNC	TCP
RTP	5004 5005	Streaming de Áudio e Vídeo	UDP
SIP	5060	Responsável pelas Sessões de Comunicações	TCP/UDP
NTP	123	Responsável pela Sincronização de Horário	UDP

Basicamente, essas são algumas funções mais detalhadas dos protocolos mais usados:

- **FTP:** File Transfer Protocol, permite a transferência de arquivos entre dois computadores através de login e senha.
- **SMTP:** Simple Mail Transfer Protocol, é utilizado para o transporte de e-mail, sendo que o SMTP é uma aplicação utilizada para transporte e não um meio de transporte. Por isso ele se localiza na camada de aplicação.
- **HTTP:** Hypertext Transfer Protocol, é utilizado para transportar páginas HTML de servidores web para navegadores. O protocolo é utilizado para realizar a comunicação entre servidores web e navegadores instalados em computadores cliente.
- **DHCP:** Dynamic Host Configuration Protocol, é um método de designar endereços IPs para os computadores conectados na rede. Ele é um serviço baseado no servidor que designa automaticamente endereços IPs para cada computador que entra na rede. Este método não exige que você tenha que entrar em cada computador e informar o IP, facilitando mudanças de redes. O DHCP pode executar todas as funções do BOOTP.
- **POP3:** Post Office Protocol Version 3, é utilizado por usuários clientes para acessar uma conta de e-mail em um servidor e pegar o e-mail. Como no SMTP, esta não é uma camada de transporte.
- **IMAP4:** Internet Mail Access Protocol Version 4, é um substituto para o POP3, diferente deste último, o IMAP se mantém conectado a fim de sincronizar as mensagens recebidas em tempo real.

Abaixo, veja alguns provedores de e-mail e seus respectivos protocolos:

Provedor	Protocolo

imap.mail.yahoo.com	IMAP
pop.mail.yahoo.com	POP
smtp.mail.yahoo.com	SMTP
imap.gmail.com	IMAP
pop.gmail.com	POP
smtp.gmail.com	SMTP
outlook.office365.com	IMAP/POP
smtp-mail.outlook.com	SMTP
imap.terra.com.br	IMAP
pop.terra.com.br	POP
smtp.terra.com.br	SMTP
imap.bol.com.br	IMAP
pop3.bol.com.br	POP
smtps.bol.com.br	SMTP

Unicast, Broadcast e Multicast

Sempre que se tem um ou mais dispositivos na rede (por exemplo, computadores), temos várias formas de comunicação entre eles.

Um desses métodos é o método Unicast, que um computador se comunica com apenas um outro computador especificamente e estabelece a comunicação apenas com esse dispositivo específico na rede (por exemplo, numa troca de arquivos).

Outra forma de comunicação é a Broadcast, nesse caso a informação é enviada a todos os dispositivos ao mesmo tempo.

Temos também a Multicast, que a informação é enviada para um grupo específico de dispositivos selecionados. Os outros fora do grupo não recebem as informações.

Camada de Enlace

A camada de Enlace (ou Data Link Layer) é a segunda camada do modelo OSI e, entre outras coisas, é responsável por traduzir as informações da camada de rede em bits para que então sejam enviadas pela camada física.

Essa camada é dividida em duas subcamadas como podemos ver abaixo:

- Controle de Link Lógico (LCC).
- Controle de Acesso ao Meio (MAC).

Nessa camada, as mensagens são formatadas em pedaços chamados frames ou quadros, que contém endereços de origem e destino.

A subcamada MAC (Media Access Control) diz como os dados serão colocados no meio físico e define qual o endereço físico do dispositivo. Outras coisas como notificação de erro, controle de fluxo e a ordem em que os quadros serão enviados podem ser descritos aqui.

A outra subcamada, a LLC (Logical Link Control), deve conhecer qual protocolo estará atuando na camada de rede. Quando o host recebe o quadro, o cabeçalho presente no LLC dirá para onde aquele quadro deverá ser destinado. Essa subcamada também pode fornecer controle de fluxo e sequência de bits de controle.

Endereço MAC

O MAC Address também é conhecido como “endereço físico” e está gravado em um chip na placa de rede.

O endereço MAC é um endereço de 48 bits sempre escrito em hexadecimal, como por exemplo *00-25-10-35-00-3B*.

Ao invés de traços, às vezes é escrito com dois pontos entre os números, como *00:23:10:35:00:3B*.

O endereço MAC é dividido em duas partes, sendo que a primeira identifica o fabricante (podendo até ser substituída pelo nome do mesmo) e a segunda identifica apenas aquela placa de rede.

As três partes de um quadro MAC, na verdade um frame:

<table>
<tr><td>Cabeçalho</td><td rowspan="3">Dados</td><td rowspan="3">Trailer</td></tr>
<tr><td>MAC Origem</td></tr>
<tr><td>MAC Destino</td></tr>
</table>

O cabeçalho tem as informações sobre o frame (entre eles, o MAC de origem e o MAC de destino. Os dados informa o que está sendo enviado, e o trailer tem informações de verificação (se ele foi alterado ou não durante o envio).

Switch L2 – Broadcast

Anteriormente sobre a camada de enlace, diferenças entre Unicast, Multicast e Broadcast e o MAC, aqui entenderemos como o switch trabalha numa rede.

Num exemplo de rede, temos o switch no meio (não confundir com roteador ou modem) e quatro computadores, cada um com seu MAC.

Vamos supor que cada computador tenha nomes de A, B, C e D, e que o computador A queira conversar com o B e não sabe qual é o tal computador, ele manda pra rede um broadcast usando protocolo ARP, que pergunta quem é o computador B, que irá responder.

No momento que o computador A entra em contato com o B, o switch lerá o quadro que tem o endereço MAC de origem e o MAC de destino. Quando ele lê o MAC de origem, imediatamente ele grava o mesmo na memória (chamada CAM), que tem uma tabela que escreve o MAC de origem e associa com a porta na qual o computador está. O mesmo ocorre com o computador de destino e seu MAC, que o switch perguntará para todos na rede qual é o tal MAC até que o B responda.

Vamos supor que o computador C mande um frame unicast para o B, já sabendo o MAC do B, nesse caso ele não precisa perguntar pros outros computadores qual é o B por já saber qual o MAC e a porta dele. Isso evita transmissão de mensagem pros computadores errados e por isso, é mais seguro.

O Domínio de Broadcast é até aonde o broadcast chega, vamos supor que a imagem acima tenha 100 computadores, se qualquer um deles mandar um broadcast pra rede, todos os computadores ligados na rede vão escutar o broadcast. O Domínio de Broadcast é até aonde chega o broadcast (por exemplo, um switch de 96 portas manda de uma das máuinas para as outras 95 portas).

Quando um dispositivo quer contatar outro na rede, ele vai usar o protocolo ARP pra perguntar se este dispositivo está na rede. Mesmo se um dos computadores mandar uma mensagem unicast pra outro, o switch manda um broadcast para descobrir o MAC de destino, caso ele ainda não saiba.

O que é Domínio de Broadcast

O domínio de broadcast é o conjunto de dispositivos que recebem um quadro broadcast enviado de um dispositivo que está na mesma rede. Seria até onde chega uma mensagem de broadcast.

Vamos supor que exista um switch com quatro portas (ele pode ter muito mais). Quando o computador A quer mandar uma mensagem para todos os outros dispositivos da rede, ele envia um quadro broadcast do qual o switch vai replicar para todas as portas. O switch coloca por padrão todas as portas no mesmo domínio de broadcast.

Lembrando do MAC Address, que tem 48 bits, um quadro broadcast é enviado para o MAC de cada dispositivo.

Diferenças entre Hub e Switch

Um hub (conhecido também como concentrador) é um equipamento passivo, enquanto um switch (conhecido também como comutador) é um equipamento ativo.

Os hubs estão em desuso em redes cabeadas hoje, mas é importante conhecer seu funcionamento.

Basicamente, o hub funciona de uma forma similar a usar um trio elétrico para dar recado a uma pessoa (o recado vai chegar, mas vai chegar pra todo mundo que está ali).

O switch, no entanto, seria como mandar uma carta (mesmo passando por alguém no caminho, só é entregue ao destinatário).

No hub, a captura de pacotes é simples, chegam a todos, e é inseguro, pouco comum hoje. Inclusive, ele manda as mensagens para todos os dispositivos sem exceção, inclusive o mesmo que enviou a mensagem.

Já no switch, tem o cascateamento, porta de uplink, espelhamento de porta, o que permite o envio de mensagens a apenas determinados dispositivos.

Usando estes conceitos podemos capturar todo ou quase todo o tráfego de uma rede LAN, num programa como o Wireshark (num hub acaba sendo mais fácil devido ao fato deste enviar pacotes a todos os hosts, num switch é um pouco mais difícil).

Tipos de Rede Intranet e Extranet

Em uma rede privada os recursos e sistemas compartilhados ficam restritos à organização e podem estar estruturados de duas formas:

- **Intranet:** Compreende uma rede privada que utiliza em uma estrutura física e lógica o módulo de internet. No entanto, os serviços de rede, como servidores de arquivos e impressão, servidor web e as aplicações são de uso interno;
- **Extranet:** Conhecida popularmente como internet. A diferença é que os recursos só podem ser acessados com autorização de um administrador da rede de uma companhia.

O Que é Vlan

Uma vlan permite segmentar um domínio de broadcast.

Vamos supor que um computador mande uma mensagem pra um switch, e todos os computadores da rede ouçam sua mensagem (supondo que tenham 48), e também outro switch ligado a ele, também com 48, totalizando 96 hosts, cada computador teria que parar 95 vezes para ouvir o broadcast dos outros pra ver se é dele, o que causaria um problema na rede.

Nesse momento, é bom saber uma quantidade máxima de computadores suportados. Para isso criamos uma vlan (ligando e configurando os switches), vamos supor que tenhamos vlan 1 e vlan 2 (podendo ter mais, não confundir com os switches, em ambos tem computadores de ambas as vlans), nesse caso, apenas os computadores que estão na mesma vlan que receberão a mensagem. Isso é útil por exemplo, numa empresa, na qual podemos dividir por exemplo, as informações do marketing e do financeiro, onde uma não interfere na outra.

Também temos o protocolo 802.1Q. Vamos supor que temos a vlan 1 e vlan 2, que coloca uma “tag” informando sobre a vlan da qual o dispositivo pertence e envia a mensagem pros dispositivos da mesma vlan. Após a entrega das informações, ele destrói essa tag, que não é recebida pelos computadores.

Introdução ao HTTP

HTTP é a sigla de HyperText Transfer Protocol, que em português significa “Protocolo de Transferência de Hipertexto”. É um protocolo de comunicação entre sistemas de informação que permite a transferência de dados entre redes de computadores, principalmente na World Wide Web (internet).

O HTTP é o protocolo utilizado para transferência de páginas HTML do computador para a internet. Por isso, os endereços dos websites (URL) utilizam no início a expressão “http://”, definindo o protocolo usado. Esta informação é necessária para estabelecer a comunicação entre a URL e o servidor web que armazena os dados, enviando então a página HTML solicitada pelo usuário.

Para que a transferência de dados na internet seja realizada, o protocolo HTTP necessita estar agregado a outros dois protocolos de rede: TCP (Transmission Control Protocol) e IP (Internet Protocol). Esses dois últimos protocolos forma o modelo TCP/IP, necessário para a conexão entre computadores clientes-servidores.

Temos também o HTTPS, que é a versão criptografada do HTTP, mas também funcionando de forma parecida.

No inspecionar elemento, em Network, podemos olhas as opções de rede do protocolo HTTP, vemos os arquivos carregados e os códigos das páginas (como 200, que é de sem erros, 304, que é de arquivo no cache do navegador ou 404, que é não encontrado). Basicamente é isso:

Número	Significado
1--	Informativo
2--	Confirmação
3--	Redirecionamento
4--	Erro do Cliente
5--	Erro do Servidor

Protocolo Spanning Tree – Parte 1

O protocolo Spanning Tree Protocol (STP) é um protocolo baseado em um algoritmo que garante que não ocorrerá loop em uma rede local. Geralmente são usados em redes de grande porte.

Em redes maiores é necessário estabelecer redundância para evitar que a rede continue funcionando mesmo quando um switch apresentar problema.

A forma que o protocolo Spanning Tree trabalha para que isso não ocorra, utiliza quadros especiais chamados BPDU – Bridge Protocol Data Unit.

BPDUs são trocados regularmente, normalmente a cada dois segundos e permitem que os switches fiquem sabendo de alterações na rede bem como parar ou iniciar encaminhamento nas portas conforme necessário.

BPDUs além de descobrirem portas que podem causar loops também ajudam a definir qual será o switch principal (core) da rede e qual a melhor forma de chegar bloqueando linhas redundantes.

Vamos dar uma olhada em três tipos de porta:

- **Root Port:** Porta usada para chegar no root bridge.
- **Designated Port:** Porta que encaminha os quadros.
- **Blocking Port:** Porta que, caso ativada, pode causar loops.

O root bridge é escolhido através do seu Bridge ID, número formado por um valor chamado “Bridge Priority” + o MAC Address.

O primeiro número é 32768 por padrão, mas pode ser alterado desde que seja um múltiplo de 4096. Por exemplo *32768.0200.0000.1111*.

Vamos supor que numa rede, tenhamos três switches, com esses números:

32768.0200.0000.1111
32768.0200.0000.2222

32768.0200.0000.3333

O root bridge é o que terá o menor número. Quanto menor o número, maior a prioridade dele.

A Root Port (RP) são as portas que os outros switches usam para chegar ao Root Bridge. No segundo switch, tem uma porta chamada Designated Port (DP), que é ligada ao terceiro switch pelo Blocking Port (BP), que bloqueia a porta, caso necessário, mas libera a conexão se precisar, caso seja um caminho mais curto.

O caminho que será escolhido para se chegar no Root Bridge leva em consideração o curso que indica o melhor caminho baseado na taxa de transferência dos links. Veja a tabela abaixo:

Data Rate	STP Cost (802.1D-1998)	RSTP Cost (802.1D-2004 / 802.1w)
4 Mbit/s	250	5.000.000
10 Mbit/s	100	2.000.000
16 Mbit/s	62	1.250.000
100 Mbit/s	19	200.000
1 Gbit/s	4	20.000
2 Gbit/s	3	10.000
10 Gbit/s	2	2.000

Mas pode ser mais rápido pra ele usar uma conexão mais curta para enviar as mensagens, independente da velocidade.

Protocolo Spanning Tree – Parte 2

Vamos ver hoje sobre os estados que uma porta de um switch com STP habilitado podem assumir:

- **Blocking:** Uma porta que causaria um loop caso estivesse ativa. Ela não recebe e nem envia dados de usuário neste estado, mas continua recebendo BPDUs e pode transformar em uma porta que faz encaminhamentos caso a situação da rede se altere e seja necessário.
- **Listening:** O switch verifica os BPDUs e verifica se ele não deve ficar bloqueado, neste caso ele não ajuda a construir a tabela MAC nem encaminha quadros.
- **Learning:** Neste estado a porta ainda não encaminha os quadros, mas “aprende” endereços MAC dos quadros que passam por ela e ajuda a construir a tabela MAC.
- **Forwarding:** Uma porta funcionando normalmente, ou seja, recebendo e encaminhando quadros, mesmo assim, continua monitorando BPDUs para saber se em algum momento não deve entrar em estado bloqueado.
- **Disabled:** Uma porta desabilitada, que pode ser feito pelo administrador da rede manualmente.

Vamos supor que na sua rede tenha um dispositivo novo conectado, uma porta bloqueada passaria um certo tempo pra estar ativa novamente. Para isso foi criado o RSTP. Ele tem umas diferenças que faz que esse processo de alteração das portas seja mais rápido, veja a tabela abaixo como exemplo:

STP (802.ID) Estado da Porta	RSTP (802.IW) Estado da Porta	A porta está inclusa na topologia ativa?	A porta está “aprendendo” endereços MAC?
Disable	Discarding	Não	Não
Blocking	Discarding	Não	Não
Listening	Discarding	Sim	Não
Learning	Learning	Sim	Sim
Forwarding	Forwarding	Sim	Sim

Pra ficar um pouco mais fácil de entender, vamos ver o papel das portas da rede (Port Roles), que é uma função variável que pode ser dada a uma determinada porta. A port root e a porta designada continuam com os mesmos objetivos, já a porta bloqueada tem os objetivos de atuar como “backup” e “alternativa”.

- **Alternate Port:** É uma porta alternativa para se chegar na Root Bridge.
- **Backup Port:** Uma porta na qual o switch não descartou as informações e pode ser rapidamente usada quando uma outra porta falhar.

Protocolo Ethernet

Ethernet é um conjunto de tecnologias para Local Area Networks (LANs).

Os padrões Ethernet compreende variantes de cabeamento e transmissão de sinal.

A velocidade de transmissão dos padrões Ethernet são medidos em bits por segundo, muito provavelmente você vai encontrar um dos seguintes padrões: Standard Ethernet (10 Mbps), Fast Ethernet (100 Mbps) e Gigabit Ethernet (1000 Mbps).

O Ethernet é definido pelo IEEE como 802.3.

Os diferentes padrões são bem compatíveis entre si.

Veja abaixo a tabela com o modelo OSI, já que o Ethernet trabalha na camada 1 e 2 dele:

<table>
<tr><th>OSI</th><th colspan="3">Ethernet</th></tr>
<tr><td rowspan="2">Enlace</td><td colspan="3">Controle de Link Lógico (LLC)</td></tr>
<tr><td colspan="3">Controle de Acesso ao Meio (MAC)</td></tr>
<tr><td rowspan="6">Física</td><td>Standard Ethernet</td><td>Fast Ethernet</td><td>Gigabit Ethernet</td></tr>
<tr><td>10 Base 5</td><td>100 Base TX</td><td>1000 Base T</td></tr>
<tr><td>10 Base 2</td><td>100 Base T4</td><td rowspan="3">1000 Base LX</td></tr>
<tr><td>10 Base T</td><td rowspan="2">100 Base FX</td></tr>
<tr><td>10 Base FX</td></tr>
</table>

O primeiro número é a velocidade da rede em Mbps.

Base vem de “bandabase” e diz respeito de como o sinal é transportado.

Atualmente, temos também o padrão 10 Gigabit Ethernet, permitindo atingir uma velocidade de 10 Gbps, também conhecido como 10G. Entre as opções estão as tecnologias: 10GBase-LR, 10GBase-ER, 10GBase-ZR, 10GBase-SR, 10GBase-LRM e 10GBase-CX4.

No final, a letra T, C ou F indica o tipo de cabo usado:

- **T:** Par trançado.
- **C:** Coaxial (ou um número 5 indicando que o cabo pode chegar à 500 m ou 2 indicando 185 m).
- **F:** Fibra óptica (pode ser S ou L também).

Pra terminar essa parte, mostraremos os modos de comunicação que existem no protocolo Ethernet. Veja abaixo:

- **Simplex:** Permite a comunicação em apenas uma direção com a largura de banda usada para a transmissão do sinal (por exemplo, o mouse).
- **Half-Duplex:** Permite o envio e recebimento de dados, mas não ao mesmo tempo.
- **Full-Duplex:** Permite enviar e receber ao mesmo tempo (como as placas de rede).

Cabo Par Trançado – Parte 1

Apesar de muita coisa hoje em dia ser sem fio, ainda é necessário cabeamento em muitas partes da rede, pelo menos até chegar ao roteador, por isso é importante conhecer os tipos diferentes de cabo usados em redes internas.

O cabo par-trançado é um dos tipos de cabos mais utilizados, possui 4 pares de fios, e cada par possui uma quantidade de tranças (torções) por metro, e cada par (trança) possui sinais iguais porém opostos, isso faz com que os pares minimizem interferências entre eles e permitem que os sinais transmitidos e recebidos possam ser comparados.

O cabo UTP (Unshielded Twisted Pair) é o mais utilizado, mas ele não tem nenhuma proteção extra.

O cabo SCTP (Screened Twisted Pair) e o FTP (Foiled Twisted Pair) oferecem proteção para todos os pares usando folha para blindagem.

O cabo S/STP (Screened Shielded Twisted Pair) e o S/FTP (Screened Foiled Twisterd Pair) oferecem proteção para o cabo e mais uma proteção que separa cada par dentro do cabo.

PS: O FTP não tem nada a ver com o protocolo FTP.

Outras características presentes nos cabos são essas:

- **CMX:** Para instalações residenciais com pouco cabo (casas comuns).
- **CM:** Para instalações horizontais em lugares com alta ocupação, com fluxo de ar forçado (por exemplo, em prédios que possuem dutos para passar cabos de todos tipos, como ambientes comerciais).
- **CMR (Riser):** Para instalações verticais como em “shafts” (por exemplo, em prédios com mais de dois andares).
- **CMP (Plenum):** Aplicação horizontal em locais onde gases tóxicos se espalhando rapidamente poderiam causar danos às pessoas (em espaços livres em locais onde também passam dutos de ar, os cabos não passam dentro desses dutos).

Cabo Par Trançado – Parte 2

Para escolhermos bem os cabos, precisamos conhecer bem as categorias deles, que são essas:

- **Categoria 3:** Indicado para redes Ethernet 10 Mbps e Token Ring 4 Mbps (em desuso, substituído pela categoria 5).
- **Categoria 5:** Indicado para redes Ethernet 100 Mbps.
- **Categoria 5e:** Indicado para redes Ethernet 1 Gbps.
- **Categoria 6:** Indicado para redes Ethernet 10 Gbps (até 55 metros).
- **Categoria 6a:** Indicado para redes Ethernet 10 Gbps (até 100 metros).

A metragem influencia na velocidade, é a distância máxima entre o switch até o computador (incluindo tomadas, filtros e etc.).

Cabo Par Trançado – Parte 3

O conector RJ-45 é o conector mais usado em redes com cabo par trançado, mas nem sempre eles são iguais, apesar de semelhantes.

A maioria dos dispositivos novos detectam automaticamente quem transmite e quem recebe e não depende mais da pinagem do cabo para se comunicar.

Fibra Óptica – Parte 1

A fibra óptica é um dos mais importantes meios de transmissão. É recomendada principalmente para aplicações que precisam trafegar altas taxas de dados em longas distâncias. Os dados são transmitidos em forma de luz, por isso é imune a interferência eletromagnética e tem baixa atenuação. Muito usada em tráfego de dados por longas distâncias e alta velocidade.

As fibras ópticas podem ser divididas em dois modos, fibra multimodo e fibra monomodo.

A fibra multimodo é usada em aplicações onde distâncias menores são consideradas, normalmente utiliza LED e o tamanho do núcleo é maior, por isso, a luz fica “batendo” no tráfego do cabo.

A fibra monomodo é usada em aplicações de longa distâncias, normalmente utiliza laser e o núcleo tem um tamanho menor, por isso trafega por um caminho “reto”.

Ambas as fibras têm uma capa, bem semelhante.

Fibra Óptica – Parte 2

Os conectores mais usados em fibra óptica são os conectores ST, mas atualmente é mais comum os conectores SC.

Outro que é menor e mais simples é o LC, por ter dois conectores integrados (um de transmissão e outro de recepção).

O mais fácil de instalar de todos, no entanto, é o MTRJ, parecido com o RJ45.

Fibra Óptica – Parte 3

Esses são os padrões da fibra óptica e suas velocidades:

Tipo de Fibra	Padrão Ethernet	Velocidade	Distância
Multimodo	100 BASE-FX	100 Mbit/s	2 Km
	1000 BASE-SX	1000 Mbit/s	200 – 500 m
	10 G BASE-SR	10 Gbit/s	300 m
Monomodo	1000 BASE-LX	1000 Mbit/s	2 Km
	10 G BASE-LR	10 Gbit/s	10 Km

Cabo Coaxial

O cabo coaxial é um tipo de cabo usado para transmitir sinais, usado não só em redes (muito raro hoje em dia), mas também em outras aplicações como CFTV (circuito fechado) e TV a cabo. Ele tem um condutor central, um isolante em torno dele, em volta uma capa metálica ou malha. Os cabos de antes geralmente são esses.

Os tipos mais comuns de cabo coaxial são:

- **RG-59:** Tipicamente usado para transmissão de vídeo analógico, especialmente CFTV.
- **RG-6:** Mais grosso que o RG-59, usado por operadores de TV a cabo.
- **RG-58:** Similar ao RG-59, utilizado antigamente me redes 10 BASE 2 Ethernet Networks.

Os conectores mais comuns são o F, muito comum nos cabos de antenas e receptores de TV por assinatura, e o BNC, geralmente usadas em CFTV.

Ainda que alguns cabos não sejam mais utilizados, é comum encontrar referências sobre eles em livros e materiais de estudos. Veja a tabela abaixo:

Padrão	Cabo	Capacidade	Distância
10 BASE 5	Coax (thicknet ou RG-8/U)	10 Mbps	500 m
10 BASE 2	Coax (thinnet ou RG-58)	10 Mbps	185 m

Servidor DNS – Instalação e Configurações Gerais de Rede no Linux

Primeiramente, configure a rede do servidor e digite o comando *sudo ifconfig*, daí veremos o IP obtido via DHCP.

Como o DNS precisa ter um IP fixo, devemos editar o arquivo de configuração, digitando *sudo vim /etc/network/interfaces*, digite i para entrar no modo de inserção e escreva abaixo esse código:

auto eth0
iface eth0 inet static

address 192.168.1.200
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
gateway 192.168.1.1

PS: Substitua eth0 pelo nome de sua interface.

Para editar o arquivo de hosts, digite *sudo vim /etc/hosts* e adicione essas entradas:

192.168.1.200 Ubuntu-32.exemplodedominio.net Ubuntu-32

PS: Esse endereço é o nome da máquina (pego depois do arroba no terminal), seguido de um nome de domínio qualquer.

Para ver o nome da máquina, digite o comando hostname (podemos editar o arquivo /etc/hostname para mudar o nome da máquina).
Dê um ping no Google, ele não conseguirá acessar a internet, por isso, iremos editar o arquivo do resolvedor DNS (*sudo vim /etc/resolv.conf*) e digitamos isso:

nameserver 8.8.8.8

PS: Esse é o servidor DNS do Google, existem vários que podemos usar. Tente dar um ping num site agora.

Instale o programa bind digitando *sudo apt install bind9*. Para ver se ele está rodando após instalar digite *sudo /etc/init.d/bind9 status*, depois vá na pasta /etc/bind e dê um ls nele.

Servidor DNS – Criação das Zonas e Testes com Clientes no Linux

Agora digite *sudo vim /etc/bind/named.conf.local* para editar o arquivo que iremos usar para adicionar as zonas DNS, entre no modo de inserção e digite isso:

// Zona de pesquisa direta:

```
zone “exemplodedominio.net” {
    type master;
    file “/etc/bind/db.exemplodedominio.net”;
};

// Zona de pesquisa reversa

zone “1.168.192.in-addr-arpa” {
    type master;
   file “/etc/bind/db.192”;
};
```

Esses arquivos em file são arquivos novos que serão criados, cuidado com as chaves e os pontos e vírgula. O nome da zona é o endereço IP de rede ao contrário (não confundir com o IP da máquina).

Edite o arquivo de opções digitando *sudo vim /etc/bind/named.conf.options*, e procure em forwarders, tire os comentários (as barras //) e deixe dessa forma:

```
forwarders {
   192.168.1.1;
   8.8.8.8;
};
```

PS: O IP ali é o IP do roteador e o DNS do provedor.

Copie os arquivos digitando *cd /etc/bind*, *sudo cp db.local db.exemplodedominio.net* e *sudo cp db.127 db.192*.

Vamos editar os arquivos copiados, o primeiro é digitando *sudo vim /etc/bind/db.exemplodedominio.net*, deixando dessa forma:

```
@   IN      SOA   Ubuntu-32.exemplodedominio.net. root.exemplodedominio.net. {
                  100          ;  Serial
                  604800       ; Refresh
                  86400        ; Retry
                  2419200      ; Expire
                  604800 )     ; Negative Cache TTL
;
exemplodedominio.net      IN    NS    Ubuntu-32.exemplodedominio.net. (
exemplodedominio.net.     IN    A     192.168.1.200
; @    IN    A     127.0.0.1
; @    IN    AAAA        ::1

Ubuntu-32    IN    A       192.168.1.200
roteador     IN    A       192.168.1.1
vendas       IN    A       192.168.1.50
www          IN    CNAME   exemplodedominio.net.
```

Agora edite o outro arquivo digitando *sudo vim /etc/bind/db.192* e deixe ele assim:

```
@       IN      SOA   Ubuntu-32.exemplodedominio.net. root.exemplodedominio.net. (
                      1            ; Serial
                      604800       ; Refresh
                      86400        ; Retry
                      2419200      ; Expire
                      604800 )     ; Negative Cache  TTL
;

        IN      NS    Ubuntu-32.
1       IN      PTR   roteador.exemplodedominio.net.
50      IN      PTR   vendas.exemplodedominio.net.
200     IN      PTR   Ubuntu-32.exemplodedominio.net
```

Reinicie o bind digitando *sudo /etc/init.d/bind9 restart*, e verificaremos os arquivos de zona digitando *named-checkzone exemplodedominio.net /etc/bind/db.exemplodedominio.net* e *named-checkzone exemplodedominio.net /etc/bind/db.192*. Reinicie a máquina.

Após reiniciar, digite *cat /etc/resolv.conf* para ver este arquivo. Para testar digi*te host -l exemplodedominio.net*. Digite *nslookup exemplodedominio.net* e *dig exemplodedominio.net*, faça o mesmo com o IP, digitando host 192.168.1.50 e dê um ping digitando *ping vendas.exemplodedominio.net*.

Para testar o encaminhador, digite primeiramente o ping num site qualquer da internet e veja se ele responde.

Na máquina cliente, edite o arquivo de configuração digitando *sudo vim /etc/resolv.conf* e deixe ele desse jeito:

nameserver 192.168.1.200
search exemplodedominio.net

Dê um ping na máquina, digitando *ping Ubuntu-32*. Podemos também pingar o vendas, digitando *ping vendas* e ver isso também num site da internet.

TCPDump – Capturar e Analisar Tráfego de Rede no Linux

O TCPDump é uma excelente ferramenta para realizar captura e análise de pacotes de rede, recomendada para profissionais que precisem realizar monitoramento e manutenção em uma rede de computadores, além de estudantes que queiram entender a fundo o funcionamento da pilha de protocolos TCP/IP.

O TCPDump, que é software livre, roda na linha de comandos, estando disponível em diversos sistemas operacionais, como Linux, BSD, OS X, AIX e outros. Ele faz uso da biblioteca libpcap para realizar a captura de pacotes, e existe uma versão da ferramenta para Windows, chamada de WinDump, que usa a biblioteca WinPcap. Neste artigo vamos focar no TCPDump em si, usando para isso um sistema Linux (Ubuntu, qualquer outro sistema Linux irá servir para testar os exemplos mostrados).

Para instalar o TCPDump no Ubuntu Linux, ou em sistemas baseados em Debiam, use o comando sudo apt install tcpdump. Para ver as opções dele digite o help dele.

Podemos por exemplo, capturar somente o tráfego a partir da interface eth0 digitando *sudo tcpdump -i eth0*. Gravar os pacotes capturados em um arquivo de nome captura.pcap digitando *sudo tcpdump -w captura.pcap*. Ler os pacotes capturados a partir do arquivo captura.pcap digitando *sudo tcpdump -r captura.pcap*. Capturar somente o tráfego associado ao protocolo ICMP, na interface eth0 digitando *sudo tcpdump -i eth0 icmp*. Capturar somente o tráfego associado ao protocolo ARP, na interface eth0 digitando *sudo tcpdump -i eth0 arp*. Capturar somente 50 pacotes a partir da interface eth0 digitando *sudo tcpdump -c 50 -i eth0*. Podemos também mostrar os pacotes capturados tanto em ASCII quandto em HEX, incluindo cabeçalho Ethernet digitando *sudo tcpdump -XX -i eth0*. Capturar pacotes mostrando IPs em vez de nome digitando *sudo tcpdump -n -i eth0*. Capturar somente pacotes maiores que 100 bytes digitando *sudo tcpdump -i eth0 greater 100*, neste exemplo, se emitirmos um comando ping a partir de outra janela de terminal, os pacotes não serão capturados, pois são menores que 100 bytes.

Capturar somente pacotes destinados à porta 53 digitando *sudo tcpdump -i eth0 port 53*, para testar, abrimos um navegador e acessamos uma página qualquer da web. Usamos filtros de condições: Capturar pacotes que usam o protocolo e cujo endereço de destino seja 64.233.186.121 digitando

sudo tcpdump -i eth0 dst 64.233.186.121 and icmp, para testar, abrimos outra janela de terminal e emitimos o comando ping para vários endereços, somente serão capturados pacotes ao ser usado o endereço discriminado no comando. Se abrirmos um navegador e tentarmos acessar esse mesmo endereço (ou o site, www.planetaunix.com.br), os pacotes não serão capturados, por contra do protocolo utilizado (HTTP em vez de ICMP), mostrando que ambas as condições (AND) precisam ser satisfeitas para que essa captura tenha efeito. Capturar somente os pacotes ICMP Echo Request enviados pelo programa ping da máquina local, cujo IP é 192.168.1.105, para um endereço remoto, como 8.8.8.8 digitando *sudo tcpdump -i eth0 icmp and src 192.168.1.105 and dst 8.8.8.8*.

Existem diversas outras opções e funcionalidades disponíveis no utilitário, e recomendamos uma leitura minuciosa das páginas de manual do TCPDump para aprofundar seus conhecimentos a respeito.

Outras ferramentas muito utilizadas para captura e análise de pacotes são o Wireshark, Tshark, WinDump, Ettercap e Ngrep, entre outras.

O Que é um RFC

Os RFCs são publicações que documentam os padrões e protocolos oficiais da internet, são gerenciados pelo IETF (Internet Enginerring Task Force). Podem conter de uma página a várias centenas de páginas de informações sobre um padrão.

Eles são identificados por um número, que é atribuído sequencialmente a cada novo RFC publicado. Se um padrão necessitar de atualização, então um novo RFC será gerado com as revisões necessárias. O processo de padronização de um RFC é documentado pelo RFC 2026.

A cada RFC é atribuído um status que diz respeito ao processo de padronização:

- Informacional.
- Experimental.
- Melhor Prática Atual (Best Current Practice – BCP).
- Trilha dos Padrões (Standard Track).
- Histórico.

E dentro das trilhas de padrões, temos esses:

- Proposto (Proposed Standard).
- Rascunho (Draft Standard).
- Padrão da Internet (Internet Standard).

Todos os RFCs podem ser consultados gratuitamente na internet.

Podemos buscas as RFCs por nome, palavra-chave, autor ou número.

No search do site (escolha a opção Advance), você pode pesquisar o RFC, informando o número do RFC ou uma palavra-chave qualquer. Também tem opções de filtro ao lado, como qualquer outro site de pesquisa.

Vamos pelo mais comum, pesquisando por palavra-chave, no exemplo, pesquisaremos ICMP.

Ali aparece informações como status, download em PDF, se ele está obsoleto, etc.

Veja alguns exemplos de RFCs:

Padrão/Protocolo	Número do RFC
ARP	826
DHCP	2131
DNS	1034 e 1035
FTP	959
HTTP	1945
ICMP	792
IP	791
IPv6	2460
MD5	1321
SSH	4251
TCP	793
UDP	768

O que é o MTU

Existe um limite de tamanho de dados de uma rede que define a quantidade de bytes que podem ser transmitidos dentro de um quadro. Pro padrão Ethernet, o limite de unidade máxima de transmissão é de 1500 bytes (existe em outros padrões também). É uma característica da camada de enlace conhecida como MTU.

Quando um datagrama a ser enviado em uma rede for maior do que o MTU da camada de enlace, o protocolo IP realizará a fragmentação dos dados, quebrando o datagrama em pedaços menores, chamados de fragmentos, cada um com tamanho menor do que o MTU.

Veja abaixo uns MTUs típicos:

Rede	MTU (em bytes)
Hyperchannel	65535
WLAN 802.11	7981
Quadros Jumbo Ethernet	1501 - 9198
Tonken Ring 802.5	4464
FDDI	4352
Ethernet	1500
IEEE 802.3/802.2	1492
PPPoE	1492
X.25	576

Para descobrir o MTU da interface, abrimos o CMD do Windows e digitamos *netsh interface ipv4 show subinterfaces*.

O Path MTU (MTU do caminho) é sobre o maior valor de MTU que pode trafegar em uma rede sem que os pacotes sofram fragmentação (esse valor pode mudar).

Para a máquina saber qual a MTU correta a ser utilizada, tem o Path MTU Discovery (Descoberta do MTU de Caminho), para determinar o caminho MTU ideal entre dois hosts IP para evitar a fragmentação dos datagramas IP. Uma das formas é ligar o bit DF (Don't Fragment) do cabeçalho IP dos datagramas transmitidos. Ou a mensagem ICMP (destino inalcançável, tamanho muito grande).

Para testar o MTU, usando o Ping (no CMD) com as opções *l/ tamanho-pacote*, que permite ajustar o tamanho (payload) do pacote enviado pelo ping para o valor "tamanho-pacote". E o */f*, que habilita o bit DF no pacote transmitido (impedindo a fragmentação do mesmo).

Vamos exemplificar, executando no prompt o comando *netsh interface ipv4 show subinterfaces*. Se for o caso, coloque ipv6 no lugar.

Agora dê um ping num site qualquer (por exemplo, *ping bosontreinamentos.com.br*).

Agora faça o mesmo, com a opção */l 1500*, no caso, *ping /l 1500 bosontreinamentos.com.br* (ou outro número, esse número é a quantidade de bytes enviados, que pode ser até 65500, o padrão é 32).

O MTU típico é de 1500, como já vimos, mas a transmissão pode ser feita com outro número maior, como 8500, nesse caso os pacotes serão fragmentados.

Ao colocar o */f*, antes do site, ele não fragmentará os pacotes, o que pode dar erro em tamanhos maiores. Como por exemplo *ping /l 1500 /f bosontreinamentos.com.br.*

O Que é Um Gateway

Pode ser traduzido como "portão de entrada". O gateway pode ser um PC com duas (ou mais) placas de rede, ou um dispositivo dedicado, utilizado para unir duas redes (como por exemplo, um roteador, ou geralmente um dispositivo que une as funções de modem e roteador podendo ter também um switch integrado e um access point). Existem vários usos possíveis, desde interligar duas redes que utilizam protocolos diferentes, até compartilhas a conexão com a internet entre várias estações.

O endereço do gateway deve ser informado nas propriedades de rede, mas numa rede onde as estações estão configuradas para obter seus endereços automaticamente é possível configurar o servidor DHCP para enviar o endereço do gateway automaticamente. A estação enviará ao gateway qualquer requisição de endereço que não fala parte da rede local.

A princípio, isso permitiria que apenas um micro acessasse a web, mas é possível compartilhar a conexão entre vários micros via NAT, opção disponível tanto no Windows quanto no Linux. Quando você compartilha a conexão entre vários micros, apenas o servidor que está compartilhando a conexão possui um endereço IP válido, só ele "existe" na internet. Todos os demais acessam através dele.

O default gateway ou gateway padrão é justamente o micro da rede que tem a conexão, é ele que os outros consultarão quando precisarem acessar qualquer coisa na internet. Por exemplo, se você montar uma rede doméstica com 4 PCs, usando os endereços IP *192.168.0.1*, *192.168.0.2*, *192.168.0.3* e *192.168.0.4*, e o PC *192.168.0.1* estiver compartilhando o acesso à internet, as outras três estações deverão ser configuradas para utilizar o endereço *192.168.0.1* como gateway padrão.

O gateway pode ter funções específicas nas redes, dependendo do planejamento do administrador de redes. Entre elas, podemos destacar:

- **Direcionamento:** No qual todas as mensagens são enviadas para o nó da rede, podendo ser roteador ou switch.
- **Proxy:** Uma lista de sites cujo acesso é ou não permitido por meio dos dispositivos da rede interna.
- **Firewall:** Um dispositivo de segurança que verifica o conteúdo dos pacotes e efetua seu bloqueio, quando nocivo aos serviços disponíveis na rede.

Introdução ao Roteamento de Redes

A internet é uma coleção de redes interconectadas, e os pontos de ligação são os roteadores. Estes, por sua vez, estão organizados de forma hierárquica, onde alguns roteadores são utilizados apenas para trocar dados entre grupos de redes controlados pela mesma autoridade administrativa, enquanto outros roteadores fazem também a comunicação entre as autoridades administrativas. A entidade que controla e administra um grupo de redes e roteadores chama-se Sistema Autônomo (RFC 1930).

O roteamento é a principal forma utilizada na internet para a entrega de pacotes de dados entre hosts (equipamentos de rede de uma forma geral, incluindo computadores, roteadores, etc.). O modelo de roteamento utilizado é o do salto-por-salto (hop-by-hop), onde cada roteador que recebe um pacote de dados, abre-o, verifica o endereço de destino no cabeçalho IP, calcula o próximo salto que vai deixar o pacote um passo mais próximo de seu destino e entrega o pacote neste próximo salto. Este processo se repete e assim segue até a entrega do pacote ao seu destinatário. No entanto, para que este funcione, são necessários dois elementos: Tabelas de roteamento e protocolos de roteamento.

Tabelas de roteamento são registros de endereços de destino associados ao número de saltos até ele, podendo conter várias outras informações.

Protocolos de roteamento determinam o conteúdo das tabelas de roteamento, ou seja, são eles que ditam a forma como a tabela é montada e de quais informações ela é composta. Existem dois tipos de algoritmo atualmente em uso pelos protocolos de roteamento: O algoritmo baseado em Vetor de Distância (Distance-Vector Routing Protocols) e o algoritmo baseado no Estado de Enlace (Link State Routing Protocols).

Esses são os tipos de roteamento:

- **Roteamento Interno:** Os roteadores utilizados para trocar informações dentro de sistemas autônomos são chamados roteadores internos (interior routers) e podem utilizar uma variedade de protocolos de roteamento interno (Interior Gateway Protocols – IGPs). Dentre eles estão: RIP, IGRP, EIGRP, OSPF e Integrated IS-IS.
- **Roteamento Externo:** Roteadores que trocam dados entre sistemas autônomos são chamados de roteadores externos (exterior routers), e estes utilizam o Exterior Gateway Protocol (EGP) ou o BGP (Border Gateway Protocol). Para esse tipo de roteamento são

considerados basicamente coleções de prefixos CIDR (Classless Inter Domain Routing) identificados pelo número de um sistema autônomo.

O que é o Roteamento?

Fazendo uma analogia, o roteamento funciona como um mapa onde as rotas são definidas e o roteador, equipamento responsável por fazer o roteamento, seria como um GPS que seleciona os melhores caminhos disponíveis para que esses dados cheguem da melhor forma ao seu destino.

Para funcionar, o roteador precisa de informações como o endereço de destino e as rotas, que são, muitas vezes, encaminhadas por outros roteadores. Porém, além das diferentes funções dos roteadores, que podem ser usados apenas para trocar dados entre uma rede local, quanto para trocar dados entre outras redes, há ainda algumas diferenças na forma como o roteador transfere um pacote de dados.

Rotas Estáticas

Na rota estática, as rotas são definidas manualmente por um administrador da rede, neste tipo de roteamento, as rotas mudam muito lentamente, a depender do administrador da rede.

Rotas Dinâmicas

Na rota dinâmica, o roteador troca informações sobre as rotas com outros roteadores. Neste tipo, os caminhos mudam de acordo com a carga do tráfego ou da topologia da rede. Esse tipo de roteamento, apesar de conseguir mudanças mais rápidas na rota, é mais suscetível a problemas com loops e oscilações.

Rotas Diretas

São as rotas criadas quando colocamos diretamente um IP na interface.

Como as Rotas são Definidas

Diferentes das pontes, roteadores possuem a capacidade de escolher o melhor caminho para encaminhar o pacote caso existam muitos caminhos que levem ao mesmo destino. Essa escolha obedece a certos critérios. O roteador pode também ouvir o tráfego e determinar quando uma rota está muito congestionada, nesse caso ele escolhe uma rota alternativa para encaminhar o pacote.

Observe que saindo de PC1 até chegar a PC4, existem dois caminhos ou 2 rotas. Quando o pacote chega a R1 com destino a R4, ele tanto pode ser encaminhado por R2 ou R3. Qual rota R1 irá escolher para encaminhar o pacote? O roteador toma essa decisão baseado em certos parâmetros, que constam em sua tabela de roteamento:

- Métrica (número de saltos até a rede destino).
- Distância administrativa (custo da rota até a rede destino).

Aquela rota que tiver o menor número de saltos será a escolhida. Caso o número de saltos seja igual para as duas situações, então aquela rota com o menor custo (menor distância administrativa) será a escolhida. Tendo por base a figura e de posse das informações da tabela, vamos ver qual será a rota escolhida, considerando que as rotas não estejam demasiadamente ocupadas.

Observe que o número de saltos é o mesmo para as duas rotas (2). Para chegar a R4 em qualquer um dos caminhos é preciso passar por2 roteadores a partir de R1, mas, observe que a distância administrativa indo por R3 é menor do que indo por R2.

Logo o pacote será encaminhado através de R3 e não de R2.

Se as distâncias administrativas fosses as mesmas, os pacotes seriam divididos entre as duas rotas.

Tipos de Roteadores

Os roteadores podem ser equipamentos externos dedicados com um sistema operacional proprietário como é o caso dos roteadores Cisco, por exemplo, ou podem ser serviços que são adicionados a um sistema operacional de rede servidor, tal como o Windows 2000. A diferença entre um e outro está na disponibilidade de recursos, nas situações em que podem ser usados e no custo.

Prefira sempre os roteadores externos, pois eles possuem melhor performance, um sistema operacional proprietário otimizado e uma série de recursos para configuração, monitoramento e diagnóstico. O problema desses roteadores é seu custo elevado. Mas para redes pequenas em que custo é uma palavra-chave, um servidor como o Windows 2000, fazendo o papel de roteador, apesar de não ter uma série de recursos disponíveis nos equipamentos de fabricantes, daria conta do recado perfeitamente.

Protocolo ARP

O protocolo ARP fornece resolução dinâmica de endereços, que é um mapeamento entre as duas formas de endereçamento distintas: Endereços IP, e qualquer outro tipo de endereço usado na camada de enlace. No caso dos quadros Ethernet, a camada de enlace usa o MAC Address (Media Access Control), endereço físico da interface. Permite obter o MAC Address de uma interface a partir do seu endereço IP.

Esses são os tipos de mensagens ARP:

- **ARP Request (Requisição ARP):** Mensagem enviada requisitando a resolução de um endereço IP em endereço físico.
- **ARP Reply (Resposta ARP):** Mensagem de resposta ao ARP Request, contendo o endereço físico resolvido.

Esses são os formatos do pacote ARP:

- **HTYPE (Hardware Type):** Especifica o tipo de protocolo da rede, como Ethernet, cujo valor é 1.
- **PTYPE (Protocol Type):** Especifica o protocolo da camada de internet para o qual a requisição do ARP é direcionada. O valor para o protocolo IPv4 é 0x0800.
- **HLEN (Hardware Length):** Tamanho do endereço de hardware, em grupos de oito bits (octetos). Um MAC Address Ethernet tem o tamanho de 6.
- **PLEN (Protocol Length):** Tamanho, em octetos, do endereço especificado no campo PTYPE. Para o protocolo IPv4, o tamanho é 4.
- **OPER (Operation):** Tipo de operação que o transmissor está realizando, sendo o valor 1 para ARP Request, e 2 para ARP Reply.

- **SHA (Sender Address Hardware):** Endereço MAC do transmissor. Quando se trata de um pacote ARP Request, contém o endereço físico do remetente. Já uma mensagem ARP Reply, contém o endereço físico procurado (resolvido).
- **SPA (Sender Protocol Address):** Endereço da camada de internet do remetente (IP).
- **THA (Target Hardware Address):** Endereço físico do destinatário pretendido. Esse campo é ignorado em um pacote ARP Request (por razões óbvias), e em um pacote ARP Reply contém o endereço físico do host que originou a requisição ARP.
- **TPA (Target Protocol Address):** Endereço da camada de internet (IP) do destinatário pretendido.

O cache ARP mantém os mapeamentos de endereços mais recentes de IPs para endereços MAC na memória do host, possuindo um tempo de expiração para cada entrada no cache de alguns minutos a partir do momento em que a entrada foi adicionada. Podemos examinar o cache ARP usando o comando *arp /a*.

A captura de pacotes trocados entre dois hosts, é realizada por meio do comando ping, usando o software analisador de pacotes Wireshark.

O ARP Probe são pacotes especiais ARP Request transmitidos em broadcast com o campo SPA (IP do remetente) contendo o valor 0.0.0.0. Utilizado por um host que solicitou um endereço IPv4 de um servidor DHCP, ou após a configuração manual de IP no host, para verificar se o IP atribuído já está em uso na rede.

Existe também o protocolo RARP, que faz o inverso do ARP, associando um endereço lógico ao físico.

Protocolo ICMP

O protocolo ICMP é o protocolo de mensagens da internet, que comunica mensagens de erro, diagnóstico e outras condições que requeiram atenção em uma rede. O protocolo IP, que fornece o mecanismo para entrega de datagramas entre dispositivos, carece dessa funcionalidade, e por isso o ICMP foi criado.

As mensagens ICMP são transmitidas em datagramas IP. Ela contém os campos tipo, código, checksum e conteúdo.

As mensagens ICMP podem ser divididas em duas grandes classes:

- **Mensagens de Erro:** Usadas para informar um dispositivo transmissor que um erro ocorreu durante a transmissão do datagrama.
- **Mensagens de Informação (Consultas/Query):** São mensagens que permitem aos dispositivos trocarem informações entre si e realizarem determinados tipos de testes e diagnósticos.

Essa são as regras especificadas para mensagens, as mensagens ICMP não são geradas:

- Como resposta a outra mensagem de erro. Isso evita o surgimento de loops infinitos de mensagens de erro. Porém, mensagens de erro podem ser geradas em resposta a mensagens de informação.
- Resposta a datagramas de broadcast ou multicast.
- Resposta a datagramas cujo endereço IP de origem não seja um endereço unicast.

- Em resposta a fragmentos de datagramas IP, exceto o primeiro, os demais fragmentos de um datagrama não geram mensagens de erro.

Alguns tipos de códigos e mensagens:

Tipo	Código	Descrição
0	0	Echo Reply (Resposta de Eco, usado pelo comando ping)
3		Destino Inalcançável
	0	Rede de Destino Inalcançável
	1	Host de Destino Inalcançável
	2	Protocolo de Destino Inalcançável
	3	Porta de Destino Inalcançável
4	0	Sourche Quench – Controle de Fluxo Elementar
8	0	Echo Request (Requisição de Eco, usado pelo comando ping)
11		Tempo Excedido
	0	TTL Igual a 0 Durante o Trânsito
	1	TTL Igual a 0 Durante Reconstrução dos Fragmentos

Mostramos o protocolo ICMP em ação usando os comandos *ping* e *tracert*, no prompt, seguido do IP ou domínio.

O TTL é o tempo de vida do pacote, que existe para que ele não fique procurando eternamente um host, iniciando em 255 e vai diminuindo de 1 em 1 (decremento) até achar o host (ele vai de 255 a 0), se ele não achar antes de chegar a 0, ele dará tempo excedido e finalizará sua vida. Isso é usado no Ping e no Traceroute (sendo mais necessário nesse último).

Como Funciona o Utilitário Traceroute

O Traceroute é uma ferramenta de diagnóstico que permite ver a rota que datagramas IP seguem quando são enviados de um host ao outro. Faz uso do protocolo ICMP e do campo TTL no cabeçalho IP do datagrama.

O propósito do TTL é evitar que datagramas entrem em um loop de roteamento, quando um datagrama chega a um roteador, seu TTL é decrementado (-1) antes de ser encaminhado. Quando um roteador recebe um datagrama cujo TTL é igual a 0, ele o descarta e envia de volta ao host que o originou uma mensagem ICMP do tipo Tempo Excedido. Essa mensagem contém o endereço IP do roteador como endereço de origem.

Para entender o funcionamento do traceroute, precisamos saber que:

- O Traceroute envia um datagrama com um TTL igual à do host de destino.
- Ao chegar ao primeiro roteador no caminho, o TTL é decrementado, ficando com o valor zero, o datagrama é descartado e a mensagem “Tempo Excedido” é enviada de volta a origem.

- Dessa forma, o primeiro roteador no caminho é identificado. Então o Traceroute envia um novo datagrama, desta vez com o TTL igual a 2, que decrementa o TTL para 1, e então será descartado no segundo roteador, e assim descobrimos o endereço IP deste roteador também.
- Esse processo continua até que um datagrama chegue ao host de destino.
- Ao chegar no host de destino, será gerado um erro ICMP do tipo “Porta Inalcançável”, e então, o Traceroute diferencia o recebimento de mensagens “Tempo Excedido” da mensagem “Porta Inalcançável” para quando parar.
- Já no Windows, são enviados datagramas ICMP do tipo Echo Request (o famoso Ping), e quando o dispositivo de origem recebe uma resposta Echo Reply, ele sabe que o pacote chegou ao seu destino.

Para trabalharmos com isso, usamos (em Windows), o comando *tracert*.

Vamos abrir o prompt, digitando *tracert* *www.google.com.br* (ou outro site/IP).

Como Funciona o Utilitário Ping

O programa Ping é um utilitário que permite testar a conectividade entre dois hosts em uma rede. Ele funciona enviando uma mensagem ICMP do tipo Echo Request a um host, e espera o recebimento de uma mensagem ICMP do tipo Echo Reply em retorno (resumindo, ele envia uma mensagem que retornará num espaço de tempo.

No geral, se não conseguirmos “pingar” um host, significa que não há conectividade entre as máquinas envolvidas no processo. É um dos primeiros passos que tomamos para determinar qual o problema que afeta uma rede onde um ou mais hosts não conseguem se comunicar entre si, ou com a rede externa.

O número de sequência se inicia em 1 e é incrementado cada vez que uma nova mensagem Echo Request é enviada. O Ping então mostra o número de sequência de cada datagrama retornado, de modo que podemos verificar se os pacotes se perderam, estão fora de ordem ou foram duplicados.

Como sabemos, o protocolo IP é um serviço de entrega de datagramas do tipo “melhor esforço”, de modo que qualquer uma dessas condições citadas pode vir a ocorrer.

Além de mostrar o número de sequência, quando a mensagem de retorno Echo Reply é recebida, também são mostrados o TTL e o RTT calculado. O Ping calcula o RTT armazenando a hora na qual o pacote Echo Request é enviado na área de dados da mensagem ICMP. Então, quando a resposta Echo Reply é recebida, ele simplesmente subtrai esse valor de hora da hora atual (momento que o datagrama é recebido). Erros e pacotes também são relatados pelo comando Ping.

Para usarmos ele, usamos o comando *ping* *www.google.com.br* (substituindo pelo site/IP desejado).

PS: O Ping é um comando para iniciar o teste de conectividade, apesar de algumas pessoas errarem, o Ping é apenas o comando, o tempo de milissegundos para o outro dispositivo se chama latência (o tempo máximo de latência deve ser de 45 ms, em média, no Brasil, quanto mais distante maior será a latência, como por exemplo, um servidor nos EUA).

Protocolo TCP – Campos do Cabeçalho

O protocolo TCP (Transmission Control Protocol) é um protocolo da camada de transporte, que realiza um serviço de entrega de pacotes confiáveis, orientado a conexão.

As principais funções realizadas pelo TCP são:

- Estabelecer, manter e terminar conexões.
- Fornecer confiabilidade.
- Fornecer controle de fluxo.
- Multiplexação.
- Endereçamento de aplicações.
- Controle de congestionamento.

Pode ver que o segmento TCP é composto por um cabeçalho TCP (geralmente com 20 bytes, mas pode ter mais), e a área de dados TCP, que é as informações transmitidas (que podem ou não estar vazia). Tudo isso é um segmento TCP, encapsulado num datagrama IP, que também tem seu cabeçalho, da mesma forma.

Essa é a descrição dos campos:

- **Número de Porta de Origem:** Número que identifica a aplicação (processo) que envia os dados.
- **Número de Porta de Destino:** Número que identifica a aplicação (processo) que deve receber os dados.
- **Número de Sequência:** Número que identifica o byte em um fluxo de dados do transmissor para o receptor.
- **Número de Confirmação:** Se a flag ACK estiver ativa, o valor desse campo será o próximo número de sequência que o destinatário espera receber.
- **Comprimento do Cabeçalho (Data Offset):** Tamanho do cabeçalho TCP em palavras de 32 bits.
- **Reservado (3 bits):** Para uso futuro. Consiste atualmente na sequência 000.
- **Flags (ECN – Explicit Congestion Notification):** Contendo NS (campo opcional adicionado ao ECN para proteger contra dissimulação acidental ou malicioso de pacotes marcados do transmissor), CWR (Congestion Window Reduced) e ECE (ECN-Echo, cuja função depende do valor da função SYN).
- **Flags (Bits de Controle):** Contendo URG (quando ativado, indica que o campo pointeiro de urgente é válido e o recurso transferência de dados com prioridade foi invocado), ACK (Bit de Confirmação. Quando ativado, indica que o segmento carrega uma mensagem de confirmação e que o valor do campo Número de Confirmação é válido, e carrega o próximo número de sequência esperado pelo host), PSH (Bit de Push. Quando ativado, indica que o transmissor do segmento usa o recurso TCP Push, o qual requisita que os dados do segmento sejam imediatamente transmitidos à aplicação no dispositivo de destino), RST (Bit de Reset. Quando ativado, indica que o transmissor encontrou um problema e deseja resetar a conexão), SYN (Bit de Sincronismo. Requisição para sincronizar números de sequência e estabelecer uma conexão entre dois hosts. O campo número de sequência contém o número de sequência inicial (ISN) do host que transmite o segmento) e FIN (Bit de Finalização. Quando ativado indica que o transmissor do segmento requisita que a conexão seja encerrada).
- **Tamanho da Janela:** O tamanho da janela de recepção indica o número de bytes que o transmissor deste segmento quer aceitar do host de destino, em cada transmissão.
- **Checksum:** Usado para verificação de erros do cabeçalho e dos dados transmitidos.
- **Ponteiro de Urgente:** Usado em conjunto com o flag URG para transferência de dados com prioridade.

- **Opções:** Campo opcional, que representa informações não cobertas pelos demais campos do cabeçalho TCP. Uma das opções mais comuns é o MSS (Maximum Segment Size).

Em resumo:

- O protocolo TCP fornece um serviço orientado a conexão, confiável, na camada de transporte da pilha TCP/IP.
- Os dados são empacotados em unidades denominadas segmentos.
- As mensagens enviadas recebem uma confirmação de recebimento, além de serem reordenadas no host de destino, que também verifica a ocorrência de erros de transmissão.
- Caso haja algum erro, os dados são retransmitidos e, caso hajam segmentos duplicados, são descartados.
- Além disso, o protocolo TCP permite enviar dados de múltiplas aplicações multiplexadas.
- Usa o mecanismo de portas de comunicação para determinar a qual aplicação enviar e entregar os dados transmitidos.

O Que é um Switch

Um switch é um equipamento de rede que permite interconectar dispositivos em uma rede de computadores, usando comutação de pacotes pra receber, processar e encaminhar quadros ao dispositivo de destino.

Vamos entender o que eles fazem:

- Utilizam os endereços de hardware (MAC Address) para processar e encaminhar dados na camada de enlace (nível 2 no modelo OSI).
- Alguns modelos também conseguem processar dados do nível 3 (camada de rede) ou superiores, incorporando assim algumas funcionalidades de roteamento.
- Um switch que pode operar em mais de uma camada é chamado de switch multilayer.
- Gerenciam o fluxo de dados na rede transmitindo uma mensagem recebida apenas para os dispositivos para os quais a mensagem foi enviada.
- O segmento de rede formado pelos dispositivos conectados a um switch é considerado um domínio de broadcast.
- Cada porta do switch é um domínio de colisão separado.

A função principal do switch é conectar os dispositivos que estão dentro de uma rede, não confunda com a funcionalidade do roteador (que conecta redes distintas entre si).

Numa rede, nós ligamos o gateway padrão da rede (como um dispositivo wireless ou o modem integrado da operadora, que costumam ter só 4 portas para conexão) ao switch para que possamos conectar inúmeros dispositivos na nossa rede. Podemos inclusive configurar, por exemplo, um servidor DHCP.

O switch é um equipamento concentrador, que encaminha os pacotes para o dispositivo ou grupo de dispositivos de destino, em vez de simplesmente encaminhar os pacotes para todos os nós da rede, como ocorria com os hubs. Aprende os endereços físicos dos nós e os associa às suas portas para uso posterior. Encaminha os quadros para seus destinos usando técnicas como Store and Forward, Cut-Through, Fragment Free e Adaptive Switching.

O switch cria uma tabela na sua memória denominada SAT (Source Address Table) com os endereços MAC das estações, que estão associados a cada porta. Quando um dispositivo transmite

um quadro, o endereço de destino é pesquisado na SAT. Se encontrado, o quadro será transmitido diretamente para a porta de destino. Se o endereço não for encontrado na SAT, o switch envia um broadcast perguntando em todas as portas sobre o endereço, e o adiciona a essa tabela.

Esses são os métodos de encaminhamento:

- **Store and Forward:** O switch armazena em buffer os dados e verifica cada quadro antes de encaminhá-lo, um quadro é recebido totalmente antes de ser encaminhado.
- **Cut-Through:** O switch inicia o encaminhamento logo após o endereço de destino quadro ter sido recebido. Não há verificação de erros neste método.
- **Fragment Free (Modified Cut-Through):** Neste método os primeiros 64 bytes do quadro onde a informação de endereçamento é armazenada, são verificados. De acordo com as especificações Ethernet, as colisões devem ser detectadas durante os primeiros 64 bytes do quadro, de modo que quadros que possuam erros devido a colisões não devem ser encaminhados.
- **Adaptive Switching:** Neste método é realizada uma seleção automática entre os outros três modos.

Essa é a classificação quanto a configuração:

- **Não-Gerenciável:** Sem opções ou interfaces de configuração. Geralmente usados em pequenos ambientes SOHO.
- **Gerenciável:** Possuem opções para alterar o modo de funcionamento do dispositivo. Podem usar interfaces de linha de comandos, web, SSH, console serial ou outros métodos de acesso, permitem alterar configurações tais como: Habilitar protocolo Spanning Tree, Port Mirroring, configurar largura de banda das portas, aplicar filtros de MAC, criar VLANs, entre diversas outras.

Podemos também classificar um switch de acordo com a sua aplicação e o tipo de local onde será utilizado:

- **Desktop:** Switches de pequeno porte, 4 a 24 portas, sem gerenciamento, para conexão de estações.
- **Workgroup (Edge):** Capacidade maior de tráfego, conecta workstations à rede, e pode ser gerenciável.
- **Enterprise (Core):** Conecta os switches workgroup e servidores de rede. Alta capacidade de transmissão e altamente gerenciáveis.
- **Campus:** Interliga grandes extensões da rede, como prédios próximos e interligações com concessionárias de serviços.

O que é uma Bridge (Ponte)

Quando o administrador de redes necessita conectar duas redes distintas, uma solução viável pode ser utilizada – as bridges (pontes). Esse tipo de equipamento possui características muito parecidas com o switch. Porém, as suas aplicações em uma infraestrutura são bem distintas.

Enquanto o switch é utilizado para conectar dispositivos da rede, a bridge é utilizada para interligar duas redes (LAN). Mas nada impede que o administrador utilize o switch para interligar duas redes, desde que devidamente configurado e planejado.

A vantagem em se utilizar as bridges é que a sua configuração é mais simples, necessitando apenas apontar o endereço das interfaces dos equipamentos das redes que estão sendo conectadas. Já ao se utilizar o switch, o ganho no processamento das informações pode proporcionar um ganho de desempenho na comunicação entre os dispositivos de rede.

Escopos de Rede

O escopo de uma rede refere-se ao seu tamanho ou alcance geográfico. O tamanho de uma rede pode variar de apenas alguns poucos metros, ligando periféricos a um computador, à milhares de computadores conectados a longas distâncias. Os principais tipos de redes quanto ao escopo podem ser LAN, MAN, WAN e PAN.

A LAN, Rede de Área Local, ou simplesmente Rede Local, geralmente está localizada em um edifício, escritório, campus ou mesmo em sua residência. Possui conectividade em alta velocidade e sua característica principal é ser uma rede privativa, ou seja, alguém (pessoa ou organização) controla essa rede e o acesso a ela, em uma área geográfica limitada.

As principais tecnologias para redes LAN são o Ethernet e o IEEE 801.11 (WLAN – Rede Wireless Local). É um dos escopos de rede mais populares e comuns.

Uma LAN tem um dispositivo central (switch), que interliga vários dispositivos, como computadores, impressoras, servidores e etc.

A MAN, Rede de Área Metropolitana, é um escopo de rede intermediário entre uma LAN e uma WAN. Trata-se de uma rede localizada em uma área geográfica confinada e bem definida, de tamanho médio, como, por exemplo, em um município ou região metropolitana. Também existem redes MAN Wireless (sem fio), como no caso das redes WiMAX.

Um bom exemplo de MAN são as redes de TV a cabo, que conecta vários prédios, casas e relacionados, cada um com sua LAN.

A WAN, Rede de Área Ampla, a comunicação se dá em uma distância relativamente (ou muito) longa. Geralmente podemos usar uma WAN para conectar uma LAN em um local a outra LAN em um local remoto, que pode estar localizada em um prédio vizinho ou do outro lado do planeta.

Um exemplo é ver a WAN como uma “nuvem”, que seria a internet, por exemplo. Um modem de banda larga costuma ter as portas LAN e WAN.

A PAN, Rede de Área Pessoal, é um escopo de rede que remete a equipamentos conectados a um computador, sendo considerada uma espécie de rede privada, consistindo em elementos que se conectam usando tecnologias variadas, como cabos USB, bluetooth, IR (infravermelho) e NFC (Near Field Communication). Conectando mouses, teclados, HDs externos, fones de ouvido wireless, celulares, etc., e sua principal característica é o espaço geográfico extremamente limitado da rede, geralmente alguns poucos metros.

Além dos escopos citados, existem outras classificações de redes menos utilizadas, como o CAN (Campus Area Network), GAN (Global Area Network), HAN (Home Area Network) e SAN (Storage Area Network).

Protocolo UDP

O protocolo UDP, que pertence à camada de transporte juntamente com o protocolo TCP, é um protocolo simples, orientado a datagrama. Ele não fornece confiabilidade na transmissão, pois envia os datagramas requisitados pela aplicação sem nenhuma garantia de que eles chegarão ao seu destino.

O UDP não estabelece conexões antes de enviar dados, apenas os empacota em datagramas e os envia. Além disso, não fornece confirmação da entrega de dados.

O protocolo UDP encontra inúmeras aplicações em comunicação de redes, como podemos ver na tabela abaixo:

Protocolo	Porta	Aplicação
DNS	53	Sistema de resolução de nomes de domínio
DHCP	67/68	Protocolo de configuração de hosts dinâmicos
SNMP	161/162	Protocolo para gerenciamento de redes
RIP	520/521	Protocolo de roteamento que não requer conexões

O UDP encontra uso em streaming de áudio e vídeo, VoIP, gaming, mecanismos de broadcast e conexões VPN (openVPN, por exemplo), entre outras.

Um segmento UDP é encapsulado em um datagrama IP.

Apesar do UDP não ser tão seguro e confiável, ele é mais rápido, em alguns casos é preferível usar ele ao invés de TCP.

Podemos ver o formato completo de um cabeçalho UDP, cujo tamanho é de 8 bytes:

Número de Porta de Origem	Número de Porta de Destino
Comprimento	Checksum
Dados	

No exemplo acima, apenas os dados não fazem parte do cabeçalho UDP. 0 do lado direito, 15 e 16 no meio e 31 no final.

Abaixo, veja os campos do cabeçalho:

- **Número de Porta de Origem:** Número que identifica a aplicação (processo) que envia os dados.
- **Número de Porta de Destino:** Número que identifica a aplicação (processo) que deve receber os dados.
- **Comprimento:** Este é um campo que especifica o comprimento em bytes do campo UDP mais os dados carregados. O tamanho mínimo é de 8 bytes devido ao comprimento do cabeçalho. O tamanho máximo possível para um datagrama UDP é de 65.507 bytes (65535 - 8 bytes do cabeçalho UDP - 20 bytes do cabeçalho IP), devido ao protocolo IPv4. Em IPv6 é possível termos pacotes maiores do que 65536.
- **Checksum:** Pode ser usado para verificação de erros do cabeçalho e dos dados transmitidos. É opcional em IPv4 e obrigatório em IPv6. Se não for usado, deve ser preenchido com zeros.

Veja abaixo a comparação dos protocolos TCP e UDP:

- O UDP não é confiável, as mensagens enviadas podem não alcançar o destino, o TCP trata disso tentando garantir a entrega da mensagem ao destino.
- O UDP não ordena os datagramas enviados, se chegarem fora de ordem não serão reordenados, o TCP os reordena no destino, caso cheguem desordenados.
- O UDP é um protocolo mais leve, pois não realiza handshake para estabelecer e finalizar conexões nem tampouco mantém registro das conexões ativas, o TCP realiza essas tarefas.
- Como o UDP não é orientado a conexão, ele pode enviar pacotes em broadcast ou multicast tranquilamente, o TCP é projetado para trabalhar em comunicação unicast.

APIPA – Endereço de Configuração IP Automática

Quando a gente utiliza o endereçamento IPv4 numa rede, devemos configurar os IPs nas estações de trabalho, isso podemos fazer manualmente ou utilizar um servidor DHCP para atribuir os endereços de forma automática. Porém, pode acontecer do servidor DHCP falhar ou não estar disponível na rede, ou ainda a sua estação não conseguir contatar o servidor DHCP para pegar a configuração de IP automática. Nesse caso, para tentar garantir que as estações consigam se comunicar entre si dentro da própria rede local, existe o esquema chamado APIPA (Endereçamento de IP Privado Automático), assim podemos garantir que as máquinas consigam se comunicar na rede local mesmo que não haja um servidor DHCP disponível para atribuir um endereço host naquele momento.

A ideia do APIPA é essa abaixo:

- Endereço de configuração automática do Windows.
- Atribui automaticamente IP a uma estação caso haja falha na comunicação com um servidor DHCP.
- Garante a comunicação entre as estações dentro de uma rede.

Há uma faixa de endereços reservados pelo IETF que são atribuídas pelo APIPA, de *169.254.0.1* até *169.254.255.254*.

O primeiro e o último bloco dessa faixa são reservados, de modo que as estações, na verdade, irão receber endereços localizados entre *169.254.1.0* até *169.254.254.255*.

A máscara de sub-rede é 255.255.0.0 (classe B).

Além de ser um indicativo de que não há conectividade com o servidor DHCP em uma rede, o APIPA pode ajudar a detectar variados problemas, como:

- Patch cable defeituoso.
- Servidor DHCP com problemas.
- Sem conexão adequada à rede sem fio.
- Cabeamento fixo com problemas.
- Problemas em uma ou mais portas do switch.

Ou seja, problemas que, em última instância, levem à quebra de comunicação entre as estações e o servidor DHCP da rede.

Abra o CMD e digite *ipconfig* para vermos a configuração atual de IP.

Para liberar a configuração de IP, use *ipconfig /release*, aí ele mostrará o IP de configuração automática em ação (169.254.x.x). Para renovar, use o *ipconfig /renew.*

Para abrir as conexões de rede, digite *ncpa.cpl*. Lá dentro, clique com o botão direito em Conexão Local, e em IPv4, lá terá a opção Configuração Alternativa, que é referente ao APIPA, onde podemos configurar também manualmente.

Ipconfig – Utilitário para Diagnóstico de Rede no Windows

O ipconfig, usado no CMD, tem a finalidade de trazer, basicamente, as configurações atuais de rede que sua máquina está usando. Mas ele também pode ser usado para outras tarefas, como mostrar o conteúdo do cache do resolvedor DNS, ou ainda fazer a renovação de uma concessão de endereço obtido via DHCP, ou ainda liberar esse endereço, entre outras coisas.

Essas são as principais funções do ipconfig:

Opção	Significado
/?	Mostra a ajuda do comando
/all	Mostra informações de configuração de rede completas
/release	Libera os endereços IP associados a um adaptador especificado
/renew	Renova os endereços IP associados a um adaptador especificado
/release6	Libera os endereços IPv6 associados a um adaptador especificado
/renew6	Renova os endereços IPv6 associados a um adaptador especificado
/flushdns	Limpa o cache do resolvedor DNS
/registerdns	Atualiza todas as conexões DHCP e registra novamente os nomes DNS
/displaydns	Mostra o conteúdo do cache do resolvedor DNS
/showclassid	Mostra todas as identificações de classe DHCP permitidas para o adaptador especificado
/setclassid	Permite modificar as identificações de classe DHCP

PS: Digitar apenas *ipconfig* mostrará as informações de configuração de rede resumida.

Fragmentação de Pacotes IP

Quanto um roteador recebe um pacote, ele examina o endereço de destino e determina para qual interface deve encaminhar esse pacote, para que possa seguir seu caminho até o destino.

Além disso, o roteador também determina o MTU da interface a ser usada. Caso o tamanho do pacote seja maior do que o MTU, e o bit DF do campo Flag do cabeçalho esteja ajustado em 0, o roteador irá fragmentar o pacote.

O propósito da fragmentação de pacotes IP, realizada pelo protocolo IP, é portanto permitir que os datagramas possam ser transmitidos em link cujo MTU seja menor do que o tamanho original desses datagramas.

Fragmentar o pacote significa dividir o pacote em unidades de menor tamanho, denominadas fragmentos. O tamanho máximo de um fragmento é o tamanho da MTU menos o tamanho do cabeçalho IPv4, que pode variar de 20 a 60 bytes.

Cada fragmento será enviado pela rede em um pacote separado, e cada um desses pacotes seguirá algumas regras específicas.

Essas são as regras da fragmentação de datagramas:

- O campo tamanho total será o tamanho do fragmento.
- O bit MF (More Fragments) no campo flags será configurado em 1 para todos os fragmentos exceto o último, que terá o valor 0 ajustado.
- O campo offset do fragmento será configurado (em 1), baseado no deslocamento do fragmento no campo de dados original, em blocos de 8 bytes.
- O checksum do cabeçalho deve ser recalculado.

Assim, se tivermos um MTU de 1500 bytes e pacotes padrão com cabeçalho de 20 bytes, os offsets (deslocamentos) dos fragmentos serão múltiplos de (1500 - 20) / 8 = 185, como por exemplo, 0, 185, 370, etc.

Vamos supor que um segmento da camada de transporte tenha um tamanho total de 4000 bytes, sem o uso de opções, e que esse segmento será enviado em pacotes IP de cabeçalho padrão de 20 bytes.

O tamanho total do pacote IP gerado teria então 4020 bytes (4000 + 20). Vamos assumir também o caso típico do envio desse pacotes por um link cujo MTU é de 1500 bytes. O pacote seria fragmentado da seguinte forma:

Fragmento	Bytes de Dados	Bytes do Cabeçalho	Bytes Totais	Flag MF	Offset do Fragmento
1	1480	20	1500	1	0
2	1480	20	1500	1	185
3	1040	20	1060	0	370

O primeiro offset será igual a zero, o segundo offset será igual a 0 + (bytes de dados / 8) = 0 + 1480 / 8 = 185, e o terceiro offset será igual ao segundo offset (185) + (bytes de dados / 8) = 185 . 1480 / 8 = 185 + 185 = 370.

Ao chegar no receptor, ele fará a remontagem dos dados fragmentados, igual estava antes.

Podemos recalcular o tamanho total do pacote a partir do offset do último fragmento e do tamanho em bytes de seus dados, da seguinte forma:

*tamanho_total = offset * 8 + bytes_de_dados;*

// Em nosso exemplo:

*tamanho_total = 370 * 8 + 1040 = 2960 + 1040 = 4000;*

Quando os pacotes chegam ao seu destino, eles devem ser remontados para que possam ser processados.

O receptor sabe que um pacote é um fragmento caso o flag MF esteja ativo, e caso o campo offset do fragmento possua um valor diferente de zero.

Fragmentos que possuam a mesma identificação pertencem ao mesmo pacote, e o campo offset do fragmento permite ordenar esses fragmentos.

Após a remontagem, o pacote é enviado para a camada de nível superior na pilha de protocolos (camada de transporte) para processamento).

Estrutura de um Pacote IPv4

Na camada de internet da pilha TCP/IP, os dados provenientes da camada de transporte são empacotados em PDUs denominadas pacotes. Um pacote IPv4 é composto por um cabeçalho e um campo de dados, que contém os dados provenientes da camada superior (transporte).

Podemos ver que ele tem 4 octetos, 32 bytes (contados a partir do 0), e os nomes dos campos do cabeçalho na ordem que aparecem.

Esses são os campos do cabeçalho IPv4:

- **Versão:** Indica a versão do protocolo IP que está sendo usado. Para o protocolo IPv4, o valor 4 é utilizado neste campo.
- **Tamanho do Cabeçalho (IHL, Internet Header Length):** Comprimento do cabeçalho do pacote em palavras de 32 bits (bits existentes no cabeçalho / 32). O campo de opções pode ter tamanho variável, é importante registrar aqui o tamanho da cabeçalho, para que seja possível definir onde ele termina, e onde se inicia o campo de dados. Para um pacote que não usa nenhuma opção, o valor do IHL será de 160 / 32 = 5, sendo que o 160 é o somatório de bits que compõem o cabeçalho do pacote.
- **DSCP (Differentiated Services Code Point):** Esse campo originalmente era definido como ToS (Tipo de Serviço). É utilizado por tecnologias que necessitem de streaming de dados em tempo-real, como por exemplo VoIP.
- **ECN (Explicit Congestion Notification):** Este campo permite uma notificação fim-a-fim de congestionamento de rede sem descartar pacotes. É um campo de uso opcional.
- **Tamanho Total:** Define o tamanho total do pacote em bytes, incluindo o cabeçalho e o campo de dados.
- **Identificação:** Identifica o datagrama (pacote) IP por meio de um número de identificação sequencial.
- **Flags:** Usado para controlar a fragmentação dos pacotes. Possui 3 bites, com esses significados (do maior pro menor): Bit 0 (o primeiro bit sempre é 0 e é reservado), bit 1 (DF – Don’t Fragment), quando ativado indica que o datagrama não pode ser fragmentado. Se a fragmentação for requerida na rede e este bit estiver ativado, o pacote será descartado) e bit 2 (MF – More Fragments), indica o último fragmento, quando o bit for 1, há mais fragmentos depois dele, quando for 0, ele é o último fragmento do conjunto do pacote.
- **Offset do Fragmento:** Determina a ordem dos fragmentos. Especifica o deslocamento de um fragmento em particular em relação ao início do pacote IP original, sem

desfragmentação. O primeiro fragmento possui offset igual a zero. É medido em blocos de oito bytes.

- **Tempo de Vida (TTL):** Tempo de vida máximo do datagrama. Impede que um pacote se perca em uma rede (internet) e entre em loop infinito entre os roteadores. Atualmente seu valor corresponde a saltos de roteadores (hops). Toda vez que um pacote passa por um roteador, o valor desse campo é decrementado (subtrai-se 1). Quando um roteador recebe um pacote cujo TTL é igual a 0, o pacote é descartado, evitando sua permanência infinita na rede.
- **Protocolo:** Indica o protocolo (presente no campo de dados) que pediu o envio do datagrama, através de um código numérico. Os códigos são definidos pela RFC 790.
- **Checksum do Cabeçalho:** Usado para verificação de erros no cabeçalho do datagrama. Quando um pacote chega em um roteador, o roteador calcula o checksum do cabeçalho e compara o valor obtido com o valor armazenado nesse campo. Se os valores não baterem, significa que houve erro durante a transmissão dos dados, e o pacote é descartado. Toda vez que um pacote passa por um roteador, um novo checksum deve ser calculado e armazenado neste campo, pois os roteadores alteram o conteúdo do cabeçalho IP ao decrementar o campo de TTL.
- **Endereço IP de Origem:** Endereço IP do remetente do pacote. Esse endereço pode ser alterado por um roteador se for utilizado um serviço de tradução de endereços, como o NAT.
- **Endereço IP de Destino:** Endereço IP do destinatário do pacote. Esse endereço também pode ser alterado por um roteador se for utilizado um serviço de tradução de endereços, como o NAT.
- **Opções + Pad:** Campo opcional. Usado em situações de teste e verificação de erros na rede. As duas funções mais importantes desse campo são traçar a rota de rede que está sendo usada na origem até o destino (traceroute) e marcar o horário com que o datagrama passa por cada roteador da origem até o destino (timestamp).
- **Dados:** São os dados que o datagrama está carregando, com o limite de 64 Kb. OS dados fazem parte do cálculo do checksum do cabeçalho. Os protocolos mais comuns encontrados no campo de dados são o TCP, UDP, ICMP, IGMP e OSPF, entre outros.

Esse é o “resumão” com os campos e os tamanhos deles:

Estrutura de um Pacote IP
Versão (4 bits)
Tamanho do Cabeçalho (4 bits)
DSCP (6 bits)
ECN (2 bits)
Tamanho Total (16 bits)
Identificação (16 bits)
Flags (3 bits)
Offset de Fragmento (13 bits)
Tempo de Vida – TTL (8 bits)
Protocolo (8 bits)
Checksum do Cabeçalho (16 bits)
Endereço IP de Origem (32 bits)
Endereço IP de Destino (32 bits)

Opções (32 bits)
Dados (até 64 Kb)

Introdução ao Modelo OSI

O modelo OSI (Open System Interconnect), é um modelo em camadas projetado para fornecer um framework par padronização de comunicação em sistemas de computadores.

Entender o modelo OSI é muito importante para quem deseja entender o funcionamento de redesde computadores, e é um tópico onipresente em testes de certificação, tais como Cisco CCNA e CompTIA Network+.

Padrões são necessários para promover interoperabilidade entre equipamentos de fabricantes distintos, e permitir economia de escala.

O modelo OSI foi desenvolvido pela ISO para facilitar a interconexão de sistemas de computadores, a partir do qual protocolos de comunicação de redes podem ser criados.

Trata-se de um modelo abstrato, conceitual, que traz o funcionamento de um protocolo ideal em redes de computadores.

O modelo OSI é composto por sete camadas:

Camada de Aplicação
Camada de Apresentação
Camada de Sessão
Camada de Transporte
Camada de Rede
Camada de Link de Dados
Camada Física

Esses são os princípios da divisão em camadas:

- Cada camada deve executar funções bem-definidas, similares.
- Os limites da camada são escolhidos para reduzir o fluxo de informações transportadas entre interfaces.
- A quantidade de camadas deve ser suficiente para que funções diferentes não precisem ser colocadas na mesma camada.
- Onde houver necessidade de um grau de abstração distinto, deve-se criar outra camada.
- Camadas separadas são criadas para manipular funções que são diferentes no processo realizado ou na tecnologia envolvida.
- Deve permitir que alterações em funções ou protocolos sejam realizadas em uma camada sem afetar as demais camadas.

O modelo OSI garante que haja interoperabilidade entre produtos de fabricantes distintos, devido à padronização dos protocolos de comunicação.

Uma rede é constituída por equipamentos e sistemas de diversos fabricantes distintos, como roteadores e switches Cisco, sistemas Microsoft ou Linux, etc., e para que esses elementos possam se comunicar sem problemas, é necessária a padronização dos processos de comunicação.

O processo de padronização também permite o barateamento de custos, pois não ficamos reféns de sistemas proprietários.

Nas camadas do modelo OSI, cabeçalhos contendo informações são adicionados aos dados a serem transmitidos, em um processo denominado “encapsulamento”. Encapsulamento é empacotar dados com informações adicionais em cada camada.

Em cada camada, damos um nome específico ao conjunto de dados com informações encapsuladas. Chamamos a esses conjuntos de PDU (Protocol Data Unit).

Veja as diferenças das camadas:

Camada	PDU
Aplicação	Dados
Apresentação	
Sessão	
Transporte	Segmento
Rede	Pacote
Link de Dados	Quadro
Física	Bits

Camada 1 – Física

Trata-se da sinalização de rede, e da conversão de bits (advindos das camadas superiores) em sinais elétricos, ópticos ou ainda em ondas eletromagnéticas para envio pelos diversos meios de transmissão utilizados, carregando os dados de um ponto a outro da rede.

Define os aspectos mecânicos e elétricos da rede. Especifica o tipo de cabeamento a ser utilizado, tensões elétricas, temporização, etc.

Nesta camada temos cabos, conectores, antenas, hubs, modens e placas de rede atuando (placas de rede atuam também na camada 2).

Camada 2 – Link de Dados

Organização dos dados a serem enviados em conjuntos de bits denominados quadros (frames), e especificação dos endereços físicos das interfaces de redes envolvidas (endereços MAC).

Um endereço MAC é responsável pela identificação única dos dispositivos em uma rede, consistindo em um endereço de 48 bits gravados em uma memória ROM presente na própria interface física da rede.

Também é responsável pela sinalização de início e fim de transmissão de um quadro, além de gerar um código para reconhecimento de erros de transmissão de dados, conhecidos como checksum.

Camada 3 – Rede

Introduz a capacidade de rotear o tráfego de um ponto da rede a outro, por meio de sub-redes, é uma camada de roteamentos. Podemos aplicar um esquema de endereçamento lógico aos pontos de rede, como por exemplo, o endereço IP.

Também pode ocorrer fragmentação dos dados a serem transmitidos, caso o tamanho desses dados exceda um limite pré-determinado, de modo que segmentos de rede que não suportem quadros de tamanho muito grande possam enviar os dados sem problemas.

Camada 4 – Transporte

No geral, a camada de transporte tem o papel de fornecer funções que permitam a comunicação entre processos de aplicações (softwares) entre computadores diferentes.

Assim, a camada de transporte fornece um mecanismo pelo qual aplicações distintas podem enviar e receber dados usando a mesma implementação de protocolos das camadas mais baixas.

Camada 5 – Sessão

Configuração das sessões de comunicações entre os dispositivos na rede. Uma sessão de comunicação pode ser iniciada, mantida e finalizada quando não houverem mais dados a transmitir, ou quando uma das partes quiser encerrar a comunicação. Sincronismo e restabelecimento de uma sessão de comunicações a partir do ponto onde houver um problema de interrupção na transmissão.

Outras funções: Determinar se a comunicação se dará em modo half-duplex ou full-duplex, gerenciar o uso de protocolos de tunelamento (para acesso remoto, por exemplo).

Camada 6 – Apresentação

Esta camada lida com as técnicas de apresentação dos dados, o que significa basicamente que ela é responsável pela forma como os dados são reconhecidos e visualizados em seu destino.

Como exemplos de suas atribuições, temos a codificação de caracteres, compressão e criptografia de dados.

Camada 7 – Aplicação

Esta é a camada de mais alto nível (conceitualmente), e é a responsável por fornecer os serviços de rede às aplicações que rodam no computador.

Assim, seu navegador ou seu programa de e-mails acessa a rede pois é capaz de se comunicar com a camada de aplicação da pilha de protocolos.

Esse é o resumo das camadas do modelo OSI:

Camada	Resumo

Aplicação	Prover serviços de rede às aplicações
Apresentação	Criptografia, codificação, compressão e formatos de dados
Sessão	Iniciar, manter e finalizar sessões de comunicação
Transporte	Transmissão confiável de dados, segmentação
Rede	Endereçamento lógico e roteamentos, controle de tráfego
Link de Dados	Endereçamento físico, transmissão confiável de quadros
Física	Interface com meios de transmissão e sinalização

Endereço IPv4 e Classes de Endereçamento

É um identificador exclusivo que identifica um computador em uma rede. Cada interface de rede possui seu próprio IP.

Consiste em um conjunto de quatro números, que variam de 0 a 255. O IP identifica tanto a rede, quanto o host (dispositivo), além de permitir a divisão em sub-redes.

Em uma rede, cada dispositivo é identificado por um número chamado endereço IP, que contém:

- 4 octetos (grupos de 8 bits).
- Representados em decimal, separados por um ponto.
- 32 bits no total.
- 2^{32} endereços possíveis = 4.294.967.296 endereços.

O ID da rede é a parte do IP que identifica os hosts que estão localizados na mesma rede física. Essas são as regras:

- O ID de rede deve ser único dentro da rede.
- Não pode iniciar com o número 127 (loopback).
- Não podemos ajustar todos os bits no ID de rede como 1, pois esse endereço é reservado para uso como endereço de broadcast.
- Não podemos ajustar todos os bits no ID de rede como 0, pois esse endereço é usado para denotar um host específico na rede local, não roteado.

O ID de host é a parte do IP que identifica um host localizado em uma rede. Combinado com o ID de rede, forma o endereço IP. Essas são as regras:

- O ID de host deve ser único dentro de uma mesma rede (para um dado ID de rede).
- Não é possível ajustar todos os bits em um ID de host como 1, pois esse endereço é reservado para broadcast da rede.
- Não é possível ajustar todos os bits em um ID de host como 0, pois esse endereço é usado para identificar a rede (ID de rede).

Esse é um exemplo de um endereço IPv4 típico: *185.45.123.55*. Esse endereço é composto por 4 octetos, separados por pontos. Cada número pode variar entre 0 e 255 (8 bits), e algumas regras de uso desses números são aplicadas.

As classes de endereço IP são usadas para definir a divisão entre a identificação de rede e a de host. Esse método divide o espaço de endereçamento do protocolo IPv4 em cinco classes por faixas de endereços. As classes de endereçamento são A, B, C, D e E.

A máscara de sub-rede, neste esquema, é implícita para cada classe, não necessitando ser especificada de forma separada. Esse esquema, na verdade, foi descontinuado com o advento do CIDR (Classless Inter-Domain Routing) em 1993. Ainda é encontrado em casos específicos, como configurações padrão de alguns componentes de hardware e software de redes. Especificação RFC 791.

Essas são as aplicações das classes de rede:

- **Classe A:** Redes com o Nº de hosts muito grande.
- **Classe B:** Redes de médio a grande porte.
- **Classe C:** Redes pequenas, como LANs.
- **Classe D:** Endereço de multicast.
- **Classe E:** Endereços experimentais, reservados para uso futuro (pesquisa).

Especificamos as classes de endereçamento de acordo com o valor do primeiro octeto do endereço, no esquema *w.x.y.z*. O primeiro octeto, representado por *w*, será o identificador da classe, tanto em decimal quanto em binário.

Essa é a faixa de endereçamento IP das classes:

Classe	Faixa (valor de w)	Bits de início (em w)	Tam. ID de Rede (bits)	Tam. ID de Host	ID Rede / ID Host
A	0 - 127	0	8	24	w.x.y.z
B	128 - 191	10	16	16	w.x.y.z
C	192 - 223	110	24	8	w.x.y.z
D	224 - 239	1110	-	-	-
E	240 - 255	1111	-	-	-

OBS: Rede 127.0.0.0 é apenas para fins de testes (loopback).

E essas são as faixas de endereçamento:

Classe	Número de Redes	Endereços por Rede (utilizáveis)	Endereço Inicial	Endereço Final	Máscara de Sub-rede Padrão
A	128	16.777.214 (2^{24} - 2)	0.0.0.0	127.255.255.255	255.0.0.0
B	16.384	65.534 (2^{16} - 2)	128.0.0.0	191.255.255.255	255.255.0.0
C	2.097.152	254 (2^{8} - 2)	192.0.0.0	223.255.255.255	255.255.255.0
D	-	-	224.0.0.0	239.255.255.255	-
E	-	-	240.0.0.0	255.255.255.255	-

PS: Lembrando que o primeiro e o último número são excluídos dos utilizáveis.

O que é DNS?

DNS (porta 53) é uma sigla que significa Domain Name System, que traduz nomes legíveis por humanos em endereços IP, utilizados pelos computadores, assim só precisamos lembrar do endereço do site (por exemplo, *https://www.google.com.br/*) ao invés do IP do mesmo. Basicamente, é um banco de dados de informações sobre hosts.

Essas são algumas das características do DNS:

- É um sistema hierárquico.
- Banco de dados distribuído.
- Muitos servidores DNS localizados por todo o mundo.
- 13 clusters de servidores-raiz (root servers), a partir de onde podemos encontrar quaisquer domínios no mundo.
- Há centenas de domínios top-level genéricos (gTLDs), como .com, .org, .edu, etc.
- Cerca de 275 domínios de nível superior para códigos de país (ccTLDs), como .br, .ar, .fr, .jp, etc.

Veja abaixo a hierarquia do DNS:

- **.:** Domínios raiz.
- ***.ao, .br, .fr, .pt, .cn*:** Domínios de nível superior (ccTLDs).
- ***.com, .org, .net, .edu, .gov*:** Domínios de nível superior (gTLDs).
- ***.nomedosite* (*.google, .facebook*, etc.):** Domínios delegados.
- ***www, ftp, mail, admin*:** Subdomínios.

Os servidores raiz (root) sabem onde estão os servidores de nomes autoritários para cada zona de nível superior. Existem 13 servidores raiz espalhados em diferentes partes da rede (clusters, na verdade). Seus nomes são *a-root-servers.net* até *m.root-servers.net*.

Um conceito muito importante também é o de FQDN (Fully Qualified Domain Name), que contém o nome completo de um domínio. Hierarquia completa de um dispositivo, como um servidor ou uma máquina cliente (em uma rede local). Sequência de rótulos de um nó até a raiz (root), separados por pontos.

O servidor DNS é chamado de nameservers (servidores de nomes), são programas que armazenam informações sobre o namespace do domínio. No geral, possuem informações completas sobre uma parte do namespace, chamada de zona, que é carregada a partir de um arquivo ou de outro nameserver. Um nameserver é autoritativo para essa zona.

Esses são os tipos de nameservers:

- **Primário:** Lê os dados de uma zona a partir de um arquivo em seu host.
- **Secundário:** Obtém os dados da zona a partir de outro servidor de nomes autoritativo para a zona, chamado de servidor mestre, que geralmente é o servidor primário (mas nem sempre).

As partes de uma URL são essas:

- **Protocolo:** É o começo da URL, onde é indicado o protocolo usado, geralmente *http://* ou *https://*.
- **Subdomínio:** É o que vem antes do domínio, o principal é o *www*, mas temos vários outros como *mail*, *admin*, *blog* ou mesmo personalizados.
- **Nome do Domínio:** É o nome do site, basicamente, por exemplo, “google” é o domínio de *https://www.google.com/*.
- **Domínios Superiores de Topo Genérico (gTLD):** Tem três ou mais letras, é classificado pela utilização do site, como *.com*, *.net*, *.edu*, *.gov*, *.org*, entre outros.
- **Domínios Superiores de Topo de Código de País (ccTLD):** Sempre tem duas letras representando o país de origem, como *.br*, *.ar*, *.uk*, *.p*t, etc.
- **Caminho:** É tudo que vem depois da barra indicando algum caminho dentro do site(por exemplo, o search e tudo que vem depois dele em *https://www.google.com/search?q=dominio*).
- **Domínio Reverso:** Faz o processo reverso a consulta ao servidor DNS. Quando um servidor recebe uma solicitação, é feia uma consulta em sua “tabela”, que por sua vez encaminha o pedido do cliente ao servidor relacionado à URL digitada pelo usuário, sendo utilizado o endereço IP.

Resolvedor DNS

DNS Resolver é o serviço cliente que acessa o servidor DNS. Responsável por iniciar e seguir as consultas que levam à resolução de nomes do recurso procurado. O resolver é responsável por executar uma consulta, interpretar as respostas e retornar a informação ao programa que a requisitou. As consultas DNS podem ser não-recursivas, recursivas, iterativas ou ainda uma combinação desses tipos.

No caso, o resolvedor acessa um site (como o Google) pelo IP, quando digitamos o nome do site, ele enviará ao servidor DNS local (ou mais próximo), e se ele tiver a resposta, ele a envia para o resolvedor, senão ele consulta o servidor raiz, que “informa” que ele está no *.com*, o local volta e pergunta pro servidor *.com*, volta e ele procura o *google.com* e assim por diante.

Existem três métodos de consulta que um resolver pode utilizar para executar uma query DNS: Consulta não-recursiva, consulta recursiva e consulta iterativa. Um resolvedor pode utilizar uma combinação dos métodos de consulta se for necessário.

Na consulta não-recursiva, o cliente resolvedor DNS consulta um servidor DNS que fornece um registro para um domínio no qual ele é autoritativo, ou então fornece um resultado parcial sem consultar outros servidores. No caso de uso do cache DNS, a consulta não-recursiva é feita sobre o cache DNS local da máquina e fornece um resultado sem a necessidade de realizar consultas repetidas a servidores DNS remotos, reduzindo assim a carga sobre esses servidores, durante um período de tempo determinado.

Na consulta recursiva, o cliente resolvedor DNS consulta um único servidor DNS, o qual então pode consultar, como se ele fosse um cliente, outros servidores DNS em nome do cliente em si. Um exemplo clássico é o de um roteador banda larga caseiro, que age como servidor DNS (stub resolver) para as máquinas na rede local, e realiza consultas recursivas ao servidor DNS do provedor de internet. Em uma consulta recursiva, o servidor DNS fornece uma resposta completa, ou informa um erro, consultando outros servidores DNS conforme necessário.

Na consulta iterativa, o cliente resolvedor DNS consulta uma cadeia de um ou mais servidores DNS. Cada servidor encaminha o cliente ao próximo servidor na cadeia, até que um servidor

consiga efetuar a resolução de nomes de forma completa. Por exemplo, uma resolução do endereço *https://www.google.com.br/* poderia ocorrer com uma consulta a um servidor raiz global (root), depois consulta ao um servidor *.br*, depois a um servidor *.com*, até chegar ao servidor *google.com.br.*

O cache DNS é uma técnica de redução da carga nos servidores DNS por meio do armazenamento local (ou em hosts intermediários) dos resultados das consultas, conhecido como “caching”. Todo resultado de uma consulta DNS é associado a um TTL (Time To Live), uma data de expiração após a qual os resultados são descartados ou atualizados. Essa temporização é configurada pelo admin no servidor autoritativo, e pode variar de segundos a semanas. Assim, alterações nos registros DNS não se propagam imediatamente pela rede, requerendo que os caches expirem e sejam atualizados após o prazo do TTL.

Qual é a Diferença entre Domínio e Hospedagem?

Grande parte dos usuários possuem bastante dúvida em diferenciar as duas questões, muitos acham que ambas são a mesma coisa, pois alguns serviços para usuários mais leigos oferecem a ligação direta entre o domínio e o servidor de hospedagem.

O que é Domínio?

Domínio é o registro de um nome, que é utilizado para conectar seu site à sua hospedagem através de uma palavra ou sequência de caracteres com a finalidade de facilitar o acesso ao seu site através de um navegador de internet.

O que é Hospedagem?

Diferente do domínio, que faz apenas a ligação de seu site para que ele seja acessado através de uma palavra ou sequência de caracteres, a hospedagem é como um espaço online reservado para seu site na internet, é por meio dela que você armazena os arquivos que mantém seu site no ar.

Existem diversos tipos de planos para diferentes tipos de questões que você precise hospedar. De acordo com seu projeto ou plano de negócio podem haver vantagens ou desvantagens em cada modelo de contratação, portanto, antes de escolher seu plano de hospedagem, mensure o quanto de servidor você irá precisar e quais compatibilidades ele precisa ter para que o seu funcionamento seja como o esperado.

Desde que você adquirir o registro de um domínio e também um plano de hospedagem, você também pode utilizar esse domínio para poder ter um ou mais e-mails personalizados. Ou seja, se seu domínio é *meusite.com.br,* você pode ter um e-mail como: *contato@meusite.com.br.*

Portanto, quando você contrata seu plano de hospedagem, você pode criar um ou mais e-mails, a depender do seu plano, de forma mais profissional, trazendo a própria logomarca, seu próprio domínio. Além disso, para planos de hospedagem que lhe permite a criação de diversas contas, você pode estar criando e-mails personalizado para setores da sua empresa, ou ainda para cada funcionário, ou colegas de trabalho.

Arquivo Hosts

O arquivo hosts é usado para relacionar hostnames a endereços de IP. O arquivo pode ser editado como administrador/root com um editor de texto comum.

Este arquivo no Windows se localiza em *C:\Windows\System32\drivers\etc\hosts* e no Linux em */etc/hosts*.

A sintaxe básica do arquivo é essa:

 # Tudo que tiver hashtag é comentário
 # Primeiro passamos o IP e depois o nome do host para o qual será associados
127.0.0.1 localhost

 # Para um exemplo de configuração de roteador, onde o gateway padrão usa o hostname "roteador":
192.168.15.1 roteador.online

Nesse caso, podemos acessar nosso roteador digitando *http://roteador.online/* no nosso navegador.

Podemos também redirecionar um domínio para outro IP, inclusive públicos, como esse exemplo abaixo, que redireciona o site do Google para o IP de loopback do nosso dispositivo, usado para bloquear o acesso ao Google:

 # Use todos os domínios possíveis para bloquear geral:

127.0.0.1 www.google.com.br
127.0.0.1 google.com.br
127.0.0.1 www.google.com
127.0.0.1 google.com

PS: Isso também pode ser usado por malwares que alteram o arquivo em questão, fazendo que eles redirecionem sites legítimos como o do Google, Facebook ou qualquer outro, para um IP onde está um site falso de phishing, portanto, fique alerta com entradas estranhas nesses arquivos, como por exemplo:

 # Isso seria um exemplo de um IP de um site falso,
 # para onde os links do Facebook seriam redirecionados:

122.215.182.11 www.facebook.com
122.215.182.11 facebook.com
122.215.182.11 web.facebook.com

Tipos de Registros DNS – Resources Records

Os Resource Records são registros no banco de dados DNS que descrevem as características da zona ou do domínio, e também definem os tipos de dados armazenados no banco DNS. Há mais de 30 tipos de registros disponíveis, como endereço IP, aliases, etc.

Veja um exemplo de arquivo de definição de zona de exemplo:

$TTL 86400; Diretiva para TTL padrão
teste.com IN SOA admin.teste.com root.teste.com (
500; Serial Number

604800; Refresh
86400; Retry
2419200; Expire
60); TTL Mínimo

// admin = nome do servidor DNS
// teste.com = nome do domínio

teste.com IN NS admin.teste.com.

teste.com IN A 192.168.1.200
;@ IN A 127.0.0.1
;@ IN AAAA ::1
admin IN A 192.168.1.200

name IN CNAME name.teste.com

Os registros de endereços definem o endereço IP de um host. Mapeiam FQDN para IP. São os registros mais consultados para resolução de nomes. A é endereço IPv4, e AAAA é o endereço IPv6. Um exemplo seria *www.google.com.br. IN A 172.217.29.131*.

O registro SOA (Start of Authority) está em toda zona. Esse registro contém campos TTL, classe e tipo, servidor autoritativo, pessoa responsável, serial number, refresh, retry, expire e TTL mínimo.

Veja pra que serve cada item do registro SOA:

- **Serial Number:** Mostra quantas vezes a zona foi atualizada. Permite definir se é necessário realizar uma transferência de zona entre um servidor primário e secundário (por comparação de números seriais).
- **Refresh:** Mostra de quanto em quanto tempo o servidor secundário da zona verifica se a zona foi alterada.
- **Retry:** Quanto tempo após enviar uma requisição de transferência de zona o servidor secundário espera por uma resposta do servidor mestre antes de tentar novamente.
- **Expire:** Quanto tempo após enviar uma requisição de transferência de zona o servidor secundário continua a responder a consultas antes de descartar sua própria zona (zona invalidada).
- **TTL Mínimo:** Se aplica aos registros na zona quando um TTL não é especificado em um registro de recurso.

O registro de nameserver (NS) indica os servidores autoritativos para a zona, e também oser servidores primário e secundário especificados no RR SOA. Também indica servidores para as zonas delegadas. Toda zona tem ao menos um registro NS na zona raiz (root).

O nome canônico (CNAME) é um alias (apelido) de um outro registro, nomes secundários, útil para registrar diversos serviços em um mesmo servidor no banco de dados do DNS. Por exemplo: *www IN CNAME google.com.br* ou *ftp IN CNAME google.com.br.*

O mail exchanger record (MX) é o nome de domínio DNS para um servidor de e-mail. Por exemplo *IN MX mail.google.com.br.*

O pointer record (PTR) é um registro de ponteiro, faz o processo inverso para A ou AAAA, mapeia IP para FQDN e está presente em um arquivo de zona reversa. Veja um exemplo abaixo:

$ORIGIN 1.168.192.IN-ADDR-ARPA.; diretiva de nome base
1 IN PTR roteador.teste.com
200 IN PTR admin.teste.com
50 IN PTR vendas.teste.com

O registro service resource record (SRV) permite especificar a localização de servidores para um protocolo, serviço ou domínio DNS específico. Por exemplo, registros que especificam quais hosts são os servidores web em uma rede. Sempre tem o formato _Serviço_Protocolo.Nome TTL Class SRV Prioridade Peso Porta Alvo, por exemplo *_http._tcp.teste.com. 32 IN SRV 10 0 80 webserver.admin.teste.com*.

O registro TXT permite associar um texto arbitrário com um hostname, é possível ter vários registros TXT para um mesmo hostname. Por exemplo *admin.teste.com. IN TXT "CEO: admin@teste.com.br"*.

O que é um Endereço IP Privado

Numa suposta rede, o que está do lado esquerdo do tracejado é a parte pública, ligada à internet, que tem o IP público válido na internet (geralmente atribuído pelo provedor), não sendo usado em redes internas.

Do lado direito, está a parte privada, dentro da nossa rede local, onde usamos IPs privados nas nossas máquinas. Esses IPs não conflitam com os IPs públicos.

O NAT do modem converter o IP público da operadora para o IP privado usado na rede local.

A IANA (Internet Assigned Number Authority) reserva blocos de endereços IP para uso em redes internas, sendo um bloco para redes classe A, um para classe B e outro para classe C, como segue:

	IP Inicial	IP Final
Classe A	*10.0.0.0*	*10.255.255.255*
Classe B	*172.16.0.0*	*172.31.255.255*
Classe C	*192.168.0.0*	*192.168.255.255*

Todas as máquinas têm algum desses IPs, seja uma rede corporativa ou doméstica, a classe C geralmente é usada para pequenas redes.

Cada bloco desses tem uma capacidade diferente com relação ao número de hosts que pode suportar. Por exemplo, o primeiro bloco (10.0.0.0) pode comportar mais de 16 milhões de endereços IP, ao passo que o bloco classe C (192.168.0.0) pode acomodar um pouco mais de 65 mil hosts.

Por este motivo, podemos ter, literalmente, IPs ilimitados para configuração de redes locais diversas.

Por exemplo: Meu provedor de internet atribui ao meu roteador um endereço IP público, digamos, *186.45.123.69*, este IP é único no mundo. Porém, eu possuo cinco dispositivos que precisam acessar a internet em minha rede interna. Como conseguir isso se só possuo um endereço IP público?

Para resolver este problema, atribuo endereços IP privados aos meus dispositivos (PC, notebook, tablet, etc.), e compartilho o IP público único que possuo entre todos eles. Quem faz a atribuição desses IPs é o roteador (ou outro dispositivo configurado como gateway padrão), via DHCP, o qual também realiza o compartilhamento do IP público.

Em sua casa você pode ter também diversos dispositivos em sua rede doméstica acessando a internet, cada um com um IP privado – e que podem ser os mesmos IPs privados que os equipamentos da minha rede – pois o que importa para o acesso à internet é o IP público atribuído, que será diferente do meu.

Há também um quarto bloco de endereços IP privados, chamados de APIPA (Automatic Private IP Addressing), cujo intervalo de endereços vai de *169.254.0.0* até *169.254.255.255*, e é usado para autoconfiguração de endereços IP quando um servidor DHCP não está presente na rede local. Com um IP nessa faixa, não conseguimos acessar a internet (o que ajuda a identificar problemas de conexão), mas podemos acessar outras máquinas na mesma rede local.

O mais comum é o endereço de loopback, na faixa de endereços de *127.0.0.0* até *127.255.255.255* (o mais usado é o *127.0.0.1*), que é, basicamente, usado para realizar testes no adaptador de rede. Os endereços na faixa de *0.0.0.0* até *0.255.255.255* também são reservados, mas sem uma aplicação específica.

Dê um *ipconfig* no prompt de para verificar a configuração dos IPs do computador.

O que é o Protocolo DHCP

O DHCP (portas 67 e 68) é um protocolo de serviço TCP/IP que permite executar configuração dinâmica de hosts em uma rede. É sucessor do BOOTP. Permite conceder endereços IP, máscaras de sub-rede, gateway padrão, servidores DNS e muitas outras configurações aos hosts.

Em termos gerais, o protocolo DHCP permite configurar dinamicamente os clientes da seguinte forma:

- Um cliente de rede envia um pacote UDP em broadcast com um pedido de serviço DHCP.
- Os servidores DHCP disponíveis recebem esse pacote e respondem com diversas configurações como IP, máscara, gateway, DNS, etc.

Basicamente, o cliente faz uma requisição DHCP e o servidor envia uma resposta DHCP.

A alocação do DHCP pode ser feita de três formas:

- **Automático:** IPs são atribuídos aos clientes na rede (sempre os mesmos).
- **Dinâmico:** Semelhante ao automático, mas com o tempo de uso de IPs restrito (lease).
- **Estática:** Endereços MAC de hosts são associados a IPs no servidor para que sempre seja oferecido o mesmo IP ao host (reserva).

O DHCP usa as mesmas portas atribuídas pelo IANA ao protocolo BOOTP:

- UDP 67 para envio de dados do cliente ao servidor.
- UDP 68 para dados enviados do servidor ao cliente.

A operação do DHCP ocorre em quatro fases: Descoberta (DHCPDISCOVER), Oferta de Concessão (DHCPOFFER), Requisição (DHCPREQUEST) e Confirmação de Concessão (DHCPACK).

O cliente envia mensagens de broadcast para a rede em busca de um servidor DHCP. Conteúdo básico da mensagem:

srcAddr=0.0.0.0, srcPort=68 dstAddr=255.255.255.255, dstPort=67

E o MAC Address do cliente.

Após o servidor receber a requisição DHCP de um cliente, é enviada por ele uma mensagem DHCPOFFER. Conteúdo da mensagem:

srcAddr=IP do servidor, srcPort=67, dstAddr=255.255.255.255, dstPort=68

Além do:

- MAC Address do cliente.
- IP oferecido pelo servidor, mais a máscara de sub-rede e duração da concessão.

O cliente então responde com uma DHCPREQUEST, requerendo as configurações oferecidas. Conteúdo básico da mensagem:

srcAddr=0.0.0.0, srcPort=68, dstAddr=255.255.255.255, dstPort=67

O servidor é identificado pelo IP, contido no campo de opções de DHCP da mensagem.

Quando o servidor recebe a mensagem DHCPREQUEST do cliente, envia um pacote DHCPACK a este com as configurações oferecidas, finalizando a configuração DHCP. O cliente verifica se o endereço fornecido não está em uso enviando um pacote ARP para a rede. Conteúdo básico da mensagem:

srcAddr=IP do servidor, srcPort=67, dstAddr=255.255.255.255, dstPort=68

Basicamente, o cliente manda o DHCPDISCOVER pro servidor, que devolve o DHCPOFFER, o cliente aceitando devolve o DHCPREQUEST e o servidor devolve o DHCPACK (aceitando a oferta e fornece o IP e outras configurações).

A concessão (lease time) é o tempo pelo qual um host pode usar as configurações recebidas. Antes do término da concessão, o cliente DHCP pode solicitar sua renovação por um período de tempo igual.

Após decorridos 50% do tempo de concessão, o host inicia o processo de solicitação de renovação, enviando pacotes DHCP para o servidor e pedindo a renovação de sua concessão atual. Caso o servidor DHCP não responda à solicitação de renovação, ao atingir 75% do período de concessão, o host iniciará o processo de obtenção de IP a partir de outros servidores (possivelmente) presentes na rede.

Os campos da mensagem DHCP são esses:

- **OP:** Operation Code. Especifica se a mensagem é uma requisição (request - 1) ou uma resposta (reply - 2).
- **HTYPE:** Especifica o tipo de hardware de rede (Ethernet, HDLC, Frame Relay, ATM, etc.).
- **HLEN:** Hardware Address Length. Tamanho do endereço de hardware (MAC). Exemplo: Ethernet = tipo 1, tamanho 6.
- **HOPS:** Usado por agentes de relay para controlar o encaminhamento de mensagens DHCP.
- **ID da Transação (XID):** Contém um número inteiro de 32 bits usado pelos clientes para sincronizar respostas com solicitações.
- **Segundos:** Número de segundos desde que o cliente tentou adquirir ou renovar uma concessão.
- **Flags:** Se um cliente não souber seu próprio IP ao enviar sua requisição, a flag terá o valor 1. Indica ao servidor se sua resposta deve ser enviada em broadcast.
- **Endereço IP do Cliente (ClAddr):** IP conhecido do cliente, configurado em 0 se o cliente não possuir IP.
- **Seu Endereço IP (YlAddr):** IP que o servidor está atribuindo ao cliente.
- **Endereço IP do Servidor (SlAddr):** Endereço IP do servidor que o cliente deve usar na sequência de boot (pode ou não ser o próprio DHCP).
- **Endereço IP do Roteador (GlAddr):** Endereço IP do roteador que roteia mensagens DHCP (Relay Agent).
- **Endereço de Hardware do Cliente (ChAddr):** Endereço MAC do cliente.
- **Hostname do Servidor (SName):** Nome do servidor DHCP.
- **Boot File Name:** Usado para especificar um caminho de arquivo de boot.

Sobre o campo de opções DHCP, cada opção consiste em um campo de código de um byte e um campo de comprimento de um byte também, seguido por alguns octetos de dados que descrevem a opção.

Código	Nome	Comprimento
1	Máscara de Sub-Rede	4 Octetos
3	Roteadores (Gateway)	Múltiplos de 4 Octetos
6	Servidores DNS	Múltiplos de 4 Octetos
7	Servidores de Log	Múltiplos de 4 Octetos
15	Nome de Domínio	1 Octeto, no Mínimo
28	Endereço de Broadcast	4 Octetos
37	TTL Padrão TCP	1 Octeto
42	Servidores NTP	Múltiplos de 4 Octetos
48	Servidores de Fontes x Window System	Múltiplos de 4 Octetos
69	Servidores SMTP	Múltiplos de 4 Octetos
70	Servidores POP3	Múltiplos de 4 Octetos
58	Tempo de Renovação de Concessão	Múltiplos de 4 Octetos

Veja uns exemplos de opções, que podem ser identificadas pelos códigos:

Código da Opção	Comprimento	Dados

03	04	*192.168.1.1*
06	04	*192.168.1.100*
42	04	*200.160.0.8*

O tipo de mensagem DHCP também é determinado no campo de opções pelos seguintes campos e valores: Código 53, comprimento 1 e dados (que é o valor que identifica a mensagem DHCP enviada).

Veja os tipos de mensagens DHCP logo abaixo:

Campo de Tipo	Tipo de Mensagem DHCP
1	DHCPDISCOVER
2	DHCPOFFER
3	DHCPREQUEST
4	DHCPDECLINE
5	DHCPACK
6	DHCPNACK
7	DHCPRELEASE

O endereço de autoconfiguração (APIPA) trata-se do endereço IP de autoconfiguração de hosts, que são os endereços da faixa *169.254.0.1* até *169.254.255.254*. Caso um host esteja utilizando um endereço dessa faixa, provavelmente trata-se de problemas de comunicação com o servidor DHCP.

Um endereço IP dinâmico pode ser reservado para uso exclusivo de um host, no processo conhecido como reserva de IP. Para isso o servidor DHCP registra em uma tabela o endereço MAC do host e o IP que ele utilizará. Desta forma, o endereço deste host nunca mudará e não necessitará de configuração manual por parte de usuário.

Um escopo DHCP nada mais é do que a faixa de IPs que serão distribuídos a uma sub-rede em particular, mais uma máscara de sub-rede, por exemplo: Faixa de *192.168.1.20* a *192.168.1.40*, com máscara de sub-rede *255.255.255.0*. Cada sub-rede terá seu próprio escopo DHCP.

No servidor podemos verificar o nome das máquinas conectadas, seus IPs privados, MAC e a concessão das mesmas.

O Que é Máscara de Sub-Rede

Uma sub-rede é uma subdivisão lógica de uma rede IP. Realizar a subdivisão de uma rede grande em redes menores permite diminuir o tráfego de rede, simplificar a administração e aumentar a performance dessa rede.

Os hosts que pertencem a uma sub-rede são endereçados com um grupo de bits mais significativo comum e idêntico em seus endereços IP. Assim ocorre uma divisão lógica do IP em dois campos, um endereço de rede (prefixo de roteamento) e um endereço (identificador) de host. Esse endereço de host identifica uma interface de rede específica.

Em computação, máscara é um dado utilizado para realizar operações de lógica binária, no geral em campos de bit. Ao utilizarmos uma máscara, um ou mais bits em um byte (ou outro agrupamento de bits) pode ser ativado, desativado ou ter seu valor lógico invertido, dependendo da operação lógica aplicada.

As operações lógicas mais comuns aplicadas em máscaras são as operações AND, OR, NOT e XOR.

Uma máscara de sub-rede tem a função de identificar em um endereço IPv4 qual porção representa o endereço de rede e qual porção representa o endereço de host. A máscara se assemelha a um endereço IPv4, ou seja, possui 4 bytes divididos por pontos em porções de 8 bits (octetos). A parte dos bits constituída por valores “1” representa qual parcela de um endereço IP serão vistos como endereço de rede e os bits que são todos zeros, representam o endereço de host.

É usada para dizer aos sistemas finais (incluindo roteadores e outros hosts) na rede quantos bits do endereço IP são usados para a identificação da rede e da sub-rede. Esses bits são chamados de Prefixo de Rede Estendido. Os bits restantes identificam os hosts dentro da sub-rede.

Os bits da máscara que identificam o número de rede (e sub-rede) são ajustados em 1 e os bits do host, em 0. Assim, trata-se de uma máscara de bit que, quando aplicada por meio de uma operação lógica AND em um endereço IP na rede, retorna o endereço de rede (prefixo de roteamento) ou de sub-rede.

Um endereço IPv4 possui dois componentes (ou partes), que são o endereço de rede e o endereço de host. O endereço de rede identifica toda a rede, de modo que todos os hosts dentro dessa rede possuem a mesma sequência de bits nessa parte. Já o endereço de host identifica a conexão a um host (equipamento) em particular, ou ainda uma interface de rede da máquina, e é exclusive de cada host dentro da rede a qual pertence.

A máscara de sub-rede é o endereço especial que efetua a separação entre essas partes. Ela pode ser padrão, quando trabalhamos com redes classful (com divisão em classes) ou ser calculada com base em uma rede sem classes (CIDR).

Existem máscaras de sub-rede padrão para cada classe de endereçamento, como podemos ver na tabela a seguir:

Classe de Endereçamento	Máscara de Sub-Rede	Endereço Inicial	Endereço Final
A	*255.0.0.0*	*0.0.0.0*	*127.255.255.255*
B	*255.255.0.0*	*128.0.0.0*	*191.255.255.255*
C	*255.255.255.0*	*192.168.0.0*	*223.255.255.255*

Portanto, se for utilizado um esquema de endereçamento de rede com classes, basta aplicar a máscara correspondente para efetuar a identificação de rede e host dentro da rede.

Resumidamente, onde está o 255 na máscara é onde está o endereço da rede, e no 0 está o endereço do host.

É possível ainda dividir a porção do endereço de host em uma sub-rede e novos endereços de host, caso seja necessário.

A máscara de sub-rede efetua tal separação do IP por meio de uma operação lógica AND bit-a-bit entre um IP e a máscara utilizada. Veja o exemplo a seguir:

- Endereço IP: *192.168.1.61*.
- Máscara de Sub-Rede Padrão: *255.255.255.0*.

A qual rede pertence esse IP? Convertendo os endereços para binário, obtemos:

- Endereço IP: *11000000.10101000.00000001.00111101*.
- Máscara de Sub-Rede Padrão: *11111111.11111111.11111111.00000000*.

Aplicando a operação lógica AND bit a bit:

- Endereço IP: *11000000.10101000.00000001.00111101*.
- Máscara de Sub-Rede Padrão: *11111111.11111111.11111111.00000000*.
- Resultado do AND: *11000000.10101000.00000001.00000000*.

O endereço obtido corresponde à porção de rede do endereço IP (*11000000.10101000.00000001.00000000*). Convertendo esse endereço de volta para o decimal, obtemos o endereço *192.168.1.0*, que é o endereço da rede a qual pertence o IP, note o final 0 o endereço, em vez de 61, que é o número que identifica o host dentro dessa rede.

Dentro de uma rede, dois endereços são especiais e nunca devem ser atribuídos a um host. São eles o endereço da rede em si, terminando em 0 (primeiro endereço, *192.168.1.0*), e o endereço de broadcast, terminado em 255 (último endereço, no exemplo, seria o endereço *192.168.1.255*). Assim, essa rede terá a capacidade para até 254 hosts, mais os endereços de rede e de broadcast, totalizando 256 endereços.

Vejamos agora um segundo exemplo de aplicação de máscara de sub-rede, agora sem o uso de classes no endereçamento IP:

- Endereço IP: *192.168.1.61*.
- Máscara de Sub-Rede Padrão: *255.255.255.224*.

PS: Com essa máscara, ele não está na classe C e em nenhuma outra.

Convertendo os endereços para binário, obtemos:

- Endereço IP: *11000000.10101000.00000001.00111101*.
- Máscara de Sub-Rede Padrão: *11111111.11111111.11111111.11100000*.

Aplicando a operação lógica AND bit-a-bit:

- Endereço IP: *11000000.10101000.00000001.00111101*.
- Máscara de Sub-Rede Padrão: *11111111.11111111.11111111.11100000*.
- Resultado do AND: *11000000.10101000.00000001.00100000*.

O endereço obtido corresponde à porção de rede do endereço IP (*11000000.10101000.00000001.00100000*). Convertendo esse endereço de volta para decimal obtemos o endereço *192.168.1.32*, que é o endereço da rede à qual pertence o IP. Note o final 32 do endereço, que fará com que essa rede acomode um número menor de hosts do que se fosse usada a

máscara padrão (precisamente 30 hosts, mais rede e broadcast). O primeiro IP válido dessa sub-rede será o endereço *192.168.1.33*.

Como são usados 27 bits para representar a porção de rede/sub-rede, também podemos representar essa rede como *192.168.1.32/27*, na notação CIDR.

A divisão em sub-redes é o processo de divisão de uma grande rede IP em múltiplas redes menores, com o propósito de aumentar sua performance, organização e segurança. Neste caso, deixamos de usar as máscaras padrão de classes e passamos a usar um esquema denominado CIDR (Classless Inter-Domain Routing), no qual a máscara a ser utilizada deve ser calculada de acordo com o endereço de rede original (a ser dividido) e o número de sub-redes ou hosts desejado.

O cálculo de máscaras de classe C é feito pela quantidade máxima de hosts (256) subtraído pelo outro número (no caso, 128, 192, 224, 240, 248, 252 e 254), depois subtrai mais dois (o endereço da rede e o de broadcast). Por exemplo:

```
  256
-224
  32
 -2
  30
```

Da mesma forma, podemos fazer cálculos com outras classes e IPs.

A notação CIDR basicamente é onde tem os primeiros números 1 em binário na porção de rede da máscara, por exemplo, a máscara *255.0.0.0* tem a notação */8*, a máscara *255.255.0.0* tem a notação */16* e a máscara *255.255.255.0* tem a notação */24*. Numa aplicação em outra máscara, a notação muda (como a máscara *255.255.255.224* tem a notação */27*. Veja a tabelinha de como ficaria a notação dessa forma:

Máscara de Sub-Rede	Notação CIDR
255.255.255.128	*/25*
255.255.255.192	*/26*
255.255.255.224	*/27*
255.255.255.240	*/28*
255.255.255.248	*/29*
255.255.255.252	*/30*
255.255.255.254	*/31*

PS: Uma rede */31* (*255.255.255.254*) não pode ser usada, pois ela só acomodaria um IP, e uma rede tem que acomodar no mínimo 3 IPs, contando o identificador de rede e o endereço de broadcast, portanto, só dá pra usar até o */30* (*255.255.255.252*).

Assim, eliminamos o endereçamento por classes e conseguimos aprimorar a agregação de rotas.

O que é o HandShake de Três Vias

O protocolo TCP é um protocolo orientado a conexão. Isso significa que, antes que qualquer dado possa ser enviado entre dois hosts, uma conexão deve ser estabelecida entre eles. Vamos estudar o processo pela qual uma conexão TCP é estabelecida entre dois hosts em uma rede.

O handshake (significa algo como “aperto de mão”) funciona assim: O Tx (computador transmission) envia uma mensagem contendo apenas um Nº de sequência (seq) a e o bit SYN atuvado. O Rx (computador receptor) responde com um pacote contendo um Nº de sequência b, Nº ACK = seq a + 1 e ACK ativados. O Tx, ao receber esse pacote, envia uma mensagem de confirmação ACK de volta ao Rx, como o Nº ACK = seq b + 1. A conexão está assim estabelecida.

Quando nossa máquina requisita a conexão remota através do protocolo TCP a um servidor na net, ela envia o bit SYN com o número da sequência (no caso 0), e o servidor responde com o ACK (com 1), e uma outra sequência (SYN) também vinda a partir do 0, que volta à nossa máquina, que envia outro ACK (com 1) e o seq dela com 1.

Para estabelecer uma conexão TCP, após a troca dos três segmentos entre os hosts, o processo de estabelecimento de conexão está completo. Chamamos a esse processo de handshake de três vias (three-way handshake). O host que envia o primeiro segmento SYN realiza uma abertura de conexão ativa. O outro host (servidor que recebe o segmento SYN), realiza uma abertura de conexão passiva.

Quando a conexão é estabelecida, após o processo do handskare de três vidas ter sido concluído, a conexão estará estabelecida e os hosts podem começar a trocar dados entre si. Ao final da comunicação, será necessário realizar um processo relativamente similar para a finalização da conexão.

Protocolo FTP – File Transfer Protocol

O File Transfer Protocol (FTP), é um protocolo para transferência de arquivos entre dois hosts (um cliente e um servidor), baseado em conexão IP e usando TCP. Desenvolvido em meados dos anos 70 para suportar compartilhamento de arquivos em redes TCP/IP e mais antigas. É um protocolo da camada de aplicação TCP/IP. O FTP está definido na RFC 959.

O FTP usa conexão de dados e controle separadas, as portas usadas são a 20 e 21, os dados são transferidos pela porta 20, e a porta 21 transmite informações de controle.

Clientes podem se autenticar por meio de um nome de usuário e senha, ou ainda usar conexão anônima (se o servidor o permitir). É possível proteger o nome de usuário e senha usando SSL/TLS, na forma de FTPS, ou ainda, usando SFTP (SSH File Transfer Protocol).

Um modo de conexão determina como a conexão de dados é estabelecida. O cliente cria uma conexão TCP a partir de uma porta aleatória como a porta 21 do servidor FTP. FTP pode operar em dois modos: Ativo ou passivo.

No modo ativo, o cliente escuta conexões de dados que chegam do servidor em uma porta informada. O servidor inicia um canal de dados a partir de sua porta 20. Problemática se o cliente estiver atrás de um firewall ou roteador NAT.

Só que essas portas aleatórias podem ser bloqueadas pelo firewall, por este não saber que se trata de uma porta segura pra conexão. Nesse caso usamos o modo passivo.

No modo passivo, o cliente usa a conexão de controle para enviar um comando PASV ao servidor e recebe um endereço IP e número de porta aleatória como respostas, que serão usadas para iniciar um canal de dados a partir de outra porta aleatória no cliente. Usada geralmente quando o cliente não consegue receber conexões TCP de entrada, como por exemplo, por conta de um firewall na rede.

Nesse caso, o cliente envia através de uma porta aleatória, se conecta com a porta 21 do servidor, que responde por essa mesma porta, que está com a conexão aberta, informando qual porta aleatória (outra porta) que deverá ser usada por ambos para transferência, de forma que o firewall não bloqueie.

Quando os dados são transferidos pela rede, podem ser usados dois tipos principais de representação de dados:

- **Modo ASCII:** Usado para texto.
- **Modo Binário (“Imagem”):** Para arquivo em geral. Dados são transmitidos byte por byte.

Além disso, existem outros dois modos de representação de dados disponíveis:

- **Modo EBCDIC:** Texto entre hosts que usam o conjunto de caracteres EBCDIC.
- **Modo Local:** Permite aos hosts usar algum formato proprietário sem necessidade de conversão dos dados para ASCII.

Os dados podem ser transferidos de três modos:

- **Modo Stream (Fluxo):** Dados enviados em um fluxo contínuo. Todo o processamento é realizado pelo TCP.
- **Modo Block (Bloco):** Os dados são divididos em vários blocos pelo FTP, e então repassados ao TCP para transmissão.
- **Modo Comprimido (Compressed):** Os dados são comprimidos usando um algoritmo, como o RLE (Run-Length Encoding).

Um servidor pode oferecer o serviço de FTP anônimo, no qual os usuários se loguem com uma conta de nome anonymous, sem o emprego de senha (o servidor muitas vezes pede o e-mail do usuário como “senha”, porém, nenhuma verificação é realizada). No geral, é empregada por servidores que armazenam atualizações de softwares para os clientes baixarem.

Sobre a segurança do FTP, ele não foi projetado para ser um protocolo seguro, e está sujeito a diversos tipos de ataques, como ataques de força bruta, captura de pacotes, spoofing, entre outros. Além disso, o FTP não criptografa os dados transmitidos, incluindo nomes de usuários e senhas. Isso pode ser remediado usando-se uma versão segura do FTP, como o FTPS, ou ainda transmitindo os dados FTP por meio de um túnel SSH ou uma VPN (mais comum).

Vários protocolos foram derivados a partir do conceito do FTP, melhorando diversos aspectos, principalmente a segurança. Os mais utilizados são os seguintes: FTPS, SSH FTP, TFTP e SFTP. Além disso, existem muitos outros modos de transferência de arquivos não baseados em FTP, como as redes P2P (como as de torrent).

Podemos instalar também softwares de clientes de FTP. Um cliente de FTP é um software que se conecta a um servidor para requisitar a transferência de arquivos, tanto em download quanto em upload. Os clientes FTP podem ser em linha de comandos ou aplicações gráficas, ou mesmo web. Um software conhecido de FTP é o Filezilla.

Para utilizar um servidor FTP via linha de comando, digite *ftp*. Dentro do FTP, digite *open nomedoservidor.com.br.* Ele pedirá o login e a senha, caso estejam configurados no servidor. Dentro do FTP podemos utilizar comandos do Unix. Para upar arquivos usamos o comando *put "/caminhodoarquivo"*, para baixar arquivos usamos *get "nomedoarquivo"* e para encerrar a conexão usamos *bye*.

12 Diferenças Entre os Protocolos TCP e UDP

A camada de Transporte da pilha TCP/IP, intermediária entre as camadas de Aplicação e Internet, é responsável por funções de comunicação entre processos de computadores diferentes. Desta forma, as aplicações podem enviar e receber dados entre si.

Na pilha TCP/IP, os dois principais protocolos da camada de transporte são o protocolo TCP (Transmission Control Protocol) e o protocolo UDP (User Datagram Protocol).

Esses são os tipos de conexão:

TCP (Transmission Control Protocol)	UDP (User Datagram Protocol)
Orientado a conexão. Os dispositivos envolvidos precisam estabelecer uma conexão antes de transmitir dados (com handshake).	Não orientado a conexão. Os dispositivos envolvidos não precisam estabelecer uma conexão antes de transmitir dados (sem handshake).
Para aplicações que requeiram alta confiabilidade, com tempo de transmissão não muito crítico, como envio de e-mails e download de arquivos.	Para aplicações que necessitem de transmissão de dados rápida e eficiente, como streaming de vídeo e jogos online.
Os pacotes de dados são organizados em uma ordem específica.	Não há ordem específica para os pacotes de dados. Se for necessária, a ordem deve ser gerenciada pela camada de aplicação.
Confiável, pois garante a entrega dos dados ao destino com mecanismos de correção de erros e retransmissão de dados.	Não confiável, pois a entrega de dados ao destina não pode ser garantida.
Possui mecanismos de verificação de erros sofisticados e recuperação de erros.	Mecanismo de verificação de erros básico, com checksum apenas, sem recuperação de erros.
Mais lento que o UDP, devido ao overhead do seu cabeçalho e rotinas de conexão/desconexão envolvidas.	Mais rápido que o TCP, mais simples e eficiente.
Pacotes perdidos podem ser retransmitidos, evitando assim perda de dados.	Pacotes perdidos não são retransmitidos.
Cabeçalho de tamanho variável, de 20 (padrão) a 80 bytes (com todas as opções).	Cabeçalho de tamanho fixo e pequeno: 8 bytes.
Não suporta broadcasting de dados. Protocolo para comunicação entre dois endpoins.	Suporta broadcasting de dados (e multicasting também).

Usados por protocolos como HTTP, FTP, SMTP e HTTPS.	Usado pelos protocolos DNS, DHCP, ANMP, RIP e TFTP.
Realiza controle de fluxo (não envia mais pacotes do que o destinatário consegue receber).	Não realiza controle de fluxo.
Doze campos.	Quatro campos.

Os 12 campos do TCP são esses:

- Número da porta de origem.
- Número da porta de destino.
- Número de sequência.
- Número de confirmação.
- Comprimento do cabeçalho.
- Reservado.
- Flags ECN.
- Bits de controle.
- Tamanho da janela.
- Checksum.
- Ponteiro de urgente.
- Opções.

Já os 4 campos do UDP são esses:

- Número de porta de origem.
- Número de porta de destino.
- Comprimento.
- Checksum.

Camada de Aplicação do Modelo OSI

Como lembramos, o modelo OSI é composto por sete camadas (numeradas de 1 a 7, de baixo pra cima):

Camada de Aplicação
Camada de Apresentação
Camada de Sessão
Camada de Transporte
Camada de Rede
Camada de Link de Dados
Camada Física

Como visto, a camada física é a de mais baixo nível (mais distante do usuário), e a camada de aplicação é a de mais alto nível (mais próxima do usuário).

A transmissão de dados é feita de camada para camada, e os dados de aplicação da máquina A é passado por todas as camadas, passa pelo caminho de comunicação e passa por todas as camadas da máquina B até chegar na camada de aplicação dela.

A camada de aplicação (7 do modelo OSI) fornece interface de comunicação entre aplicações e serviços de rede. Também define processos de autenticação de usuários nas aplicações. Arquitetura cliente-servidor, habilita usuários (humanos ou sistemas) a acessarem recursos de rede. A camada de aplicação é crucial, pois permite que aplicações sejam acessadas e executadas em ambientes de rede, incluindo a web.

É a camada mais próxima do usuário final, fornecendo uma interface entre as aplicações que são utilizadas para a comunicação e a rede por onde as informações (mensagens) são transmitidas. Diversos protocolos na camada de aplicação são usados para realizar a troca de dados entre os programas que são executados nos hosts de origem e de destino. Também é empregada na pilha TCP/IP, porém um pouco mais complexa, englobando mais de uma camada dessa pilha. Definida pela RFC 1123.

Processos são programas ou serviços em execução em um sistema. Em rede, os processos funcionam de forma combinada, em pares, de modo que um processo origina e envia mensagens e um outro processo as recebe, podendo responder com outras mensagens. O processo que origina a comunicação é chamado de processo cliente, ao passo que o processo de destino é o processo servidor. Exemplo clássico é o processo de resolução de nomes DNS, que utiliza o protocolo de camada de aplicação homônimo (DNS).

Podemos descrever as camadas que compõe a pilha TCP/IP em termos do modelo OSI. Neste caso, a camada de aplicação TCP/IP engloba as camadas de aplicação, apresentação e sessão do modelo OSI, como podem ver:

TCP/IP	Referente ao Modelo OSI
Aplicação	Aplicação
	Apresentação
	Sessão
Transporte	Transporte
Rede (Internet)	Rede
Física	Enlace
	Física

Como há inúmeras aplicações que fazem uso da camada de aplicação, há vários protocolos que as servem, alguns exemplos:

Aplicação	Protocolo
E-mail	SMTP, IMAP, POP
Acesso à Web	HTTP, HTTPS
Transferência de Arquivos	FTP
Conexão Remota	SSH

Configuração de Rede	DHCP
Configuração de Data e Hora	NTP
Segurança de Conexão	TLS/SSL
Comunicação entre Dispositivos IoT	MQTT
Gerenciamento Remoto de Hosts	SNMP

Camada de Apresentação do Modelo OSI

A camada de apresentação (6 do modelo OSI) se relaciona com a sintaxe e a semântica na comunicação entre sistemas. É responsável pelos processos de codificação de caracteres e tradução, compressão e criptografia dos dados tanto na origem quanto no destino da transmissão. É incluída na camada de aplicação da pilha TCP/IP.

As funções da camada de apresentação são codificação de caracteres, formatação de dados, comunicação entre sistemas diferentes, segurança e privacidade nas transmissões de dados e aumento da performance da transmissão.

A comunicação entre sistemas é um processo de troca de informações em formatos variados que são convertidas em bits ao serem transmitidas. Computadores podem utilizar sistemas de codificação distintos, assim, a camada de apresentação no transmissor se ocupa de traduzir a informação, deixando-a em um formato comum. A camada de apresentação do receptor traduz a informação do formato recebido para o formato específico que será processado no dispositivo.

No processo de tradução, os formatos comuns de dados incluem JPEG, GIF, PNG, MPEG, etc.

Quando enviamos informações confidenciais, o sistema deve garantir a privacidade da comunicação. Com a criptografia ou cifragem, o emissor modifica os dados originais para um formato codificado, por meio de algoritmos específicos, e envia a mensagem pela rede. Ao chegar no destino, a mensagem é convertida de volta em seu formato original por meio do algoritmo adequado no processo chamado descriptografia ou decifragem. Um exemplo banal é o envio de uma senha durante o processo de logon em um sistema.

Enviar dados no formato original (como áudio, vídeo ou imagens) pode ocupar muito espaço na transmissão. Assim, aplicamos um processo de compressão no qual a quantidade de bits transmitidos é reduzida antes do envio da mensagem, tornando a transmissão mais rápida. Quando a mensagem chega ao seu destino ela é descomprimida, voltando ao seu formato original.

A tabela a seguir lista alguns dos protocolos da camada de apresentação mais comuns:

Aplicação	Protocolo
Segurança Criptográfica na Transmissão	TLS
Segurança Criptográfica na Transmissão	SSL
Definição de Tipos de Conteúdo	MIME
Independent Computing Architecture (Citrix)	ICA
Representação de Dados de Rede	NDR

Terminal de Acesso Remoto	Telnet

Camada de Sessão do Modelo OSI

A camada de sessão (camada 5 do modelo OSI) tem por função estabelecer, gerenciar e finalizar conexões entre aplicações. Assim ela configura, coordena e termina a troca de dados entre aplicações em cada ponta de uma conexão, mantendo as sessões de comunicação.

Responde a requisições de serviço da camada de Apresentação e emite requisições de serviço para a camada de Transporte.

Também incluída na camada de Aplicação da pilha TCP/IP.

Essas são as funções da camada de sessão:

- **Estabelecer, Manter e Terminar Sessões:** Permite que dois processos estabeleçam, usem e finalizem uma conexão.
- **Sincronização:** Permite que os processos criem pontos de sincronização de dados. Assim, erros podem ser identificados com mais facilidade, e os dados podem ser ressincronizados.
- **Controle de Diálogo:** Os processos podem escolher iniciar a comunicação entre si em modos half-duplex, simplex ou full-duplex.

A tabela a seguir lista alguns dos protocolos da camada de sessão mais comuns:

Aplicação	Protocolo
Call Control Protocol (Comunicação Multimídia)	H.245
Layter 2 Tunneling Protocol (para VPNs	L2TP
Network Basic Input Output System (Serviços de Comunicação em Rede Local)	NetBIOS
Network File System (Acesso a Arquivos em Uma Rede)	NFS
Remote Procedure Call (Execução de Processos em Hosts Remotos)	RPC
Real Time Control Protocol (Estatísticas e Controle de Informações em uma Sessão RTP)	RTPC

Camada de Transporte do Modelo OSI e Protocolos

A camada de transporte (modelo OSI, camada 4) tem por função fornecer um fluxo de dados entre dois hosts, para a camada de aplicação. Responde a requisições de serviço da camada de sessão e emite requisições de serviço para a camada de rede. Corresponde à camada homônima na pilha TCP/IP.

Podemos descrever as camadas que compõe a pilha TCP/IP em termos do modelo OSI. Algumas funções da camada de sessão OSI estão na camada de transporte TCP/IP. Veja abaixo:

TCP/IP	Referente ao Modelo OSI
Aplicação	Aplicação
	Apresentação
	Sessão
Transporte	Transporte
Rede (Internet)	Rede
Física	Enlace
	Física

As funções da camada de transporte são essas:

- Fornece serviços de comunicação host a host para aplicações.
- Fornece serviços como controle de fluxo e comunicação orientada a conexão.
- Permite a entrega de pacotes na mesma ordem que foram enviados.
- Permite entrega confiável de pacotes, se pacotes forem perdidos, podem ser reenviados.
- Multiplexação: O uso de portas permite que várias aplicações no mesmo computador acessem a rede de forma simultânea.

Já sobre as portas de comunicação é isso:

- São usadas para determinar qual processo em um host local se comunica com qual processo em um host remoto.
- Para um processo se comunicar com outro processo utilizam-se portas. Uma porta é um número de 16 bits (de 0 a 65535), que identifica qual protocolo da camada superior (ou programas) devem entregar as mensagens recebidas.
- As portas podem ser bem conhecidas, registradas ou efêmeras.
- As portas são sempre associadas com um endereço IP e um protocolo de transporte.

Sobre os soquetes (sockets):

- Um soquete é uma API para protocolos de comunicação.
- Usado por um processo para solicitar serviços de rede do sistema operacional.
- Composto por: Protocolo, endereço, processo (por exemplo *{TCP, 192.168.22.35, 80}* ou *192.168.22.35:80*).

Veja uns exemplos de portas bem conhecidas:

Aplicação/Serviço	Porta
FTP	21
SSH	22
Telnet	23
DNS	53
DHCP	67
	68

HTTP	80
IMAP	143
HTTPS	443

A tabela a seguir lista alguns dos protocolos da camada de transporte mais comuns (modelo TCP/IP):

Aplicação	Protocolo
Fluxo de dados confiável (conexão) entre dois hosts. Assim a entrega dos pacotes, chamadas de segmentos, de um host ao outro é garantida.	TCP
Envia pacotes de dados chamados de datagramas de um host a outro, sem garantir de que esses pacotes cheguem ao seu destino.	UDP
Steam Control Transmission Protocol. Orientado a mensagens como o UDP, com controle de congestionamento como o TCP. Fornece caminhos redundantes que aumentam a resiliência e confiabilidade da conexão. Nativo no FreeBSD v.7, portado para outros sistemas.	SCTP

Camada de Rede do Modelo OSI e Protocolos

Como sabemos, o modelo OSI é composto por sete camadas, a de rede é a terceira.

A camada de rede tem por função principal realizar a entrega de pacotes entre dois hosts de rede. Responde a requisições de serviço da camada de transporte e emite requisições de serviço para a camada de link de dados. Seu trabalho é levar pacotes da origem até o destino. Corresponde à camada de internet na pilha TCP/IP.

Sobre a camada de rede:

- Introduz a capacidade de rotear o tráfego de um ponto da rede a outro, por meio de sub-redes (camada de roteamento).
- Aplica um esquema de endereçamento lógico aos pontos de rede, por exemplo, o endereço IP.
- Fragmenta os dados a serem transmitidos, caso o tamanho desses dados exceda um limite, de modo que segmentos de rede que não suportem quadros de tamanho grande possam também enviar dados sem problemas.
- O PDU da camada de rede é chamado de pacote.
- PDU (Protocol Data Unit) é um nome dado a um conjunto de dados presentes em uma determinada camada da pilha de protocolos.

Podemos descrever as camadas que compõe a pilha TCP/IP em termos do modelo OSI. A camada de internet TCP/IP é, na verdade, um subconjunto da camada de rede do modelo OSI.

TCP/IP	Referente ao Modelo OSI
Aplicação	Aplicação
	Apresentação

	Sessão
Transporte	Transporte
Rede (Internet)	Rede
	Enlace
Física	Física

Essas são as funções da camada de rede:

- Endereçamento lógico e conversão de endereço físico.
- Encaminhamento de pacotes entre segmentos de rede distintos.
- Roteamento – Mecanismo para que roteadores se interconectem a redes físicas distintas.
- Controle de tráfego e QoS (Quality of Service).
- NAT (Network Address Translation).
- Entrega de relatórios de erros.

Sobre o endereçamento lógico (o IP):

- Endereçamento IP.
- Oculta a rede física, criando uma visão virtual da rede.
- Protocolo de entrega de pacote não-confiável, de melhor esforço e sem conexão.
- Melhor esforço: Os pacotes enviado podem ser perdidos, ficar fora de ordem ou serem duplicados.
- Duas versões: IPv4 e IPv6.
- Exemplo de IPv4: *193.35.62.31*.
- Exemplo de IPv6: *2001:0ba6:0000:0000:0000:ff00:0051:9647*.

Essa é a estrutura de um pacote IPv4:

Estrutura de um Pacote IP
Versão (4 bits)
Tamanho do Cabeçalho (4 bits)
DSCP (6 bits)
ECN (2 bits)
Tamanho Total (16 bits)
Identificação (16 bits)
Flags (3 bits)
Offset de Fragmento (13 bits)
Tempo de Vida – TTL (8 bits)
Protocolo (8 bits)
Checksum do Cabeçalho (16 bits)
Endereço IP de Origem (32 bits)
Endereço IP de Destino (32 bits)

Opções (32 bits)
Dados (até 64 Kb)

Alguns dos dispositivos que operam na camada de rede do modelo OSI incluem: Roteadores, firewall, switches (L3) e access points.

A seguir estão listados alguns dos protocolos da camada de rede mais comuns (modelo TCP/IP):

Aplicação	Protocolo
Internet Protocol – Protocolo que permite realizar endereçamento lógico de hosts em redes locais e remotas	IP
Internet Control Message Protocol – Protocolo que comunica mensagens de erro e outras condições que requeiram atenção em uma rede	ICMP
Routing Information Protocol – Protocolo para roteamento de pacotes com o algoritmo distance-vector	RIP
Open Shortest Path First – Protocolo para roteamento de pacotes, que emprega o algoritmo shortest path first	OSPF
Multiprotocol Label Switching – Protocolo de encaminamento de pacotes baseados em rótulos	MPLS

Um dos programas que usa o ICMP é o famoso “ping”.

Camada de Link de Dados do Modelo OSI

A camada de link de dados, ou enlace (modelo OSI, camada 2) tem por função fornecer transferência de dados nó a nó, ou seja, realizar a ligação entre dois nós conectados em rede. Responde a requisições de serviço da camada de rede e emite requisições de serviço para a camada física. Corresponde à camada de interface de rede/física na pilha TCP/IP.

Podemos descrever as camadas que compõem a pilha TCP/IP em termos do modelo OSI. A camada de internet TCP/IP é, na verdade, um subconjunto da camada de acesso à rede (física) do modelo OSI.

TCP/IP	Referente ao Modelo OSI
Aplicação	Aplicação
	Apresentação
	Sessão
Transporte	Transporte
Rede (Internet)	Rede
Física	Enlace
	Física

Essas são as funções da camada de link de dados:

- Realiza endereçamento físico de dispositivos de rede.
- Detecta e tenta corrigir erros que possam ocorrer na camada física.
- Define protocolo para controle de fluxo entre os nós.
- Sinalização de início e fim de transmissão de quadros.
- Gera um código para reconhecimento de erros de transmissão de dados (checksum).

A camada de link de dados é dividida em duas subcamadas pelo padrão IEEE 802:

- **MAC:** Medium Access Control (controle de acesso ao meio). Controla como os dispositivos na rede obtém acesso a um meio de transmissão, com permissão para transmitir dados.
- **LLC:** Logical Link Control. Identifica e encapsula protocolos de camada de rede, e controla verificação de erros e sincronismo de quadros.

Sobre o endereçamento físico (MAC Address):

- O endereço MAC é responsável pela identificação única dos dispositivos em uma rede, consistindo em um endereço de 48 bits gravado em uma ROM presente na interface física de rede.
- MACs são atribuídos às NIC pelos fabricantes, e permitem identificar o fabricante da placa por meio de um número de identificação registrado.
- Exemplo de endereço MAC: *30-e4-db-9f-a3-48*.

Sobre o quadro (frame):

- O PDU na camada 2 é chamado de quadro (tamanho configurável) ou ainda célula (tamanho fixo). Caso o pacote de dados recebido da camada de rede for maior que o tamanho do quadro em uso na rede, ele será dividido em tantos quadros quanto necessários para transmitir o pacote na íntegra.

Estrutura de um quadro Ethernet (frame):

Preâmbulo 7 bytes	SFD 1 byte	MAC Destino 6 bytes	MAC Origem 6 bytes	Comprimento 2 bytes	Dados e Pad 46 a 1500 bytes	FCS 4 bytes

Sobre essa estrutura:

- **Preâmbulo:** Marca o início do quadro, São sete bytes 10101010. Com o SFD forma um padrão de sincronismo: Ao encontrar sete bytes 10101010 e um byte 10101011, o dispositivo receptor sabe estar diante do início de um quadro.
- **SFD (Start of Frame Delimiter):** É um quadro 10101011.
- **MAC de Destino:** Endereço MAC da placa de rede de destino.
- **MAC de Origem:** Endereço MAC da placa de rede de origem.
- **Comprimento:** Nº de bytes transmitidos no campo de dados do quadro.
- **Dados:** Dados enviado pela camada LLC.
- **Pad:** Se o campo de dados tiver menos de 46 bytes, são inseridos zeros para completar os 46 bytes.
- **FCS (Frame Check Sequence):** Controle de correção de dados.

Alguns dos dispositivos que operam na camada de enlace do modelo OSI incluem switches, access points, NICs e bridges.

A seguir listamos alguns dos protocolos da camada de enlace mais comuns (modelo TCP/IP):

Aplicação	Protocolo
Point-to-Point Protocol – Empregado em redes de cabos seriais, links telefônicos, redes celulares e links de fibra óptica. Acesso à internet dial-up	PPP
Ethernet. Comunicação em redes locais (LAN), metropolitanas (MAN) e de área ampla (WAN). Transmissão de dados via cabo coaxial, par trançado e fibras ópticas. Trabalha com PDUs chamados de quadros	802.3
Wi-Fi. Protocolos para implementação de redes de computadores WLAN – Wireless LAN, em bandas de frequência como 2,4 Ghz, 5 Ghz, 60 Ghz e outras	802.11
Bluetooth. Troca de dados entre dispositivos fixos e móveis em curtas distâncias e construção de PANs	802.15
Padrão de redes que suporta VLANs em redes Ethernet IEEE 802.3	IEEE 802.1Q

Camada Física do Modelo OSI

Como lembrando, o modelo OSI é composto por sete camadas (numeradas de 1 a 7, de baixo pra cima):

Camada de Aplicação
Camada de Apresentação
Camada de Sessão
Camada de Transporte
Camada de Rede
Camada de Link de Dados
Camada Física

A camada física (modelo OSI, camada 1) tem por função principal a transmissão e recepção de dados digitais (bits) entre um dispositivo e um meio de transmissão físico. Responde a requisições de serviço da camada de enlace e emite/recebe sinais de e para o meio físico. Corresponde à camada física na pilha TCP/IP.

Podemos descrever as camadas que compõe a pilha TCP/IP em termos do modelo OSI. Veja abaixo:

TCP/IP	Referente ao Modelo OSI
Aplicação	Aplicação
	Apresentação

	Sessão
Transporte	Transporte
Rede (Internet)	Rede
	Enlace
Física	Física

A transmissão de dados é feita de camada para camada, e os dados de aplicação da máquina A é passado por todas as camadas, passa pelo caminho de comunicação e passa por todas as camadas da máquina B até chegar na camada de aplicação dela.

Os meios de transmissão são o meio físico para a propagação de sinais de telecomunicações, os tipos principais são: Cabos metálicos, coaxial, par trançado, fibras ópticas e ondas de rádio.

Essas são as funções da camada física:

- Entrega bit-a-bit ou símbolo-a-símbolo.
- Especificação mecânica de conectores elétricos e cabos.
- Especificação elétrica de níveis de sinal de linhas de transmissão e impedância.
- Interfaces de rádio, alocação de frequências do espectro eletromagnético.
- Modulação de multiplexação de sinais.
- Comutação de circuitos.
- Controle de fluxo e sinalização start-stop.
- Não inclui o meio onde os dados trafegam.

Sobre a codificação de sinais:

- Os níveis lógicos que representam bits são codificados em sinais elétricos ou eletromagnéticos para transmissão por um meio.
- Essa conversão é feita por meio da codificação dos sinais.
- Existem diversos sistemas de codificação, como Manchester, 4B/5B, MLT-3, 4D-PAM-5, etc.

Alguns dos dispositivos que operam na camada física do modelo OSI incluem: Placas de rede (NIC), modems, hubs, repetidores e conversores de fibra.

A seguir listamos alguns dos protocolos da camada física mais comuns (modelo TCP/IP):

Aplicação	Protocolo
Funcionalidade física do padrão Ethernet.Inclui especificações como 10BASE-5, 10BASE-T, 100BASE-T, 100BASE-FX e outros	Ethernet
Synchronous Digital Hierarchy. Transferência de fluxos de bits digitais síncronos por fibras ópticas, como canais de voz em comunicação telefônica	SDH
Estabelece um padrão de comunicação de modems em taxas de até 56 kb/s	V.92
Optical Transport Network. Fornece funcionalidade de transporte, multiplexação, comutação e gerenciamento em canais de fibras ópticas	OTN
Low-Rate Wireless PAN (LR-WPAN). Base de especificações como	IEEE 802.15.4

Zigbee, 6LoWPAN e SNAP para comunicação entre dispositivos sem fio de baixo custo e baixa velocidade	

Resumindo:

- Trata da sinalização de rede, e conversão de bits digitais em sinais elétricos, ópticos ou ondas eletromagnéticas para envio por meio de transmissão utilizados, carregando os dados de um ponto a outro da rede.
- Define aspectos mecânicos e elétricos da rede. Especifica níveis de tensão, taxas de transmissão, distâncias máximas, esquemas de modulação, frequência de dispositivos wireless e tipos de conectores físicos, entre outros.
- Nesta camada temos cabos, conectores, antenas, hubs, modems e placas de rede atuando. Define especificações de modos de transmissão: Simplex, half duplex e full duplex.

Cabeamento Estruturado

Cabeamento estruturado é o conjunto que envolve componentes e arquitetura de cabeamento de dados para comunicações, especificado por normas e padrões, e adotado de forma voluntária pelos fabricantes e empresas. Assim, podemos construir uma infraestrutura de cabeamento de telecomunicações (telefonia e dados) que consistem em elementos padronizados, ou seja, uma rede estruturada de dados. Podemos dizer que um cabeamento estruturado é uma infraestrutura de cabeamento bem organizada.

Uma infraestrutura de cabeamento estruturada bem planejada e instalada fornece uma série de benefícios, tais como:

- Performance melhorada e previsível.
- Flexibilidade para acomodar alterações de layout, quantidade e tipo de dispositivos, de forma rápida e controlada.
- Fornece redundância.
- Aumento da disponibilidade da rede e elementos associados, como o Data Center.
- Diminui o tempo necessário para encontrar problemas de conectividade.
- Simplifica a instalação e a manutenção da infraestrutura de comunicações, principalmente quando a quantidade de equipamentos for grande, além de tornar flexível sua alteração e atualização.
- Permite que sejam usados equipamentos de diferentes fabricantes com total interoperabilidade.
- Com uma rede estruturada, é possível compartilhar os caminhos de dados com outros tipos de transmissão, como telefonia, vídeo, som ambiente, sensores e alarmes, etc.

Um sistema de cabeamento estruturado é instalado em sistemas de piso ou sistemas aéreos de canaletas e dutos (aparentes ou embutidos). Deve seguir requisitos mínimos relacionados a distâncias, arquitetura de interligação, padrões de pinagem e transmissão e interconectividade.

Um sistema de cabeamento estruturado completo é composto por seis subsistemas:

- Entrada de facilidades.
- Sala de equipamentos.
- Cabeamento backbone (vertical).
- Cabeamento horizontal.

- Salas de telecomunicações.
- Área de trabalho.

A entrada de facilidades é o espaço reservado para receber os cabos de entrada das operadoras de serviço (telefonia, TV a cabo, etc.) e outros serviços externos, onde estes serão conectados à rede interna. Inclui hardware de conexão e equipamentos de proteção.

A sala de equipamentos é o espaço dentro do edifício que acomoda terminações e equipamentos de telecomunicações. É onde são feitas as conexões entre os cabeamentos que vão para a sala de telecomunicações. Inclui main, intermediate e horizontal cross-conects.

O cabeamento vertical interliga as salas de telecomunicações instaladas nos andares de um edifício comercial, ou vários edifícios a uma sala de equipamentos. Também chamado de cabeamento primário. Pode empregar cabeamento metálico de par trançado ou fibra óptica.

A sala de telecomunicações é o espaço reservado que contém o ponto de transição entre o cabeamento vertical e o cabeamento horizontal, podendo abrigar equipamentos ativos como switches e também patch panels. Pode ser um armário de telecomunicações em vez de uma sala, dependendo do tamanho da estrutura.

A área de trabalho é a área interna que possui pontos de telecomunicação e energia elétrica para a conexão dos equipamentos dos usuários. Cada área de trabalho deve possuir duas tomadas de conexão (telecomunicações).

Um sistema de cabeamento estruturado é constituído de um conjunto de elementos que podem incluir: Cabos metálicos e de fibra óptica, patch panels, dutos, painéis e tomadas, racks, cabos e patch cords, conectores, etc.

O Que são Meios de Transmissão

O meio de transmissão é o meio físico para a propagação de sinais de telecomunicações. Trata-se do caminho físico por onde trafegam informações, entre um transmissor e um receptor. Canal de comunicações por meio do qual os dados são enviados de um lugar a outro. Os meios de transmissão podem ser classificados em vários tipos, dependendo da natureza do meio físico empregado.

Basicamente, existem dois meios de transmissão:

- **Guiados:** Com cabos (meio sólido), como coaxial, par trançado e fibra óptica.
- **Não-Guiados:** Sem fios, como rádio, IR e micro-ondas.

Abaixo, veremos alguns dos meios guiados:

O cabo coaxial consiste em dois fios condutores, sendo um o condutor dos sinais e o outro uma malha de blindagem que o rodeia, isolada. Esse conjunto é inserido dentro de uma capa isolante. O cabo coaxial mais comum, de nome 10BASE-2, usa um conector do tipo BNC. Esse tipo de cabo possui impedância (Z), medida em ohms (Ω). Trata-se da soma de três grandezas: Resistência elétrica, reatância capacitiva e reatância indutiva. A impedância influencia na reflexã ode sinais entre dois dispositivos conectados. Para redes locais, seu valor padrão é de 50 Ω.

As vantagens do cabo coaxial são:

- Por ser blindado, pode ser mais longo que cabos de par trançado comuns.
- Pode transmitir sinais de alta largura de banda.
- Possui boa imunidade a ruídos eletromagnéticos.
- Seu custo de instalação é baixo.

Já as desvantagens:

- Se quebra e apresenta mau contato com relativa frequência, por não ser flexível.
- Normalmente empregado em topologia barramento, que traz dificultado de expansão e manutenção da rede.
- Necessita de terminador de impedância.
- Devido a sua espessura, é difícil passar esse tipo de cabo por canaletas e tubos.
- Se o cabo se rompe, pode interromper toda a rede.

O cabo de par trançado possui 4 pares de fios isolados, no qual cada par consiste em dois fios enrolados um ao redor do outro para evitar interferência mútua e diafonia (daí o nome “par trançado”). Existem dois tipos principais: UTP (sem blindagem) e STP (com blindagem).

A fibra óptica é um fio fino e leve, transparente, usado para transmitir dados por meio de pulsos de luz (laser/LED). Evite interferência eletromagnética sem a necessidade de blindagens metálicas. O sinal é menos atenuado, e assim é possível usar cabos muito mais longos. As fibras ópticas atingem altas taxas de transferência de dados.

As fibras ópticas encontram inúmeras aplicações atualmente, entre elas:

- Redes de backbone.
- Conexão de banda larga de alta velocidade à internet.
- Conexão de alta velocidade entre servidores e SAN.
- Cabos submarinos.
- Aplicações militares e sensoriamento remoto.

Existem algumas desvantagens no uso de fibras ópticas em redes de dados, como:

- Instalação e manutenção são difíceis.
- Seu custo é bem maior em comparação com cabos metálicos.
- Trata-se de um meio frágil, que pode se romper com certa facilidade.
- Necessita de hardware de conexão e transmissão especial.
- Unidirecional, necessita duas fibras para TX e RX.

Agora veremos os meios de transmissão não-guiados:

As transmissões wireless são tecnologias que permitem a transmissão de dados sem o uso de fios, por meio não-guiado. Os dados são transmitidos por meio de ondas eletromagnéticas (rádio, IR, micro-ondas) que se propagam pelo espaço.

Existem vários padrões de redes sem fio, como:

- **Wi-Fi:** Redes LAN sem fio.
- **Bluetooth:** Comunicação entre dispositivos/redes PAN.
- **WiMAX:** Internet de longo alcançe sem fios.

- **Satélite.**
- **IrDA:** Conexão de dados em infravermelho.
- **Redes 3G/4G/5G.**

Essas são as vantagens das redes wireless:

- Permitem o acesso em locais remotos, onde não é possível passar cabos.
- Ampliação da rede é extremamente simples, desde que o equipamento suporte tráfego adicional.
- Novos padrões possuem taxa de transferência elevada.

E essas são as desvantagens:

- Problemas de segurança e privacidade são comuns.
- Taxa de transmissão de dados pode ser limitada em relação a meios de transmissão guiados (cabos metálicos e fibras ópticas).
- Sinais podem ser atenuados por obstáculos, como paredes, necessitando de repetidores.

As transmissões sem fio podem ser dar por três tipos de meios não-guiados (ondas eletromagnéticas):

- **Ondas de Rádio:** Atinge longas distâncias e penetram em paredes. Transmissão multicast de AM e FM, TV e telefones sem fio.
- **Micro-ondas:** Área de cobertura variável, dependente da antena e potência. Comunicação móvel, comunicação via satélite, redes WLAN. Usa antenas direcionais.
- **Infravermelho:** Curtíssimas distâncias, em uso com dispositivos alinhados. Não atravessa obstáculos. Usada em conjunto com mouses e teclados sem fio.

O Wi-Fi são redes locais que não utilizam cabos para comunicação entre os hosts. Usa um equipamento central comutador chamado de “access point”. O AP funciona como um switch wireless. As redes Wi-Fi operam em padrões de transmissão distintos, como a, b, g, n e ac. Código IEEE do padrão Wi-Fi é 802.11. O padrão mais atual hoje é 802.11ac.

O access point é um dispositivo de comunicação utilizado em redes wireless locais WLANS, que age como um equipamento transmissor e receptor de sinais de rádio, funcionando como uma espécie de switch sem fio. Comunica-se com uma rede cabeada, fornecendo às estações acesso à infra de rede do local, e à internet, por meio de comunicação via rádio.

Equipamentos de Rede – Introdução e Principais Tipos

Como sabemos, numa rede temos vários tipos de equipamentos além dos computadores, então vamos ver uma breve introdução de alguns dos principais equipamentos.

NIC (Placa de Rede)

A placa de rede opera nos níveis 1 e 2 do OSI. Suas funções são:

- Interligar o equipamento com a rede (cabeada/wireless).
- Converter sinais elétricos em pacotes de dados.
- Determinar se os pacotes são destinados ao computador.

- Converter dados em sinais elétricos para transmissão pela rede.

Switch (Comutador)

Um switch é um equipamento de rede que permite interconectar dispositivos em uma rede de computadores usando comutação de pacotes para receber, processar e encaminhar quadros ao dispositivo de destino. Sobre ele:

- O switch é um equipamento concentrador, que encaminha os pacotes para o dispositivo ou grupo de dispositivos de destino, em vez de encaminhar os pacotes para todos os nós da rede, como ocorrem com os hubs.
- Aprende os endereços físicos dos nós e os associa às suas portas para uso posterior.
- Encaminhar os quadros para seus destinos usando técnicas como Store and Forward, Cut-through, Fragment Free e Adaptive Switching.

O switch, em uma rede com topologia estrela, é o dispositivo central, de onde sai todas as conexões para os computadores.

Roteador

Equipamento que efetua o encaminhamento de pacotes entre redes de computadores distintas. Os pacotes de dados são encaminhados de um roteador ao outro até atingir o dispositivo de destino, ou sejam, descartados. Os roteadores efetuam a leitura dos pacotes IP, podendo analisar o conteúdo de seus cabeçalhos, e então tomar decisões baseando-se nos dados lidos.

Roteador de Banda Larga

Comum em ambientes domésticos, compartilha sua conexão com a internet a todos os dispositivos conectados a ele. Quase todos os roteadores banda larga possuem um switch integrado (geralmente de 4 portas), permitindo conectar os computadores da sua rede diretamente ao roteador sem a necessidade de qualquer periférico extra. A maioria também possui um access point integrado.

Access Point (AP)

Access point (ponto de acesso) é um dispositivo utilizado em redes sem fio locais (WLANs), que age como um equipamento transmissor e receptor de sinais de rádio, operando como uma espécie de switch sem fio. O AP se conecta a uma rede cabeada, fornecendo as estações conectadas acesso à infra de rede do local, e à internet.

Modulador/Demodulador (Modem)

Equipamento que converte um sinal modulado de um padrão específico para outro padrão, para que possam ser transmitidos por um meio específico. Por exemplo, transformar dados digitais em sinais elétricos para transmissão de dados via banda larga.

Repetidor

Dispositivo de rede usado para regenerar ou replicar um sinal enfraquecido. São empregados para reforçar sinais distorcidos por perdas na transmissão. Um repetidor digital é capaz de reconstruir um sinal e retransmiti-lo, permitindo estender a área de alcance da rede. Opera na camada física da rede.

Firewall

Sistema de hardware ou software cuja função é proteger uma rede de ameaças provenientes de outra rede, como a internet, e de outros hosts na própria rede. Controla o tráfego de dados entre as redes de acordo com as regras preestabelecidas (as políticas de segurança). Apenas o tráfego autorizado poderá atravessar o firewall.

Servidores

Computadores especiais que fornecem serviços e dados aos usuários de uma rede, incluindo os computadores clientes. Existem inúmeros tipos de servidores, tais como:

- Servidores de arquivo e impressão.
- Servidor de banco de dados.
- Servidores DHCP e DNS.
- Servidor de aplicações.
- Servidor web/FTP.
- Servidor de domínio.

Balanceador de Carga

Um load balancer redireciona requisições de clientes de rede para servidores, de modo a maximizar a velocidade e capacidade de uso da rede. Suas principais funções são:

- Distribuir requisições de clientes ou a carga de rede de forma eficiente entre diversos servidores.
- Assegurar alta disponibilidade e confiabilidade, evitando congestionamento de serviços.
- Fornecer flexibilidade para expansão ou manutenção dos servidores.

Network Attached Storage (NAS)

Um NAS é um dispositivo de armazenamento de dados conectado a uma rede local, que permite o acesso a esses dados pelos usuários. É uma solução de baixo custo para armazenamento e compartilhamento de arquivos em redes locais, operando como uma espécie de “nuvem” pública, porém local.

Racks

Chassis de metal (armação) usadas para armazenar equipamentos de redes conectados. Muito comum em data centers, pode ser encontrado em diversos tamanhos, sempre medido em uma unidade chamada “U”, que corresponde a uma altura de 1,75 polegadas (44,45 mm), assim indicando o número de equipamentos que podem ser instalados no rack. A largura de um rack é padronizada em 19 polegadas (48,26 cm).

Patch Panel

Hardware de conexão empregado em racks para realizar a conexão entre o cabeamento secundário de uma rede e os switches da rede local. Trata-se de um painel de conectores RJ-45 fêmea afixado

em um rack. Da parte traseira do patch panel partem cabos que se conectam aos diversos equipamentos da rede. Cada conector do patch panel é chamado de porta.

Meios de Transmissão

Meio físico para a propagação de sinais de telecomunicações. Caminho físico por onde trafegam informações, entre um transmissor e um receptor. Os meios de transmissão podem ser classificados em vários tipos, dependendo da natureza do meio físico empregado. Os meios de transmissão mais usados são os guiados (coaxial, par trançado, fibra óptica) e os não-guiados (rádio, IR e micro-ondas).

As melhores marcas de equipamentos são: Cisco, Hewlett Packard (HP), MikroTik, Ubiquiti, Aruba, Linksys, Netgear, Intelbras e TP-Link.

Qual a Diferença entre Switch e Roteador

Um switch é um equipamento de rede que permite interconectar dispositivos em uma rede de computadores, usando comutação de pacotes para receber, processar e encaminhar quadros ao dispositivo de destino. Possui múltiplas portas para a conexão de dispositivos Ethernet em uma rede local.

O switch funciona assim:

- O switch é um equipamento concentrador, que encaminha os pacotes para o dispositivo ou grupo de dispositivos de destino, em vez de simplesmente encaminhar os pacotes para todos os nós da rede, como ocorriam com os hubs.
- Armazena endereços MAC dos dispositivos em uma tabela de comutação, associando-os à porta onde estão conectados. Assim é possível encaminhar os dados diretamente do transmissor ao receptor.
- Encaminhar os quadros para seus destinos usando técnicas como Store and Forward, Cut-Through, Fragment Free e Adaptive Switching.

Numa rede com topologia estrela, o switch estaria no centro dela.

O roteador é o equipamento que efetua o encaminhamento de pacotes entre redes de computadores distintas, baseado em endereços IP. Os roteadores efetuam a leitura dos pacotes IP, podendo analisar o conteúdo de seus cabeçalhos, e então tomar decisões baseando-se nos dados lidos. Os pacotes podem ser então encaminhados de um roteador a outro até atingir o dispositivo de destino, ou serem descartados.

Essas são outras funções que um roteador faz:

- Realizar NAT (Network Address Translation), para acesso à internet às estações na rede local.
- Atribuir endereços IP a dispositivos via DHCP (Gateway padrão).
- Auxiliar na segurança da rede por meio de filtragem de pacotes.

Um switch tem muitas portas, enquanto um roteador tem poucas portas, geralmente 4.

Temos também o roteador de banda larga, comum em ambientes domésticos, compartilha sua conexão com a internet a todos os dispositivos conectados. Quase todos os roteadores possuem um

switch integrado (geralmente de 4 portas), permitindo conectar os computadores da sua rede diretamente ao roteador sem a necessidade de qualquer periférico extra. Muitos também possuem Access Point integrado.

Numa rede, os dispositivos são disponibilizados, a partir da internet pública, são o modem, roteador e switch, nessa ordem, que liga os computadores.

Característica	Switch	Roteador
Camada de Rede	2 ou 3	3
Escopo de Rede	LAN	LAN/WAN/MAN
Função	Conecta dispositivos em uma LAN, gerencia VLANs	Comuta redes distintas, ou LAN e modem
Formatos de Dados Transmitidos	Quadro (L2) ou Pacote (L3)	Pacote
Endereço de Rede	MAC Address	Endereço IP
Número de Portas	Pode ser grande: De 4 a 48 ou mais, em modelos enterprise	Pequeno: 2, 4 ou 8, geralmente
Faz NAT?	Não	Sim

Resumindo, um switch só se conecta numa mesma rede, o roteador só se conecta com redes diferentes.

O que é um Modem e Diferença para um Roteador

Modem é um dispositivo que codifica e decodifica dados (modula/demodula sinais) de modo que eles possam ser transmitidos entre uma rede LAN e uma WAN, geralmente para acesso à internet.

O funcionamento de um modem é assim: Ele é um dispositivo que modula um sinal de portadora analógica para codificar informações digitais e demodula o sinal para decodificar as informações transmitidas.

Modulação e demodulação são operações nas quais um sinal é codificado para transmissão e decodificado na recepção de voz ou dados, com o emprego de modems e sistemas de codificação variados.

Os tipos de modems mais comuns são esses:

- **Dial-Up:** Linha discada, conexão por cabo telefônico, equipamento interno ou externo. Sinal de internet oferecido pela companhia telefônica. Modems típicos. Sistema em desuso.
- **DSL:** Digital Subscriber Line (Linha Digital de Assinante). Conexão por cabo telefônico, banda larga. Sinal de internet oferecido pela companhia telefônica.
- **Cable Modem:** Conexão por cabo coaxial, banda larga. O sinal de internet é comumente fornecido junto com sinais de TV a cabo.

O modem discado, são modens típicos, permitiam a conexão à internet por meio de uma linha discada, com velocidade típica de até 56 Kbps. Internos ao PC (onboard/offboard) ou externos.

Já os modems de banda larga, são modems que permite a conexão de uma rede local à internet por meio de uma conexão de alta velocidade (banda larga). Os dois tipos mais comuns são DSL (Digital Subscriber Line) e Cable Modem.

Os modems DLS são modems que permitem a conexão da rede local à internet usando conexão dedicada de alta velocidade por linha telefônica. Conexão depende da distância. Existem algumas variantes dessa tecnologia como ADSL (mais comum), SDSL, HDSL e VDSL.

Os modems a cabo (coaxial) empregam redes de transmissão de TV a cabo para trafegar a conexão à internet, com compartilhamento de banda entre usuários. Conexão não depende de distância.

Temos também os modems de fibra óptica, mas estes não são chamados assim, e sim de terminais de rede óptica. Isso ocorre porque eles trabalham de forma diferente, transformando sinais ópticos em elétricos/digitais e vice-versa.

A diferença de um modem para roteador, é que o roteador compartilha a conexão com a internet com os dispositivos conectados à rede interna. Quase todos os roteadores banda larga possuem switch integrado (geralmente de 4 portas), para conectar computadores da rede diretamente à rede sem necessidade de outros equipamentos. Muitos também possuem access point integrado para conexão sem fio.

O gateway trata-se de um dispositivo que combina ambas as funções, contendo um modem e roteador integrados. Muitas vezes possui também um switch integrado, geralmente com 4 portas, e um access point para conexão Wi-Fi à LAN, além de outras funcionalidades.

O modem wireless/pen modem é o seguinte: Telefones celulares que acessam a internet possuem um modem embutido que traduz os sinais de ondas de rádio usados para comunicação com as torres de telefonia. Também é possível usar um modem 3G/4G USB para permitir acesso à internet em um PC ou notebook.

Um modem típico não filtra os dados que passam por ele, portanto não possui um sistema de segurança integrado. Alguns equipamentos, porém, possuem mecanismos de segurança embutidos, principalmente appliances que concentram vários dispositivos em um. Conexão via cable modem é compartilhada, e, apesar de criptografada, ainda pode ser um problema potencial de segurança.

Veja o comparativo modem x roteador:

Característica	Modem	Roteador
Camada de Rede	1	3
Escopo de Rede	WAN/LAN	LAN/MAN/WAN
Função	Conexão a internet/WAN por meio da transmissão de dados via cabo coaxial ou linhas telefônicas (par trançado)	Comuta redes distintas, ou LAN e modem.
Formatos de Dados Transmitidos	Pacote	Pacote
Endereço de Rede	Nenhum/Endereço IP	Endereço IP (WAN + LAN)
Número de Portas	Duas. Uma conecta ao provedor/WAN e outra ao	Pequeno: 2, 4, 8

	roteador/computador	
Faz NAT?	Não	Sim

O Que é uma DMZ?

DMZ, ou rede de perímetro/screened network, é uma zona intermediária entre a rede pública e a rede interna da empresa, criada com firewalls. Usada para dar acesso externo a serviços da empresa. Pode ser acessada tanto interna quando externamente. Servidores na DMZ (Bastion Hosts) não acessam máquinas na rede interna, mas podem ser acessados por elas.

Esse é o funcionamento de uma DMZ:

- Tradicionalmente, uma zona desmilitarizada é uma zona “buffer” entre países, onde operações militares não são permitidas, como ocorre por exemplo na fronteira entre as duas Coreias.
- Esse conceito foi importado em redes significando um perímetro de segurança no qual determinados equipamentos são colocados.
- Essa zona “insegura” contém recurso que precisamos acessar, e que devem ser acessíveis também a partir do ambiente externo, que é o que a torna insegura.
- Já a rede interna contém recursos valiosos para a empresa, como bancos de dados, arquivos confidenciais e outros elementos que não devem ser acessados por ninguém forma da organização.
- Uma DMZ pode ser criada com um ou dois firewalls.

Esses são uns exemplos de serviços em DMZ:

- Servidor web.
- Servidor DNS.
- Servidor de e-mail.
- Servidor FTP.
- Serviços de VoIP.
- Banco de dados (bem específico).
- Proxy reverso.

Serviços que podem ser acessados a partir da internet são colocados dentro da DMZ.

Dados importantes devem ser mantidos forma da DMZ, protegidos na rede interna.

No caso do dual firewall, é recomendado usar firewalls de fabricantes diferentes. Componente da estratégia de segurança denominada “defesa em profundidade” ao adicionar uma camada extra de segurança.

Podemos criar uma DMZ com o emprego dos seguintes equipamentos de rede:

- Roteador com função DMZ integrada.
- Firewall com função DMZ.
- Firewalls comuns em configuração dual (indicado).
- Switch com VLAN.

DMZ Host é uma configuração comum em roteadores domésticos de banda larga. Não é uma DMZ real, mas sim um endereço na rede interna que recebe tráfego de rede específico, não direcionado para as demais estações na rede interna.

Alguns problemas que podem surgir ao implementar uma DMZ em uma rede corporativa incluem:

- A performance da rede pode sofrer impacto negativo.
- Custo mais elevado, por conta de equipamentos e softwares adicionais.
- Configuração e manutenção requerem especialistas.
- Determinar o que proteger pode ser confuso.

Campos de Cabeçalho de um Pacote IPv6

Antes de mais nada, saiba que:

- O IPv6 é a versão maios atual do protocolo IP.
- Emprega endereços de 128 bits, o que significa 2^{128} endereços distintos para hosts: 340.282.366.920.938.463.374.607.431.768.211.456 emdereços.
- Substitui o IPv4 para eliminar problema de esgotamento de endereços disponíveis.
- Suporta payload maior, aumentando throughput e eficiência.
- Menos vulnerável a escaneamento de IPs e outras atividades maliciosas.
- Especificação principal: RFC 2460.

A seguir temos a estrutura de um pacote IPv6:

- Um pacote IPv6 é composto por um cabeçalho IPv6 mais um payload (conteúdo).
- O payload consiste no PDU (Protocol Data Unit) da camada superior mais cabeçalhos de extensão opcionais.

Os campos do cabeçalho IPv6 são esses:

- Versão.
- Classe de Tráfego.
- Identificador de Fluxo.
- Tamanho do Conteúdo.
- Próximo Cabeçalho.
- Limite de Encaminhamento.
- Endereço IP de Origem.
- Endereço IP de Destino.

O cabeçalho IPv6 tem 8 campos, 40 bytes como tamanho fixo, porém permite cabeçalhos de extensão.

Sobre os campos e suas funções:

Campo	Função
Versão	Versão do protocolo. Valor 6. 4 bits
Classe de Tráfego	Classe ou prioridade do pacote IPv6. 8 bits
Identificador de Fluxo	Rotular pacotes que pertencem ao mesmo fluxo de dados, de

	modo a requisitar manipulação especial por roteadores IPv6 intermediários. 20 bits
Tamanho do Conteúdo	Tamanho total da carga (payload). 16 bits
Próximo Cabeçalho	Tipo de cabeçalho de extensão imediatamente após o cabeçalho IP básico. 8 bits
Limite de Encaminhamento	Indica o número máximo de nós IPv6 intermediários que o pacote pode atravessar. 8 bits
Endereço IP de Origem	Endereço IP do remetente original do pacote. Tamanho: 128 bits
Endereço IP de Destino	Endereço IP do destinatário original do pacote. Tamanho: 128 bits

Mudanças do pacote IPv6 em relação à IPv4:

IPv4	IPv6
Versão	Igual, mas com números diferentes para versão
Comprimento do Cabeçalho IP	Campo removido no IPv6, o cabeçalho IPv6 possui tamanho fixo de 40 bytes
Tipo de Serviço	Substituído pelo campo Classe de Tráfego
Tamanho Total	Tamanho do conteúdo (payloiad length), que mostra apenas o tamanho do payload
Identificação, Flags de Fragmentação, Offset de Fragmento	Removidos no IPv6. As informações sobre fragmentação estão em um cabeçalho de extensão
TTL (Time to Live)	Substituído pelo campo Limite de Salto
Protocolo	Substituído pelo campo Próximo Cabeçalho
Checksum do Cabeçalho	Removido no IPv6. Verificações de erro são realizadas na camada de link de dados
Endereço de Origem	Igual, mas contendo um endereço de 128 bits
Endereço de Destino	Igual, mas contendo um endereço de 128 bits
Opções	Removido no IPv6. As opções IPv4 foram substituídas pelos cabeçalhos de extensão

Informações opcionais são tratadas em cabeçalhos de extensão no IPv6. Não há quantidade máxima ou tamanho fixo para esse cabeçalhos.

Seis cabeçalhos de extensão são definidos pelas especificações do IPv6. Novos cabeçalhos podem ser definidos sem que seja preciso alterar os cabeçalhos base.

IPv6 e IPv4 coexistirão por muitos anos. Veja alguns dos impactos previsos nesse longo período de transição:

- **Falhas:** Os administradores devem efetuar um plano de contingência para que as redes continuem operando com IPv4 e IPv6.

- **Contabilização:** Deve-se recalcular os limites de utilização dos recursos, pois, com os dois protocolos em operação, o consumo muda em relação às redes somente com IPv4.
- **Configuração:** Para permitir que os dois protocolos possam conviver nas redes, é necessário diversas configurações.
- **Desempenho:** Com a mudança de cenário (redes com os dois protocolos operando), o desempenho da rede necessita de adaptações para garantira do acordo de nível de serviço (Service Level Agreement – SLA).
- **Segurança:** O administrador deve optar por alguma técnica que garanta a interoperabilidade, sem que gere riscos à segurança da rede e/ou usuários.

Comandos ip no Linux

Os comandos *ip* são usados para mostrar e configurar parâmetros de rede para as interfaces em uma máquina.

Há dois conjuntos principais de programas para a configuração de rede do Linux: Os pacotes net-tools e *iproute2*.

Os antigos programas do conjunto net-tools (como o clássico ifconfig) pertencem ao sistema de redes Linux NET-3. A maioria está obsoleta atualmente.

Já os programas do pacote iproute2 (como o ip, tratado neste tutorial), são o sistema de configuração de rede atual do Linux. O iproute2 consiste em uma série de utilitários, dos quais o ip é o foco desse nosso artigo, mas além do ip, outros utilitários que compõe o pacote iproute2 são:

ss
bridge
rtmon
nstat
tc
devlink

E vários outros.

A tabela a seguir mostra os principais objetos disponíveis para uso com os comandos ip, suas abreviações e função:

Objeto	Abreviação	Função
address	*a, addr*	Endereço em um dispositivo (IPv4 ou IPv6)
addrlabel	*addrl*	Configuração de rótulo para seleção de endereço
link	*l*	Dispositivo de rede
maddress	*m, maddr*	Endereço multicast
mroute	*mr*	Entrada de cache de roteamento multicast
neighbour	*n, neigh*	Entrada de cache ARP ou NDISC
rule	*ru*	Regra no banco de políticas de roteamento
tunnel	*t*	Túnel sobre IP

No dia a dia de trabalho do administrador de redes Linux, é mais comum o uso dos objetos *address* e *link*, por se tratarem de objetos usados na configuração direta de endereçamento e interfaces de redes físicas, mas é importante conhecer todos eles, pois em algum momento eles podem ser necessários.

Exemplos

Vejamos alguns exemplos de aplicação do comando ip para gerenciamento de parâmetros de rede em um servidor (ou estação). Note que para executar a maior parte dos comandos é necessário possuir privilégios de administrador:

Mostrar as interfaces de rede disponíveis no computador:

sudo ip link show

Ver os ips das interfaces de rede:

sudo ip addr show

 # Ou simplesmente:

sudo ip a

Ver somente informações sobre o protocolo IPv4 nas interfaces:

sudo ip -4 a

Para o protocolo IPv6:

sudo ip -6 a

Reiniciar a máquina ou o serviço de rede após.

Desabilitar uma interface de rede, como a enp0s3:

sudo ip link set enp0s3 down

Para reabilitar a mesma:

sudo ip link set enp0s3 up

Ver o ip de uma interface específica, como a enp0s3:

sudo ip addr ls enp0s3

 # Ou

sudo ip addr show enp0s3

Ver estatísticas de comunicação (tx e rx) de uma interface específica (opção *-s*):

sudo ip -s link show enp0s3

Atribuir um endereço IP a uma interface específica:

sudo ip addr add 192.168.12.100/26 dev enp0s3

PS: Esta configuração é perdida ao reiniciar o sistema. Para mantê-la, editar o arquivo de configuração */etc/network/interfaces* (Debian e derivados) ou os arquivos em */etc/sysconfig/network-scripts/* (Red Hat e derivados).

Excluir um endereço IP de uma interface específica:

sudo ip addr del 192.168.12.100/26 dev enp0s3

Ajustar o nome da interface de rede enp0s3 para eth0:

sudo ip link set enp0s3 name eth0

Verificar as rotas de rede (tabela de roteamento):

sudo ip route show

Adicionar uma rota estática:

sudo ip route add 10.20.30.0/26 via 192.168.100.10 dev enp0s3

PS: Esta configuração é perdida ao reiniciar o sistema. Para mantê-la, editar o arquvio de configuração */etc/network/interfaces* (Debian e derivados) ou os arquivos em */etc/sysconfig/network-scripts/* (Red Hat e derivados).

Por exemplo, no Debian, adicionamos a linha:

up ip route add 10.20.30.0/26 via 192.168.100.10 dev enp0s3

Ao arquivo */etc/network/interfaces* para adicionar a rota estática de forma permanente.

Remover uma rota estática:

sudo ip route del 10.20.30/26

Adicionar um endereço de gateway padrão geral:

sudo ip route add default via 192.168.100.10

Se o gateway padrão para a rede já existir, será emitida uma mensagem de erro.

Configurar um endereço MAC em uma interface:

sudo ip link set dev enp0s3 address 00:0ª:75:20:f5:bd

Alterar o MTU em uma interface. Por exemplo, aplicar um MTU de 9000 na interface enp0s3:

sudo ip link set mtu 9000 dev enp0s3

Geralmente alteramos o MTU em redes gitabit para permitir o tráfego de Jumbo Frames (quadros jumbo), de modo a aumentar a performance de transmissão da rede.

Consultar a tabela ARP:

sudo ip neigh

Consultar a tabela ARP de uma interface específica:

sudo ip neigh show dev enp0s3

Visualizar a ajuda dos comandos ip:

sudo ip help

Ou ainda, visualizar a ajuda apenas dos comandos de endereçamento:

sudo ip addr help

Habilitar o modo promíscuo na interface enp0s3:

sudo ip link set enp0s3 promisc on

Enumeração DNS

Todo site possui um IP válido na rede. O responsável por realizar a tradução de nome para IP e vice-versa. Com a ferramenta apropriada poderemos levantes as seguintes informações através de um determinado alvo:

- IP pelo qual o alvo responde.
- Os nx do alvo.
- Os mx do alvo.

Existem diversos tipos diferentes de registros DNS disponíveis, no entant5o, abaixo será mostrado apenas o que significam os mais comuns de serem encontrados durante o gerenciamento de um domínio:

- **A:** O A, também conhecido por hostname, é o registro central de um DNS, ele vincula um domínio ou subdomínio a um endereço IP direto.
- **AAAA:** Executa a mesma função de A, porém, para um endereço IPv6.
- **NS:** Name Server (Servidor de Domínio), especifica servidores DNS para o domínio ou subdomínio. Pelo menos, dois registros NS devem ser definidos para cada domínio. Geralmente, um principal e outro secundário.
- **CNAME:** Significa Canonical NAME. Especifica um apelido (alias) para o hostname (A). É uma forma de redirecionamento.
- **MX:** Sigla para Mail eXchanger. Aponta o servidor de e-mails. Pode-se especificar mais de um endereço, formando-se assim uma lista em ordem de prioridade para que haja alternativas no caso de algum e-mail não puder ser entregue.
- **PTR:** PoinTeR, aponta o domínio reverso a partir de um endereço IP.

- **SOA:** Start Of Authority. Indica o responsável por respostas autoritárias a um domínio, ou seja, o responsável pelo domínio. Também indica outras informações úteis como número serial da zona, replicação, etc.
- **TXT:** Refere-se a TeXT, o qual permite incluir um texto curto em um hostname. Técnica usada para implementar o SPF.
- **SPF:** Sender Policy Framework, é uma tentativa de control de falsos e-mails. Permite ao administrador de um domínio definir os endereços das máquinas autorizadas a enviar mensagens neste domínio.
- **SRV:** Abreviação de SeRVice, permite definir localização de serviços disponíveis em um domínio, inclusive seu protocolos e portas.

O que é Torrent?

Torrent é a extensão dos arquivos compatíveis com o protocolo de compartilhamento BitTorrent, uma tecnologia criada pela empresa também chamada BitTorrent, introduzida em 2001. Ela funciona criando uma rede P2P entre todos os usuários do protocolo, com o intuito de distribuir arquivos entre todos os usuários da rede.

Funciona assim: Em um modelo de rede cliente-servidor, um computador ou servidor fica responsável por armazenar e distribuir os dados em uma rede, enquanto os usuários, ou clientes, o acessam para utilizar as informações que procuram.

A computação em nuvem nada mais é do que o modelo cliente-servidor aplicado à internet, onde o fornecedor do armazenamento atua como o repositório dos dados.

No modelo P2P (de peer-to-peer, ou ponto-a-ponto), não existe um servidor dedicado, porque todos os usuários são também servidores. Cada um dele detêm os dados dos arquivos compartilhados, e ao mesmo tempo estão baixando e mantendo os arquivos disponíveis para outros na rede.

No protocolo BitTorrent, o usuário que disponibiliza o arquivo completo na rede é o servidor original (ou seed, que é o termo padrão), e os que começam a baixar os dados são os primeiros clientes (ou peers). Com o tempo, os peers começam a também enviar fragmentos dos arquivos de volta para a rede, mesmo que o download não esteja completo.

Uma vez que ele termine, o peer automaticamente se torna mais um seed, apenas enviando os dados de volta e não baixando mais nada. A lógica por trás do BitTorrent é que quanto mais seeds um arquivo tenha, mais usuários o estão disponibilizando, e logo, o download é mais rápido e eficiente.

O que é um Roteador

Um roteador (router, em inglês) é um equipamento de rede que efetua o encaminhamento de pacotes de dados entre redes de computadores distintas. Esses pacotes de dados são encaminhados de um roteador para outro até que atinjam o dispositivo de destino, ou seja, descartados. Os roteadores efetuam a leitura dos pacotes IP, podendo analisar o conteúdo de seus cabeçalhos, e então tomar decisões baseando-se nos dados lidos.

Os roteadores são conectados em redes distintas, efetuando a conexão entre essas redes, em contraste com um switch, que efetua a conexão de dispositivos finais, como computadores e notebooks, dentro de uma mesma rede.

Existem diversos tipos de roteadores, classificados de acordo com sua aplicação e capacidade específicas. Na lista abaixo elencamos alguns dos tipos mais comuns de roteadores existentes:

- **Roteador Interno:** Os roteadores desta categoria possuem todas as suas interfaces conectadas à mesma área.
- **Roteador de Borda (Edge Router):** Localizado na borda da rede de um provedor de internet. Este roteador no geral opera com protocolo BGP (Border Gateway Protocol) e efetua a conectividade entre provedores ou grandes organizações.
- **Roteador Core:** Localizado dentro de um sistema autônomo, como um backbone, e carrega tráfego entre roteadores de borda.
- **Roteador Banda Larga:** Appliance de uso doméstico que traz integradas em um mesmo equipamento funções de roteador e switch, no mínimo.
- **Roteador Wireless:** Appliance de uso doméstico que traz integradas em um mesmo equipamento funções de um roteador banda larga acrescidas de funcionalidade de access point (ponto de acesso), permitindo efetuar a conectividade de equipamentos a uma rede Wi-Fi.

Basicamente, usamos os roteadores em duas aplicações principais:

- Conectar duas ou mais redes distintas, efetuando separação de domínios de broadcast.
- Escolher um caminho (rota) a ser seguido pelos pacotes até que cheguem a seus destinos, por meio de protocolos de roteamento adequados.

Mais Sobre Endereços IPv6

Um endereço IPv6 é formado por oito blocos de quatro dígitos hexadecimais (hextetos), separados por dois pontos. Cada bloco pode conter números de 0000 a ffff. Por exemplo, um endereço IPv6 pode ser *2001:0db8:85a3:0000:0000:8a2e:0370:7334*.

A configuração do IPv6 não usa mais a máscara de sub-rede no formato tradicional do IPv4. Em vez disso, utiliza o prefixo da sub-rede. O prefixo indica quantos bits do endereço são usados para identificar a rede. Por exemplo, um prefixo de */64* significa que os primeiros 64 bits do endereço IP são usados para identificar a rede e os bits restantes são usados para identificar o host.

Para entender a estrutura da rede, aqui estão algumas informações relevantes sobre os tipos de endereços IPv6:

- **Endereço Global Unicast:** Similar aos endereços públicos no IPv4, esses endereços são roteáveis na internet. Um exemplo é *2001:0db8:85a3:0000:0000:8a2e:0370:7334*.
- **Endereço Link-Local:** Usado para comunicação dentro da mesma rede local (link). Não é roteável e é automaticamente configurado por cada dispositivo. Todos os endereços link-local começam com *fe80::*. Um exemplo é *fe80::1a2b:3c4d:5e6f:7a8b*.
- **Endereço Unique Local:** Semelhante aos endereços privados do IPv4, esses endereços são usados em redes internas e não são roteados na internet. Eles têm o prefixo *fc00::* ou mais raramente, *fd00::*. Um exemplo é *fc00::1234:5678:9abc*.
- **Endereço de Loopback:** Usado para testes de diagnóstico no próprio dispositivo. No IPv6, o endereço de loopback é *::1* (ou *0:0:0:0:0:0:0:1*).
- **Endereço de Auto-Configuração:** No IPv6, quando um dispositivo não consegue obter um endereço IP a partir de um servidor DHCPv6, ele pode gerar um endereço IPv6 link-local automaticamente. Não há um equivalente exato ao APIPA do IPv4, mas endereços link-local são criados automaticamente.

PS: Num endereço IPv6, podemos omitir zeros a esquerda, e sequência de 0000 em outros campos pode ser colocado apenas um “0” ou deixar uma sequência de um ou mais zeros como um espaço vazio (como “::”). Um exemplo seria *2001:db8:85a3::8a2e:370:7334*.

Saiba também que:

- O identificador de rede, assim como no IPv4, deve ser único dentro da rede, a mesma regra vale pro identificador de host.
- Endereços IPv6 não utilizam um padrão de broadcast. O conceito de broadcast foi substituído por multicast em IPv6, portanto, não existem endereços reservados para tal.
- Endereços com todos os bits ajustados como 0 são usados para a identificação da própria rede ou para endereçamento de grupos (multicast).
- Não se usa um identificador de host com todos os bits ajustados como 0 ou 1 para denotar um endereço específico, pois a abordagem é diferente da usada em IPv4.
- Com o IPv6, todas as redes locais devem ter prefixos */64*, necessário para funcionalidades como a da autoconfiguração. Endereços *fe80::* tem a máscara */10*, endereços *fc00::/fd00::* tem a máscara */7* ou */8*, ao passo que o endereço de loopback (*::1*) tem a máscara */128*.
- Usuários receberão de seus provedores redes */48*, mas alguns provedores podem entregar aos usuários domésticos redes com tamanho */56*.

Proxy Server

O proxy server ajuda a impedir que usuários não autorizados se conectem à rede, como a de uma empresa. Ele permite ao administrador controlar quem acessa a rede da empresa e quais serviços essas pessoas utilizam.

A Microsoft possui o Microsoft Proxy Server que, uma vez instalado, funciona como uma barreira (firewall) entre a rede da empresa e a internet.

Além disso, o proxy server pode manter armazenada uma cópia das páginas visitadas (cache), tornando mais rápida a navegação pelos endereços mais acessados da internet.