CAPA

terça-feira, 16 de junho de 2020 10:55

Internet e Protocolos

Centro Paula Souza

SÃO PAULO
GOVERNO DO ESTADO
Secretaria de Desenvolvimento Econômico

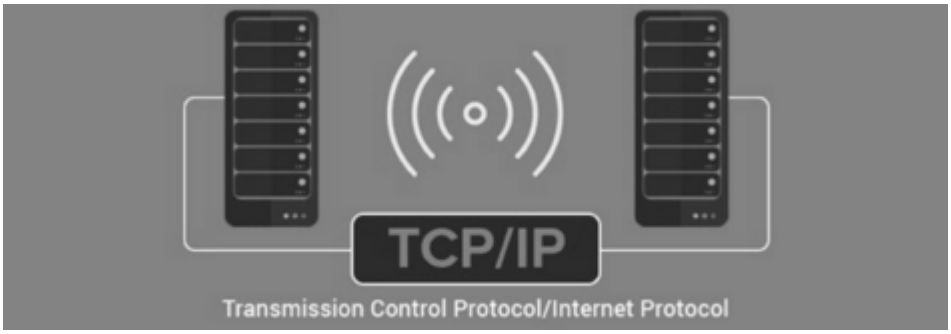
Etec Jorge Street

Internet e Protocolos

Professor Alberto Ciarcia Junior
alberto.ciarcia@etec.sp.gov.br

TCP/IP

sexta-feira, 1 de maio de 2020 17:11



Camadas do modelo TCP/IP

O conceito TCP/IP é também um modelo de referência para definição de camadas, entretanto resumido a apenas quatro camadas. É formalmente conhecido como TCP/IP por conta dos conjuntos de protocolos Internet. É usualmente conhecido como TCP/IP por conta dos protocolos fundamentais serem TCP e IP, embora não sendo apenas eles os utilizados neste modelo.

Camada de aplicação

A camada de aplicação do modelo TCP/IP fornece às aplicações a capacidade de acesso a serviços de outras camadas, definindo os protocolos onde os aplicativos usarão para trocar dados. protocolos da camada de aplicação mais amplamente conhecidos incluem HTTP, FTP, SMTP, Telnet, DNS, SNMP e RIP (Routing Information Protocol – Protocolo de Roteamento de Informação.

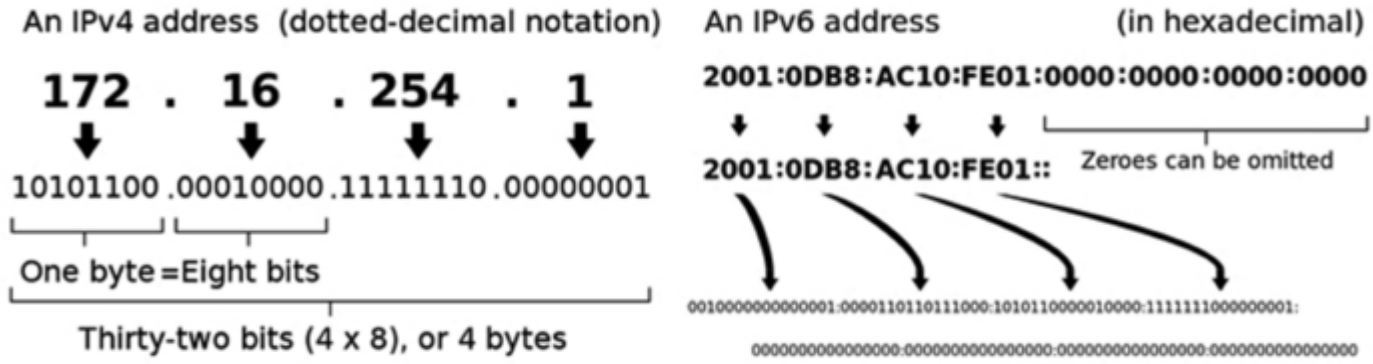
Camada de transporte

Também conhecida como a camada de transporte de hospedeiro-para-hospedeira, a camada de transporte fica responsável pelo fornecimento da camada de aplicação com serviços de sessão de comunicação e datagrama. Os protocolos de núcleo desta camada são o TCP e UDP. O protocolo TCP fornecendo um serviço de comunicação orientada a conexão confiável um-para-um. Responsável pelo sequenciamento e reconhecimento de pacotes enviados além da recuperação de pacotes perdidos na transmissão. O protocolo UDP fornece um serviço de comunicação orientada a conexão não confiável um-para-um ou um-para-muitos. O UDP é utilizado tipicamente quando a quantidade de dados a serem transferidos é pequena (tal quando os dados possam ser enviados em um único pacote).

Camada de Internet

Camada responsável pelo endereçamento de Internet do hospedeiro, empacotamento e funções de encaminhamento. Os principais protocolos dessa camada de protocolo Internet são IP, ARP (Address Resolution Protocol – Protocolo de Resolução de Endereços), ICMP (Internet Control Message Protocol – Protocolo de Controle de Mensagem para Internet e IGMP (Internet Group Management Protocol – Protocolo de Gerenciamento de Internet por

Grupos). O IP é um protocolo de roteamento responsável pelo endereçamento IP, encaminhamento, a fragmentação e remontagem de pacotes. O ARP é responsável pela descoberta do endereço da camada de acesso à rede, como um endereço de hardware associado a um determinado acesso na camada Internet. O ICMP é responsável por fornecer funções de diagnóstico e relatar erros durante uma entrega malsucedida dos pacotes IP. O IGMP é responsável pela gestão de grupos IP multidestino. Nesta camada o IP adiciona um cabeçalho aos pacotes tornando-se conhecida como endereço de IP.



Camada de Acesso à Rede

A camada de acesso à rede (ou camada de enlace) é responsável por inserir os pacotes TCP/IP no caminho de rede e receber pacotes TCP/IP fora dele. O TCP/IP foi projetado para ser independente do método de acesso à rede, formato de quadro e tipo de mídia. Em outras palavras, é independente de qualquer tecnologia de rede específica. Desta maneira o TCP/IP pode utilizadores para conectar diferentes tipos de rede como Ethernet, Token Ring, X.25, Frame Relay e ATM (Asynchronous Transfer Mode – Modo de Transferência Assíncrona).

Como são processados os dados durante uma transmissão !?

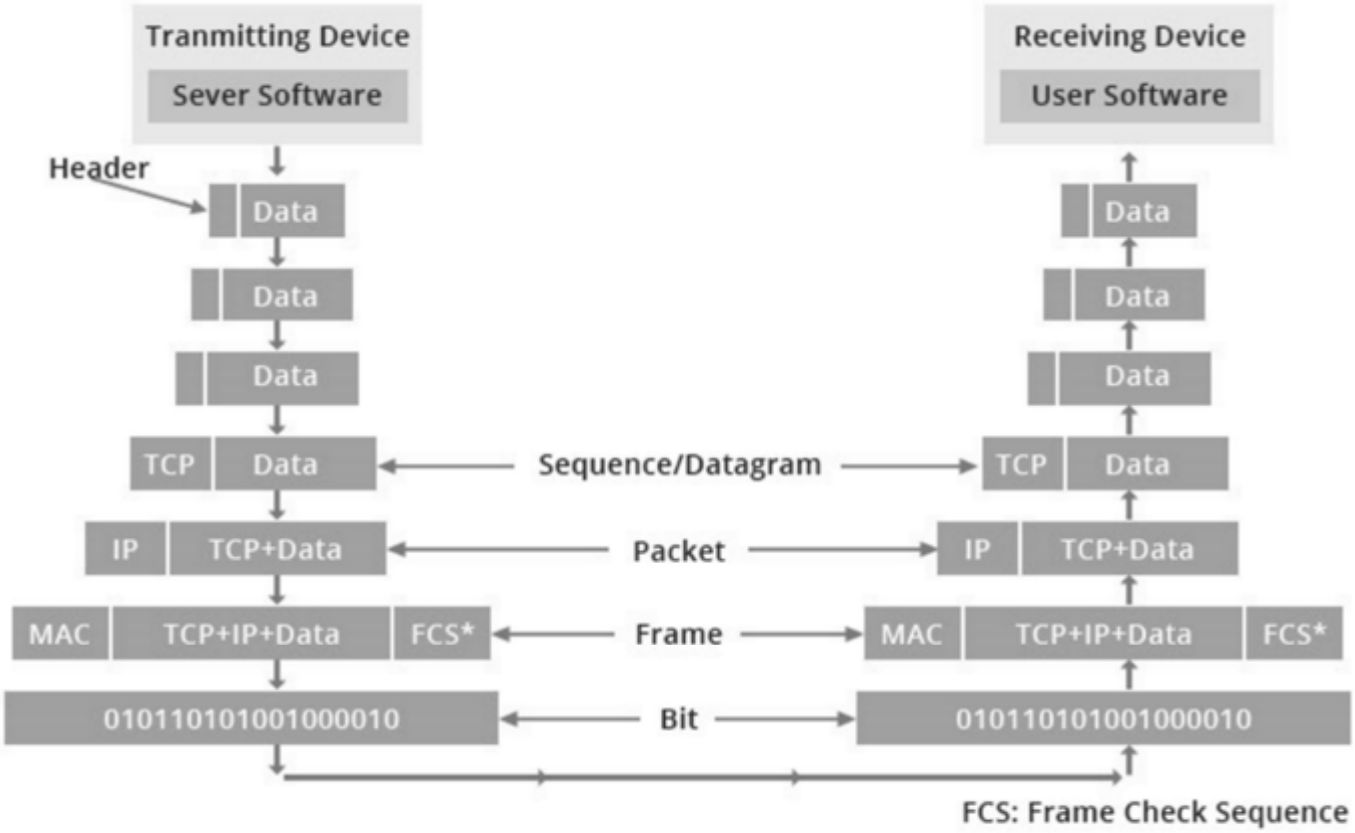
Num sistema por camadas, dispositivos de uma camada de transferência com formatos diferentes, no qual é conhecido como PDU (protocol data unit – unidade de dados de protocolo). A tabela abaixo mostra os PDUs entre as diferentes camadas .

Unidade de dados de protocolo (PDU) a ser processado em camadas diferentes.

Tipo de modelo	Camadas OSI	Protocol Data Unit (PDU)	Camadas TCP / IP
Camadas de acolhimento	Camada de aplicação	Dados	Camada de aplicação
	Camada de apresentação		camada de sessão
	camada de sessão		Inscrição
	Camada de transporte	Segmento (TCP) / Datagram (UDP)	Camada de transporte
Camadas de mídia	Camada de rede	Pacote	Camada de Internet
	Dados Link Layer	Quadro, Armação	Camada de Acesso à Rede
	Camada física	Mordeu	

Por exemplo durante a solicitação do usuário para acessar uma página de internet no computador, o software servidor remoto em primeiro lugar repassa os dados solicitados

para a camada de aplicação, onde é processado a partir de uma camada para outra descendo para cada camada com suas respectivas funções designadas. Esses dados são então transmitidos através da camada física da rede até que o servidor de destino ou outro dispositivo as receba. Neste ponto os dados são devolvidos para as camadas superiores, cada camada realizando suas operações atribuídas até que esses dados sejam utilizados pelo software de recepção, no caso no browser ou navegador.

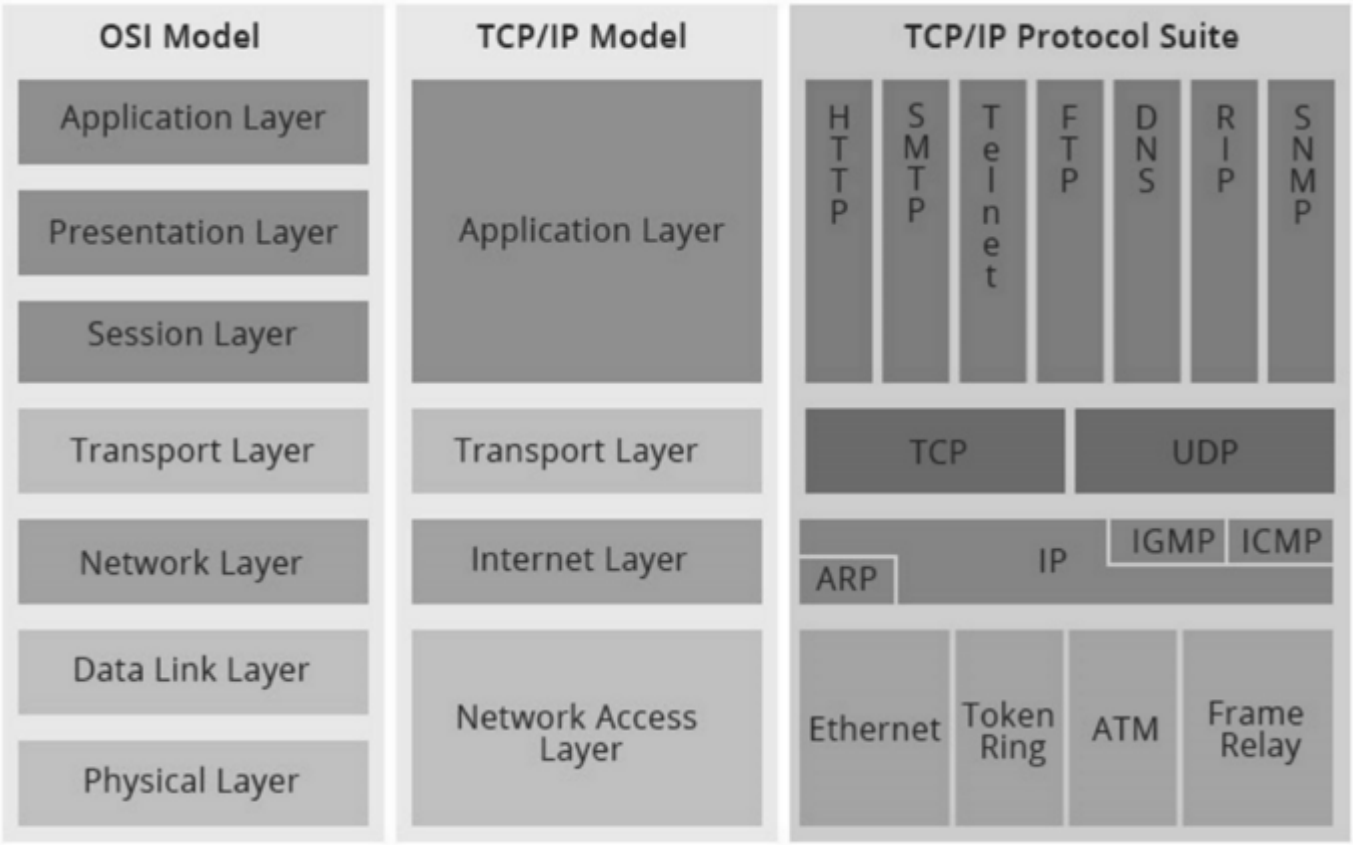


Durante a transmissão, cada camada acrescenta um cabeçalho, rodapé ou ambos para a PDU proveniente da camada superior, que direciona e identifica o pacote. Este processo é chamado de encapsulamento. O cabeçalho (e rodapé) e os dados em conjunto formam o PDU para a camada seguinte. Este processo continua até chegar à camada de nível mais baixo (ou camada de acesso rede camada física), pela qual os dados são transmitidos para o dispositivo de recepção. O dispositivo de recepção inverte o processo, desencapsulando os dados em cada camada com a informação de cabeçalho e rodapé gerenciando as operações. Em seguida a aplicação finalmente acessa esses dados. Processo em ritmo contínuo até todos os dados serem transmitidos e recebidos.

TCP Modelo IP / vs. Modelo OSI

segunda-feira, 25 de maio de 2020 14:49

O modelo TCP/IP é mais antigo que o modelo OSI. A figura abaixo exibe a relação correspondente de suas camadas.



Ao comparar as camadas do modelo de TCP/IP com do modelo OSI, a camada de aplicação do modelo TCP/IP é semelhante às camadas 5, 6, 7 do modelo OSI combinadas mas o modelo TCP/IP não tem uma camada de apresentação separada, ou camada de sessão. A camada de transporte do TCP/IP engloba tanto as responsabilidades da camada de transporte OSI quanto algumas das responsabilidades da camada de sessão OSI. A camada de acesso de rede do modelo TCP/IP contempla a conexão de dados e camadas física do modelo OSI. Nota-se a camada de Internet do TCP/IP não tirar proveito dos serviços de sequenciamento e reconhecimento que podem estar presentes na camada de enlace de dados do modelo OSI. A responsabilidade é da camada de transporte no modelo TCP/IP.

O modelo OSI é apenas um modelo conceitual, considerando-se os significados dos dois modelos de referência. Utilizado principalmente para descrever, discutir e entender as funções de rede individuais. Entretanto o modelo TCP/IP é primeiramente projetado para resolver um conjunto específico de problemas, não para funcionar como uma descrição para geração de todas as comunicações de rede como no modelo OSI. O modelo OSI é genérico independente de protocolo, mesmo assim a maioria dos protocolos e sistemas o adotam, enquanto o modelo TCP/IP é baseado em protocolos padrão desenvolvidos para da Internet. Outro fator a ser observado no modelo OSI está em nem todas as camadas serem utilizadas em aplicações mais simples. Enquanto as camadas 1, 2, 3 serem obrigatórias a qualquer comunicação de dados, a aplicação pode utilizar algumas camadas de comunicação únicas para a aplicação ao invés das camadas superiores habituais no modelo.

A Importância do TCP/IP e OSI na solução de problemas

Com o conhecimento da divisão de camadas, podemos diagnosticar onde o problema está quando falha uma conexão. O princípio está em verificar a partir do nível mais baixo ao invés de partir do nível mais alto. Por cada camada inferior atender a uma camada mais elevada, será mais fácil lidar com problemas nas camadas inferiores. Por exemplo quando o computador não consegue conectar-se a Internet, a primeira ação está em verificar se o cabo de rede está conectado ao computador, ou se o ponto de acesso sem fio WAP (Wiresless Access Point / AP – Ponto de Acesso para Rede Sem Fio) está conectado ao switch senão os conectores RJ45 estão em boas condições.

Entenda como Funciona o Protocolo TCP-IP

terça-feira, 2 de junho de 2020 13:49

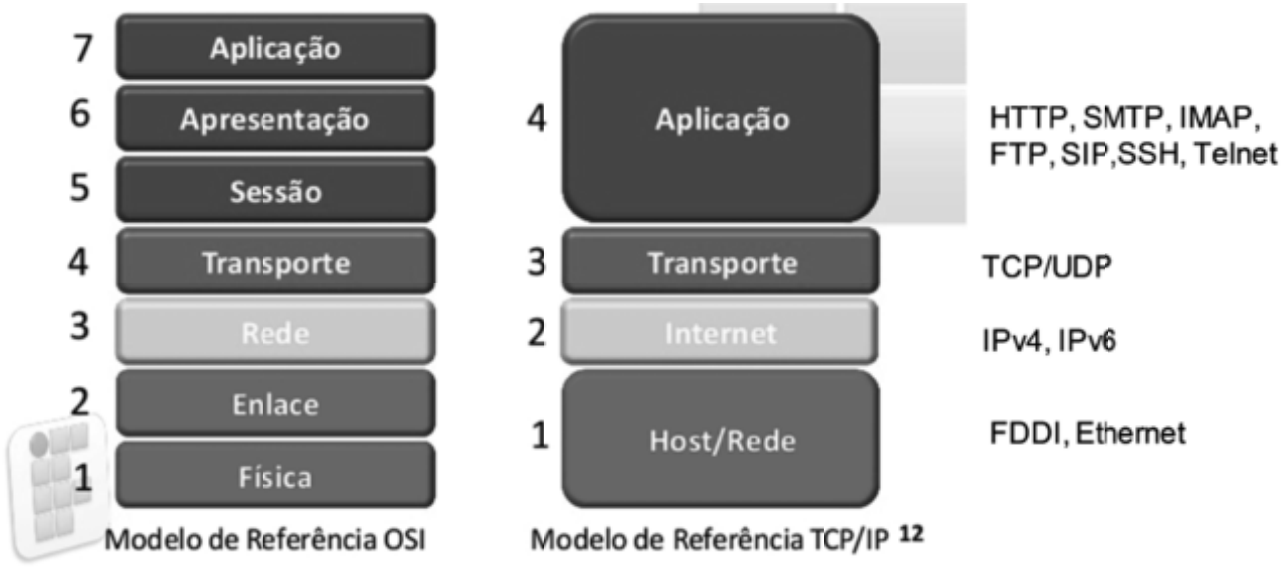
Entenda como Funciona o Protocolo TCP-IP

O tcp-ip (Protocolo de controle de transmissão) é um dos procolos de comunicação mais utilizados atualmente. Neste tutorial eu vou explicar como ele funciona de uma forma simples e compreensível. Ao final da leitura você vai entender o motivo pelo qual os dados precisam ser organizados para que então possam ser transmitidos e como isso é feito no protocolo tcp-ip.

Afinal de contas o que é protocolo tcp-ip ? O protocolo é como uma linguagem utilizada para fazer dois computadores ou um computador e um dispositivo (como o CLP) conversarem entre si. Antes de ir mais afundo neste tutorial, é recomendado que você saiba como funciona o modelo OSI, que é fundamental para entender como o protocolo tcp-ip funciona.

tcp-ip não é propriamente um protocolo, mas um conjunto deles ou uma pilha de protocolos como usualmente é chamado. Observe que o próprio nome já se refere a dois protocolos diferentes: TCP (Transmission Control Protocol) e IP (Internet Protocol). Além disso, existem vários outros protocolos relacionados ao tcp-ip em que podemos citar alguns: FTP, HTTP, SMTP e UDP e neste artigo explicaremos como funciona cada um deles.

Abaixo podemos visualizar a arquitetura do tcp-ip:



Como podemos observar na Figura acima, o tcp-ip possui 4 camadas sendo que tudo se inicia a partir de um programa conversando na camada de aplicação. Nesta camada você vai encontrar protocolos como o SMTP (para e-mail), FTP (para transferência de arquivos) e HTTP (para navegar na internet) sendo que cada tipo de programa fala para um protocolo diferente da camada de Aplicação, dependendo do propósito do programa.

Depois de processar a requisição, o protocolo na camada de Aplicação vai falar com outro protocolo na camada de Transporte, usualmente o TCP. Esta camada é responsável por pegar o dado enviado pela camada de Aplicação, dividindo este dado em pacotes a fim de enviar ele para a camada inferior, a da Internet. Também, durante o recebimento do dados, a camada de Transporte é responsável por colocar os pacotes de dados recebidos da camada de Internet em ordem (os dados podem ser recebidos fora de ordem) e também checar se o conteúdo dos pacotes estão intactos.

Na camada de Rede, nós temos o IP (Internet Protocol) que pega os pacotes recebidos da camada de Transporte e adiciona uma informação de endereço virtual. Exemplo: adiciona o endereço do computador que está enviando dados e o endereço do computador que vai receber estes dados.

Estes endereços virtuais são chamados de endereços IP. Em seguida, o pacote é então enviado para a camada inferior, Interface de Rede e quando os dados chegam nesta camada eles são chamados de datagramas.

A Interface de Rede vai pegar os pacotes enviados pela camada de Rede e enviar os mesmos através da rede (ou receber da rede, se o computador estiver recebendo dados). O que vai ter dentro desta camada vai depender do tipo de rede em que o computador estiver inserido. Hoje em dia, o tipo de rede mais utilizado para comunicação entre computadores é a Ethernet (que é encontrada em diferentes faixas de velocidade) e pode ser cabeada (cabo de par trançado CAT5 ou CAT6) ou WI-FI (sem fio). Ainda dentro da camada de Interface de Rede Ethernet, você pode encontrar camadas Ethernet como a LLC (Logic Link Control), MAC (Media Access Control) e a Física que é o meio físico (cabo por exemplo). Os pacotes transmitidos através da rede são chamados de quadros.

Vamos entender melhor cada camada do protocolo tcp-ip:

1 – Camada de Aplicação

Esta camada faz a comunicação entre os programas e os protocolos de transporte no tcp-ip. Existem diferentes protocolos que trabalham na camada de aplicação e os mais conhecidos são o HTTP (HyperText Transfer Protocol), SMTP (Simple Mail Transfer Protocol), FTP (File Transfer Protocol), SNTP (Simple Network Protocol), DNS (Domain Name System) e Telnet. Abaixo mostramos uma lista dos tipos que podem ser encontrados com uma pequena descrição sobre cada um:

- FTP – File Transfer Protocol: Permite a transferência de arquivos entre dois computadores através de login e senha.
- TFTP – Trivial File Transfer Protocol: Permite a transferência de arquivos entre dois computadores sem a necessidade de login e senha. É mais limitado e pouco utilizado.
- NFS – Network File System é um protocolo que permite que os sistemas UNIX e Linux montem remotamente sistemas de arquivos entre um e outro.
- SNMP – Simple Network Management Protocol é utilizado para gerenciar todos os tipos de elementos de rede baseando no envio e recebimento de vários dados.
- 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 clientes.
- BOOTP – O protocolo Bootstrap é utilizado para designar um endereço IP para computadores que não possuem disco rígido, onde o servidor fornece um arquivo juntamente com o sistema operacional para executá-lo.
- 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.
- BGP – Border Gateway Protocol: Quando dois sistemas estão utilizando BGP, eles estabelecem uma conexão TCP, e então enviam um para outro suas tabelas BGP. O BGP utiliza método de vetorização de distância sendo que ele detecta falhas, enviando mensagens de atividade aos seus vizinhos a cada 30 segundos. Ele troca informações sobre redes alcançáveis com outros sistemas BGP, incluindo o caminho completo dos sistemas que estão entre eles.
- EGP – Exterior Gateway Protocol é utilizado entre roteadores de diferentes sistemas.
- IGP – Interior Gateway Protocol. O nome é utilizado para descrever o fato de que cada sistema na internet pode escolher seu próprio protocolo de roteamento. RIP e OSPF são exemplos de protocolos de gateway interior.

- RIP – Routing Information Protocol é utilizado para atualizar dinamicamente tabelas de roteamento em WANs e na internet. O algoritmo vetor distância é utilizado para calcular a melhor rota para o pacote.

- OSPF – Open Shortest Path First (roteamento dinâmico de protocolo). Aqui é aplicado um protocolo de estado de link ao invés de um protocolo de vetor de distância em que ele testa o estado da sua ligação com cada um dos seus vizinhos e envia as informações adquiridas para eles.

- POP3 – Post Office Protocol version 3 é utilizado por usuários clientes para acessar uma conta de email 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.

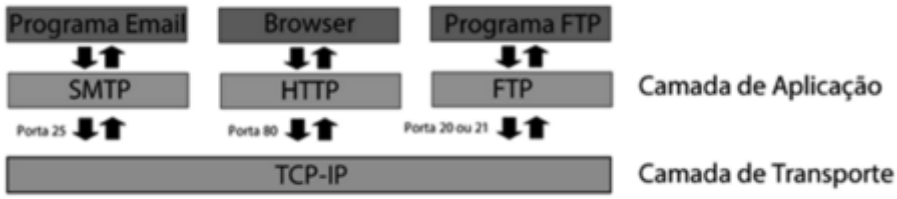
- Telnet é utilizado para abrir uma sessão remota em outro computador. Ele se baseia em TCP para o transporte e é definido pela RFC854.

- Quando você solicita ao seu programa de e-mail para que ele faça o download dos e-mails que estão armazenados no servidor, você está fazendo uma solicitação na camada de aplicação do tcp-ip, que neste caso é servido pelo protocolo SMTP. Por outro lado, quando você digita www no navegador a fim de abir uma página, o navegador vai requerer o tcp-ip na camada de aplicação servido pelo protocolo HTTP e é por isso que as páginas iniciam-se com http://.

- A camada de Aplicação fala com a camada de transporte através de portas que são numeradas seguindo um padrão para diferentes aplicações. Por exemplo, o protocolo SMTP sempre utiliza a porta 25 e o HTTP sempre utiliza a porta 80. Por outro lado o FTP utiliza a porta 20 (para transmissão de dados) e 21 (para controle).

A utilização do número da porta permite ao protocolo de Transporte (tipicamente TCP) saber qual o tipo de conteúdo está dentro do pacote (por exemplo, saber que o dado que está sendo transportado é um e-mail), fazendo com que o lado que está recebendo o dado saiba para qual aplicação este dado vai. Então, quando um pacote chegar na porta 25, o protocolo TCP vai saber que deve entregar o dado ao protocolo conectado a porta, o SMTP, que por sua vez entrega o dado à aplicação que o requisitou (o programa de e-mail).

Na Figura abaixo podemos ver uma representação de requisições utilizando o tcp-ip:



2 – A Camada de Transporte

Quando há a transmissão de dados no tcp-ip, a camada de transporte é responsável por pegar este dado da camada de Aplicação e dividir ele em vários pacotes menores. O TCP (Transmission Control Protocol) é o protocolo mais utilizado na camada de Transporte e como falado anteriormente, ele pode tanto quebrar a informação em pacotes quanto organizar de forma a colocar em ordem a mensagem. Assim, quando ele está recebendo dados, o mesmo tem a função de organizar eles para que a mensagem possa ser interpretada pela camada de Aplicação.

Enquanto o TCP organiza os pacotes, ele também utiliza o sistema de reconhecimento da informação para verificar se os dados estão integros. 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 rrápido do que o TCP.

Quando o UDP é utilizado, a aplicação que estiver solicitando os dados que será a responsável por verificar a integridade dos mesmos e reordenar os pacotes, fazendo a função que o TCP faria. Ambos

os protocolos UDP e TCP vão buscar o dado da camada de Aplicação e acrescentam um endereço virtual (cabeçalho) a cada pacote que por sua vez é removido quando chega no receptor da informação. Neste cabeçalho existem informações importantes como o número da porta de entrada, a sequência do dado e a soma para verificação da integridade (checksum). Por ter menos funcionalidades, o cabeçalho UDP possui somente 8 bytes enquanto que o cabeçalho TCP possui 20 ou 24 bytes. Abaixo citamos alguns protocolos desta camada que compõem o tcp-ip:

- TCP – Conexão confiável utilizada para controlar o gerenciamento das aplicações a nível de serviços entre computadores. Faz tanto o transporte em sequência do dado quanto a checagem da integridade dos mesmos.
- UDP – Conexão não confiável utilizada para controlar o gerenciamento das aplicações a nível de serviços entre computadores e é utilizado para o transporte de algum dados onde a própria aplicação faz a verificação da integridade dos dados;
- ICMP – Internet control message protocol (ICMP) fornece o gerenciamento e o relatório de erros para ajudar no gerenciamento de dados durante a comunicação entre computadores. Esta conexão é utilizada para reportar o status do computador que está sendo conectado ao computador que está tentando conectar como por exemplo reportar que o computador de destino não está acessível.
- IGMP – Internet Group Management Protocol utilizado para suportar mensagens multicasting e rastrear grupos de usuários na rede de computadores.

- Na Figura abaixo, podemos ver de forma genérica como funciona a camada de Transporte no tcp-ip, tanto transmitindo quanto recebendo dados.

3 – A Camada de Rede

No tcp-ip, cada computador na rede é identificado com um único endereço virtual, chamado de endereço IP. A camada de Rede ou Internet é a responsável por adicionar o cabeçalho no pacote de dado recebido da camada de Transporte, onde além de outros dados de controle, será adicionado o endereço IP fonte e o endereço IP de destino. Ou melhor, o endereço IP do computador que está enviando o dado e o endereço IP do computador que vai receber este dado.

Se não estiver sendo utilizado nenhum endereço virtual, você deve saber o endereço MAC do computador de destino, que além de ser uma tarefa difícil, não ajuda no roteamento dos pacotes, devido ao fato de que este endereço não utiliza a estrutura de nomenclatura tipo árvore. Em outras palavras, com o endereço IP, os computadores de uma mesma rede pertencerão a endereços IPs sequenciais (Ex.: 192.168.1.10 e 192.168.1.12). Já com endereços MAC, como cada máquina conectada na rede tem um único endereço físico, não podemos identificar sequencialmente (Ex.: 00-14-22-01-23-45 e 01-24-10-12-14-54).

O roteamento é o caminho que o pacote de dado deve utilizar para chegar ao seu destino e quando há uma requisição de dado para um servidor, este dado, antes de chegar no seu computador, passa por vários locais (chamados roteadores). Você quer ver como funciona? Basta clicar no menu iniciar do Windows –> Acessórios –> CMD. Depois que abrir o prompt de comando, tente ver qual o caminho percorrido pelo dado quando você tenta acessar o google digitando o comando tracert www.google.com. Veja Figura abaixo:

Veja pela figura que no meu caso, o dado passa por 10 pontos diferentes até chegar ao seu destino.

Em todas as redes que estão conectadas na internet, existe um dispositivo chamado roteador, que faz a ponte entre os computadores da sua rede local e a internet. Todos os roteadores possuem uma tabela com redes conhecidas e também uma configuração chamada gateway padrão apontando para outro roteador na internet. Quando um computador envia um pacote de dados pela internet, o roteador conectado na sua rede primeiro e tenta verificar se o computador de destino é conhecido. Em outras palavras, ele verifica se o outro computador está na mesma rede ou em uma rede que o roteador conhece o caminho. Se não conhece, envia um pacote de dados para o gateway padrão (outro roteador) e o processo se repete até que o pacote de dado chegue no seu destino e foi isso que aconteceu no exemplo acima.

Existem vários protocolos que trabalham na camada da Internet e podemos citar os seguintes:

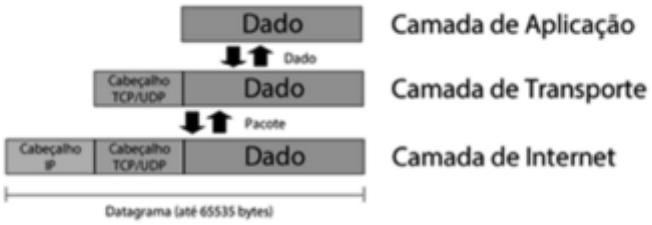
- ARP – Address Resolution Protocol: habilita o empacotamento do dado do IP em pacotes ethernet e é o sistema e protocolo de mensagem que é usado para encontrar a ethernet (hardware) através de um número específico de IP. Sem este protocolo, o pacote de ethernet pode não ser gerado do pacote de IP porque o endereço ethernet pode não ser determinado.

- IP – Internet Protocol. Exceto para ARP e RARP todos os pacotes de dados de todos os protocolos serão empacotados em um pacote de dados IP sendo que o IP fornece o mecanismo para usar o software para endereçar e gerenciar pacotes de dados sendo enviados por computadores.

- RARP – Reverse address resolution. Este protocolo é utilizado a fim de permitir que um computador sem um armazenamento de dado permanente tenha um endereço IP a partir do seu endereço ethernet.

Como o IP é o mais utilizado, vamos falar um pouquinho sobre ele. O IP é o responsável por pegar o pacote de dados recebido pela camada de Transporte e dividir este pacote em datagramas, que é definido como um pacote sem nenhum sistema de verificação de integridade de dados, ou seja, um protocolo não confiável. Devemos frisar aqui que quando o dado vai ser transferido, o TCP implementa este reconhecimento de integridade (acknowledge), fazendo com que mesmo que o IP não seja capaz de reconhecer erros, o TCP o faz, tornando a conexão confiável.

Cada datagrama IP pode ter no máximo 65.535 bytes, incluindo o cabeçalho, que pode utilizar 20 ou 24 bytes. Assim, datagramas IP podem possuir 65.515 ou 65.511 bytes de dado e caso o pacote recebido pela camada de Transporte for maior do que isto, o protocolo IP vai dividir o pacote em vários datagramas o quanto for necessário.



Na Figura 4, nós podemos visualizar o datagrama gerado na camada de Internet pelo protocolo IP. É interessante frisar que o que a camada de Internet enxerga como dado é o pacote todo pego da camada de Transporte, incluindo o cabeçalho TCP ou UDP. Este datagrama vai estar sendo enviado para a camada de Interface de Rede (se estamos transmitindo o dado) ou vai ser pego pela camada de Interface de Rede (se estivermos recebendo o dado).

4 – A Camada de Interface de Rede

No tcp-ip, os datagramas gerados na camada de Rede vão ser enviados para a camada inferior, a camada de Interface de Rede (caso estivermos enviando dados) ou a camada de Interface de Rede estará recebendo dados da rede e enviando para a camada de Internet (caso estivermos recebendo dados).

Esta camada é definida por qual o tipo de rede física seu computador está conectado. Sabemos que quase sempre seu computador estará conectado a rede Ethernet (lembrando sempre que wireless também são redes Ethernet).

Como já sabemos, tcp-ip é um conjunto de protocolos que trabalham nas camadas 3 a 7 do modelo OSI e a Ethernet é um conjunto de protocolos que pertencem às camadas 1 e 2 do modelo OSI. Isso significa que a Ethernet lida com o aspecto físico da rede, complementando o tcp-ip que lida com os dados especificamente.

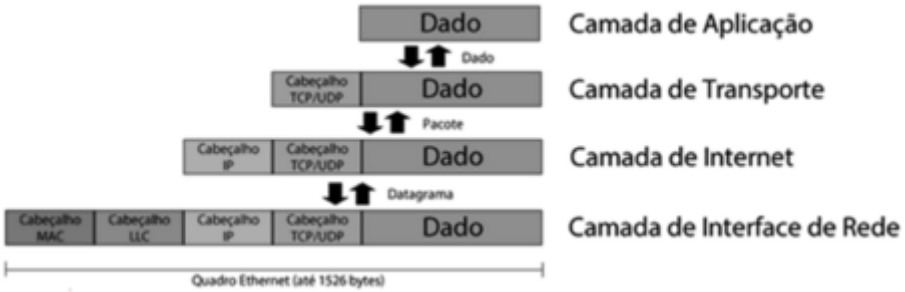
A Ethernet possui três camadas a citar: Logic Link Control (LLC), Media Access Control (MAC) e Physical. As camadas LLC e MAC correspondem juntas a segunda camada do modelo OSI e você pode ver a arquitetura Ethernet na Figura 6.

A camada LLC é responsável por adicionar informação sobre qual o protocolo na camada de Rede vai entregar dados para ser transmitido e por este motivo, quando esta camada receber um pacote da rede, ela deve saber para qual protocolo da camada de Internet deve ser entregue o dado.

A camada Media Access Control (MAC) é responsável por montar o quadro que vai ser enviado pela rede e adiciona tanto o endereço fonte MAC quanto o endereço destino MAC. Como explicado anteriormente o endereço MAC é um endereço físico da placa de rede do computador.

Já a camada física é responsável por converter o quadro gerado pela camada MAC em eletricidade (se for uma rede cabeada) ou em ondas eletromagnéticas (se for uma rede wireless). Tanto a camada LCC quanto a MAC acrescentam seu próprio cabeçalho ao datagrama vindo da camada de Internet. Assim, uma estrutura completa de quadros gerados por estas duas camadas podem ser vistas na Figura 7. Veja que os cabeçalhos adicionados pela camada superior podem ser visto como dado pela camada LLC e a mesma coisa ocorre com o cabeçalho adicionado pela LLC que pode ser visto pela camada MAC como um dado.

A camada LLC adiciona cabeçalhos de 3 ou 5 bytes e este datagrama possui um tamanho máximo de 1500 bytes, formando um máximo de 1.497 ou 1.492 bytes por dado. A camada MAC adiciona um cabeçalho de 22 bytes e 4 bytes CRC (correção de dado) no final do datagrama recebido da camada LLC, formando o quadro Ethernet. Assim, o tamanho máximo de um quadro Ethernet é de 1.526 bytes.



Os protocolos que fazem parte da camada de Interface de Rede do tcp-ip são:

- SLIP – Serial Line Internet Protocol. Este protocolo coloca pacotes de dados em quadros em preparação para o transporte através do hardware de rede, sendo utilizado para enviar dados por linhas seriais. Aqui, não há correções de erros, endereçamento ou identificação de pacotes e também não temos autenticação sendo que o SLIP suporta apenas o transporte de pacotes IP.

- CSLIP – Compressed SLIP é a compressão de dados essencial para o protocolo SLIP que utiliza a compressão Van Jacobson capaz de reduzir drasticamente o tamanho do pacote também podendo ser utilizado com o PPP sendo chamado de CPPP.

- PPP – Point to Point Protocol é uma forma de encapsulamento de dados serial que representa uma melhoria com relação ao SLIP capaz de prover uma comunicação serial bidirecional e é bem parecido com o SLIP, se diferenciando por suportar AppleTalk, IPX, TCP/IP e NetBEUI junto com o TCP/IP.

- Ethernet – Como vimos Ethernet é um conjunto de camadas e provem o encapsulamento de quadros antes de serem enviados para computadores.

https://www.citisystems.com.br/protocolo-tcp-ip/

IPv4

segunda-feira, 29 de junho de 2020 20:06

IP significa Protocolo de Internet, que é usado para entregar datagramas entre hosts em uma rede. Tipicamente, é um método pelo qual os dados serão enviados de um dispositivo de computador a outro dispositivo de computador pela Internet. O IPv4 é a quarta versão do Protocolo Internet que foi adaptado e é agora amplamente utilizado na comunicação de dados através de diferentes tipos de redes. É considerado como um dos protocolos centrais dos métodos de Internetworking baseados em padrões na Internet e foi a primeira versão que foi desdobrada para a produção durante o tempo de ARPANET. IP significa um protocolo que depende de redes de camada comutadas por pacotes, assim como a Ethernet. Ele fornece uma conexão lógica entre dispositivos de rede diferentes fornecendo a identificação de cada dispositivo.

Funcionalidade

O IPv4 utiliza um esquema de endereços de 32 bits que permite um total de 2 a 32 endereços ou um pouco mais de 4 bilhões de endereços. Este é baseado no modelo de melhor esforço. O modelo certifica-se de que não existe a possibilidade de duplicar a entrega. Todos estes aspectos são tratados pela camada superior de transporte. Esta versão do IP é utilizada como base da Internet e estabelece todas as regras e regulamentos para as redes de computadores que funcionam com base no princípio da troca de pacotes. A responsabilidade deste protocolo é estabelecer conexões entre dispositivos de computador, servidores e dispositivos móveis que são baseados em endereços IP. Na troca de informação em IPv4, ela é realizada pelos pacotes IP. Um pacote IP é dividido em 2 grandes campos, nomeadamente o cabeçalho e o campo de dados. O campo de dados é utilizado para transportar informações importantes, enquanto um cabeçalho contém todas as funções do protocolo.

Funções IPv4 na camada de rede da pilha de protocolos TCP ou IP. Sua principal tarefa é principalmente transferir os blocos de dados do host de envio para o host de destino, onde os emissores e receptores são computadores que são identificados exclusivamente pelos endereços do Protocolo de Internet. A coisa boa sobre o endereço de IP é que ele é usado como um identificador único de dispositivos de computação que são unidos a uma rede local ou a Internet. É tipicamente utilizado para endereçar e transmitir dados através da rede. Sem isto, o dispositivo não consegue determinar onde está realmente a transmitir dados. Todos os dispositivos que estão operando através de uma rede, tais como dispositivos de computador, impressoras de rede, telefones, servidores e mais realmente precisam de seu próprio endereço de rede.

Os endereços de IP são um pouco semelhantes aos dados de passaporte. Os endereços IPv4 são, na maioria das vezes, escritos de uma forma com 4 números decimais a partir de 0 até 255 e separados por um ponto.

Por exemplo: 172.128.1.2

Existe um endereço mínimo e um endereço máximo; o endereço mínimo possível é 0.0.0.0 e o endereço máximo possível é 255.255.255.255. Sem este endereço IP, um dispositivo não será identificado na rede ou não será capaz de trocar informações com outros dispositivos na rede privada ou numa rede pública.

Além disso, esta versão de IP funciona na camada de rede do modelo OSI e na camada de Internet

do modelo TCP ou IP. Isto dá a responsabilidade ao IP de identificar o host com base nos endereços lógicos e rotear os dados entre eles através da rede subjacente. Este IP que tem um protocolo de 3 camadas recebe os segmentos de dados da 4ª camada que é transporte e o divide no que é conhecido como o pacote. O pacote IP encapsula a unidade de dados que é recebida da camada acima e adiciona suas próprias informações de cabeçalho.[3]

Componentes

A seguir estão as duas partes de um endereço IP, baseadas no desenho original do IPv4:

Identificador de rede

Isto é uma porção do endereço de IP que é usado para identificar indivíduos ou dispositivos diferentes em uma rede como uma rede de área local ou a Internet. Esta é a concepção, a fim de garantir a segurança de uma rede e os recursos relacionados. Este é o octeto mais significativo do endereço.

Identificador do anfitrião

Isto refere-se ao nome que é declarado no programa hospedeiro.

Modos de endereçamento

A seguir estão os três tipos diferentes de modos de endereçamento suportados pelo IPv4:

Modo de endereçamento Unicast

Este endereço ajuda a identificar um nó único de uma rede. Isto refere-se simplesmente a um único remetente e um único receptor embora possa ser usado tanto no envio como na recepção. Neste modo, os dados serão enviados apenas para um host destinado. O campo do endereço de destino tem um endereço IP de 32 bits do host de destino. Esta é a forma mais comum de endereçamento do Protocolo Internet.

Modo de endereçamento de transmissão

Refere-se a um endereço de rede no qual todos os dispositivos conectados a uma rede de comunicação de acesso múltiplo serão habilitados para receber diagramas. Uma mensagem que será enviada para um endereço de difusão pode ser recebida por todos os anfitriões ligados à rede. Neste modo, o pacote é endereçado a todos os hosts em um segmento de uma rede. O campo do endereço de destino tem um endereço de difusão especial. Quando a máquina verá um pacote na rede, ela é obrigada a processá-lo.

Modo de endereçamento multicast

No IPv4, isto é definido pelo padrão mais significativo de 1110. Isto inclui os endereços de 224.0.0.0 a 239.255.255.255. Este modo é uma mistura dos dois modos anteriores. Com este pacote, o endereço de destino contém um endereço especial que começa em 224.x.x.x.x e pode ser entretido por mais de um host. Com o crescimento da Internet, espera-se realmente que o número de endereços IPv4 não utilizados acabe por se esgotar, porque todos os dispositivos, como os computadores, os smartphones e as consolas de jogos ou os que se ligam à Internet, exigirão um endereço.

História da empresa

Os atuais protocolos de Internet incorporados em sistemas modernos fazem uso de tecnologias mais complexas e intrincadas que são baseadas em desenvolvimentos feitos a partir do Protocolo NCP (Programa de Controle de Redes) do ARPANET (Advanced Research and Project Agency Network). Vinton Cerf e Robert Kahn são conhecidos como os antepassados do TCP/IP (Transmission Control Protocol / Internet Protocol). Trabalhando com o TCP, o IP foi introduzido como um datagrama que não dependia de um protocolo conectado, mas continha um cabeçalho e uma carga útil. O cabeçalho codificou os endereços de origem e de destino do pacote de dados, enquanto a carga útil transportava os dados reais. Cerf e Kahn trabalharam com a Agência do Departamento de Defesa dos EUA no ping da primeira versão principal do IP que ainda é amplamente utilizada atualmente - IPv4.

Mais especificamente, o IPv4 foi implantado pela primeira vez em 1983 para a produção na ARPANET. O IPv4 é descrito na publicação RFC 791 da IETF em 1981, substituindo uma definição anterior em 1980. No entanto, o governo dos Estados Unidos chegou à conclusão de que os endereços IPv4 apresentavam um conjunto limitado de endereços, apenas cerca de 4 bilhões de combinações possíveis, para os 7 bilhões de pessoas no mundo e começou uma nova versão que agora está sendo integrada às redes existentes - o IPv6.

terça-feira, 23 de junho de 2020 11:27

Sub-redes

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 bit 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.

Máscara

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.

Máscara de Sub-Rede

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 da rede (e subrede) 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.

Endereços de Rede e de Host

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 exclusivo de cada host dentro da rede à 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)

Máscaras de Sub-Rede Padrão

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
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

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.

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 da aplicação 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** (classe C)
Máscara de sub-rede padrão: **255.255.255.0**

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

Endereço IP: **11000000.10101000.00000001.00111111**
Máscara de sub-rede padrão: 11111111.11111111.11111111.00000000

Aplicando a operação lógica AND bit a bit:

11000000.10101000.00000001.00111101 AND
11111111.11111111.11111111.00000000 =
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 decimal obtemos o endereço **192.168.1.0**, que é o endereço da rede à qual pertence o IP. Note o final **0** (zero) do 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, terminado 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..

Exemplo com endereçamento sem classes

Vejamos agora um segundo exemplo de aplicação de máscara de subrede, agora sem o uso das classes de endereçamento IP.

Endereço IP: **192.168.1.61**
Máscara de sub-rede padrão: 255.255.255.224

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:

11000000.10101000.00000001.00111101 AND
11111111.11111111.11111111.11100000 =
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 subrede 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.

Notações para máscaras de sub-rede

Podemos expressar Máscaras de sub-rede em notação ponto-decimal como um endereço, como por exemplo a máscara 255.255.255.0 usada anteriormente, ou ainda usando a notação **CIDR** (Classless Inter-Domain Routing), que consiste no primeiro endereço da rede, seguido de uma barra **/** e do número de bits (comprimento) do prefixo. Em nosso exemplo anterior, poderíamos representar o endereço IP mais a sua máscara como **192.168.1.0/24**, pois há 24 bits de valor "**1**" na máscara de sub-rede utilizada.

Divisão em sub-redes

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 desejados.

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

http://www.bosontreinamentos.com.br/redes-computadores/o-que-e-mascara-de-sub-rede/

Como calcular máscaras de sub-rede

segunda-feira, 29 de junho de 2020 18:55

Como calcular máscaras de sub-rede

Imagine o seguinte cenário, na empresa onde você foi chamado para trabalhar, existe apenas um único switch de 48, porém, na sua empresa existem departamentos estratégicos que não poderão compartilhar informações. De que forma você poderá criar uma separação de redes neste cenário. A resposta é simples, é criando VLANs no switch, mas para isso, o switch tem que ser gerenciável. Poderíamos atribuir uma máscara de subrede Classe C e definirmos para cada grupo um endereço 192.168.X.X, conforme o exemplo a seguir:

- Financeiro: 192.168.0.0
- RH: 192.168.1.0
- Compras: 192.168.2.0
- Vendas: 192.168.3.0

O problema nestes casos é que eu teria um desperdício de IPs na minha rede, uma vez que, atribuiremos IP's para no máximo o número de máquina que poderão se conectar ao Switch. Desta forma, e sabendo que o nosso switch tem 48 portas, iremos subnetar nossa rede, iremos dividir nossa rede em parte menores, cada uma representando um departamento, ou seja, dividimos nossa rede em sub-redes.

O que é sub-rede

Toda endereço IP tem uma máscara correspondente. Essa máscara que identifica qual parte do endereço pertence a rede e qual parte ao host.

Por exemplo, o endereço 192.168.0.50 com uma máscara 255.255.255.0, identifica como parte da rede o endereço 192.168.0 e o host como 50:

Endereço de Rede: 192.168.0

Endereço do Host: 50

Para dividir essa rede, nós podemos "dividir" essa máscara. Para isso, podemos usar valores diferentes entre 0 ou 255. Quando fazemos isso, damos o nome de sub-rede.

Mas quais valores podemos colocar?

- Calculando as máscaras de sub-rede

Cada três dígitos na máscara, correspondem a uma parte do endereço IP do host. Essas partes são formadas por oito bits, por isso recebem o nome de octetos.

Cada bit no octeto, possui um valor em decimal correspondente a sua posição.

Por serem bits, só possuem dois estados, ou 0, representando o host, ou 1, representando a rede.

No caso, essa máscara (255.255.255.0), pode ser representada em binário como: 11111111.11111111.11111111.0000000.

Máscara: 255.255.255.0

Binário..: 11111111.11111111.11111111.00000000

Caso todos os oito bits da máscara de sub-rede possuir valor 1, o valor em decimal 255, caso todos os bits forem 0, possui o valor 0 em decimal.

Mas por que quando todos os bits são 1, o valor em decimal fica é 255?

Isso é por causa da conversão de binário para decimal.

Criando sub-redes

Vimos que os bits 1 na máscara especifica a porção da rede e que os bits 0 especificam o host no endereço IP. Para criar nossas redes, podemos pegar alguns bits 0 e transformá-los em 1.

Por exemplo, se pegarmos o primeiro bit 0 na máscara e transformá-lo em bit 1, teríamos a seguinte máscara em binário: 11111111.11111111.11111111.1000000

Mas como fica o valor dela em decimal?

Sabemos que os três primeiros octetos têm o valor em decimal de 255. Já para saber o valor do último, basta realizar a conversão:

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

Ou seja, temos: $1 \times 2^7 + 0 \times 2^6 + 0 \times 2^5 + 0 \times 2^4 + 0 \times 2^3 + 0 \times 2^2 + 0 \times 2^1 + 0 \times 2^0$.

Que nos deixa com 128.

Logo, a máscara dessa rede é: 255.255.255.128.

Mas quantas redes temos com essa máscara?

Para saber quantas redes temos com essa nova máscara basta elevar o **número 2**, que são o número de bits possíveis, ao número de bits emprestados da porção do host.

Neste caso pegamos um bit da porção do host, portanto temos **2^1 **redes. Ou seja, temos duas redes.

Mas quantos hosts cada rede comporta?

Os hosts são definidos como bits 0 na máscara de sub-rede, certo? Então para saber quantos hosts nossa rede comporta basta elevar 2 ao número de bits 0 na máscara.

Neste caso temos sete bits 0 (10000000), logo, 2^7, que nos dá 128.

Então cada uma de nossas redes comportam 128 hosts?

Dentre os endereços IPs, dois precisam ser reservados. Um para especificar a rede e outro para especificar o dominio de broadcast. Então, na verdade temos 128 - 2 hosts, logo temos 126 hosts em cada sub-rede.

Mas quais são esses endereços reservados?

O endereço que especifica a rede é sempre o primeiro endereço IP, já o de broadcast é o último endereço IP da rede.

Em uma rede classe C com máscara padrão, o **endereço da rede é 192.168.0.0** e o de **broadcast é 192.168.0.255**. Só que no nosso caso são duas sub-redes, cada uma com um endereço de rede e de broadcast.

A primeira rede possui o **endereço de rede 192.168.0.0**, já o endereço de broadcast nós descobrimos somando 1 ao número de hosts, que neste caso são 126, mais o endereço de rede. Ou seja, temos **1 + 126 + 0. **Dessa forma temos que o **endereço de broadcast da primeira sub-rede é 192.168.0.127.**

Já o endereço de rede da segunda sub-rede é o endereço de broadcast da primeira sub-rede mais 1.

Ou seja, temos como endereço de rede da segunda sub-rede 192.168.0.128. O endereço de broadcast conseguimos obter da mesma forma.

Somamos 1 ao número de hosts, mais o endereço de rede. Portanto, 1 + 126 + 128, isso nos dá o endereço de broadcast 192.168.0.255.

Bom, calculamos as sub-redes, mas com essa máscara temos apenas duas sub-redes. Porém, temos quatro departamentos e queremos colocar cada um em uma sub-rede. Como podemos fazer isso?

Se nós pegamos um bit a mais na máscara de sub-rede como no exemplo, nós temos duas sub-redes. Então, se nós pegarmos dois bits, teremos dois elevado a dois, que é número de bits que pegamos na porção do host, isso nos deixa com quatro que é o número de sub-redes que queremos.

Ou seja, nossa máscara ficará em binário: 11111111.11111111.11111111.1100000. Realizando a conversão:

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

Ou seja, temos: $1 \times 2^7 + 1 \times 2^6 + 0 \times 2^5 + 0 \times 2^4 + 0 \times 2^3 + 0 \times 2^2 + 0 \times 2^1 + 0 \times 2^0$.

Que nos deixa com 128.

Logo, a máscara dessa rede é: 255.255.255.192.

Ou seja, nossa máscara de sub-rede será 255.255.255.192. Mas quantos hosts cada sub-rede comportará?

Para saber isso, basta elevar 2 ao número de bits 0 na máscara, menos os dois bits reservados de cada rede, ou seja, como temos seis bits zero nossa conta fica $2^6 - 2$, isso nos deixa com 62 hosts para cada rede.

Se quisermos saber qual é o endereço de cada sub rede, basta realizar os mesmos passos de antes.

O endereço de rede primeira sub-rede será 192.168.0.0, já o seu endereço de broadcast será um mais o número de hosts mais o endereço de rede. Isso nos deixa com ** 1 + 62 + 0**. Logo, o endereço de broadcast da nossa primeira sub rede será 192.168.0.63.

Dessa forma, após calcular cada sub-rede teremos o seguinte resultado:

Endereço de Rede: 192.168.0.0,

Endereço de Broadcast: 192.168.0.63

Endereço de Rede: 192.168.0.64,

Endereço de Broadcast: 192.168.0.127

Endereço de Rede: 192.168.0.128,

Endereço de Broadcast: 192.168.0.191

Endereço de Rede: 192.168.0.192,

Endereço de Broadcast: 192.168.0.255

Todos esses endereços utilizando a máscara 255.255.255.192.

Dessa forma conseguimos alocar cada departamento em uma sub-rede, o que otimiza a rede e isola os problemas.

Para saber mais

Como cada sub-rede é uma rede distinta, elas precisam de um roteador para se comunicarem umas com as outras.

Neste exemplo, utilizamos um IP da classe C para criar as sub-redes, porém conseguimos realizar essa configuração com todas as classes de IPs disponíveis.

Nós podemos utilizar outra notação quando falamos de máscaras de rede. Ao invés de utilizar a máscara em seu formato decimal, podemos dizer apenas a quantidade de bits um contidos nela.

Por exemplo, a máscara padrão da classe C, 255.255.255.0, em formato binário fica 11111111.11111111.11111111.0000000. Ou seja, ela tem 24 bits 1. Então caso desejemos falar que o endereço IP 192.168.0.35 utiliza a máscara padrão, podemos utilizar a notação /24. Ficando assim 192.168.0.35 /24.

O nome dessa notação é CIDR.

Dividir e calcular

Atribuir endereços IPs a redes é o um dos trabalhos de um administrador de redes. Saber qual endereço atribuir e qual máscara utilizar faz parte desse trabalho.

Quando estamos instalando uma rede, é bacana separarmos os departamentos para isolar possíveis problemas, melhorar a performance da rede, além da segurança.

Uma forma de fazer isso é criando VLans, porém mesmo com essa configuração, algumas redes podem ter problemas com o broadcast. Então uma forma de resolver isso é dividindo a rede em parte menores, criando sub-redes.

IPV6

segunda-feira, 29 de junho de 2020 19:58

IPv6

IPv6 (Internet Protocol versão 6) é a versão mais recente do Protocolo Internet. Este é um protocolo de comunicação que fornece um sistema de identificação e localização de computadores ou dispositivos em redes e rotas de tráfego através da Internet. Esta versão do Protocolo Internet é um conjunto de especificações do grupo de trabalho de engenharia da Internet que é realmente uma versão atualizada do IPv4. Como esta é a versão mais recente, ela é usada para identificar diferentes dispositivos na Internet para que eles possam ser localizados. O IPv6 é por vezes referido como a "próxima geração da Internet", porque aumentou as suas capacidades e o crescimento do IPv6 permitirá que o atual desenvolvimento passe por implantações mais recentes e modernas em grande escala. Esta versão usa 128 bits, ao contrário da versão anterior, conhecida como IPv4, que usa apenas 32 bits para o endereço IP.

Existem características básicas similares entre IPv6 e IPv4. Atualmente, diferentes dispositivos usam o IPv6 como endereço de origem e destino para passar pacotes por uma rede e ferramentas como ping work for network testing como o que os usuários também fazem com o IPv4 com variações mínimas. O IPv6 está em funcionamento há anos, a fim de resolver os lapsos e as quedas de endereços IPv4.

Funcionalidade

A última versão do IPv6 utiliza um recurso especial chamado auto-configuração. Isso funciona para procurar e atribuir a configuração do endereço IP a hosts para a rede. Pode ser apátrida, como o DHCPv6, e também pode ser apátrida. Este recurso especial ajuda de uma forma que permite que dispositivos diferentes de uma rede se dirijam a si mesmos com um endereço unicast link-local. É uma idéia muito comum que cada dispositivo em uma rede Ethernet tenha um endereço de interface. O processo começa com o roteador de rede que obtém o dispositivo de rede, o endereço da interface de prefixo ou o endereço físico do Mac; e continua adicionando seu próprio endereço da interface de prefixo. É preciso lembrar, o tempo todo, que o endereço IPv6 tem 64 bits de comprimento e o endereço mac é de 48 bits. Assim, há 16 bits extras e esses 16 bits extras serão adicionados no centro do endereço mac com o FFFE para completar o recurso de auto-configuração do endereço IPv6 do dispositivo Ethernet. Assim, o IPv6 está realmente bem equipado com tantas características melhoradas e oportunidades ilimitadas, ao contrário do IPv4.

Tipos

A seguir estão os tipos de endereços IPv6:

Endereço Global Unicast

Este tipo de endereço IPv6 é globalmente único na Internet. Isto é semelhante aos endereços públicos do IPv4. É roteável na internet e tem 2 partes: um ID de sub-rede e um ID de interface. Compartilha o mesmo formato de endereço que um endereço anycast IPv6. Esse endereço é atribuído pela Internet Assigned Numbers Authority (IANA).

Endereço local único

Este endereço tem um propósito similar ao do endereço privado do IPv4. Este é o endereço que pode ser usado dentro de uma sociedade empresarial em vários locais. Isto também não se destina a ser encaminhado na internet pública. Este endereço é a substituição do endereço do site-local que permite a comunicação dentro do site enquanto é roteável para várias redes locais.

Endereço Unicast

Refere-se a um endereço IPv6 um-para-um. Isto simplesmente significa que o endereço de pacotes para um endereço unicast é destinado apenas para uma única interface.

Anycast

Isto é semelhante a um endereço multicast com apenas uma ligeira diferença. Isto é usado para endereçar pacotes destinados a múltiplas interfaces, mas envia pacotes para a primeira interface que irá encontrar como o que é definido na distância de roteamento.

Link - endereço local

Refere-se a um endereço privado que não se destina a ser encaminhado na Internet. Este tipo de endereço IPv6 pode ser usado localmente por redes locais (LAN) privadas ou temporárias para compartilhar e distribuir os arquivos entre diferentes dispositivos na LAN.

Endereço multicast

Isto refere-se a um para muitos. Com este tipo, os pacotes são entregues em todas as interfaces que serão identificadas pelo endereço multicast.

Comparação IPv4 e IPv6

A seguir estão as diferenças entre IPv6 e IPv4:

Características	IPv4	IPv6
Comprimento do endereço de bit	32-bit	128-bit
Configuração do endereço	Suporta configuração manual e de endereço DHCP	Suporta configuração automática e renumeração de endereços
Capacidade de integridade de conexão ponta a ponta	Inatingível	Realizável
Representação de endereços	Em decimal	Hexadecimal
Campo de soma de controle	Disponível	Não disponível
Criptografia e Autenticação	Não fornecido	Fornecido

IPv4

Além disso, o mais recente IPv6 oferece mais funcionalidades. Simplifica aspectos da configuração de endereços, renumeração de redes e anúncios de roteadores. Ele também simplifica o processamento de pacotes em roteadores através da colocação da responsabilidade pela fragmentação de pacotes nos endpoints. Ele pode lidar com pacotes de forma mais eficiente, melhora o desempenho e aumenta a segurança. E permite que os provedores de serviços de internet reduzam o tamanho das tabelas de roteamento, tornando-as mais hierárquicas.

Com isso, o rápido crescimento dos dispositivos móveis, incluindo telefones celulares, computadores e dispositivos manipulados sem fio, criou a necessidade de blocos adicionais de endereços IP, razão pela qual o IPv6 é realmente benéfico de muitas maneiras. Uma melhoria importante em relação ao IPv4 é o suporte nativo de dispositivos móveis. Com o IPv6, suporta o protocolo IPv6 móvel, que permite realmente que diferentes dispositivos móveis alternem entre redes diferentes e recebam uma notificação de roaming sem ter em conta a localização física. O protocolo IPv6 realmente melhora o IPv4 com o aumento das medidas de autenticação e privacidade. Desta forma, o IPv6 pode realmente fornecer um quadro de segurança eficiente de extremo a extremo para a transferência de dados a nível do host ou da rede. A implantação do mais recente IPv6 está realmente a crescer em todo o mundo. A substituição completa do antigo IPv4 demorará algum tempo, uma vez que continua a ser a versão mais comum e amplamente utilizada do Protocolo

Internet.

História da empresa

Recentemente, os protocolos de internet que são construídos em sistemas modernos dependem de tecnologias mais complexas e intrincadas que são baseadas em desenvolvimentos feitos a partir do protocolo do ARPANET (Advanced Research and Project Agency Network) NCP (Network Control Program). Vinton Cerf e Robert Kahn são conhecidos como os antepassados do TCP/IP (Transmission Control Protocol / Internet Protocol). Trabalhando com o TCP, o IP foi introduzido como um datagrama que não dependia de um protocolo conectado, mas continha um cabeçalho e uma carga útil. O cabeçalho codificou os endereços de origem e de destino do pacote de dados, enquanto a carga útil transportava os dados reais. Cerf e Kahn trabalharam com a Agência do Departamento de Defesa dos EUA no ping da primeira versão principal do IP que ainda é amplamente utilizada atualmente - IPv4.

Mais especificamente, o IPv4 foi implantado pela primeira vez em 1983 para a produção na ARPANET. O IPv4 é descrito na publicação RFC 791 da IETF em 1981, substituindo uma definição anterior em 1980. No entanto, o governo dos Estados Unidos chegou à conclusão de que os endereços IPv4 apresentavam um conjunto limitado de endereços, apenas cerca de 4 bilhões de combinações possíveis, para os 7 bilhões de pessoas no mundo e começou uma nova versão que agora está sendo integrada às redes existentes - o IPv6. Quando o IPv6 se destinava a substituir o IPv4, o IPv6 tinha-se tornado um padrão preliminar para a IETF em 1998. Posteriormente, foi ratificado como norma da internet em 14 de julho de 2017.

Entendendo o IPv6

IPv6 nada mais é do que a nova versão dos endereços IP. Ele veio resolver alguns problemas que o IPv4 apresentava, como, por exemplo, o esgotamento de endereços IPv4 disponíveis.

Como o aumento do número de dispositivos conectados a internet, os endereços disponíveis foram chegando ao fim. Algumas técnicas como o NAT atrasaram um pouco a mudança, porém com o crescimento acelerado de dispositivos conectados, os endereços disponíveis foram acabando.

O computador entende bits. Ou seja, tudo que passamos para o computador é traduzido para zeros e um. Com os endereços IPs acontece o mesmo.

No endereço IPv4, por exemplo, 192.168.0.1, temos quatro grupos, ou octetos, nos quais podemos utilizar números para escrever o endereço. Cada octeto é um conjunto de oito bits. Logo, temos 32 bits disponíveis para escrever um endereço. Ou, aproximadamente, 4,2 bilhões de endereços.

Já com o IPv6, temos oito grupos, porém esses grupos não são divididos em oito bits cada, mas em 16 bits, separados por dois pontos (:). Portanto, temos 128 bits disponíveis para escrever nosso endereço. Logo, temos, aproximadamente, 340 undecilhões de endereços. Ou, 3,4 x 10^38 endereços.

Isso significa que temos endereços praticamente inesgotáveis. Por ser um valor muito grande, em vez de utilizar valores decimais, nós representamos os endereços IPv6 com valores hexadecimais. Ou seja, números de 0 a 9 e letras de A a F.

Cada grupo de 16 bits, também chamado de decahexateto, ou duocteto, possui quatro símbolos hexadecimais. Portanto, percebemos que cada símbolo hexadecimal representa 4 bits.

Sabendo disso, podemos escrever um endereço IPv6 dessa forma: 2001:0BAA:0000:0000:0000:24D2:12AB:98BC. Oito grupos, com quatro símbolos hexadecimais separados por dois pontos (:).

"Esse endereço é muito maior que um endereço IPv4, não é complicado lê-lo?"

De fato, os endereços IPv6 são maiores que os endereços IPv4, por isso foram criadas algumas

regras de abreviação.

Abreviando o IPv6

Nós podemos omitir os zeros a esquerda quando estamos escrevendo o endereço. Dessa forma, escrevendo novamente o endereço, teremos este resultado 2001:BAA:0:0:0:24D2:12AB:98BC

Já fica um pouco menor, porém conseguimos encurtar mais o endereço. Quando temos uma sequência de blocos com valor zero, conseguimos abreviá-las digitando duas vezes dois pontos (::). Aplicando essa regra, nosso endereço fica assim:

2001:BAA::24D2:12AB:98BC

Contudo, devemos prestar atenção, pois essa regra só pode ser usada uma única vez. Isso porque se tivermos duas vezes essa abreviação, os equipamentos de rede não conseguirão saber a posição precisa de cada grupo.

Por exemplo, vamos imaginar o seguinte endereço:

2001:AB14::1205::35FE

Qual a posição do grupo 1205? Esse endereço pode ficar tanto assim:

2001:AB14:0000:0000:1205:0000:0000:35FE

quanto assim:

2001:AB14:0000:0000:0000:1205:0000:35FE

Por isso só podemos utilizar essa abreviação uma única vez.

Outra coisa que muda em relação ao IPv4 é a máscara de rede. No IPv6 utilizamos a notação CIDR para dizer qual parte do endereço pertence a rede e qual parte pertence ao host. Essa notação diz qual parte do endereço pertence a rede e qual pertence ao host.

Dessa forma, deixa de existir máscaras de sub-rede. Já que a identificação da rede está no próprio endereço.

Legal, já sabemos como funciona o endereço IPv6, mas como eu posso configurá-lo?

A configuração do IPv6 é parecida com a do IPv4. Vamos ver sua configuração em um roteador Cisco.

Portas

terça-feira, 16 de junho de 2020 10:50

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.

Os protocolos que usam principalmente portas são os protocolos da camada de transporte, tais como o Protocolo de controle de transmissão (TCP) e User Datagram Protocol (UDP) do conjunto de protocolos da internet. A porta é identificada por um protocolo, com um número de 16 bits, vulgarmente conhecido como port number(número de porta). O port number é adicionado a um endereço de IP do computador, completando o endereço de destino para uma sessão de comunicação. Isto é, os pacotes de dados são encaminhados através da rede para um endereço de IP de destino específico, e em seguida, ao atingir o computador de destino, são encaminhados para o processo específico ligado ao número de porta de destino.

Note que é a combinação de endereço de IP e um número de porta, devem ser únicos, então, IP's e protocolos podem usar o mesmo número de porta para se comunicar. Isto é, em um dado host ou interface, o UDP e TCP precisam ter o mesmo número de porta, ou em um host com duas interfaces ambos podem estar associados a uma porta com o mesmo número.

Das milhares de portas numeradas, cerca de 250 das portas conhecidas são reservadas por convenção para identificar os tipos de serviços específicos em um host. No modelo cliente-servidor de arquitetura de aplicação, as portas são usadas para fornecer um serviço de multiplexação em cada número da porta do lado do servidor que os clientes da rede conectam para início do serviço, após o qual a comunicação pode ser restabelecida em outros números específicos de conexão de porta.

llllllwm2A controladora de status da porta com as seguintes cores e legendas.:

- Oficial se a aplicação e a combinação da porta está no IANA list of port assignments;
- Não-oficial se a aplicação e a combinação de porta não está na lista de portas do IANA; e
- **Conflito** se a porta é utilizada usualmente por dois ou mais protocolos.
- **EPI** se a porta é utilizada como padrão interno.

Portas 0 a 995

Porta	Descrição	Status
0/TCP,UDP	Reservada.	Fora de Serviço
1/TCP,UDP	TCPMUX (Serviço de porta TCP multiplexador)	Oficial
2/TCP,UDP	iConnect Telecom (Porta de Serviço) http://www.iconnect.net.br/	Não-

		oficial
5/TCP,UDP	RJE (Remote Job Entry - Entrada de trabalho remoto)	Oficial
7/TCP,UDP	ECHO protocol (Serviço Echo)	Oficial
9/TCP,UDP	DISCARD protocol (Serviço zero para teste de conexão)	Oficial
11/TCP,UDP	SYSTAT protocol (Serviço de Estado do Sistema para listar as portas conectadas)	Oficial
13/TCP,UDP	DAYTIME protocol (Envia data e hora para a máquina requerente)	Oficial
17/TCP,UDP	QOTD protocol (Envia a citação do dia para a máquina conectada)	Oficial
18/TCP,UDP	Message Send Protocol (Protocolo de envio de mensagem)	Oficial
19/TCP,UDP	CHARGEN protocol (Character Generator Protocol - Protocolo de geração de caracter)	Oficial
20/TCP	FTP (File Transfer protocol - Protocolo de transferência de arquivo) - Porta de dados do FTP	Oficial
21/TCP	FTP (File Transfer protocol - Protocolo de transferência de arquivo) - Porta do Protocolo de Transferência de Arquivos	Oficial
22/TCP,UDP	SSH (Secure Shell - Shell seguro) - Usada para logins seguros, transferência de arquivos e redirecionamento de porta	Oficial
23/TCP,UDP	Telnet protocol - Comunicação de texto sem encriptação	Oficial
25/TCP,UDP	SMTP (Simple Mail Transfer Protocol - Protocolo simples de envio de e-mail) - usada para roteamento de e-mail entre servidores (Atualmente é utilizada a porta 587,conforme Comitê Gestor da Internet no Brasil CGI.br	Oficial
26/TCP,UDP	RSFTP - protocolo similar ao FTP	Não-oficial
35/TCP,UDP	QMS Magicolor 2 printer	Não-oficial
37/TCP,UDP	TIME protocol (Protocolo de Tempo)	Oficial
38/TCP,UDP	Route Access Protocol (Protocolo de Acesso ao roteador)	Oficial
39/TCP,UDP	Resource Location Protocol (Protocolo de localização de recursos)	Oficial
41/TCP,UDP	Graphics (gráficos)	Oficial
42/TCP,UDP	Host Name Server (Servidor do Nome do Host)	Oficial
42/TCP,UDP	WINS [3]	Não-oficial/ Conflito
43/TCP	WHOIS (protocolo de consulta de informações de contato e DNSprotocol)	Oficial
49/TCP,UDP	TACACS Login Host protocol(Protocolo de Login no Host)	Oficial
53/TCP,UDP	DNS (Domain Name System - Sistema de nome de domínio)	Oficial
57/TCP	MTP, Mail Transfer Protocol (Protocolo de transferência de e-mail)	
67/UDP	BOOTP (BootStrap Protocol) server; também utilizada por DHCP (Protocolo de configuração dinâmica do Host)	Oficial
68/UDP	BOOTP client; também utilizada por DHCP	Oficial
69/UDP	TFTP(Trivial File Transfer Protocol) (Protocolo de transferência de arquivo trivial)	Oficial
70/TCP	Gopher (Protocolo para indexar repositórios)	Oficial
79/TCP	Finger protocol (Serviço finger para informações de contato do usuário)	Oficial
80/TCP	HTTP (HyperText Transfer Protocol - Procolo de transferência de HiperTexto) -	Oficial

	usada para transferir páginas WWW	
80/TCP	HTTP Alternate (HyperText Transfer Protocol - Protocolo de transferência de HiperTexto)	Oficial
81/TCP	Skype protocol	Oficial
81/TCP	Torpark - Onion routing ORport	Não-oficial
82/UDP	Torpark - Control Port	Não-oficial
88/TCP	Kerberos (Protocolo de comunicações individuais seguras e identificadas) - authenticating agent	Oficial
101/TCP	HOSTNAME (Serviços de nomes para máquinas SRI-NIC)	
102/TCP	ISO-TSAP protocol (Aplicações de rede do Ambiente de Desenvolvimento ISO (ISODE)	
107/TCP	Remote Telnet Service (Serviço remoto Telnet)	
109/TCP	POP (Post Office Protocol): Protocolo de Correio Eletrônico, versão 2	
110/TCP	POP3 (Post Office Protocol version 3): Protocolo de Correio Eletrônico, versão 3 - usada para recebimento de e-mail	Oficial
111/TCP,UDP	sun protocol (Protocolo da Chamada de Procedimento Remoto (RPC) para execução de comandos remotos, usado pelo Sistema de Arquivo de Rede (NFS)	Oficial
113/TCP	ident - antigo identificador de servidores, ainda usada em servidores IRC para identificar seus usuários	Oficial
115/TCP	SFTP, (Simple File Transfer Protocol) (Protocolo de simples transferência de arquivo)	
117/TCP	UUCP-PATH (Serviços da Localidade do Protocolo de Cópia Unix-para-Unix)	
118/TCP,UDP	SQL Services	Oficial
119/TCP	NNTP (Network News Transfer Protocol) (Protocolo de transferência de notícias na rede) - usada para recebimento de mensagens de newsgroups	Oficial
123/UDP	NTP (Network Time Protocol) (Protocolo de tempo na rede) - usada para sincronização de horário	Oficial
135/TCP,UDP	EPMAP (End Point Mapper) / Microsoft RPC Locator Service (Microsoft RPC Serviço de localização)	Oficial
137/TCP,UDP	NetBIOS NetBIOS Name Service	Oficial
138/TCP,UDP	NetBIOS NetBIOS Datagram Service (Serviço de datagrama NetBios)	Oficial
139/TCP,UDP	NetBIOS NetBIOS Session Service (Serviço de sessão NetBios)	Oficial
143/TCP,UDP	IMAP4 (Internet Message Access Protocol 4) (Protocolo de Acesso a mensagens na Internet) - usada para recebimento de e-mail	Oficial
152/TCP,UDP	BFTP, Background File Transfer Program (Protocolo de transferência de arquivo em Background(fundo)	
153/TCP,UDP	SGMP, Simple Gateway Monitoring Protocol (Protocolo de simples monitoramento do gateway)	
156/TCP,UDP	SQL Service (Serviço SQL)	Oficial
158/TCP,UDP	DMSP, Distributed Mail Service Protocol (Protocolo de serviço de e-mail distribuído)	
161/TCP,UDP	SNMP (Simple Network Management Protocol) (Protocolo simples de gerenciamento de rede)	Oficial
162/TCP,UDP	SNMPTRAP	Oficial

170/TCP	Print-srv (Print Server)	
179/TCP	BGP (Border Gateway Protocol)(Protocolo de Gateway de Borda)	Oficial
194/TCP	IRC (Internet Relay Chat)	Oficial
201/TCP,UDP	AppleTalk Routing Maintenance	
209/TCP,UDP	The Quick Mail Transfer Protocol (Protocolo de rápida transferência de mail)	
213/TCP,UDP	IPX (Internetwork Packet Exchange) (Troca de pacote na área de trabalho da internet)	Oficial
218/TCP,UDP	MPP, Message Posting Protocol (Protocolo de postagem de mensagem)	
220/TCP,UDP	IMAP, Interactive Mail Access Protocol, version 3 (Protocolo de acesso interativo ao mail)	
259/TCP,UDP	ESRO, Efficient Short Remote Operations (Operações remotas de curta eficiência)	
264/TCP,UDP	BGMP, Border Gateway Multicast Protocol	
311/TCP	Apple Server-Admin-Tool, Workgroup-Manager-Tool, (Ferramenta de gerenciamento de workgroup)	
318/TCP,UDP	TSP, Time Stamp Protocol	
323/TCP,UDP	IMMP, Internet Message Mapping Protocol (Protocolo de mapeamento de mensagem da internet)	
383/TCP,UDP	HP OpenView HTTPs Operations Agent	
366/TCP,UDP	SMTP, Simple Mail Transfer Protocol (Protocolo de simples transferência de mail). ODMR, On-Demand Mail Relay	
369/TCP,UDP	Rpc2portmap	Oficial
371/TCP,UDP	ClearCase albd	Oficial
384/TCP,UDP	A Remote Network Server System (Sistema servidor de rede remota)	
387/TCP,UDP	AURP, AppleTalk Update-based Routing Protocol	
389/TCP,UDP	LDAP (Lightweight Directory Access Protocol)(Protocolo de acesso a diretório lightweight)	Oficial
401/TCP,UDP	UPS Uninterruptible Power Supply (Suprimento de potência Ininterruptível)	Oficial
411/TCP	Direct Connect (Rede de conexão direta, Conexão direta) Hub port	Não-oficial
412/TCP	Direct Connect Client-To-Client port	Não-oficial
427/TCP,UDP	SLP (Service Location Protocol) (Protocolo de serviço de localização)	Não-oficial
443/TCP	HTTPS - HTTP Protocol over TLS/SSL (transmissão segura)(Camada de transporte seguro)	Oficial
444/TCP,UDP	SNPP, Simple Network Paging Protocol (Protocolo simples de paging de rede)	
445/TCP	Microsoft-DS (Active Directory, Windows shares, Sasser (vírus), Agobot, Zobotworm	Oficial
445/UDP	Microsoft-DS SMB (Bloco de mensagem de servidor) file sharing	Oficial
464/TCP,UDP	Kerberos Change/Set password	Oficial
465/TCP	SMTP over SSL - Conflito registrado com protocolo Cisco	Conflito
500/TCP,UDP	ISAKMP, IKE-Internet Key Exchange	Oficial
502/TCP,UDP	Modbus, Protocol	
512/TCP	exec, Remote Process Execution (Processo de execução remota)	

512/UDP	comsat, together with biff: notifica usuários acerca de novos e-mail's não lidos	
513/TCP	Login	
513/UDP	Who	
514/TCP	rsh protocol(protocolo de shell remoto) - usado para executar linha de comando não interativa em sistema remoto e visualizar a tela de retorno	
514/UDP	syslog protocol - usado para log do sistema	Oficial
515/TCP	Line Printer Daemon protocol - usada em servidores de impressão LPD	
517/UDP	Talk	
518/UDP	NTalk	
520/TCP	efs	
520/UDP	Routing - RIP (Protocolo de informação do roteador)	Oficial
513/UDP	Router	
524/TCP,UDP	NetWare Core Protocol (NCP) (Protocolo de core do NetWare)	Oficial
525/UDP	Timed, Timeserver	
530/TCP,UDP	RPC (Procedimento de chamada remota)	Oficial
531/TCP,UDP	AOL Instant Messenger, IRC Mensageiro instantâneo AOL	Não-oficial
532/TCP	netnews	
533/UDP	netwall, For Emergency Broadcasts	
540/TCP	UUCP (Unix-to-Unix Copy Protocol)	Oficial
542/TCP,UDP	commerce (Commerce Applications)	Oficial
543/TCP	klogin, Kerberos login	
544/TCP	kshell, Kerberos Remote shell	
546/TCP,UDP	DHCPv6 client	
547/TCP,UDP	DHCPv6 server	
548/TCP	AFP (Apple Filing Protocol) (Protocolo de arquivamento da Apple)	
550/UDP	new-rwho, new-who	
554/TCP,UDP	RTSP (Real Time Streaming Protocol) (Protocolo de streaming em tempo real)	Oficial
556/TCP	Remotefs, rfs, rfs_server	
560/UDP	rmonitor, Remote Monitor (Monitor remoto)	
561/UDP	monitor	
563/TCP,UDP	NNTP protocol over TLS/SSL (NNTPS)	Oficial
587/TCP	email message submission (SMTP) (RFC 2476)	Oficial
591/TCP	FileMaker 6.0 Web Sharing (alternativa ao HTTP)	Oficial
593/TCP,UDP	HTTP RPC Ep Map	Oficial
604/TCP	TUNNEL	
631/TCP,UDP	IPP, (Internet Printing Protocol) (Protocolo de impressão na internet)	
636/TCP,UDP	LDAP sobre SSL	Oficial
639/TCP,UDP	MSDP, Multicast Source Discovery Protocol (Protocolo de descoberta de fonte multicast)	
646/TCP	LDP, Label Distribution Protocol (Protocolo de distribuição de rótulo)	

647/TCP	DHCP Failover Protocol	
648/TCP	RRP, Registry Registrar Protocol (Protocolo de registro)	
652/TCP	DTCP, Dynamic Tunnel Configuration Protocol (Protocolo de configuração dinâmica de túnel)	
654/TCP	AODV, Ad hoc On-Demand Distance Vector	
665/TCP	sun-dr, Remote Dynamic Reconfiguration (Reconfiguração remota dinâmica)	Não-oficial
666/UDP	Doom, First online first-person shooter	
674/TCP	ACAP, Application Configuration Access Protocol (Protocolo de acesso a configuração da aplicação)	
691/TCP	MS Exchange Routing	Oficial
692/TCP	Hyperwave-ISP	
694/UDP	Linux-HA High availability Heartbeat port	Não-oficial
695/TCP	IEEE-MMS-SSL	
698/TCP	OLSR, Optimized Link State Routing	
699/TCP	Access Network	
700/TCP	EPP, Extensible Provisioning Protocol (Protocolo de provisionamento extensível)	
701/TCP	LMP, Link Management Protocol (Protoloco de gerenciamento de link)	
702/TCP	IRIS over BEEP	
706/TCP	SILC, Secure Internet Live Conferencing (Conferência ao vivo da seguraça da internet)	
711/TCP	TDP, Tag Distribution Protocol (Protocolo de distribuição de marcadores)	
712/TCP	TBRPF, Topology Broadcast based on Reverse-Path Forwarding	
720/TCP	SMQP, Simple Message Queue Protocol (Protocolo de simples mensagem em fila)	
749/TCP, UDP	kerberos-adm, Kerberos administration	
750/UDP	Kerberos version IV	
782/TCP	Conserver serial-console management server	
829/TCP	CMP (Certificate Management Protocol)	
860/TCP	iSCSI	
873/TCP	rsync File synchronisation protocol	Oficial
901/TCP	Samba Web Administration Tool (SWAT)	Não-oficial
902	VMware Server Console[1]	Não-oficial
904	VMware Server Alternate (se a porta 902 estiver em uso - ex: SUSE linux)	Não-oficial
911/TCP	Network Console on Acid (NCA) - local tty redirection over OpenSSH	
981/TCP	SofaWare Technologies Remote HTTPS management for firewall devices running embedded Checkpoint Firewall-1 software	Não-oficial
989/TCP,UDP	FTP Protocol (data) over TLS/SSL	Oficial
990/TCP,UDP	FTP Protocol (control) over TLS/SSL	Oficial
991/TCP,UDP	NAS (Netnews Admin System)	

992/TCP,UDP	Telnet protocol over TLS/SSL	Oficial
993/TCP	IMAP4 sobre SSL (transmissão segura)	Oficial
995/TCP	POP3 sobre SSL (transmissão segura)	Oficial