NOÇÕES BÁSICAS DE REDE

Financiado pela União Europeia. Os pontos de vista e as opiniões expressas são as do(s) autor(es) e não refletem necessariamente a posição da União Europeia ou da Agência de Execução Europeia da Educação e da Cultura (EACEA). Nem a União Europeia nem a EACEA podem ser tidos como responsáveis por essas opiniões.

Índice

1. Introdução

Cibersegurança, o que é isso? O que é isso e por que é tão importante? Em uma época em que a tecnologia nunca sai de nosso lado e somos confrontados com ela praticamente em todos os lugares, não podemos esquecer nossa segurança cibernética neste mundo digital tão confortável. On-line, não somos invisíveis e nossas atividades deixam vários traços ou informações atrás de nós. Praticamente todos os dias usamos as facilidades da Internet, seja em redes sociais, fóruns ou em todos os tipos de plataformas de venda. Onde compartilhamos nossos dados pessoais e financeiros, enviamos números de conta, pagamos com cartões, telefones e várias moedas digitais. Quais são os perigos que se escondem na Internet? Roubo de identidade, clonagem de cartões de pagamento, perda de arquivos/dados privados, phishing de contas bancárias, fraude. Na vida real, nós nos mantemos seguros, olhamos por nós mesmos, compramos remédios, antecipamos. Por que não fazemos isso on-line? Quantos de vocês têm um anti-vírus instalado em seu computador? Todos eles? E em seu telefone? Alguém? Aqui devemos nos perguntar se realmente passamos a maior parte do nosso tempo na web em frente a uma tela de computador ou talvez em nosso telefone? De acordo com várias estatísticas, mais de 70% de todo o tráfego na web já vem de dispositivos móveis, principalmente nossos smartphones. Você já comprou algo em seu telefone ou já o usou para inserir suas informações de faturamento para várias transações? Dispositivos devidamente preparados para a web são apenas a metade da batalha; o outro fator que garante a segurança relativa é a conscientização do usuário da internet. Você pode ser o mais bem preparado e ter o melhor equipamento, mas mesmo assim sem o know-how certo você pode criar muitos problemas desnecessários e desagradáveis para si mesmo.

1.1. Comunicação em rede

Hoje, poucos podem imaginar o mundo ao nosso redor sem computadores, telefones e muitos outros produtos eletrônicos de consumo. Estes dispositivos nos oferecem uma infinidade de funções e capacidades para facilitar nossas atividades diárias, assim como para nos ajudar em nosso trabalho e estudo. Muitas destas funções seriam inúteis sem um aspecto importante, a capacidade de comunicar e trocar dados rapidamente.

Graças a esta possibilidade, somos capazes de alcançar amigos que estão atualmente do outro lado do mundo em poucos segundos, pagar a conta de eletricidade em poucos segundos ou comprar novos treinadores sem sair de casa. É claro que não vou discutir aqui todas as vantagens do acesso à Internet, pois este não é o tema principal do curso, mas espero que você perceba que tudo o que você pode fazer com seu computador ou smartphone tem uma coisa em comum. Esse denominador comum é, ou melhor, é a rede de computadores, que foi criada há décadas e é a base da Internet de hoje.

O que é a Internet hoje em dia? Nada mais é do que uma rede de computadores, uma rede muito elaborada com muitos dispositivos conectados, mas ainda assim é uma rede.

2. Conceitos básicos

Vamos definir os termos básicos relacionados às redes de computadores:

Rede de computadores - Uma coleção de dispositivos, tais como computadores, impressoras, telefones e televisores, que estão interligados para o intercâmbio de dados. Um meio de transmissão é usado para conectar os dispositivos e um protocolo de comunicação é usado para transmitir dados.

Endereço IPv4 - Este é um número de 32 bits, inserido em forma decimal para facilitar o uso (por exemplo, 192.168.31.190), para identificar dispositivos e dados de endereço na rede.

HOST - Um dispositivo com um endereço IP que é a fonte ou destinatário dos dados enviados através da rede, ou seja, recebe dados de outros dispositivos ou envia tais dados. O termo host é às vezes usado de forma intercambiável com o termo dispositivo terminal, pois normalmente se refere a um computador, tablet ou smartphone, ou seja, um dispositivo com o qual o usuário da rede tem contato direto.

Cliente - O dispositivo, ou mais precisamente seu software, utiliza os serviços fornecidos pelo servidor. O cliente mais comum atualmente é um navegador web, que permite ao usuário visualizar o conteúdo de páginas web hospedadas por um servidor web. Exemplos de um cliente também incluiriam FileZilla, que permite a troca de arquivos pela Internet, e todo tipo de software de e-mail para facilitar o uso do correio. Os consoles de jogos ou smartphones também serão clientes, desde que estejam conectados à Internet, é claro.

Servidor - Este é um computador com software especializado dedicado instalado para dar suporte a outros computadores. O serviço que um servidor pode fornecer é, por exemplo, um website, e-mail ou recurso de arquivo. Um servidor pode ser qualquer computador no qual tal software esteja instalado e configurado, como APACHE, que é utilizado para manter e compartilhar websites, ou MySQL, que é um sistema de gerenciamento de banco de dados. Um servidor é normalmente um computador dedicado com alto poder de computação capaz de lidar com múltiplas conexões e consultas simultaneamente.

Meio de transmissão - Em outras palavras, o meio que é o elemento de rede através do qual os dispositivos se comunicam entre si e trocam dados. Este meio pode ser cabo de cobre, cabo de fibra ótica e ondas de rádio (WiFi).

Protocolo de comunicação - Este é o método ou linguagem de comunicação e intercâmbio de dados entre dispositivos que define as regras e princípios dessa comunicação.

Internet - É um conjunto de redes interligadas de ampla área que formam uma rede global de computadores. As origens da Internet podem ser rastreadas desde a criação da rede ARPANET no final dos anos 60, e a primeira conexão à Internet na Polônia foi lançada em setembro de 1990. A Internet é vista por muitos como uma coleção de sites para navegar, mas este não é o caso, pois a Internet é uma coleção de muitas redes amplas espalhadas pelo mundo, e os sites são serviços de rede específicos.

Intranet - Esta é uma rede interna privada que utiliza exatamente os mesmos padrões de comunicação (protocolos) da Internet, mas só tem acesso aos usuários autorizados, como funcionários de uma determinada empresa. Na maioria dos casos, o acesso a uma intranet, ou a esta rede interna da empresa, é feito através de um website, portanto, diz-se que a comunicação utiliza os mesmos padrões que a Internet.

Extranet - é uma extensa variedade de intranets que permitem o acesso a seus recursos não apenas aos funcionários de uma determinada empresa, mas também a outros usuários.

DNS (Domain Name System) - Um serviço de rede que muda um nome legível por humanos, conhecido como nome mnemônico, para o endereço IP de um dispositivo em uma rede. É um serviço básico da Internet, mudando os endereços dos sites para os endereços IP correspondentes dos servidores onde esses sites são armazenados, por exemplo, mudando o endereço da Internet onet.pl para o endereço IP 214.180.141.140.

DHCP (Dynamic Host Configuration Protocol) - é um protocolo de configuração automática que atribui um endereço IP, máscara de sub-rede ou endereço de gateway padrão a um host. É o método mais comum de atribuição de endereços IP a computadores em uma rede, pois não requer configuração manual de endereços IP em cada computador.

3. Unidades de dados em redes

A unidade básica usada em computação para armazenar dados é 1 bit [b].

Em redes de computadores, por outro lado, a unidade de bits por segundo é usada para determinar a largura de banda (velocidade) da rede, expressa em b/s ou bps (bits por segundo).

Obviamente 1 bit/s é pequeno, portanto, para usar múltiplos desta unidade para se referir ao tamanho do arquivo, capacidade do disco ou memória operacional, independentemente dos bits e não dos bytes, estes múltiplos são:

1. kilobit [Kb],

2. megabit [Mb],

3. gigabit [Gb],

4. terabit [Tb].

Como em uma rede de computadores a unidade está em bits, ao contrário do tamanho do arquivo ou da capacidade do disco, onde são usados bytes[B] em vez de bits[b], surge aqui um problema de conversão, ou seja, conversão da unidade.

1 byte[B] é igual a 8 bits[b] Portanto, se quisermos o tamanho de um arquivo em bytes, temos que multiplicar o número de bytes por 8. Por exemplo, se quisermos calcular quantos megabytes um arquivo de tamanho 3 MegaBytes contém, multiplicamos seu tamanho por 8. O resultado é 24 MB.

3 MB - 8 = 24 MB

Para a conversão inversa, ou seja, de bits para bytes, precisamos fazer o inverso da multiplicação, ou seja, da divisão. Por exemplo: um arquivo de 40 Mb será convertido para 5 MB.

40 MB ÷ 8 = 5 Mb

A capacidade de converter unidades é mais adequada para realizar cálculos em exemplos específicos. Duas soluções são descritas abaixo.

Exemplo 1

Assumindo que a largura de banda de nossa conexão é fixa em 300 Mb/s, vamos calcular a quantidade de dados que faremos o download da Internet em duas horas.

dados:

Tempo: 2 horas

Largura de banda: 300 Mbps

Calcular:

1. segundos de minutos são multiplicados por minutos:

120 minutos - 60 segundos = 7200 segundos

2. convertemos a unidade de transferência de dados de megabits para megabytes por segundo:

300MB/s ÷ 8 = 37,5MB/s

3. multiplicamos a produção pelo tempo:

37,5 MB/s - 7200 segundos = 270000 MB ~ 270 GB

Resposta ao exemplo 1: Em duas horas, faremos o download de 270 GB.

Exemplo 2

Vamos calcular o tempo que leva para baixar um arquivo de 5 GB, assumindo que a largura de banda de nossa conexão é constante e chega a 300 Mbps.

Dados:

Tamanho do arquivo: 5 GB

Largura de banda da conexão: 300 Mbps

Calcular:

1. converter a unidade de transmissão de dados de megabits para megabytes por segundo:

300 Mb/s ÷ 8 = 37.5 MB/s

2. converter unidades de armazenamento de arquivos de gigabytes para megabytes:

5 GB => 5120 MB

3. Dividir o tamanho do arquivo pelo rendimento:

5120 MB ÷ 37,5 MB / s = 136,5 segundos ~ 2 minutos 16 segundos

Resposta ao exemplo 2: Baixamos um arquivo de 5 GB sobre uma conexão de 300 Mbps em aproximadamente 2 minutos e 16 segundos.

TAREFAS DO FAÇA-VOCÊ-MESMO

- Calcule quando o conteúdo de um DVD (4,7 GB) pode ser transferido através de um link de 50 Mbps.
- Calcule quantos dados podem ser transferidos em uma conexão de 500 Mbps em 15 minutos.

4. Meios de transmissão

Os meios de transmissão são uma questão extremamente importante relacionada às redes de computadores. Há muitas razões para isso, a mais importante das quais é que a escolha do meio certo é a base e a garantia de um funcionamento normal e eficiente das redes de computadores.

4.1. Medium

Em outras palavras, o meio que é o elemento de rede através do qual os dispositivos se comunicam entre si e trocam dados. Este meio pode ser cabo de cobre, cabo de fibra ótica e ondas de rádio (Wi-Fi).

DIVISÃO DOS MEIOS DE TRANSMISSÃO

MODELO	CABO DO COPO	CABO DO COPO	CABO DE FIBRA ÓTICA	CABO DE FIBRA ÓTICA
TIPO	CABO COAXIAL	CABO DE PAR TRANÇADO	FIBRA ÓTICA MONOMODO	FIBRA ÓTICA MULTIMODO

4.2. Cabo coaxial

1. Construção:

- núcleo de cobre,

- isolamento plástico,

- escudo de cobre,

- manga externa.

Termina com um conector chamado BNC. Às vezes, no final de um cabo coaxial, encontramos também o chamado terminador BNC, cuja função é remover os reflexos do sinal transmitido através do cabo.

2. Tipos:

Há dois tipos de cabo coaxial: cabo coaxial fino e cabo coaxial grosso. As diferenças entre as duas variedades são as seguintes:

TIPO	AGRADECIMENTO	COMPRIMENTO MÁXIMO	PADRÃO DE REDE	CAPACIDADE MÁXIMA
CABO FINO	5 mm	185 m	10base-2	10 Mb/s
CABO GROSSO	10 mm	500 m	10base-5	10 Mb/s

Vale ressaltar que o cabo coaxial não é mais utilizado na construção de novas redes. Foi substituída por soluções mais eficientes, tais como par trançado e fibra ótica.

4.3. Cabo de par trançado

1 Construção:

· 8 fios de cobre entrançados em 4 pares,

· Camisa exterior.

É terminado com um conector RJ45, também conhecido como 8P8C.

Dependendo do tipo de cabo de par trançado, existem também folhas e telas de protecção para proteger o cabo de elementos indesejáveis que podem afectar a transmissão de dados, tais como ondas electromagnéticas.

2. tipos de cabos de par trançado:

· UTP - par torcido não blindado,

· FTP - par torcido protegido por folha de alumínio,

· STP - cabo blindado de par trançado.

Na prática, podemos encontrar diferentes variantes dos tipos acima referidos, as mais importantes das quais são as mais importantes:

· U/UTP - par torcido não blindado

· F/UTP - Par torcido de tronco enrolado

· U/FTP - cabo de par torcido com cada par numa tela de alumínio separada,

· F/FTP - par torcido com cada par num ecrã de folha de alumínio separado e, adicionalmente, todo o pacote também num ecrã de folha de alumínio

· S/FTP - par torcido com cada par numa tela de folha separada e, adicionalmente, todo o feixe numa tela de rede O material mais comum utilizado na blindagem de par torcido é a película de poliéster revestida com uma camada de alumínio e cobre.

O tipo de cabo de par trançado que deve ser escolhido para construir uma rede depende do local onde a rede está a funcionar e do nível de interferência electromagnética presente no local. Em pequenas redes locais, seja numa escola ou em casa, o tipo básico de UTP é mais comummente utilizado porque é suficiente para uma rede tão pequena e é também o tipo mais barato de cabo de par entrançado.

3. categorias de cabos de par trançado

Para além dos tipos de pares torcidos, existem classes que definem, entre outras coisas, os padrões de rede em que podem ser utilizados.

CATEGORIA	PADRÃO DE REDE
3	Ethernet 10Base-T
5/5e	Fast Ethernet 100Base-TX Gigabit Ethernet 1000Base-T
6	Gigabit Ethernet 1000Base-T
6a	10-Gigabit Ethernet 10GBase-T
7	10-Gigabit Ethernet 10GBase-T

4 Parâmetros técnicos

· Atenuação do sinal - é a relação entre a tensão de saída e a tensão de entrada, expressa em decibéis [dB]

· Propagação do sinal - Esta é a velocidade do impulso eléctrico em relação à velocidade da luz, expressa como uma percentagem [%].

· Resistência - é a resistência de um cabo à corrente expressa em ohms [Ω].

· Perto de Crosstalk (PRÓXIMO) - trata-se de interferência num determinado conjunto causada pela transmissão de dados num conjunto vizinho Também do ponto de vista da instalação, um parâmetro importante é o raio de curvatura do cabo,

que, para a maioria das soluções, é 4 vezes o seu diâmetro exterior.

4.4. Cabo de fibra óptica

Completamente diferente do meio de transmissão discutido anteriormente é o cabo de fibra óptica, devido aos diferentes materiais utilizados para o núcleo. No caso de cabo coaxial e de par trançado, o núcleo ou fio é de cobre, enquanto que no caso de cabos de fibra óptica estamos a lidar com fibra de vidro. A utilização de fibra de vidro como material de construção do núcleo também requer diferentes tipos de sinais de transmissão. No caso de suportes de cobre, trata-se de corrente eléctrica,

no caso de fibra óptica, luz, sendo o tipo mais utilizado a luz infravermelha. 1 Construção:

- Núcleo - tem um índice de refracção mais elevado,
- Revestimento - tem um índice de refracção mais baixo,
- revestimento de protecção de pintura,
- Revestimento de reforço para proteger o núcleo durante a instalação,
- concha exterior.

Podemos também encontrar os seguintes tipos de conectores:

- LC
- MT - RJ
- MU
- DIN

2 Tipos de fibras ópticas:

Tal como com o cobre e a fibra óptica, podemos discutir os diferentes tipos deste meio. As divisões mais comuns são as fibras ópticas monomodo e multimodo.

No caso de fibras ópticas monomodo, apenas um feixe de luz passa através do núcleo de vidro, resultando no chamado fenómeno de desfocagem do sinal, ou seja, atenuação do sinal.

Utilizando este tipo de fibra óptica, os sinais podem ser transmitidos a longas distâncias sem equipamento de amplificação de sinal.

Na fibra multimodo, uma porção maior do feixe é enviada através do núcleo, resultando num maior grau de desfocagem do sinal em comparação com a fibra monomodo. Isto porque cada feixe enviado através do núcleo deve percorrer um caminho diferente desde o emissor até ao receptor.

É por isso que a fibra óptica multimodo é utilizada em curtas distâncias, até alguns quilómetros.

Outra diferença entre a fibra óptica monomodo e multimodo é o diâmetro do núcleo utilizado. Para a fibra óptica monomodo, este é entre 8 e 10 micrómetros [µm], enquanto que para a fibra óptica multimodo é de 50 ou 62,5 micrómetros.

4.5. Resumo

Utilitários de cobre

BENEFÍCIOS	FALHAS
Barato para comprar	Pequenas distâncias entre nós de rede
Diagnóstico e reparação simples de falhas	Susceptível a electromagnética interferência
Montagem e instalação sem complicações	Mais lento que as fibras ópticas

Meios de fibra óptica

BENEFÍCIOS	FALHAS
Definitivamente mais rápido	Montagem e instalação complicadas
Virtualmente imune a electromagnetismo interferência	Definitivamente mais caro de comprar porque do equipamento necessário
Transfere dados em longas distâncias	Borrão de sinal

Meios de comunicação sem fios

Várias soluções são utilizadas para meios de comunicação sem fios, mas apenas uma delas, ondas de rádio, é realmente utilizada. A conhecida tecnologia Wi-Fi utiliza este meio para a transmissão de dados.

As ondas de rádio são radiação electromagnética na gama de frequências de 3 Hz a aproximadamente 3 THz. As fontes de ondas de rádio podem ser naturais ou artificiais, tais como as emitidas por estações de rádio móveis. O seu principal objectivo é transmitir informação e, no caso das telecomunicações, dados. Existem vários tipos de ondas de rádio, com ondas longas, médias, curtas e ultra-curtas a serem utilizadas para a transmissão de dados.

Ao discutir as ondas de rádio, vale a pena mencionar as normas utilizadas nas redes sem fios. Eles são importantes em termos de escolha do router Wi-Fi correcto.

PADRÃO	FREQÜÊNCIA	MÁXIMA CAPACIDADE DE PRODUÇÃO
802.11a	5 GHz	54 Mbps
802.11b	2,4 GHz	11 Mbps
802.11g	2,4 GHz	54 Mbps
802.11n	2,4 GHz | 5 GHz	150 Mbps | 600 Mbps
802.11ac	5 GHz	Vários Gbps

5. Tipos de Redes de Computadores

As redes informáticas podem ser divididas de várias maneiras, tendo em conta diferentes critérios. A norma básica para subdividir uma rede é pela área em que a rede opera, pelo que a subdivisão por área de rede (cobertura) é a seguinte:

Local Area Network (LAN) - uma rede que cobre a menor área, tal como um estúdio, escola ou vários edifícios escolares. Uma LAN também aparece na sua casa se utilizar mais ou um computador.

Metropolitan Area Network (MAN) - uma rede que cobre uma área maior do que uma sala ou edifício. Uma rede MAN está espalhada por uma cidade ou área metropolitana. Rede de Área Ampla (WAN) - uma rede de área ampla que combina redes LAN e MAN.

Para além das normas regionais, as redes também podem ser divididas de acordo com a sua arquitectura. Fazemos a distinção entre redes com uma arquitectura cliente-servidor e uma arquitectura peer-to-peer.

Numa arquitectura cliente-servidor, existe pelo menos um computador ao serviço dos utilizadores da rede (estes são os servidores) e muitos computadores que utilizam os serviços do servidor (estes são os clientes). Utilizamos a arquitectura cliente-servidor quando navegamos na web, quando enviamos e-mails ou quando trabalhamos com bases de dados.

A situação é diferente com a arquitectura peer-to-peer, também conhecida como Peer2Peer (P2P).

Neste caso, o serviço não é prestado por um ou mais computadores, mas sim por vários computadores com os mesmos direitos. Cada computador da rede pode simultaneamente utilizar e partilhar recursos. Ao utilizar serviços de partilha de ficheiros como o BitTorrent, estamos a utilizar uma arquitectura peer-to-peer.

5.1. Topologias de rede

Dividimos a topologia da rede em física, o que define como os dispositivos estão ligados entre si, e lógica, que descreve a forma como os dados são transferidos entre dispositivos. Cada rede informática, mesmo a mais pequena, tem uma topologia física e lógica, que define como os dispositivos estão ligados entre si e como os dados são transferidos.

Topologia da rede informática define as relações entre os dispositivos da rede, as ligações entre eles e a forma como os dados fluem.

5.2. Topologias físicas

Estas são as topologias básicas que são a base para a construção de topologias alargadas em estrela e malha em grande redes.

Topologia física de autocarros

A topologia do autocarro é caracterizada pelo facto de todos os dispositivos estarem ligados a um meio de transmissão comum. O meio de transmissão comum nesta topologia é o cabo coaxial. Uma desvantagem desta topologia é a baixa taxa de transmissão (até 10 Mbps).

Esta topologia é utilizada para construir uma rede de área local. Utilizo deliberadamente a palavra "foi" aqui porque já não é comummente utilizada. Para além do seu baixo rendimento, é também muito susceptível a falhas na rede. Quando o cabo coaxial se rompe, toda a rede deixa de funcionar. A vantagem indubitável da utilização desta topologia é o baixo custo de implementação, uma vez que não há necessidade de centenas de metros de cabo ou qualquer equipamento intermédio.

Topologia física do anel

Numa topologia em anel, cada dispositivo está ligado aos seus dois vizinhos, formando um círculo fechado. Tal como na topologia do autocarro, este desenho não utiliza um grande número de cabos e equipamento adicional.

Além disso, podem ser utilizados vários meios de transmissão, desde o cabo coaxial ao par trançado de cobre até ao cabo de fibra óptica. A desvantagem desta topologia é que a interrupção do meio ou a falha de um dos computadores pode perturbar toda a rede. Para evitar isto, são utilizados os chamados anéis duplos, ou seja, a duplicação do número de ligações entre dispositivos. Tal topologia é então chamada de topologia de duplo anel.

Topologia física das estrelas

Numa topologia estelar, os dispositivos são ligados a um ponto central, o ponto de acesso à rede. No passado, este ponto era utilizado como um ponto central, mas agora é utilizado um interruptor. É a topologia mais comum em redes locais porque é fácil de conceber, construir e escalar, tolerante a falhas e fácil de gerir.

Outra vantagem é que pode ser construído utilizando uma variedade de meios de transmissão, tais como cobre de par trançado, cabo de fibra óptica ou ondas de rádio (WLAN). No entanto, uma desvantagem significativa pode ser o custo de construção, uma vez que é necessário equipamento adicional (interruptores) e muitos metros de cabo.

5.3. Topologias lógicas

A topologia lógica da rede inclui:

- de ponto a ponto,
- passe a ficha,
- Acesso múltiplo.

Topologia lógica ponto-a-ponto

Numa topologia ponto-a-ponto, os dados só são transmitidos de um dispositivo para outro. Estes dispositivos podem ser ligados uns aos outros directamente, por exemplo, um computador a um interruptor, ou indirectamente, em longas distâncias, utilizando um dispositivo intermédio, por exemplo, ligando dois routers a vários quilómetros de distância.

Em ambos os casos, podemos falar de ligações lógicas ponto-a-ponto. Esta é uma topologia lógica, muitas vezes utilizada em LANs que utilizam uma topologia física estelar.

Topologia lógica para transferência de fichas

Numa topologia com passagem de fichas, os dados são passados sequencialmente para dispositivos de rede. O dispositivo que recebe um lote de dados analisa-o para ver se aponta para ele. Se os dados não se destinarem a ele, encaminhá-los-á para um dispositivo vizinho. Desta forma, todos os dispositivos transferem dados entre dispositivos de origem e de destino.

Topologia lógica de acesso múltiplo

A topologia de multi-acesso (por vezes também chamada de topologia de radiodifusão ou de barramento lógico) permite aos dispositivos de uma rede comunicar através de um único meio físico de transmissão. Foi principalmente utilizado com topologias físicas de bus e de estrelas nas fases iniciais do seu desenvolvimento, quando os hubs ainda eram utilizados como pontos de acesso à rede.

Cada dispositivo nesta topologia pode ver os dados enviados através da rede, pois são enviados para todos os dispositivos, mas apenas o dispositivo específico ao qual os dados são dirigidos pode interpretá-los. Como os dispositivos da rede partilham um meio comum, é necessário implementar mecanismos para controlar o acesso a este meio, estes são: CSMA/CD, CSMA/CA e passe simbólico.

Método de acesso à ligação (rede)

O método CSMA/CD, um método de detecção de colisão, envolve a monitorização do estado da ligação. Se o dispositivo que vai iniciar uma transmissão detecta que a ligação está inactiva, inicia essa transmissão. Se, durante a transferência, detectar que outro dispositivo da rede também está a enviar os seus dados, a transferência será interrompida. Passado algum tempo, tenta de novo a transferência. As versões mais antigas da Ethernet utilizam este mecanismo.

O método CSMA/CA, um método para evitar colisões, também envolve a monitorização do estado da ligação, mas a detecção de que o transportador, ou seja, o dispositivo onde o meio de transmissão está inactivo, começa por enviar informações sobre a sua intenção antes do início da transmissão. Este mecanismo existe nas redes sem fios.

O método de transferência de fichas envolve o envio de uma peça especial de dados chamada ficha ou ficha de dispositivo em dispositivo, cuja posse inicia a transferência.

6. Modelos em camadas ISO/OSI e TCP/IP

A intercomunicação de dispositivos numa rede informática consiste em várias etapas, com vários componentes. Cada uma delas é igualmente importante, uma vez que cada uma executa as tarefas necessárias para uma comunicação adequada. Estas etapas são definidas pelo chamado modelo hierárquico.

Qualquer pessoa familiarizada com o modelo estratificado sabe que a compreensão deste é a base para um maior conhecimento e competências no campo das redes informáticas.

Existem dois modelos em camadas, o modelo de protocolo TCP/IP e o modelo de referência ISO/OSI.

Por um lado, são semelhantes uns aos outros e, por outro, cada modelo comunica de forma ligeiramente diferente. No entanto, antes de discutirmos estes dois modelos e explicarmos as diferenças entre eles, dir-vos-emos

porquê e por que razão os deve utilizar, para que são utilizados e quais são os benefícios da sua utilização.

Dividir o processo de comunicação em rede em camadas traz muitos benefícios, os mais importantes dos quais são

- definição mais fácil das regras e princípios de comunicação (estes são protocolos de comunicação),
- a capacidade de trabalhar com equipamento de rede e software de diferentes fabricantes,
- é mais fácil de compreender a possibilidade de todo o processo de comunicação,
- capacidade de gerir o processo de comunicação.

Antes dos dados do dispositivo de origem chegarem ao dispositivo final, este tem de percorrer um longo caminho, durante o qual é primeiro devidamente etiquetado, etiquetado, descrito com informação específica que permita a sua identificação, e depois transferido entre vários dispositivos intermediários até chegar ao destinatário, que deve então traduzi-lo.

Sem tal modelo, que divide a comunicação em mais pequena, mais compreensível e mais manejável de gestão e define as tarefas que precisam de ser realizadas em cada camada, será difícil gerir adequadamente a comunicação em rede, porque as numerosas soluções e tecnologias criam um enorme caos, descontrolado. Imagine uma situação em que não existe tal acumulação, não existem regras que descrevam a comunicação, e cada fabricante de hardware e software cria o seu próprio sistema independente.

Claro que, na solução de uma empresa, a comunicação será muito eficiente e rápida, mas as soluções de duas empresas separadas podem ser incompatíveis entre si. Na prática, utilizamos hardware e software de rede de diferentes empresas, graças à divisão em camadas separadas com regras e tarefas que descrevem o seu funcionamento. Estas regras e tarefas são as mesmas para todos, mas cada empresa, cada fabricante, seja hardware ou software, pode implementá-las à sua própria maneira.

Um exemplo típico são os sistemas operativos. Alguns utilizadores usam Windows, alguns vêm de uma distribuição Linux e outros de MacOS. Cada um destes sistemas é diferente e cada um executa tarefas na web de uma forma diferente, mas em última análise em cada um destes sistemas, uma página web ou e-mail terá o mesmo aspecto ou, pelo menos, semelhante. Portanto, alguns dos benefícios mais importantes da utilização do modelo hierárquico incluem:

- gestão do processo de comunicação em rede,
- definir as suas regras e tarefas,
- interoperabilidade a nível do hardware e software entre produtos de rede de diferentes fabricantes,
- e controlar a correcção da comunicação.

Agora que conhecemos a finalidade dos modelos hierárquicos, passemos à discussão das suas características mais importantes. Ambos os modelos tiveram origem há muito tempo, na década de 1970, mas ainda são actuais e estão em uso hoje. O primeiro é o modelo TCP/IP, conhecido como o modelo protocolar. Cada uma das suas camadas executa tarefas específicas utilizando protocolos específicos. Por outro lado, os modelos ISO/OSI, conhecidos como modelos de referência, são mais comummente utilizados para análise a fim de melhor compreender os processos de comunicação que ocorrem numa rede e são modelos para a concepção de soluções de rede, tanto de hardware como de software.

No caso do modelo TCP/IP, podemos distinguir 4 camadas, que são Aplicação, Transporte, Internet e Acesso à Rede.

A camada de aplicação permite aos utilizadores utilizar serviços web tais como a web, e-mail, partilha de ficheiros, ligações a terminais e mensagens instantâneas. Digo sempre aos meus alunos que esta é a camada mais próxima do utilizador porque nos permite tirar o máximo partido dos benefícios dos serviços web modernos. Por exemplo, quando nos sentamos em frente de um computador e lançamos um navegador web, estamos a utilizar o a teia ao nível da camada de aplicação.

Abaixo desta encontra-se a camada de transporte, cuja principal tarefa é tratar a comunicação entre dispositivos de forma eficiente. Nesta camada, os dados são divididos em partes mais pequenas, e depois complementadas com informações adicionais, permitindo a sua distribuição à aplicação apropriada no dispositivo alvo e a sua montagem no dispositivo alvo no na ordem correcta.

Depois há a camada da Internet, cuja principal tarefa é encontrar o mais curto e a rota mais rápida para o dispositivo alvo através da WAN, muito semelhante ao GPS de um carro, mas também usa endereços lógicos (endereços IP) para endereçar os dados.

Finalmente, temos a camada de acesso à rede, que codifica os dados como bits puros (zeros e uns) e passa-os para o meio de transmissão e dirige-se a eles, desta vez através de um endereço físico (endereço MAC).

O modelo ISO/OSI consiste em 7 camadas (aplicação, apresentação, sessão, transporte, rede, ligação de dados, física).

Na extremidade superior deste modelo, podemos distinguir a camada de aplicação, que funciona aqui de forma muito semelhante ao modelo TCP/IP, na medida em que permite que as aplicações de rede sejam utilizadas pelos utilizadores finais da rede.

Depois há a camada de apresentação, que transmite informação à camada de aplicação sobre o formato de dados utilizado, por exemplo, informa que tipos de ficheiros serão transmitidos, e é responsável pela correcta codificação dos dados no dispositivo de origem e descodificação no dispositivo de destino.

Abaixo desta é a camada de sessão, que gere as sessões dos utilizadores através de website ou comunicação vídeo, por exemplo.

Indo um passo mais além, temos a camada de transporte, que mais uma vez é exactamente a mesma do modelo TCP/IP e em ambos os casos a função desta camada é exactamente a mesma.

Depois há a camada de rede, que é o equivalente da camada de Internet do modelo TCP/IP, ou seja, funções muito semelhantes, como o endereçamento e a determinação do melhor caminho para transmitir dados.

A seguir temos a camada de ligação de dados, cuja tarefa principal é controlar o acesso ao meio de transmissão e abordar os dados, mas desta vez para os transportar entre anfitriões na LAN.

Finalmente, a camada física codifica os dados em bits puros (1s e 0s) e transmite-os através do meio de transmissão para o dispositivo apropriado.

Os dois modelos são muito semelhantes. A diferença resultante pode ser vista nas camadas superiores; no caso do modelo ISO/OSI, está dividido em 3 camadas, enquanto no caso do modelo TCP/IP, a mesma função é executada por apenas uma camada. As camadas podem ser vistas com uma diferença semelhante, no modelo ISO/OSI temos duas camadas separadas de ligação de dados e camadas físicas, enquanto que no caso do modelo TCP/IP existe apenas uma camada de acesso à rede.

7. Processo de comunicação

Vejamos agora o processo de comunicação utilizando o modelo TCP/IP. Como mencionei anteriormente, este modelo descreve um conjunto de protocolos operacionais que formam o que se chama um protocolo, por vezes referido como uma pilha de protocolos. De onde veio o nome? Expliquei que quando queremos mostrar uma página web, primeiro a camada de aplicação utiliza o protocolo HTTP, depois na camada de transporte utilizamos um

um protocolo desta camada, tal como TCP ou UDP, e depois na camada da Internet um protocolo IP, na camada de acesso à rede, tal como a norma Ethernet. A comunicação é baseada num conjunto de protocolos, um por cima do outro. A exactidão só pode ser garantida se toda a pilha de protocolos for utilizada para comunicação.

Primeiro, o utilizador da rede cria dados na camada da aplicação, isto pode ser uma consulta a um servidor web ou podem estar a escrever mensagens num mensageiro. Os dados são então enviados para a pilha, primeiro para a camada de transporte, onde são divididos em pedaços mais pequenos,

e depois para a camada da Internet, onde lhes é dado um endereço que permite que os dados sejam enviados através da WAN. Em seguida, vão para a camada de acesso à rede e são novamente atribuídos endereços, desta vez aos endereços dos dispositivos na rede local. Finalmente, os dados são inseridos no meio de transmissão e enviados através de um intermediário para o dispositivo final, onde passam através da pilha, são remontados e são passados para a camada de aplicação.

Lembre-se

O processo de transferência de dados da fonte para o destino transporta os dados através das camadas do dispositivo da fonte, que é depois codificado e transmitido através do meio de transmissão para o dispositivo de destino, onde os dados vão em vez disso para a pilha.

Antes de mergulharmos no processo de comunicação, precisamos de fazer mais uma pergunta muito importante. A fim de assegurar que os dados chegam aos anfitriões e aplicações certos e permanecem o mais inalterados possível, comunicando-lhes a informação certa, chamamos a esta informação de controlo.

Esta informação é acrescentada em três camadas. A camada de transporte adiciona os números da porta de aplicação (a porta de aplicação no anfitrião de origem e a porta de aplicação no anfitrião de destino), a camada de Internet ou de rede, o endereço IP (incluindo anfitrião de origem e anfitrião de destino), a camada de rede ou de ligação de dados, o endereço MAC (anfitrião de origem) e o router de rede local). Todo o processo de percorrer as camadas na pilha, dividindo-as em partes mais pequenas e acrescentando informação de controlo (ou seja, dados adicionais) é denominado encapsulamento. Evidentemente, existe um processo inverso de remoção desta informação adicional do dispositivo alvo, chamado decapsulamento.

Lembre-se

Os dados fluem através de camadas no dispositivo de origem, circundando-o com informação para identificar a aplicação e o dispositivo alvo, enquanto que o processo inverso, em que os dados fluem através de camadas e removem esta informação adicional sobre o hospedeiro alvo, é a decapsulação.

Acrescentar esta informação de controlo a cada camada individualmente alteraria ligeiramente a estrutura das camadas, o que é lógico porque estamos a acrescentar alguma informação aos dados que não estavam lá antes. Por conseguinte, a nomenclatura dos conjuntos de dados também muda. Normalmente, os dados enviados através da rede são chamados unidades de dados de protocolo (PDUs), mas à medida que nos deslocamos entre camadas, os seus nomes mudam, por isso: Na camada da aplicação, referimo-nos simplesmente a PDUs como dados. Mais tarde, na camada de transporte, referir-nos-emos aos PDUs como segmentos ou datagramas, dependendo do protocolo utilizado nessa camada. Um PDU na camada da Internet já é um pacote, e na camada de acesso à rede teremos uma moldura. Utilizaremos a mesma nomenclatura ao analisar a comunicação utilizando o modelo ISO/OSI.

8. Discussão sobre a utilização de camadas

Chegou o momento de compreender o processo de comunicação por camadas com mais detalhe. Discutiremos isto utilizando o exemplo do envio de um e-mail. Originalmente, os utilizadores da Internet criavam e-mails utilizando programas de e-mail ou navegadores web. A camada de aplicação codifica correctamente estes dados e passa-os para a camada de transporte.

Esta camada divide os dados em partes mais pequenas, segmentos que são mais fáceis de transmitir através da rede. É como quando queremos mover um canto enorme de um lugar para outro, é difícil mover tudo porque nem sequer cabe pela porta, por isso desmontamo-lo em vez de tentarmos combiná-lo com movê-lo completamente. adiciona também informação de controlo que nos permite mais tarde montar os segmentos no dispositivo final na ordem correcta (embora isto nem sempre seja adicionado, dependendo do protocolo utilizado nesta camada), mas mais importante, adiciona também o número da porta da aplicação (a porta da aplicação no servidor e a porta no cliente), informação que nos permite mais tarde determinar que se trata de um e-mail e não de uma página web. Falaremos mais sobre as portas de aplicação quando discutirmos as funções e protocolos da camada de aplicação e da camada de transporte.

Estes segmentos são então transportados para a camada da Internet, onde são atribuídos endereços IP - o dispositivo de envio e o dispositivo de recepção. Este processo é utilizado para que o router (ou seja, o dispositivo intermediário entre o remetente e o receptor da mensagem) saiba para onde enviar a mensagem. A partir deste ponto, o nosso segmento é endereçado pelo pacote.

O pacote vai então para a camada de acesso à rede, onde é criado um frame e fornece o endereço físico do dispositivo de envio e o endereço físico do router ao qual o computador ao qual a mensagem está a ser enviada está ligado. Com este endereço, os frames podem então chegar a este router, que depois os envia para a WAN.

Contudo, antes da própria transmissão, a moldura é codificada em bits e passada através do router para o dispositivo de destino.

Quando estes bits são recebidos pelo hospedeiro de destino, um processo inverso de encapsulamento e decapsulação, em que os quadros são convertidos em pacotes, os pacotes são convertidos em segmentos e a camada de transporte remonta-os na ordem correcta. Uma vez concluído este processo, os dados são enviados para a camada de aplicação, onde a mensagem é exibida. Quando se pretende exibir uma página web ou enviar um ficheiro pela Internet, o processo de comunicação será semelhante, excepto que serão utilizados diferentes protocolos da camada de aplicação para lidar com o envio de páginas web ou ficheiros em vez de enviar e receber e-mails.

Finalmente, uma nota importante - o processo de comunicação entre os dispositivos aqui discutidos é simplificado e chamamos-lhe um contrato. Porquê? Bem, porque omitimos o processo de transferência de dados entre dispositivos intermediários (ou seja, routers). O processo de encaminhamento, ou seja, a transferência de dados entre routers numa vasta rede de área e a possibilidade de utilizar diferentes meios de transmissão no processo, do remetente ao receptor, é uma questão vasta e complexa que não iremos discutir agora. Evidentemente, é uma fase extremamente importante da comunicação e iremos certamente prestar-lhe atenção, mas apenas se os nossos conhecimentos e competências em redes de computadores nos permitirem fazê-lo.

Bem, agora cada um de vós sabe como é o processo de comunicação quando apresentado e apresentado no modelo de protocolo TCP/IP em camadas, que parece muito semelhante no modelo de referência ISO/OSI. Assim, se lhe for pedido (por exemplo, por um professor para fazer um teste) que descreva o processo de comunicação baseado no modelo ISO/OSI, não deverá ter qualquer problema.

9. Endereçamento em rede

Esclareçamos agora uma questão muito importante, a saber, o tratamento na rede. Deve ter notado que esta questão surge 3 vezes quando se discute o processo de comunicação, porque a informação relacionada com endereços ou números é acrescentada a até três camadas.

Mas desta vez, vamos começar na parte inferior da pilha e ver que a camada de acesso à rede do modelo TCP/IP e a camada de ligação de dados do modelo ISO/OSI surgiram com o conceito de endereços físicos. Perguntamos qual é este endereço físico. Não. Um endereço físico, também conhecido como endereço MAC, é um número hexadecimal codificado de 48 bits na placa de rede do dispositivo final, ou computador. Este endereço pode ser da forma: 28-80-23-D6-BE-14, dado na fase de criação do cartão. É composto por duas partes iguais, sendo a primeira o identificador do fabricante e a segunda o identificador do cartão.

Todos estes códigos hexadecimais são utilizados para encontrar um anfitrião na rede local, a LAN, é este endereço, o endereço físico do anfitrião de origem e do router na rede local, o gateway que liga a nossa rede local e a WAN, em TCP/ O processo de encapsulamento da camada de acesso ao modelo IP da rede e a camada de ligação de dados do modelo ISO/OSI.

Avançando para cima, temos a camada Internet do modelo TCP/IP e a camada Rede do modelo ISO/OSI. Nestas camadas, os endereços IP, também chamados endereços lógicos, são adicionados durante o processo de encapsulamento. Estes endereços são o endereço IP do computador remetente e o endereço IP do computador receptor. Não vou entrar nos detalhes da construção, utilização e cálculo dos endereços IP aqui, pois já existe um episódio no nosso canal (clique para entrar) que é inteiramente dedicado aos endereços IP, e direi apenas que estes endereços estão localizados em redes diferentes para transmitir dados Os anfitriões estão normalmente a centenas de quilómetros de distância geograficamente.

Finalmente, temos a camada de transporte, que não utiliza o endereçamento para detectar hospedeiros como as camadas previamente discutidas, mas em vez disso utiliza números de portas para atribuir dados a aplicações específicas no sistema operativo. Lembre-se, que os computadores actuais permitem a execução simultânea de múltiplas aplicações. Ao mesmo tempo, podemos utilizar o browser para navegar na Internet, ouvir rádio na Internet, enviar e receber correio electrónico e até jogar jogos online. Se as aplicações não forem particionadas, se não forem atribuídos números de porta na camada de transporte para permitir a identificação de serviços de rede específicos, podemos experimentar que as mensagens de correio electrónico recebidas aparecerão no ecrã em graus mais baixos durante a jogabilidade, em editores de texto Haverá mensagens do mensageiro instantâneo. Veja como tudo isto é pensado, logicamente disposto, sem hipótese, e é por isso que adoro tanto as redes de computadores.

9.1. Resumo

Em redes informáticas, a fim de facilitar a descrição e o controlo das várias fases da comunicação e para a normalização, é utilizado um modelo em camadas para que o hardware e o software de diferentes fabricantes sejam compatíveis entre si. A comunicação numa rede é efectuada utilizando regras e regras conhecidas como a adopção de protocolos de comunicação. O processo de comunicação em rede envolve a passagem de dados pela pilha num dispositivo de origem, codificando-os em bits e enviando-os para um dispositivo de destino, onde os dados são passados e interpretados no dispositivo de destino. Em cada camada, os dados vêm com informações de controlo, números de portas e endereços lógicos e físicos, que são depois codificados e enviados para o destinatário. O processo de fluxo de dados pela pilha e transferência de informação de controlo e endereços é chamado encapsulamento, enquanto que no final, à medida que os dados sobem a pilha, este processo é chamado decapsulamento.

10. Protocolos de camada de aplicação

10.1. Protocolo HTTP

Quando lançamos um navegador web, um programa de mensagens instantâneas ou de partilha de ficheiros, estas aplicações criam uma interface de comunicação entre a rede informática e o utilizador. É claro que o software de aplicação em si, o próprio programa de computador, não é suficiente para uma comunicação eficiente, uma vez que os protocolos de comunicação acima referidos são necessários para tal, mas são implementados nestes programas. Um exemplo de um protocolo de camada de aplicação, provavelmente um dos mais populares, HTTP, é implementado em navegadores web e, como todos os programas de mensagens instantâneas e outros programas que comunicam através de uma rede, também implementam um protocolo correspondente.

Quando introduzimos o endereço de uma página web no browser, o chamado URL (Uniform Resource Locator), e após premir a tecla Enter, o nosso browser liga-se ao servidor onde a página é armazenada e solicita um recurso específico - a maioria dos quais são geralmente ficheiros que contêm páginas de conteúdo. Se o servidor tiver o recurso solicitado, envia o seu conteúdo para o browser, que interpreta o código HTML do qual a página é composta, e exibe o seu conteúdo ao utilizador. Na realidade, o processo é algo complicado. Tomemos como exemplo um endereço web: http://www.cybersecurity.co.uk/fundamentals.html .

Uma vez introduzido e confirmado, o navegador verifica primeiro o tipo de protocolo, depois o nome de domínio da Internet e finalmente considera o nome de um ficheiro específico.

Mais tarde, o nosso navegador chama o servidor DNS para alterar o nome mnemónico (ou seja, cybersecurity.pl) para o endereço IP do servidor em que a página é armazenada.

O browser, conhecendo este endereço, envia um pedido ao servidor para aceder ao ficheiro tomijerry.html localizado no domínio alamakota.pl. Se o servidor tiver o recurso em resposta, envia uma mensagem apropriada com o conteúdo do ficheiro solicitado. O conteúdo deste ficheiro, código HTML, é interpretado pelo navegador e apresentado como uma página web.

O protocolo HTTP tem como padrão a porta 80 e define vários tipos básicos de mensagens, ou seja, um pedido de comunicação entre um cliente e um servidor web, os mais importantes dos quais são: GET e POST.

10.2. Método GET

GET é utilizado para solicitar uma página web específica a um servidor. A sua sintaxe é parecida com esta:

GET /fundamentals.html HTTP/1.1

Para além do nome do recurso solicitado, contém também a versão de protocolo utilizada. Quando o servidor recebe tal mensagem, tal pedido, responde ao cliente com a mensagem apropriada (com os cabeçalhos mostrados abaixo) e o recurso solicitado: HTTP/1.1 200 OK/fundamentals.html

O pedido GET também contém as seguintes informações: o nome do anfitrião (por exemplo wp.pl), o nome do navegador que enviou o pedido, os tipos de ficheiro aceites pelo navegador e a língua ou codificação de caracteres preferida da página. A resposta do servidor contém as seguintes informações: a hora do servidor, o nome da aplicação do servidor (por exemplo, APACHE) ou a hora de expiração do documento.

Se, por alguma razão, o servidor web não puder enviar de volta o recurso, ele envia de volta um

mensagem de erro, tal como 404 notificando que o recurso solicitado não foi encontrado ou 403 notificando que o acesso ao recurso é proibido. As mensagens seleccionadas e os códigos de erro são apresentados no quadro abaixo.

[tabela da pasta abaixo]. Código de erro do cliente:

Código Descrição Significado

400 Mau Pedido O servidor não pôde processar o pedido devido a um erro do cliente

401 Pedidos não autorizados Pedidos de recursos que requerem autenticação

403 Proibido O servidor compreende o pedido, mas a configuração de segurança impede-o de devolver o recurso solicitado

404 Não Encontrado O servidor não conseguiu encontrar um recurso no URL especificado

405 Método não permitido O método contido no pedido não é permitido para o recurso indicado

406 Não Aceitável O recurso solicitado não pode devolver uma resposta que o cliente possa tratar

407 Autenticação por procuração necessária Autenticação por procuração necessária

408 Tempo limite de pedido Tempo limite de pedido decorrido - o cliente não enviou o pedido ao servidor dentro de um período de tempo especificado

409 Conflito O pedido não pôde ser satisfeito devido a um conflito com o estado actual do recurso

411 Comprimento pedido - servidor recusado a completar o pedido devido à falta do cabeçalho Content-Length no pedido

415 Tipo de Meios de Comunicação Não Suportados Forma de pedido desconhecida - o servidor recusou-se a aceitar o pedido porque a sua sintaxe não foi compreendida pelo servidor [fim da tabela].

Código de erro do servidor:

Código Descrição Significado

500 Erro interno do servidor Erro interno do servidor - o servidor encontrou um problema que o impede de completar o pedido

501 Não Implementado O servidor não tem as capacidades necessárias para a consulta

502 Erro de gateway inválido O servidor - actuando como gateway ou intermediário - recebeu uma má resposta do servidor anfitrião e não pôde satisfazer o pedido do cliente

503 Serviço indisponível Serviço indisponível - o servidor não consegue actualmente completar o pedido do cliente devido a sobrecarga

504 Gateway Timeout Exceeded - o servidor agindo como gateway ou intermediário não recebeu uma resposta do servidor HTTP, FTP, LDAP, etc. especificado dentro do tempo especificado ou é necessário um servidor DNS para tratar o pedido

505 Versão HTTP Não Suportada - o servidor não suporta ou recusa-se a suportar a versão HTTP especificada pelo cliente

10.3. Método POST

Outro tipo de mensagem é uma mensagem POST, que é utilizada para enviar dados para um servidor. Por exemplo, quando existe um formulário numa página que envia dados para o servidor, tal como um formulário de registo, os dados que colocamos no mesmo são enviados com uma mensagem POST.

Embora o protocolo HTTP seja muito popular e provavelmente o mais amplamente utilizado de todos os protocolos da camada de aplicação, não é seguro. O método POST envia os dados para o servidor em texto simples. Se a transmissão entre cliente e servidor for interceptada, é possível ler a informação que se pretende enviar para o servidor.

Isto é muito perigoso, e é por isso que hoje em dia a maioria dos sites pode enviar alguma informação para o servidor, por exemplo os sites que requerem um login já utilizam HTTPS, que codifica a comunicação entre o cliente e o servidor, funcionando na porta 443.

Outros tipos de mensagens que os clientes podem enviar para o servidor web são: Dados para a minha tabela:

Remover o pedido para remover o recurso do servidor O chefe pede recursos do servidor sob a forma de cabeçalhos

Link Request estabelece relações entre os recursos existentes OPÇÕES Pedir ao servidor para identificar os métodos suportados Colocar pedidos ao servidor para receber o ficheiro do cliente

Trace solicita ao servidor que devolva os cabeçalhos da mensagem enviada pelo cliente

10.4. Correio electrónico

O correio electrónico utiliza dois protocolos de camada de aplicação que funcionam em conjunto. Um é utilizado para enviar correio, que é o protocolo SMTP, e o outro para receber mensagens, que é o POP3. Actualmente, o IMAP também pode ser utilizado para receber mensagens

e-mail. Estes protocolos estão estreitamente relacionados com as aplicações, os processos em curso nos computadores e servidores clientes que criam e recebem mensagens. Estes processos são MUA (Mail User Agent), MTA (Mail Transfer Agent) e MDA (Mail Delivery Agent). O processo MUA corre na máquina cliente e os outros dois processos correm no servidor de correio.

Segue-se um processo simplificado para o envio de e-mails utilizando um proxy:

1 O utilizador cria uma mensagem de correio electrónico e utiliza o processo MUA para a encaminhar para o servidor de correio e o processo MTA em execução nesse servidor.

2. este processo analisa os cabeçalhos das mensagens, incluindo. Para definir o destinatário da mensagem e verificar se o utilizador para quem a mensagem aponta está na sua lista de utilizadores.

(3) Se assim for, passa a mensagem ao processo MDA, que é responsável pela sua entrega ao destinatário apropriado.

(4) Se o destinatário da mensagem não tiver uma conta neste servidor, o processo MTA encaminha a mensagem para o processo MTA noutro servidor onde se encontra a conta do utilizador.

5 O servidor passa a mensagem para o processo MDA, que entrega a mensagem ao destinatário pretendido. O quadro seguinte mostra as portas em que o protocolo de correio electrónico funciona.

Protocolo	Número do porto
IMAP	143
POP3	110
SMTP	25
IMAP encriptado	993
POP3 encriptado	995
SMTP encriptado	465 ou 587

10.5. Protocolo FTP

Um terceiro serviço web igualmente popular é a capacidade de enviar e receber ficheiros via FTP (File Transfer Protocol). O serviço é também um protocolo de comunicação quando desejamos carregar ficheiros de sítios web para um servidor web ou simplesmente desejamos carregar alguns ficheiros para um servidor e partilhá-los com outros utilizadores. Para realizar a operação de upload de ficheiros para o servidor ou de download de recursos do servidor, precisamos de utilizar um cliente FTP e, claro, tal serviço deve também estar a correr no servidor. Os clientes FTP estão disponíveis em todos os sistemas operativos, por exemplo através da linha de comando, o que é inconveniente mas funciona.

Se utilizar apenas FTP para descarregar ficheiros, pode fazê-lo com segurança utilizando um navegador web. A maioria, se não todos, os navegadores populares têm clientes FTP incorporados.

Contudo, se quiser carregar ficheiros para um servidor, é aconselhável utilizar software dedicado como FileZilla ou WinSCP - estes são gratuitos e podem ser facilmente descarregados a partir da web.

Cliente FTP WinSCP

Com este protocolo, devem ser estabelecidas duas ligações entre o cliente e o servidor, a fim de comunicar correctamente. A primeira ligação é apenas utilizada para enviar comandos e mensagens e chama-se uma ligação de controlo (funciona na porta 21), enquanto a segunda ligação funciona na porta 20 e é utilizada para transferir ficheiros de e para o servidor. Para proteger o acesso ao servidor FTP, é utilizada a autenticação do utilizador, que é exactamente a mesma que para iniciar sessão em perfis ou e-mails em redes sociais, mas por vezes, quando o recurso está disponível para um público maior, é concedido acesso anónimo aos chamados utilizadores, pelo que não é necessária autorização.

Esta solução só deve ser utilizada se o utilizador tiver autorização para descarregar dados a partir do servidor. O carregamento de ficheiros, ou seja, a sua colocação no servidor, é sempre acessível apenas aos utilizadores com um login e uma palavra- passe.

10.6. Protocolo SSH

Outro protocolo comummente utilizado na camada de aplicação é o protocolo de gestão remota do hospedeiro conhecido como SSH (Secure Shell). Para os profissionais não informáticos, o nome tem pouco significado, uma vez que não é um protocolo, website ou e-mail utilizado por 'comedores de pão comuns'. Os administradores utilizam-no para gerir servidores, frequentemente localizados em locais geográficos diferentes, não necessariamente no seu local de trabalho. Por exemplo, também é utilizado por pessoas que compraram servidores VPS e, portanto, os gerem. Este protocolo é derivado de outro protocolo de acesso remoto, o protocolo TELNET, e é provavelmente uma versão melhor. Porquê? Porque o TELNET, a propósito, é provavelmente o protocolo mais antigo na camada de aplicação, não encripta a comunicação entre cliente e servidor, as mensagens são enviadas em texto simples, pelo que é possível interceptar a comunicação e perguntar em que sessão a informação está a ser enviada. Na sua opinião, esta é uma situação inaceitável, pelo que o anfitrião é gerido remotamente utilizando o protocolo SSH encriptado.

O algoritmo padrão para encriptar comunicações é o RSA, mas o algoritmo DSA ligeiramente mais fraco também pode ser utilizado para encriptar dados. Quando o servidor SSH é instalado, é criado um par de chaves - as chaves públicas e privadas do servidor - que são utilizadas para encriptar e desencriptar comunicações. Quando um cliente se liga ao servidor pela primeira vez, salva a chave pública do servidor num ficheiro_hosts conhecido no disco.

Depois cria uma chamada chave de sessão, que é utilizada para encriptar toda a comunicação. A chave de sessão é encriptada com uma chave pública previamente recebida e enviada de volta para o servidor. A partir deste ponto, toda a comunicação é encriptada com a chave de sessão.

Por defeito, o SSH funciona na porta 22. PUTTY é um dos programas clientes mais populares para a utilização do SSH, é gratuito, pode ser descarregado a partir da web e não requer instalação. Para se ligar remotamente a um anfitrião, basta lançá-lo, introduzir o nome do anfitrião ou o seu endereço IP, seleccionar SSH se não for seleccionado por defeito, e clicar em Abrir. Se estiver a ligar-se a um anfitrião remoto pela primeira vez, confirme que deseja ligar-se e podemos geri-la remotamente.

10.7. Protocolo DNS

O DNS é um protocolo, um serviço que traduz nomes de domínio legíveis por pessoas em endereços IP para dispositivos na Internet. Imagine uma situação em que o DNS não existe, mas queremos exibir os nossos sítios Web preferidos no browser. Precisamos de introduzir o endereço IP em vez do nome de domínio, ou seja, o endereço em forma de palavras, por exemplo: 212.56.93.112. Para a maioria de nós isto não é problema, alguns números podem ser memorizados. Por outro lado, existem muitos websites na Internet e é difícil lembrar muitos endereços numéricos. Além disso, é fácil cometer um erro em tais registos digitais, e no mundo da Internet, um erro tão pequeno pode levar a uma página diferente da que esperávamos.

Este é um dos lados da moeda, e o outro lado é que o endereço IP do servidor pode não mudar com muita frequência. Quando o nosso website muda de endereço IP e o serviço DNS não funciona, temos de reaprender esse endereço e lembrá-lo. O DNS resolve-nos este problema porque altera este endereço na sua base de dados de registos e atribui-o ao nome do domínio. Então, para nós, utilizadores, não importa qual é o endereço IP do sítio, o importante é, que conhecemos o seu endereço e nome de domínio e que não mudam.

DNS é um serviço que corre numa arquitectura cliente-servidor, mas aqui não estamos a tratar os clientes como programas informáticos, tais como browsers ou programas de partilha de ficheiros. Este computador apenas executa um serviço de sistema chamado DNS Resolver, que trata de todas as aplicações em computadores clientes cujos nomes precisam de ser alterados. Sempre que configuramos um dispositivo de rede, ou apenas um computador, devemos especificar dois endereços de servidor DNS para que, se um não comunicar, o outro actue como uma substituição do nome.

Os servidores DNS armazenam todo o tipo de registos, incluindo registos A e AAAA contendo endereços de dispositivos finais e registos MX que suportam trocas de correio, pois é importante lembrar que o DNS não só traduz endereços de domínio em endereços IP para sítios web, mas também se aplica ao servidor de correio electrónico. A troca de nomes parece-me ser assim:

1. O cliente envia uma consulta para o servidor DNS, que verifica se o registo existe na sua base de dados.

2. Se assim for, traduz o nome para um endereço IP e envia-o de volta ao cliente:

3. Caso contrário, contacta outros servidores para que o registo em questão seja incluído na sua base de dados:

O envio de pedidos a outros servidores para um servidor DNS que não encontra um registo na sua base de dados pode causar muito tráfego de rede, o que é uma situação confusa. Para evitar tráfego de rede excessivo e desnecessário, quando outro servidor encontra um registo e envia-o para o servidor atribuído ao seu dispositivo, este último guarda o registo numa cache, para que no futuro não tenha de se referir a outro servidor para o mesmo endereço. Isto irá certamente acelerar alterações posteriores de nome, uma vez que os nossos servidores DNS já não procuram registos em outros servidores, mas substituem os nomes imediatamente. Da mesma forma, os serviços DNS nos computadores pessoais armazenam nomes previamente traduzidos. Isto pode ser verificado através da introdução de ipconfig/displaydns num PC Windows. Veremos então quais os mapeamentos que são armazenados na cache de serviços DNS do nosso computador.

10.8. Hierarquia DNS

Esta hierarquia de servidores DNS toma a forma de uma árvore invertida, com a raiz, o servidor DNS de nível superior, no topo. O servidor de nível superior armazena informações sobre como chegar ao servidor de nível superior, que por sua vez armazena informação sobre como chegar ao servidor de segundo nível, etc. Os domínios de primeiro nível especificam o país (. pl.de ou . uk) ou o tipo de organização (. org . com ou . gov).

Num endereço de exemplo como Pocztowy.wp.pl, distinguimos entre um domínio de primeiro nível (. pl), depois um domínio de segundo nível (wp.pl) e finalmente um domínio de terceiro nível (Pocztowy.wp.pl Naturalmente, nem todos os endereços têm de conter tantos níveis de domínios quanto possível, não apenas domínios de primeiro e segundo nível, tais como wp.pl, pasja-informatyki.pl, Szkola.pl.

10.9. Protocolo DHCP

Tal como o DNS discutido anteriormente, DHCP é um protocolo que funciona como um serviço e não como um programa ou aplicação. DHCP permite aos computadores ligados a uma rede obterem endereços IP, máscaras de sub-rede, endereços de gateway e servidores DNS e outras configurações a partir de um conjunto de endereços pré-configurado. Um servidor DHCP pode ser configurado num computador separado e será um dispositivo separado na rede que atribui endereços IP a computadores clientes, ou pode funcionar num servidor existente como um serviço separado, um processo separado.

Actualmente, o router na nossa casa também nos permite configurar um serviço deste tipo. A atribuição de endereços a computadores clientes através do serviço DHCP (a chamada atribuição dinâmica) é uma solução muito conveniente para administradores, especialmente em grandes redes onde aparecem frequentemente novos computadores e os seus utilizadores. Numa rede com 100, 200 ou 500 computadores e um grande número de dispositivos móveis, a simples configuração de endereços IP seria uma tarefa entediante e, mais importante ainda, demorada.

É claro que nem todos os dispositivos da rede podem obter endereços desta forma, como alguns, tais como servidores de aplicações, bases de dados, autenticação de utilizadores, impressoras de rede ou routers, devem e devem ter endereços atribuídos estaticamente, ou seja, distribuídos manualmente. Porquê? Porque um serviço DHCP configurado num servidor nem sempre atribui permanentemente um determinado endereço IP a um computador. Apenas aluga tal endereço durante um período de tempo especificado na configuração de DHCP, talvez horas, dias, mas não permanentemente, embora existam excepções a isto, informá-lo-ei quando configurar um servidor DHCP específico.

A máquina desactivada devolve o endereço alugado, que é devolvido à piscina. Outra máquina pode então arrendar esta morada. Quando um servidor, router ou impressora de rede aluga estes endereços, podem ter de os devolver ao pool após um período de tempo e não há garantia de que voltarão a receber o mesmo endereço. Os computadores clientes que comunicam com qualquer servidor ou outro dispositivo importante em funcionamento na rede referem- se a ele pelo seu endereço IP, se o endereço IP mudar frequentemente, alguns serviços para utilizadores na rede local podem não estar disponíveis durante algum tempo, especialmente na empresa Ainda mais Inaceitável.

Para que um computador Windows possa obter um endereço de um servidor DHCP, a opção "Obter um endereço IP automaticamente" deve ser seleccionada na configuração de rede.

10.10. Resumo

Os protocolos da camada de aplicação descritos nesta secção são apenas uma pequena parte da lista geral de protocolos da camada de aplicação disponíveis. Existem muitos outros serviços numa rede informática, cada um deles funcionando com um protocolo diferente. É difícil listá-los aqui, pelo que os mais populares e comummente utilizados são listados. Para aqueles interessados em explorar o tema dos protocolos de comunicação na camada de aplicação com maior profundidade, remeto-vos para a literatura. A tabela seguinte contém um conjunto de protocolos populares da camada de aplicação e os seus números de porta. Eles são certamente úteis para verificação antes de exames ou testes profissionais.

Protocolo	Descrição	Porto
HTTP	Protocolo de transferência de hipertexto	80
HTTPS	Protocolo HTTP encriptado usando os protocolos SSL ou TLS	443
POP3	Protocolo para a recepção de mail	110 (encriptado 995)
IMAP	Protocolo de recepção de correio para gerir pastas na caixa de correio	143 (encriptado 993)
SMTP	Protocolo de envio de correio	25 (criptografados 465 ou 587)
FTP	Protocolo de transferência de ficheiros	21 (comandos) e 20 (ficheiros)
FTPS	Protocolo FTP encriptado	990
TELNET	Protocolo de ligação terminal	23
SSH	Terminal encriptado protocolo de ligação	22
DNS	Protocolo para mudança de domínio nomes para endereços IP	53

DHCP	Protocolo para automático configuração dos anfitriões na rede	67 e 68 (IPv6 - 546 e 547)
LDAP	Protocolo de serviços de directório (por exemplo, AD no WS)	389 (codificado 639)
SNMP	Equipamento de rede protocolo de configuração	161
MySQL	Gestão de bases de dados sistema	3306
PostgreSQL	Gestão de bases de dados sistema	5432

11. Tarefa da camada de transporte

A camada de transporte ou camada de transporte (estes nomes podem ser utilizados de forma intermutável) é uma parte muito importante do processo de comunicação. As tarefas mais importantes desta camada incluem:

· estabelecer e manter ligações (sessões) entre anfitriões,

· ligações de pista entre hospedeiros,

· Dividir os dados em peças mais pequenas,

· Identificar aplicações individuais,

· controlo do fluxo de dados,

· Retransmissão em caso de perda de dados.

O seguimento de chamadas, que são conversas entre anfitriões, permite que múltiplas aplicações enviem e recebam dados simultaneamente. Num computador, podemos verificar o nosso correio, utilizar a banca electrónica ou comunicar com os nossos amigos. Neste momento, parece-nos natural que seja realmente difícil imaginar uma situação sem esta possibilidade, mas vale a pena lembrar que isto é possível graças à camada de transporte.

A capacidade de utilizar múltiplos serviços ao mesmo tempo também inclui a divisão de dados, ou seja, parti-los em pedaços mais pequenos. Isto permite uma comunicação mais eficiente, já que grandes quantidades de dados não são transmitidas simultaneamente. Se não fosse a segmentação, apenas uma aplicação poderia receber dados de cada vez e as outras aplicações que utilizamos teriam de esperar pela sua vez. Como se pode ver na imagem abaixo, segmentos são enviados alternadamente, segmentos de páginas web, segmentos de correio electrónico, segmentos de mensageiros instantâneos, etc. são enviados alternadamente. Todo o processo de transmissão alternada de segmentos de múltiplas aplicações é chamado multiplexing.

Outra tarefa ou função importante da camada de transporte é passar dados para a aplicação relevante. Cada aplicação tem o seu próprio identificador para o definir de forma única. Este identificador é o número da porta da aplicação.

É atribuído a um segmento ou datagrama durante o encapsulamento ao nível da camada de transporte e garante a entrega de dados a uma aplicação específica. Tal como os endereços IP, os números de porta são atribuídos pela IANA (Internet Assigned Numbers Authority), que divide os números de porta em 3 grupos:

Nome do grupo de portos	Intervalo de numeração	Aplicação
Bem conhecido	0 - 1023	Serviços de servidor e aplicações
Registado	1024 - 49151	Serviços aos utilizadores e aplicações
Dinâmico	49152 - 65535	Seleccionados aleatoriamente para aplicações do cliente

Portas bem conhecidas, ou seja, portas 0 a 1023, estão registadas para serviços e aplicações específicas de servidores, por exemplo, servidores web para a porta 80 e servidores POP3 para a porta 110 por defeito. Um conjunto de aplicações com portas conhecidas, incluindo protocolos da camada de transporte, como se mostra abaixo.

Protocolo da camada de aplicação	Número do porto	Protocolo da camada de transporte
HTTP	80	TCP

HTTPS	443	TCP
POP3	110 (encriptado 995)	TCP
IMAP	143 (encriptado 993)	TCP
SMTP	25 (criptografados 465 ou 587)	TCP
FTP	21 (comandos) e 20 (ficheiros)	TCP
FTPS	990	TCP
TELNET	23	TCP
DNS	53	TCP ou UDP
DHCP	67 e 68 (IPv6 - 546 e 547)	UDP
LDAP	389 (codificado 639)	TCP ou UDP
SNMP	161	UDP

O segundo grupo, portos registados, é utilizado por aplicações instaladas no computador do utilizador. Por exemplo, se instalarmos a aplicação do sistema de gestão de bases de dados MySQL no nosso computador, esta será executada na porta 3306.o terceiro grupo

e último grupo, o número da porta dinâmica, é atribuído aleatoriamente à aplicação cliente, por exemplo, quando um cliente envia um pedido ao servidor para partilhar uma página web, o servidor por defeito aceita o pedido na porta 80, mas o cliente recebe o pedido do servidor. A resposta recebida não será enviada para a porta 80, uma vez que esta é reservada para o processo do servidor web, mas para um número aleatório de portas atribuídas a partir do pool dinâmico de portas.

Múltiplas aplicações não podem funcionar com o mesmo número de porta. Uma vez que uma aplicação esteja a funcionar na porta 53 (DNS), é impossível que outra aplicação já não possa funcionar nessa porta.

Se já sabemos o que é um porto de aplicação, vamos introduzir outro conceito. Esta será uma tomada.

Já encontrou o conceito de tomadas ao discutir as placas-mãe e os processadores nas classes de tecnologia informática, e também aparece nas redes informáticas. Uma tomada é uma combinação de um endereço IP e um número de porta:

192.168.20.20:80

Um socket identifica de forma única um processo particular em execução num dispositivo, por exemplo, quando o nosso navegador invoca um servidor web para servir uma página web, os pedidos do servidor serão enviados para o seu socket, o processo (aplicação do servidor web).

O TCP é um protocolo complexo, orientado para a ligação, que visa garantir a transferência de dados e o controlo do fluxo fiáveis. Até 20 bytes de dados de controlo são adicionados ao cabeçalho TCP durante o encapsulamento, mas isto é necessário para a fiabilidade TCP. As aplicações que utilizam este protocolo incluem navegadores web, clientes de correio electrónico e programas de transferência de ficheiros. Pode ver o modo de segmento TCP abaixo. Os números entre parênteses indicam o número de bits reservados para o campo.

BIT (0)	BIT (15) BIT (16)	BIT (31)
Porto de origem (16)	Porto de destino (16)	
Número sequencial (32)		
Número de confirmação (32)		

Rubrica compriment o (4)	Reservado (6)	Bocados de código (bandeiras) (6)	Janela (16)
Checksum (16)			Índice de urgência (16)
Opções (0 ou 32)			
Dados da camada de aplicação (comprimento variável)			

- Porto de origem - o porto da aplicação que envia os dados.
- Porto de destino - o porto de aplicação para o qual os dados são enviados.
- Número de sequência - o número do último byte no segmento.
- Número de reconhecimento - o número do próximo byte esperado pelo destinatário.
- Comprimento - o comprimento de todo o segmento TCP.
- Bocados de código (bandeiras) - informação do segmento de controlo.
- Janela - Quantidade de dados que podem ser transmitidos sem confirmação.
- Checksum - utilizado para verificar os dados carregados.
- Indicador de emergência - apenas utilizado quando a bandeira URG é hasteada.

11.1. Cabeçalho TCP

O TCP é um protocolo complexo, orientado para a ligação, que visa garantir a transferência de dados e o controlo do fluxo fiáveis. Até 20 bytes de dados de controlo são adicionados ao cabeçalho TCP durante o encapsulamento, mas isto é necessário para a fiabilidade TCP. As aplicações que utilizam este protocolo incluem navegadores web, clientes de correio electrónico e programas de transferência de ficheiros. Pode ver o modo de segmento TCP abaixo. Os números entre parênteses indicam o número de bits reservados para o campo.

<table>
<tr><td colspan="3">BIT (0)</td><td>BIT (15) BIT (16)</td><td>BIT (31)</td></tr>
<tr><td colspan="3">Porto de origem (16)</td><td colspan="2">Porto de destino (16)</td></tr>
<tr><td colspan="5">Número sequencial (32)</td></tr>
<tr><td colspan="5">Número de confirmação (32)</td></tr>
<tr><td>Rubrica comprimento (4)</td><td>Reservado (6)</td><td>Bocados de código (bandeiras) (6)</td><td colspan="2">Janela (16)</td></tr>
<tr><td colspan="3">Checksum (16)</td><td colspan="2">Índice de urgência (16)</td></tr>
<tr><td colspan="5">Opções (0 ou 32)</td></tr>
<tr><td colspan="5">Dados da camada de aplicação (comprimento variável)</td></tr>
</table>

- Porto de origem - o porto da aplicação que envia os dados.
- Porto de destino - o porto de aplicação para o qual os dados são enviados.
- Número de sequência - o número do último byte no segmento.
- Número de reconhecimento - o número do próximo byte esperado pelo destinatário.
- Comprimento - o comprimento de todo o segmento TCP.
- Bocados de código (bandeiras) - informação do segmento de controlo.
- Janela - Quantidade de dados que podem ser transmitidos sem confirmação.
- Checksum - utilizado para verificar os dados carregados.
- Indicador de emergência - apenas utilizado quando a bandeira URG é hasteada.

11.2. Reconciliação em 3 partes

TCP é um protocolo de ligação, o que significa que antes de um anfitrião de origem poder enviar quaisquer dados para um anfitrião de destino, deve ser estabelecida uma ligação entre eles. Esta combinação é chamada um aperto de mão de três vias. O hospedeiro de origem, ou seja, o cliente, envia um segmento contendo a bandeira SYN (SYN é uma bandeira de sincronização de número de série), e o segmento também contém o número de série aleatório do cliente (também chamado ISN, SEQ=100), que é utilizado para fragmentos de dados fundidos subsequentes.

Ao receber este segmento, o anfitrião de destino, ou seja, o servidor, é informado de que o cliente deseja estabelecer uma ligação com ele. Em resposta, o servidor envia um segmento com as bandeiras SYN e ACK definidas (a bandeira ACK informa o cliente de que o servidor recebeu o segmento anterior), o número de sequência recebido do cliente é aumentado em 1 (ACK = 101) e o seu número de sequência aleatório (SEQ = 300).

Finalmente, o cliente envia o segmento de volta ao servidor com a bandeira ACK definida, acusando a recepção da mensagem anterior com o número de sequência do servidor aumentado em 1 (SEQ=101, ACK=301). Isto completa o processo de ligação e permite que os dados sejam transmitidos correctamente. O processo de reconciliação em três etapas é mostrado abaixo.

Só após uma ligação TCP ter sido estabelecida com o servidor é que o cliente pode enviar os dados relevantes, tais como um pedido para uma página web ou ficheiro.

Finalmente, quando todos os dados tiverem sido transmitidos, a sessão deve ser encerrada. O cliente envia então um segmento para o servidor com a bandeira FIN, que informa o servidor da sua intenção de encerrar a sessão, que responde com um segmento de reconhecimento com a bandeira ACK de que recebeu tal segmento. O servidor envia então também um segmento com a bandeira FIN, e o cliente responde com um segmento de reconhecimento com a bandeira ACK. Isto faz com que a sessão TCP seja encerrada.

Bandeira	Aplicação
URG	Indica a existência de um campo indicador de urgência no cabeçalho (urgente)
ACK	Indica a existência de um campo de número de reconhecimento no cabeçalho.
PSH	Transmissão forçada de pacotes (push)
RST	Reconexão (reset)
SON	Sincronização de números sequenciais
FIN	Fim dos dados do remetente

11.3. Janela TCP

A fiabilidade da entrega de dados dentro de uma sessão TCP depende do envio pelo cliente de um aviso de recepção de dados previamente enviados. Antes de o servidor poder enviar outra porção de dados ao cliente, deve receber este aviso de recepção. Isto por vezes causa atrasos na entrega de segmentos, uma vez que estes não são enviados continuamente. Contudo, estes problemas são aceitáveis quando a fiabilidade da comunicação é exigida.

Assumindo que 1000 bytes de dados serão enviados num segmento com número de sequência 1, quando o cliente recebe 1 parte dos dados, enviará um segmento com número de confirmação 1001 para o servidor. O próximo byte, começando com o byte 1001. Quando o servidor enviar mais 1000 bytes, o número de confirmação recebido será 2001, o próximo número será 3001, o próximo 4001 e assim por diante.

Claro que, na realidade, quando o anfitrião tem de confirmar a recepção de uma quantidade tão pequena de dados de cada vez, isto pode causar uma grande sobrecarga de largura de banda, por exemplo, o tempo de carregamento da página pode ser longo. Por conseguinte, mais dados são enviados e reconhecidos pelo feedback. A quantidade de dados que o servidor pode enviar antes de receber uma confirmação do cliente é chamada o tamanho da janela, neste caso 3000 bytes.

Este tamanho é especificado no cabeçalho do segmento TCP e, para além de determinar a quantidade de dados que podem ser transmitidos sem reconhecimento, permite o controlo do fluxo de dados entre dispositivos. Se um cliente encontrar um bloqueio durante a recepção de dados e um segmento for perdido, o dispositivo pode enviar informação ao servidor para reduzir o tamanho desta janela, a quantidade de dados que pode ser recebida sem aviso de recepção, retardando a transferência, mas evitando a perda de um segmento. Passado algum tempo, o tamanho da janela volta ao seu tamanho original. A mudança no tamanho da janela durante a transferência é chamada janela dinâmica ou janela deslizante.

11.4. Protocolo UDP

Outro protocolo que implementa algumas funções da camada de transporte é o protocolo UDP. Contudo, neste caso é muito mais simples, uma vez que o protocolo não implementa qualquer mecanismo para garantir a fiabilidade da entrega de dados ou o controlo do fluxo.

O protocolo UDP é um protocolo simples sem ligação e a sua maior vantagem é a baixa sobrecarga de dados de controlo adicionados durante o processo de encapsulamento. O UDP adiciona apenas 8 bytes de dados de controlo no datagrama. O cabeçalho de um datagrama UDP tem este aspecto:

BIT (0)	BIT (15) BIT (16)	BIT (31)
Porto de origem (16)	Porto de destino (16)	
Comprimento (16)	Checksum (16)	
Comprimento da camada de aplicação (comprimento variável)		

· Porta de origem - especifica a porta de aplicação a partir da qual os dados devem ser enviados.

· Porto de destino - especifica o porto de aplicação para o qual os dados são enviados.

· Comprimento - campo de 16 bits especificando o comprimento de todo o datagrama UDP

· Checksum - um campo de 16 bits utilizado para validar os dados que estão a ser enviados.

UDP sem ligação significa que o anfitrião de origem não envia qualquer informação para estabelecer uma ligação com o anfitrião de destino antes do início do processo de comunicação. A regra geral é que se um dispositivo de origem quiser iniciar uma transferência, quer enviar os dados que acabou de completar sem acordo prévio.

Se o compararmos com a comunicação interpessoal, no caso do protocolo TCP seria algo parecido: Ei Tom, concentra-te porque estou prestes a falar contigo e só quando receber esta mensagem é que começará uma conversa normal, claro que só se Tom responder: OK, vou começar a ouvir. No caso da UDP, não notificou o Tom que eu estava prestes a começar a comunicar algo importante para ele, eu apenas comecei a conversa.

As aplicações ou serviços que utilizam este protocolo de transporte incluem DNS, DHCP, telefonia VoIP e streaming de vídeo.

Porquê estes? Bem, a resposta é simples, estas aplicações valorizam a velocidade sobre a fiabilidade da comunicação, ou melhor, a necessidade de receber todos os dados que estão a ser transmitidos. Imagine uma situação em que estamos a ver uma transmissão de vídeo ou a jogar um jogo com amigos, como o CS. É difícil competir no jogo ou assistir a qualquer coisa quando os pacotes chegam atrasados.

Alguém pode perguntar: mas porquê o atraso? Bem, os segmentos TCP, por exemplo, são muito maiores do que os datagramas UDP, e o TCP tem de reconhecer os dados entregues, pelo que são enviados através da rede em grandes volumes, mais do que em UDP.

Para aplicações que utilizem este protocolo específico, pode ser tolerado, que ocasionalmente os pacotes podem ser perdidos ou corrompidos. Para os serviços DNS, se um datagrama for perdido, a consulta é simplesmente reenviada para o servidor DNS e não seria uma tragédia se o datagrama não chegasse durante a sessão, uma vez que as mensagens podem sempre ser repetidas. Para aplicações que utilizam o protocolo TCP, a perda ou confusão já não é aceitável. Os datagramas são recebidos pela ordem em que são recebidos, e se existirem múltiplos datagramas, é da responsabilidade da aplicação específica assegurar que sejam correctamente montados.

11.5. Comando NETSTAT

Como posso mostrar as ligações ligadas do nosso computador a vários servidores no Windows? Para tal, pode utilizar Wireshark, através do qual pudemos verificar tudo o que passa pela nossa placa de rede, e também utilizar o comando NETSTAT na consola Windows. Uma vez introduzido, podemos manter um registo das ligações activas que temos. A saída deste comando mostra o tipo de protocolo da camada de transporte utilizado para a ligação, a tomada do meu computador, ou seja, o endereço IP com o número da porta, a tomada do servidor ao qual estamos ligados, e o estado da ligação.

Os programas podem ser chamados com vários argumentos, e uma lista e descrição dos mesmos será exibida quando o comando netstat /help for introduzido.

Como podem ver na imagem acima, existem muitas destas ligações, e isso porque, em primeiro lugar, utilizo o Windows 10, que é conhecido por enviar algo para os servidores da Microsoft quase sempre, e além disso, configurei a sincronização com os serviços de nuvem e existe um programa antivírus que também se liga aos seus servidores. Então como verificamos a que serviços o nosso computador está ligado? Basta executar o comando netstat -f e copiar o nome do domínio (PPM -> Tag -> Select Domain Name -> CTRL + C ou PPM -> Copy).

Podemos ver o proprietário do domínio através de whois.domaintools.com e do seu motor de busca. Basta colar no nome de domínio copiado. Como se pode ver, o proprietário deste domínio é o Google.

12. Tarefas e protocolos da camada de rede

A Camada de Rede (modelo ISO/OSI - Camada 3), também conhecida como Camada da Internet, recebe dados fragmentados da Camada de Transporte e depois realiza operações para permitir a transmissão de pacotes através da rede. Estas operações incluem:

- Endereçamento de dados utilizando endereços IP;
- Encapsulamento de dados, ou seja, a atribuição de informações adicionais requeridas pelo protocolo da camada de rede em uso;
- Routing, ou seja, seleccionar a melhor rota para a encomenda;
- Decapsulação, que remove esta informação adicional quando o pacote chega ao seu destino.

Sabemos que a comunicação em rede é regida por certas regras, um protocolo de comunicação. Sabemos também que cada camada utiliza o seu próprio protocolo, independente da outra. A camada de rede, onde elas também aparecem, não é diferente. O protocolo de comunicação mais comum para esta camada é o IPv4. A razão mais importante para o utilizar é que se trata de um protocolo aberto. Isto significa que não pertence a nenhuma empresa ou negócio, pelo que pode comunicar entre dispositivos de diferentes fabricantes. Já segue o IPv6, que é também um protocolo aberto.

Actualmente, muitos fabricantes de dispositivos e software estão a utilizar estes protocolos em paralelo. Talvez no futuro o IPv6 venha a substituir completamente o IPv4, mas não creio que seja demasiado cedo. Claro que também existem protocolos proprietários, tais como o protocolo IPX propriedade da Novell, que é especializada no desenvolvimento de sistemas operativos de rede, ou o protocolo AppleTalk desenvolvido pela Apple. No entanto, é seguro dizer que o IPv4 é de longe o protocolo da camada de rede mais amplamente utilizado.

12.1. Protocolo IPv4

O protocolo IPv4 está concebido de tal forma que não há necessidade de adicionar muitos dados de controlo durante o processo de encapsulamento. Fornece apenas a funcionalidade básica necessária para transmitir pacotes desde a origem até ao destino. É sem ligação, o que significa que não estabelece uma ligação antes do envio de dados e funciona numa base de "melhor esforço", o que significa que não utiliza controlo de fluxo ou qualquer reconhecimento de entrega de dados como faz o protocolo TCP, mas faz tudo o que está ao seu alcance para tornar a comunicação eficiente. É também um protocolo independente do meio, o que significa que os dados podem ser transferidos entre anfitriões, independentemente do meio utilizado.

Afinal de contas, numa rede podemos estar a utilizar um par torcido, noutra fibra e numa terceira onda de rádio. O protocolo IP funciona exactamente da mesma forma em todas as redes. O problema que pode surgir ao enviar dados através de diferentes meios é o tamanho máximo do pacote, que é o valor MTU (Maximum Transmission Unit), se o pacote for demasiado grande, os routers ligados à rede dividi-lo-ão em pedaços mais pequenos. Este processo chama-se fragmentação, que é outro termo do nosso dicionário de Internet.

Para ajudar a compreender como funciona o IPv4 e como os pacotes são transmitidos através da Internet, vou utilizar o exemplo de um pacote enviado pela minha tia dos Estados Unidos para explicar como funciona. O pacote consiste em 3 caixas de cartão unidas entre si. A minha tia escreveu um endereço para o presente e enviou-o para a empresa de correio rápido. Quando ela envia a embalagem, ela desiste de opções adicionais, tais como confirmação de recepção ou rastreio. Um empregado da empresa marca a embalagem com o destino e o endereço de devolução antes de libertar a encomenda. Foi transportada de carro para o porto juntamente com dezenas de outras encomendas, onde foi embalada num contentor e depois atravessou o oceano.

No porto de destino, os contentores são desembalados, as encomendas são seleccionadas e depois transportadas de carro para as várias cidades e pontos de recolha locais. A partir do ponto de recolha de carro, a encomenda deve ser entregue no endereço especificado, mas acontece que as três caixas combinadas são demasiado grandes para serem transportadas num carrinho, pelo que o estafeta separa-as em caixas individuais e entrega-as como tal. Como a sua tia não escolheu as opções adicionais, a empresa de correio não lhe entregou um recibo. Pode fazê-lo você mesmo, por exemplo, telefonar à sua tia para lhe dizer obrigado

Converter isto em comunicação IP ficaria assim:

· A encomenda é enviada sem notificação prévia ao destinatário - temos um modo sem ligação;

· Durante o processo de encapsulamento, é atribuída uma fonte e um endereço de destino

- no nosso caso, o endereço de casa do destinatário é o endereço de destino e o endereço de casa da tia é o endereço de retorno;

· A remessa não continha muitos dados de controlo, o que poderia atrasar a comunicação - para o que a minha tia desistiu de uma opção extra, confirmação e rastreio;

· As encomendas chegam ao seu destino via fibras ópticas, pares torcidos

e ondas de rádio - uma vez que as encomendas são entregues por vários meios de transporte: barcos, carros grandes, carros pequenos;

· A parcela é demasiado grande para ser enviada na sua totalidade através de uma das redes, tornando-a fragmentada - ou seja, a parcela é dividida a dada altura para que possa ser transportada num pequeno carro;

· A IP não enviou um aviso de recepção do pacote - tal como a empresa não garantiu à tia que o pacote tinha chegado. Como qualquer protocolo de comunicação, o IPv4 também tem cabeçalhos padronizados para adicionar informação de controlo. Um exemplo de um cabeçalho IPv4 típico é mostrado abaixo.

<table>
<tr><td>Versão</td><td>IHL</td><td>Tipo de serviço</td><td colspan="2">Comprimento da embalagem</td></tr>
<tr><td colspan="3">Identificação</td><td>Bandeira</td><td>Movendo um fragmento</td></tr>
<tr><td>TTL</td><td colspan="2">Protocolo</td><td colspan="2">Cheque de cabeçalho</td></tr>
<tr><td colspan="5">Endereço de origem</td></tr>
<tr><td colspan="5">Endereço de
destino</td></tr>
<tr><td colspan="3">Opções</td><td colspan="2">Preenchimento</td></tr>
</table>

· endereço IP de destino - o endereço IP do dispositivo para o qual os dados são dirigidos;

· endereço IP de origem - o endereço IP do dispositivo que está a enviar os dados;

· Time to Live (TTL) - Um campo de 8 bits que indica o tempo de vida restante do pacote. O valor TTL diminui pelo menos 1 de cada vez que o pacote passa pelo router (ou seja, após cada salto). Quando o valor atinge 0, o router descarta o pacote e retira-o do fluxo de dados da rede. Este mecanismo impede a transmissão infinita de pacotes que não podem chegar ao seu destino entre os chamados loops de encaminhamento. Se forem permitidos loops de encaminhamento, a rede ficará sobrecarregada com pacotes que nunca chegarão ao seu destino. A diminuição do valor TTL em cada laço assegura que eventualmente chegará a 0, e os pacotes com um campo TTL de 0 serão descartados.

· Protocolo - este valor de 8 bits especifica o protocolo de camada mais alto (transporte) utilizado, tal como UDP ou TCP.

· Tipo de Serviço (ToS) - contém um valor de 8 bits que determina a prioridade de cada pacote.

· Fragment Offset - Um campo utilizado na reconstrução de pacotes divididos por routers. Indica a ordem em que cada pacote deve ser organizado durante a reconstrução.

· Mais Fragmentos (MF) bandeira - Um único bit utilizado com o campo Fragment Offset para partição de pacotes e reconstrução. A colocação da bandeira MF indica que o fragmento não é o último fragmento no pacote. Quando o anfitrião receptor repara num pacote recebido com MF = 1 conjunto, verifica o campo Fragment Offset para colocar o fragmento durante a reconstrução do pacote. Quando o hospedeiro receptor repara que um pacote de entrada tem MF = 0 conjunto e tem um valor não nulo no campo offset do fragmento, utilizará o fragmento como o último bloco do pacote reconstruído.

· DF (Don't Fragment) flag - Uma única bit que, se definida, indica, que a fragmentação dos pacotes não é permitida. A fragmentação de pacotes não é permitida se a bandeira DF estiver hasteada.

· Versão - contém o número da versão do protocolo IP (neste caso IPv4).

· Comprimento do cabeçalho (IHL) - determina o tamanho do cabeçalho do pacote.

· Comprimento do pacote - este campo dá o tamanho total do pacote em bytes, incluindo o cabeçalho e os dados incluídos.

· Identificação - este campo é utilizado para identificar de forma única o fragmento de um pacote IP dividido.

· Header checksum - este campo é utilizado para verificar a existência de erros de cabeçalho de pacotes.

· OPÇÕES - este é o espaço no cabeçalho do IPv4 para campos adicionais para suportar outros serviços. No entanto, é raramente utilizado.

12.2. Endereçamento IPv4

Uma das principais tarefas da camada de rede é o endereçamento. O endereçamento em redes IP é muito semelhante ao endereçamento que nós humanos utilizamos. Claro que só ao nível lógico é que o mecanismo de endereçamento é diferente. Os anfitriões na rede são agrupados para facilitar a gestão e o endereçamento.

Tal como as pessoas, vivemos em ruas específicas da cidade. Como resultado, a remessa da minha tia americana acima chegará ao destinatário sem qualquer problema. Primeiro por ferry para a Polónia, depois por camião para a sua cidade, e depois por carro mais pequeno para a rua e número da casa. Isto é muito semelhante ao endereçamento do anfitrião. Os pacotes enviados entre redes chegam primeiro à rede a que o anfitrião pertence, e são depois enviados para um anfitrião específico. Este tipo de endereçamento chama-se endereçamento hierárquico porque a informação geral, que é, no caso de transferência de dados, o endereço da rede, é lida primeiro, seguida pela informação específica, que é o endereço IP do anfitrião específico.

Numa rede informática, os anfitriões podem comunicar uns com os outros de três maneiras:

· utilizar uma única transmissão;

· via multi-missão;

· via transmissão.

A emissão unicast é a mais comum e é utilizada para uma ligação típica entre dois anfitriões. Por exemplo, quando um cliente envia um pedido a um servidor, utiliza um único transporte de difusão para o fazer.

A utilização de transmissão multicast pode reduzir significativamente o consumo de largura de banda de uma rede, uma vez que um único pacote não é enviado para múltiplos anfitriões como uma transmissão unicast, mas um único pacote é enviado que pode chegar a múltiplos destinatários simultaneamente.

Os encaminhadores podem utilizar multicast para trocar informações de encaminhamento e distribuir software. O multicast utiliza um conjunto especial de endereços, chamados endereços de grupo, e no protocolo IPv4 esta é a gama mostrada abaixo:

de 224.0.0.0.0 a 239.255.255.255

A Broadcast, por outro lado, envia um pacote a todos os anfitriões de uma determinada rede. Isto utiliza um endereço especial, o endereço de difusão, de modo que os endereços de todos os anfitriões da rede não são armazenados nos pacotes IP. É tecnicamente impossível, então, utilizar uma e duas emissões, por exemplo, quando o endereço de um determinado dispositivo é desconhecido. Este tipo de transporte é mais frequentemente utilizado em redes locais, e a radiodifusão raramente é utilizada para comunicar com anfitriões fora de uma determinada rede local.

Ao longo do grupo de endereços IPv4, existem vários grupos de endereços conhecidos como endereços para fins especiais. Estes são endereços que não são utilizados para comunicação WAN. Entre estes endereços especiais encontram-se os chamados endereços de loopback. Um endereço de loopback nada mais é do que um endereço próprio. Para além do endereço IP válido utilizado para comunicação, a cada computador da rede é também atribuído o seu próprio endereço, o mais comum 127.0.0.1. Além disso, cada endereço no pool é utilizado para verificar a configuração do IPv4 no anfitrião.

Outro tipo especial de endereço é o endereço da ligação local. Estes tipos de endereços são utilizados quando um anfitrião deve obter um endereço IP de um servidor DHCP, mas por alguma razão o endereço não está disponível. O anfitrião receberá então um endereço do grupo de endereços da ligação local. As transferências de dados utilizando tais endereços só podem ter lugar na rede local onde os dados do anfitrião estão a correr. Existe também um conjunto final de endereços especiais, endereços TEST-NET. Tal como os endereços ligados localmente, estes só são utilizados para comunicação na rede local, para fins educativos. Podem ser utilizados em documentação ou exemplos, tais como cursos em linha. No entanto, não devem ser utilizados permanentemente. As gamas de endereços especiais são apresentadas no quadro abaixo:

Gama de endereços	Nome
127.0.0.1 - 127.255.255.254	Loopback
169.254.0.1 - 169.254.255.254	Local-Link
192.0.2.0 - 192.0.2.254	Educativo (Test-Net)

12.3. Teste da camada de rede

Cada sistema operativo implementa programas que nos permitem testar a camada de rede. Um destes é o programa PING, que é utilizado para testar a conectividade entre anfitriões. Este nome está disponível em Windows e em várias distribuições Linux. A outra é o programa TRACERT, que é utilizado para testar o encaminhamento entre um anfitrião de origem e um anfitrião de destino. Nos sistemas baseados no kernel Linux, o mesmo programa chama-se TRACEROUTE.

PING utiliza outro protocolo de camada de rede, ICMP, para enviar um datagrama de pedido de eco e esperar por uma resposta. Quando a resposta é recebida, mostra-nos o tempo decorrido entre o envio do pedido e a recepção do feedback. O PING pode ser utilizado para testes:

· A chamada pilha local, ou seja, para verificar a correcta instalação do protocolo IP no computador, basta introduzir o comando PING na consola Windows, usando um dos endereços de feedback, ou seja, na gama 127.0.0.1 a 127.255.255.254:

· É estabelecida uma ligação a um anfitrião na rede local, depois em vez do endereço do loopback, é introduzido o endereço do anfitrião na rede local (por exemplo 192.168.0.1):

· Ligue-se ao anfitrião na rede remota. Aqui, se quiser verificar a comunicação com o servidor onde a página é armazenada, pode introduzir o nome do domínio, ou seja, facebook.com, em vez do endereço IP:

Por vezes podemos não receber uma resposta a um pedido de eco enviado pelo programa PING, mesmo que a rede remota esteja a funcionar e a comunicar correctamente. Isto acontece porque alguns administradores de rede restringem ou impedem completamente a inserção de datagramas ICMP nas suas redes por razões de segurança.

Outra parte dos testes da camada de rede é examinar o encaminhamento de pacotes do hospedeiro de origem para o hospedeiro de destino. Milhares de routers operam na rede de área ampla, criando o que é conhecido como Internet, ligações entre redes locais espalhadas por todo o mundo.

Para verificar que routers um pacote está a ser enviado, por exemplo, de um computador para um servidor web, utilizaremos TRACERT para Windows ou TRACEROUTE para Linux. Funcionam exactamente da mesma forma e, à semelhança do PING, utilizam o protocolo ICMP

protocolo e mensagens de eco. Para realizar o teste, basta digitar TRACERT na consola juntamente com o endereço do anfitrião alvo. Este pode ser um endereço IP, ou um endereço de domínio se se quiser testar o encaminhamento para um host específico, como o wp.pl.

13. Tarefas da camada de ligação de dados

O papel principal e essencial da camada de ligação de dados é fornecer camadas superiores com acesso ao meio de transmissão. Os dados que descem pela pilha à medida que passam pelas camadas devem, a dada altura, ser entregues ao meio através do qual chegam ao seu destino, o hospedeiro receptor. Esta é a função principal da camada de ligação de dados: armazena dados das camadas mais altas no meio.

A camada de rede discutida na secção anterior deste curso incluía segmentos

com endereços IP recebidos da camada de transporte durante o processo de encapsulamento para formar os pacotes. Estes pacotes chegam à camada de ligação de dados antes de serem enviados para o hospedeiro de destino, e depois passam através da camada de ligação de dados para o meio de transmissão. Antes disso, porém, os pacotes receberam mais informação de controlo, desta vez o endereço físico do dispositivo, o endereço MAC de 48 bits.

Os pacotes tornam-se então quadros e são estes quadros que vão para a portadora para posterior transmissão para o anfitrião de destino. O endereço MAC é atribuído durante o fabrico do cartão e armazenado na ROM. A ROM é apenas de leitura, pelo que não é possível alterar os endereços atribuídos a nível de cartão ou hardware. Contudo, tais endereços podem ser alterados ao nível do sistema do dispositivo, por exemplo, no sistema operativo. Por vezes, os administradores fazem tais alterações ao nível do sistema, por exemplo, quando não querem reconfigurar o hardware da rede, como por exemplo quando um novo computador entra na rede.

A própria camada de ligação de dados é o intermediário entre o meio de transmissão e o software de rede. No caso de dispositivos terminais, ou seja, computadores, servidores ou telefones, é a única camada implementada não só no domínio do software, mas também no domínio do hardware. A representação física da camada de ligação de dados é a placa de rede que instalamos no nosso computador. Estas placas são a interface entre o software de rede e o meio de transmissão. Uma vez que a camada de ligação de dados funciona a dois níveis, a nível do hardware e do software, as suas funções e as tarefas estão também divididas em duas subcamadas mais pequenas:

- LLC (Logical Link Control),
- MAC (controlo de acesso aos meios de comunicação social).

A sub-camada LLC enquadra informação sobre o protocolo da camada de rede em uso, de modo que diferentes protocolos da camada de rede, tais como IPv4, IPv6 ou IPX, podem utilizar o mesmo meio de transmissão e placa de rede, e as suas funções no computador são executadas pelo controlador da placa de rede. Por outro lado, o subcamada MAC define as regras de acesso ao meio e executa as funções de endereçamento. O método MAC foi discutido no primeiro episódio desta série.

Em resumo - a camada de ligação de dados:

- receber dados da camada de rede,
- criar molduras que possam ser transmitidas através do meio,
- dá o endereço físico da moldura,
- Responsável pelo controlo do acesso ao meio.

Esta camada é implementada em dispositivos finais como computadores, mas também em routers e switches.

Quadro e comunicação da camada de ligação de dados.

Existem muitas soluções e muitas normas de rede para implementar a funcionalidade de Camada 2. Temos normas Ethernet, temos redes sem fios, e finalmente temos muitos protocolos de rede que funcionam sobre WANs, tais como Frame Relay. Portanto, não existe um frame universal. Cada padrão de rede tem a sua própria estrutura, específica para uma solução particular. Para resumir o tópico, podemos assumir que uma estrutura típica de segundo nível consiste em 3 partes principais:

Manchete	Dados	Rodapé
endereços MAC de origem e destino sinal de arranque da moldura	pacotes de rede/camada da Internet	soma de verificação do sinal de fim de quadro

Vamos agora seguir o processo de comunicação entre dispositivos, centrando-nos nas funções da camada de ligação de dados. Suponhamos que o nosso computador envia um pedido a um servidor web numa rede remota.

Os dados para enviar tal pedido já estão encapsulados num único pacote com o número de porta e endereço lógico da aplicação, ou seja, o endereço IP do computador e do servidor.

Antes de um pacote entrar no meio de transmissão, a camada de ligação de dados deve construir uma moldura com os endereços MAC correspondentes do emissor e receptor da moldura. No caso do endereço MAC do remetente, a coisa é óbvia, é apenas o endereço MAC do computador, mas e o endereço do anfitrião de destino? Se o computador e o servidor web não estiverem na mesma rede e o endereço MAC da sua placa de rede não puder ser determinado, isto é tecnicamente impossível. Porquê? Porque os endereços MAC só são utilizados para comunicação dentro de uma rede e nunca fora da rede. Portanto, o endereço MAC da interface do router ao q1u2al.oTnaosrseofcaosmpduatacdaormesatdá aligdadeo será armazenado no campo da moldura que contém o endereço MAC de destino.

A moldura é enviada através do meio de transmissão para o primeiro router. Este último, ao receber o frame, descapsula-o para que possa ler o endereço IP do dispositivo para o qual o pacote está a ir. Os endereços IP não podem ser lidos directamente dos fotogramas de Camada 2, pelo que é necessária a decapsulação. Uma vez lido o endereço IP do pacote (uma vez decapsulado o frame, os dados tornam-se novamente um pacote), compare-o com a entrada na tabela de encaminhamento e encontre a entrada que indica que a rede do servidor é encaminhada através de outros routers.

Criará então um novo frame no qual o endereço de origem será o endereço MAC da interface que se liga ao outro router, e o endereço MAC de destino desse router.

O frame passa então através do meio para o segundo router, que encapsula novamente o frame para ler o endereço IP do pacote. Descobre que o destinatário dos dados é um dispositivo que opera na rede, directamente ligado a ele, pelo que o processo de encapsulamento realizado pelo segundo router volta a acontecer, desta vez introduz o endereço MAC do seu segundo router no campo de endereço MAC. A interface é utilizada como endereço de origem e o endereço MAC do servidor de endereços é utilizado como endereço de destino.

Os quadros preparados desta forma vão para o servidor, que também os decapsula. Desta vez, porém, é o dispositivo para o qual os dados apontam, pelo que os descapsula completamente, ou seja, lê adicionalmente o número da porta da aplicação a fim de enviar os dados para a aplicação específica correspondente, neste caso um serviço web.

O serviço de rede prepara então os dados de resposta. Os dados vão primeiro para a camada de transporte, onde o número da porta de aplicação é atribuído, depois para a camada de rede, formando um pacote com o endereço IP correspondente, e finalmente para a camada de ligação de dados, onde um frame é preparado a partir do pacote, marcado com os endereços MAC do servidor e router para o servidor ligado.

A resposta é então transmitida aos meios de comunicação social, que são então enviados para o cliente. Durante este processo, passa por dois routers, que realizam um processo de decapsulação e recapsulação, e como têm de ler o endereço IP, podem transmitir a resposta. Finalmente, a resposta pertence ao cliente. Isto desempacota os dados, permitindo ao navegador exibir a página web.

13.1. Protocolo ARP

Como utilizadores da rede, quando transferimos dados de um dispositivo para outro, sabemos o endereço IP ou o nome de domínio do dispositivo, pelo que podemos realizar tais transferências. Pior ainda são os endereços MAC, com base nos quais nós utilizadores da rede não determinamos o destinatário dos dados, isto acontece fora de nós. Em redes de computadores baseadas em IPv4, um protocolo chamado ARP (Address Resolution Protocol) é utilizado para obter informações sobre o endereço MAC de um determinado dispositivo.

O ARP é um mecanismo que permite mapear endereços lógicos (isto é, IP) para endereços físicos (isto é, MAC). Suponha que um computador que quer enviar dados para outro dispositivo conhece o seu endereço IP, mas não sabe o seu endereço MAC. Para saber este endereço, o computador que envia os dados criará uma moldura de difusão ARP e difundi-lo-á para todos os dispositivos na mesma rede antes de enviar os dados especificados. O campo de endereço de origem do frame armazena o endereço do computador que preparou o frame e o campo de endereço de destino armazena o endereço MAC de difusão: FF-FF-FF-FF-FF-FF-FF.

Cada dispositivo que recebe um frame descapsula-o num pacote e verifica se o endereço IP do campo de destino é o seu endereço. Se o endereço IP de destino não for o seu, ignorará o pacote; se for o seu endereço IP, criará um novo frame armazenando o seu endereço MAC e enviá-lo-á para transmissão.

O computador que envia o quadro de difusão conhece agora o endereço físico do dispositivo com o qual pretende comunicar e pode iniciar essa comunicação. A informação de mapeamento IP para MAC é armazenada na tabela ARP de cada dispositivo para utilização posterior. Por defeito nos sistemas Windows, tais entradas duram até 10 minutos e são depois apagadas. Para visualizar a tabela ARP, execute arp -a a partir da consola. Como pode ver, há aqui várias entradas, o que significa que houve comunicação entre o meu computador e outro dispositivo nos últimos 10 minutos.

13.2. Ethernet

O trabalho sobre esta norma remonta aos anos 70, quando a Xerox, uma das maiores empresas tecnológicas, decidiu conceber uma norma de comunicação em rede aberta que iria servir as pessoas durante anos. No final da década de 1970, desenvolveu uma norma para redes locais e tornou-se o protótipo para Ethernet. Actualmente, a Ethernet é o padrão que pode ser encontrado na maioria das redes locais de computadores em todo o mundo e, devido às suas muitas vantagens, tornou-se também o padrão para redes de cidades e, em alguns casos, até mesmo para redes de área ampla.

A Ethernet é um conjunto completo de soluções de rede implementadas tanto na camada de ligação de dados como na camada física. O desenvolvimento desta tecnologia está actualmente a ser supervisionado pelo IEEE (Institute of Electrical and Electronics Engineers), que publicou a sua norma em 1985 e a descreve sob os números 802.2 e 802.3. A norma 802.2 inclui funções relacionadas com a sub-camada LLC, que está relacionada com a sub-camada MAC e a camada física do modelo OSI.

Muitos factores contribuem para o sucesso de soluções baseadas em Ethernet, incluindo:

- fácil de implementar,
- fiabilidade,
- capacidade de adaptação de novas tecnologias,
- Os custos de implementação são relativamente baixos.

13.3. Evolução da Ethernet

Vamos agora discutir a evolução da Ethernet. As versões iniciais da norma,chamadas redes espessas (chamadas thick Ethernet) e redes finas (chamadas so-denominadas thin Ethernet), tinham poucas capacidades em comparação com o que temos hoje. As versões mais antigas operam num meio de transmissão em cobre (cabo coaxial).Utilizam uma topologia física de bus, que se caracteriza por todos os dispositivos estarem ligados a um meio comum. A solução requer um controlo de acesso aos meios de transmissão, que é implementado utilizando a abordagem CSMA/CD.

Após muitos anos de utilização de soluções baseadas na topologia dos autocarros como meio de transmissão, verifica-se que esta solução já não é suficientemente eficiente. O rápido crescimento da rede levou a exigências de largura de banda e fiabilidade cada vez maiores por parte dos utilizadores. Em vez de cabos coaxiais, são amplamente utilizados cabos de par trançado, cabos UTP e novas topologias. Apareceram topologias estelares, as mesmas utilizadas actualmente, mas utilizando hubs em vez de switches como ponto central da rede. Ninguém tinha ouvido falar de comutadores nessa altura.

A utilização de hubs melhorou em certa medida o desempenho das redes informáticas, mas rapidamente se tornou evidente que esta solução também não era a ideal. A característica básica de um hub é que transmite dados a todos os dispositivos a ele ligados. Funciona desta forma, que um computador que queira enviar dados para outro dispositivo efectue esta comunicação através do centro. Este último, por outro lado, não é tão inteligente a ponto de transferir dados para o dispositivo apropriado, simplesmente envia dados para todos os que a ele estão ligados.

Apenas os dispositivos para os quais os dados são enviados analisam o endereçamento para determinar se são destinatários. Se não forem destinatários, ignoram os dados, e se o forem, interpretam-nos.

Este tipo de solução significa que embora a topologia física seja uma topologia estelar, é logicamente semelhante à utilizada na geração anterior de Ethernet. Também aqui é utilizado um método de acesso por link baseado em CSMA/CD, que se tornou ineficiente devido ao rápido crescimento da rede. Além disso, cada hub cria um chamado domínio de colisão.

Quanto mais dispositivos estiverem ligados ao centro, maior será o domínio da colisão, e quanto maior o domínio da colisão, maior a probabilidade de colisões, limitando a produção e criando requisitos para retransmissões frequentes de dados. Mais colisões não são o único problema associado à utilização de hubs. Outras desvantagens de tais dispositivos incluem a escalabilidade limitada e o aumento dos atrasos na transmissão de dados, entre outras coisas devido aos choques acima mencionados.

Os esforços para resolver os pontos fracos da Ethernet baseada em hubs continuaram ao longo dos anos até à invenção de um dispositivo de rede inteligente chamado switch, que resolvia os problemas que flagelavam as versões anteriores da Ethernet.

Os interruptores nas redes informáticas ainda hoje existem e não há qualquer indicação de que isto venha a mudar em breve. Porque é que estes dispositivos são tão populares e porque são tão inteligentes? Bem, ao contrário de um hub, um comutador não envia dados para todos os dispositivos ligados a ele, mas apenas para o dispositivo específico ao qual os dados se destinam, contornando obviamente a transmissão, como a transmissão ARP discutida anteriormente. Existe uma topologia lógica ponto-a-ponto entre a porta de comutação à qual o dispositivo está ligado e o próprio dispositivo. Os dados enviados para um determinado dispositivo são-lhe enviados e apenas a ele.

A utilização de um interruptor elimina quase completamente o risco de colisões, uma vez que os dispositivos não têm de competir entre si pelo acesso ao meio. Ao mesmo tempo, o tamanho do domínio da colisão é limitado, uma vez que tal domínio consiste apenas nas portas do interruptor e nos dispositivos a ele ligados. Há muitas mais vantagens dos interruptores. Cada dispositivo ligado a uma porta de comutador tem uma largura de banda dedicada disponível.

Por exemplo, se um switch oferecer uma taxa de transferência de 100 Mbps, esta largura de banda estará disponível para cada dispositivo ligado a ele.

Com um hub, esta largura de banda é partilhada entre todos os dispositivos. Utilizando um comutador, os dados também podem ser transmitidos em modo full-duplex, o que significa que os dispositivos ligados a ele podem receber e enviar dados em simultâneo.

Existem várias versões da norma Ethernet em uso hoje em dia. A mais popular destas é a norma que oferece rendimentos nominais até 100 Mbps, conhecida como norma FastEthernet. A transmissão neste padrão é feita sobre apenas 2 pares de cobre em vez de 4 pares torcidos. É uma solução comum utilizada em muitas redes informáticas.

Na maioria dos casos, satisfaz os requisitos das redes informáticas.

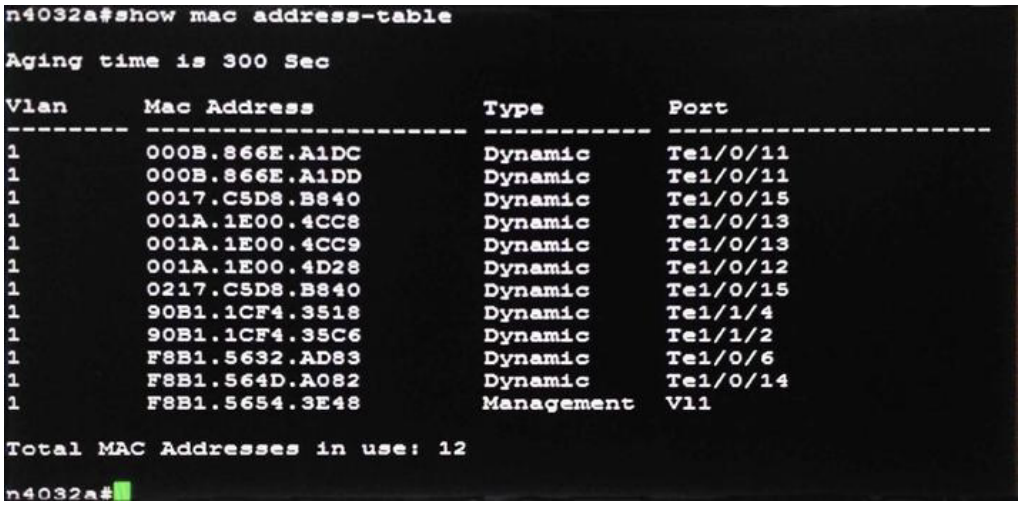
A norma Gigabit Ethernet pode ser utilizada quando a procura de largura de banda da rede aumenta com a quantidade de dados a ser transmitida. Nominalmente, fornece uma taxa de transmissão de 1 Gbps. Se for utilizada a norma 1000BASE-T, todos os cabos de cobre de par trançado são utilizados para a transmissão. Esta versão de Ethernet é utilizada por grandes redes locais que utilizam comunicação.

Usando a norma Ethernet, os dados também podem ser transmitidos através de ligações de fibra óptica, caso em que a norma Gigabit Ethernet é chamada 1000BASE-SX ou LX. Existem também normas Ethernet que fornecem comunicação a 10 ou mesmo 100 Gbps. São principalmente utilizadas em redes metropolitanas e de área ampla porque são muito, muito dispendiosas de implementar e poucas pessoas podem dar-se ao luxo de utilizar este tipo de solução numa rede local. A tabela abaixo mostra as versões mais populares das normas Ethernet e o meio de transmissão que elas utilizam:

Norma Ethernet	Máximo rendimento	Meio de transmissão utilizado	Distância máxima
100BASE-TX (fastEthernet)	100 Mbps	UTP (cat. 5/5e)	100 metros
100BASE-FX (fastEthernet)	100 Mbps	Fibra óptica (simples/multi-modo)	400/2000 metros
100BASE-TX (gigabitEthernet)	1 Gbps	UTP (cat. 6)	100 metros
100BASE-SX (gigabitEthernet)	1 Gbps	Fibra óptica multimodo	550 metros
100BASE-LX (gigabitEthernet)	1 Gbps	Fibra óptica monomodo	2000 metros
10GBASE-T (10gigabitEthernet)	10 Gbps	UTP (cat. 6/7)	100 metros
10GBASE-LX4 (10gigabitEthernet)	10 Gbps	Modo único/multi-modo fibra óptica	300/10000 metros

Os comutadores descritos acima utilizam endereços MAC para transferir dados entre dispositivos ligados às portas dos comutadores. Cada comutador tem algo chamado tabela de endereços MAC. Isto nada mais é do que uma recolha de informação que determina qual o dispositivo,

Na realidade, qual o endereço MAC de um dispositivo está ligado a uma determinada porta.



As entradas em tal tabela são acrescentadas dinamicamente e não pelo administrador. O interruptor recupera a informação armazenada na tabela durante o processo de aprendizagem. A partir de um frame recebido, o comutador lê o endereço MAC de origem e adiciona-o à sua tabela, atribuindo o número da porta em que recebeu o frame. Por sua vez, se não souber para quem enviar tal frame porque não há entrada para o endereço MAC do destinatário na tabela, ocorre um processo chamado flooding.

Isto pode ser comparado à radiodifusão, uma vez que a moldura é enviada para todos os dispositivos excepto o remetente. O dispositivo ao qual o frame não é endereçado descarta-o, enquanto que o dispositivo receptor responde e envia o frame para o interruptor. O comutador lê o endereço MAC do remetente a partir do frame e armazena-o na sua tabela. Todo o processo de aprendizagem e inundação é mostrado no vídeo tutorial. Moldura Ethernet

Uma vez que a norma Ethernet funciona na segunda camada do modelo OSI, pode adivinhar, que também cria as suas próprias estruturas. Claro que sim, a Ethernet encapsula a sua própria moldura, chamada moldura Ethernet. Pode ver uma moldura de exemplo abaixo:

Tamanho do campo em bytes	7	1	6	6	2	46 - 1500	4
Nom e do campo	Preâmbulo	Marcador de partida da moldura	MAC do destinatário endereço	Remetente MAC endereço	Comprimento /Tipo	Dados e preenchimento	Moldura Código de Controlo (FCS)

· Preâmbulo e Marcador de início de armação - estes campos são utilizados para informar o dispositivo alvo de que está pronto para receber armações;

· O endereço MAC alvo, que é o endereço físico do destinatário da moldura;

· O endereço MAC de origem, que é o endereço físico do anfitrião de envio;

· Comprimento/Tipo - O campo comprimento especifica o tamanho do quadro, enquanto o tipo especifica o protocolo utilizado pelas camadas superiores, sendo o mais comum o IPv4;

· Dados - este é o pacote recebido da camada de rede. O tamanho mínimo deste campo deve ser de 46 bytes e o tamanho máximo deve ser de 1500 bytes. Se o pacote for menor que 46 bytes, é suplementado com dados aleatórios para aumentar o tamanho de todo o quadro para o mínimo exigido, ou seja, um máximo de 64 bytes.

· Frame check code - campo contendo frame checksum, utilizado para detectar possíveis erros de frame. O dispositivo que envia os dados calcula a soma de controlo e coloca-a na moldura, o receptor de dados também calcula a soma de controlo após a recepção dos dados; se ambas as somas de controlo estiverem correctas, a moldura é aceite, se forem diferentes, a moldura é considerada danificada e rejeitada.

O tamanho total da moldura pode ir até 1518 bytes (o preâmbulo e o início do sinal da moldura não são tidos em conta ao calcular o tamanho da moldura).

Existe também uma estrutura Ethernet moldura com um comprimento máximo de 1522 bytes. Estas molduras são utilizadas em LANs virtuais, nas chamadas VLANs.

14. Questões básicas da comunicação VoIP

Definições-chave

VoIP - https://pl. wikipedia. org/wiki/Voice_over_Internet_Protocol PBX - https://pl.wikipedia.org/wiki/PBX

Codec - https://pl.wikipedia.org/wiki/Kodek

SIP - https://pl. wikipedia. org/wiki/Session_Initiation_Protocol

O que é o VoIP?

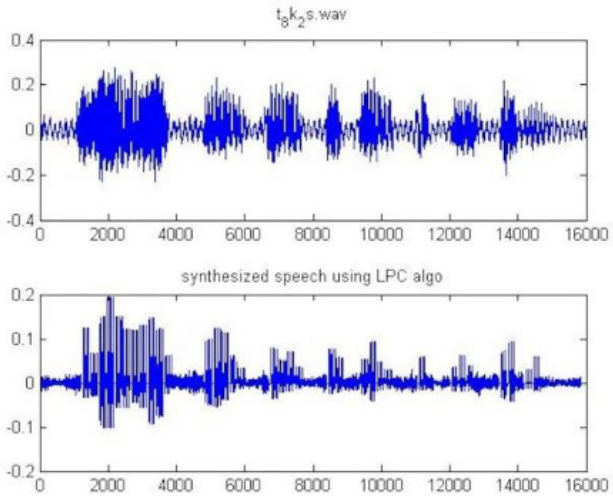
VoIP é um acrónimo de Voice over Internet Protocol (Voz sobre Protocolo Internet). É uma tecnologia que permite o envio e recepção de áudio através de uma rede informática, esta tecnologia é utilizada para fazer 'chamadas telefónicas' em tempo real.

Embora a tecnologia VoIP se tenha tornado muito popular durante a última década, a história da VoIP começa há quase 100 anos no instituto de investigação Bell Labs.

Em 1938, Homer Dudley, engenheiro dos Laboratórios Bell, criou o primeiro sintetizador de voz electrónico, conhecido como o Vocoder. O conceito de funcionamento era semelhante ao da actual transmissão de pacotes (IP), que grava amostras de voz num telefone e as reproduz em outro. Actualmente, a mesma tecnologia é utilizada não só na telefonia VoIP, mas também em implantes cocleares.

Não é possível fazer chamadas através da Internet sem uma rede informática. A história das redes informáticas começa em 1969 na Agência de Projectos de Investigação Avançados - uma agência do governo dos EUA. O trabalho da agência levou ao desenvolvimento do protocolo de rede TCP/IP e ao lançamento da primeira rede de computadores, a ARPANET. Esta rede continuou a funcionar formalmente até 1990.

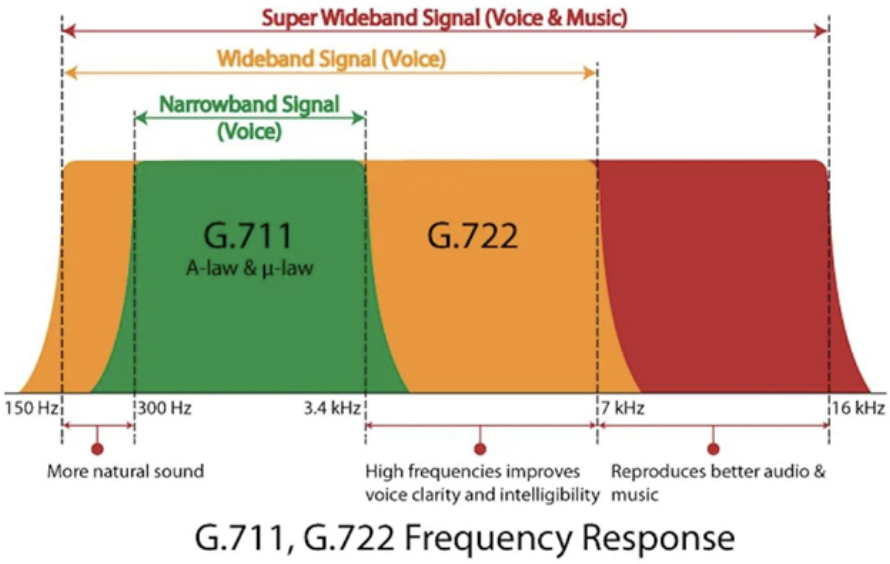
Em 1973, no MIT, Bob McAuley, Ed Hofstetter e Charlie Radar desenvolveram o primeiro pacote de voz transmitido através da ARPANET.



(Fonte: https://www.mathworks.com/matlabcentral/fileexchange/13529-speech-compression-using-linear-predictive-coding Esta transmissão de voz foi possibilitada pela LPC, ou Linear Predictive Coding - a base da moderna tecnologia VoIP. LPC é uma técnica de análise de voz que se baseia num modelo de previsão linear para processar e re-sintetizar formas digitais comprimidas de sinais de voz e fala.

Na altura, as ARPANETs não podiam ser utilizadas em privado. O primeiro cibercriminoso 'técnico' foi Leonard Kleinrock, que em 1973 enviou uma mensagem à ARPANET sobre a sua máquina de barbear eléctrica desaparecida.

Em 1974, Lincoln Lab e Culler Harrison Inc. transmitiram com sucesso pacotes de dados de voz de teste entre eles. Em 1976, a Culler Harrison e a Lincoln Labs realizaram uma teleconferência via LPC. Em 1982 fizeram progressos significativos, utilizando o LPC para se ligarem através da rede local de cabos, rede de pacotes móveis e interface com a PSTN (Public Switched Telephone Network).



Rysunek 2: Pierwszy szerokopasmowy kodek audio

(Fonte: https://www.gl.com/newsletter/g722-wideband-audio-codec-support-across-tdm-voip-platforms-newsletter.html)

Em 1988, a UIT-T aprovou o codec de áudio de banda larga G.722, um programa que permite converter áudio em linguagem 'digital' e, uma vez transmitido através da rede, converter de volta para um sinal de áudio. O codec G.722 ofereceu uma qualidade de discurso significativamente melhorada em comparação com os seus predecessores. G.722 oferece taxas de dados até 64 kbps, tornando-o ideal para comunicação VoIP - especialmente em redes locais (LANs).

Em 1989, o programador Brian C. Wiles criou o RASCAL, o primeiro sistema que transmitia voz através de redes Ethernet com sucesso - a primeira aplicação VoIP.

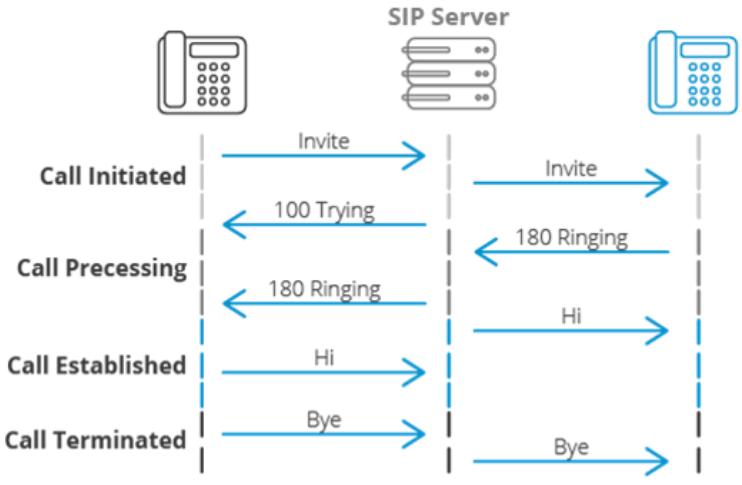
Em 1991, John Walker da Autodesk escreveu e lançou o NetFone, mais tarde conhecido como Speak Freely, o primeiro telefone VoIP baseado em software.

1993 trouxe o primeiro sistema de videoconferência, Teleport. Os criadores do Teleport foram David Allen e Herold Williams, que venderam o seu produto aos Hotéis Hilton.

A primeira aplicação comercial VoIP tornou-se o programa VocalTec Internet Phone em 1995. O programa utilizava o protocolo H.323, os requisitos eram um processador 486, 8 MB de RAM, uma placa de som de 16 bits e uma ligação à Internet SLLP ou PPP. O VocalTec era mais barato do que as chamadas telefónicas tradicionais para chamadas internacionais e de longa distância.

Em 1996, foi desenvolvido o SIP (Session Initiation Protocol). A primeira versão do SIP tinha apenas um comando - 'fazer uma chamada' - mas em 1999 as capacidades do SIP tinham sido expandidas para seis comandos. Programa VocalTec Internet Phone. O programa utilizava o protocolo H.323, os requisitos eram um processador 486, 8 MB de RAM, uma placa de som de 16 bits e uma ligação à Internet SLLP ou PPP. O VocalTec era mais barato do que as chamadas telefónicas tradicionais para chamadas internacionais e de longa distância.

Em 1996, foi desenvolvido o SIP (Session Initiation Protocol). A primeira versão do SIP tinha apenas um comando - 'fazer uma chamada' - mas em 1999 as capacidades do SIP tinham sido expandidas para seis comandos.

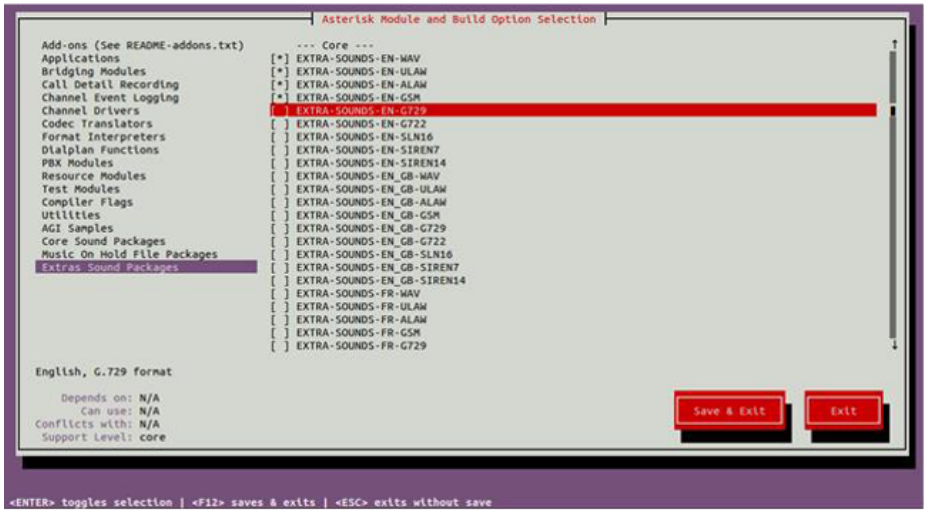


Rysunek 3: Protokół SIP

(Fonte: https://www.3cx.pl/voip-sip/sip/)

O SIP tornou-se o protocolo preferido para a telefonia móvel VoIP.

Em 1999, Mark Spencer decidiu programar o seu próprio sistema IP-PBX, um programa que funciona como uma central telefónica, e chamar-lhe Asterisk. O Asterisk é um programa de código aberto que rapidamente ganhou popularidade e ainda hoje está a ser desenvolvido e melhorado por milhares de programadores.



Rysunek 4: Instalacja asterix w systemie Linux

(Fonte: https://www.howtoforge.com/how-to-install-asterisk-17-on-ubuntu-2004/)

Em 2003, o Skype foi criado e rapidamente se tornou o comunicador de voz mais utilizado. Com o tempo, o Skype evoluiu para um mensageiro instantâneo de vídeo com capacidades de transferência de ficheiros. Hoje em dia, é propriedade da Microsoft.

Em 2006, Truphone, a primeira aplicação VoIP móvel, foi lançada para utilizadores de Nokia, iPhone, Android e Blackberry. A aplicação utiliza SIP para fazer chamadas através de uma ligação à Internet em vez de através de redes móveis.

Entre 2011 e 2015, os EUA assistiram a um grande aumento na popularidade da telefonia VoIP. A nível mundial, houve um aumento do número de fornecedores de VoIP, o que fomentou a concorrência e está a liderar ou já levou à deslocação dos sistemas telefónicos herdados.

A pandemia da COVID de 2020 mudou a natureza do trabalho para o trabalho remoto durante a noite em muitos sectores da economia. As comunicações unificadas baseadas na tecnologia VoIP permitem às equipas trabalhar remotamente e contactar clientes através de múltiplos canais, incluindo: videochamadas, aplicações móveis, chamadas em conferência, mensagens de texto de equipa, voicemail.

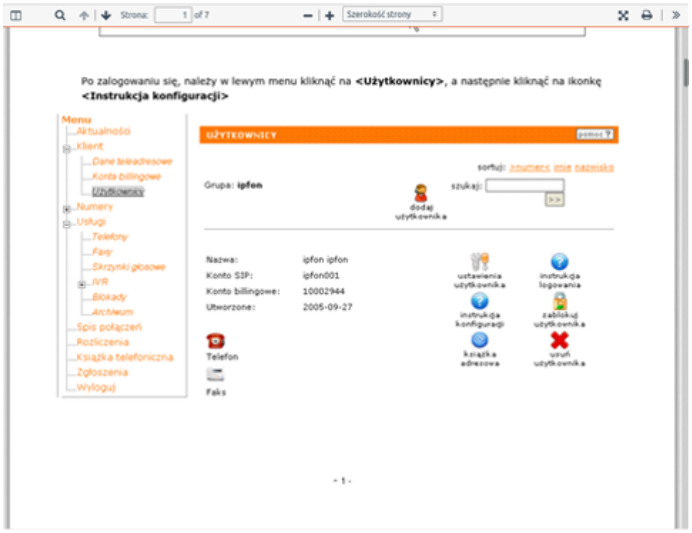
Algumas das aplicações de software mais populares que utilizam tecnologia VoIP incluem: Equipas Microsoft (o mensageiro padrão para o sistema operativo MS Windiows11), Google Meet, Zoom.

VoIP em casa, VoIP para negócios

Soluções VoIP para utilizadores domésticos

Os utilizadores domésticos são aqueles que geralmente requerem um único número de telefone.

A fim de estabelecer um número de telefone público da RTPC com um prefixo de estado e área (cidade), é necessário registar-se com um fornecedor de serviços VoIP. O fornecedor de VoIP irá, no processo de registo, criar uma conta SIP - um login e senha, e dizer-lhe como configurar o SIP. Tendo a informação da conta, podemos entrar no PBX e utilizar telefonia VoIP em aplicações para telemóveis, aplicações instaladas na Microsoft, Apple, sistemas operativos Linux, ou finalmente telefones VoIP.



Rysunek 5: Przyklad uzyskania danych logowania do konta SIP

(Fonte: https://docplayer.pl/64633184-Uzyskanie-nazwy-i-hasla-konta-sip.html)

Soluções VoIP para empresas

A fim de gerir vários telefones VoIP numa empresa, é necessário criar um PBX. O PBX pode ser ou um dispositivo físico instalado nas instalações da empresa ou um PBX virtual (software fornecido pela empresa que vende serviços telefónicos).

No caso de um PBX virtual, os telefones fixos dos empregados da empresa devem apoiar a VoIP. O custo de um telefone VoIP é comparável a um telefone tradicional, por isso, para as novas instalações da empresa, um telefone VoIP parece ser a melhor escolha.

As empresas com linhas e aparelhos tradicionais da RTPC podem ficar com os números de telefone atribuídos de duas maneiras: aquisição de um PBX VoIP com módulos PSTN/ISDN sem substituição de telefones, transferir os números para uma central telefónica virtual e substituir os telefones por telefones com capacidade VoIP.

Visão geral das aplicações VoIP

As aplicações relacionadas com VoIP podem ser divididas em:

- cliente - instalado em telefones/computadores VoIP do utilizador final
- aplicações de servidor - instaladas em servidores regulares ou em PBXs dedicados.

Aplicações do cliente

A tecnologia moderna de telemóveis baseia-se na tecnologia digital, pelo que o áudio é transmitido através de um codec.

Nos smartphones actuais, é possível adicionar um número VoIP sem instalar software adicional. Nas definições do Android ou iOS, podemos introduzir os detalhes da nossa conta SIP e utilizar a telefonia VoIP. Há também muitas aplicações VoIP que dão funcionalidade adicional (por exemplo, livro de endereços partilhados, etc.). Ao escolher como queremos utilizar a telefonia VoIP, é melhor seguir as recomendações do fornecedor do serviço VoIP. Os prestadores de serviços têm frequentemente a sua própria aplicação dedicada à utilização de serviços VoIP.

Em computadores de secretária, portáteis ou tablets sem possibilidade de ligação a uma rede móvel, podemos utilizar a VoIP através da Internet. Assim, basta ligar o seu portátil a WiFi e instalar uma aplicação VoIP para fazer chamadas telefónicas.

Existem muitas aplicações populares que permitem ligações telefónicas VoIP à rede telefónica pública comutada (PSTN) : Equipas Microsoft, ZOIPER, Blink, Zoom, etc. Podemos seguir a lista de aplicações clientes VoIP em: https://en. wikipedia. org/wiki/List_of_SIP_software ;

Aplicações de servidor

O servidor SIP gere as chamadas na rede, recebe pedidos de clientes VoIP para estabelecer e terminar chamadas.

O servidor SIP de código aberto mais popular é o Asterix (https://www.asterisk.org). Para executar o Asterix numa empresa, é necessário ter um servidor com o sistema operativo Linux instalado. Existem pacotes de software de deduplicação em distribuições Linux que contêm o servidor Asterix. A melhor maneira de instalar o servidor Asterix é descarregar uma distribuição Linux especialmente preparada - FreePBX (https://www.freepbx.org/downloads/). O Asterix tem muitas das características da telefonia moderna, incluindo, entre outras: SMS, música enquanto espera/ligação, voicemail.

15. Desempenho da rede. Métodos de redução do tráfego na rede.

Factores que afectam o desempenho da rede informática

O desempenho de uma rede informática é influenciado por:

1. As partes passivas de uma rede informática, que são as partes de uma rede informática que servem apenas para transferir dados entre dispositivos de rede activos. As partes passivas de uma rede de computadores incluem: cabos de cobre, cabos de fibra óptica, tomadas de rede, e patamares.

2. Dispositivos activos, são as partes de uma rede informática que transmitem/recebem informação ou são utilizados para transmitir/alimentar dados numa rede informática. Os dispositivos activos incluem: cartões de rede, comutadores, amplificadores/repetidores de rede.

3. Interferência electromagnética, que é o que afecta os cabos de transmissão sem fios e de cobre (par torcido).

15.1. Qualidade do cabo de par trançado

Os cabos de par trançado transportam informações sob a forma de impulsos eléctricos. Um cabo de par trançado contém 8 cordões (fios) de cobre revestidos com isolamento. Os condutores são torcidos em pares para assegurar uma melhor transmissão de dados. A velocidade e a qualidade da transmissão de dados sob a forma de impulsos eléctricos são mais afectadas por interferências electromagnéticas.

O fabrico de cabos de par trançado é influenciado por:

- o acabamento do condutor de cobre, ou seja, a pureza do metal, as dimensões do perfil retido
- a qualidade e quantidade do isolamento.

Dependendo da quantidade de isolamento e dos métodos de blindagem utilizados (protecção contra interferências), os cabos de par trançado são definidos por categoria 1 a 8 e o tipo de blindagem: U - não blindado, F - blindado em folha, S - blindado em malha, SF - blindado em folha e malha. Uma categoria superior de cabo assegura uma transmissão de dados mais rápida, por exemplo: categoria 5 UTP, ScTP, STP assegura a transmissão até 1 Gb/s; categoria 6 UTP, ScTP, STP - 10 Gb/s.

Os cabos de rede são terminados com conectores RJ45. A qualidade do material utilizado e a blindagem RJ45 afecta obviamente a transmissão de dados.

Exemplos de danos em cabos de pares torcidos

Na Figura 1, vemos um cabo de Categoria 6 feito numa fábrica utilizando uma linha de produção especializada. O cabo inserido na tomada mantém as suas propriedades e a terminação RJ45 funciona correctamente depois de ligar repetidamente o computador. A protecção contra a queda de cabos indesejados funciona correctamente - um clique característico.

15.2. Fibra Óptica

Introdução

As fibras ópticas transportam a informação sob a forma de impulsos de luz. Graças ao fenómeno de reflexão interna total, a luz que corre no interior de uma fibra óptica fica retida ali. É portanto possível transmitir informação a uma distância muito maior sem perda do que com cabos de cobre.

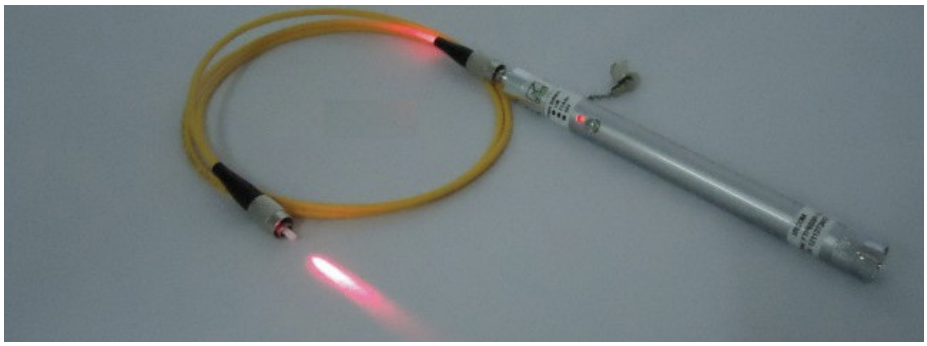
A luz que viaja dentro de uma fibra óptica é atenuada. Como não foi inventado nenhum método para produzir uma fibra óptica perfeitamente reflectora, ocorre o fenómeno da perda de potência óptica. Actualmente, os cabos de fibra óptica são capazes de transmitir informação a uma distância máxima de cerca de 100 km sem perdas. Graças à utilização de amplificadores ópticos em certos intervalos, podemos ligar locais muito distantes através de redes de fibra óptica.

A qualidade das redes de fibras ópticas é principalmente influenciada pela qualidade do trabalho realizado durante a sua colocação. Deve ser dada atenção a isso: o raio de curvatura máximo do cabo - dependendo da norma, o raio de curvatura é: 30, 10 7,5 mm, a qualidade do equipamento de corte - após o corte, o bordo da fibra óptica não deve ser desgastado, qualidade da máquina de soldar

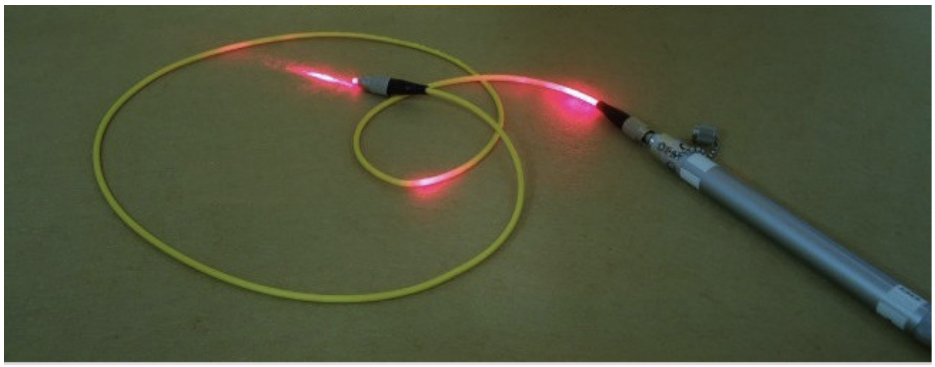
Exemplos de defeitos

Uma forma de testar um cabo de fibra óptica é utilizar um localizador de falhas visuais:

- corrigir a fibra óptica



- e danificado



Os danos acima mencionados ocorreram muito provavelmente por excederem o raio de curvatura da fibra óptica.

15.3. Comutadores de rede, cartões de rede

Um comutador de rede é um dispositivo responsável pela transferência de dados entre anfitriões em redes informáticas. Um anfitrião é qualquer dispositivo ligado a uma rede de computadores - um computador portátil, impressora, televisão, etc.

O switch tem o maior impacto no desempenho da rede. O rendimento das portas expresso em bits por segundo (100Mbit/s, 10 Gbit/s), ou seja, quantos dados podem ser transferidos para o switch num máximo de uma unidade de tempo, é o factor mais importante que determina o desempenho de uma rede informática.

O interruptor lida com múltiplas ligações entre anfitriões em simultâneo, pelo que é importante prestar atenção a parâmetros tais como a quantidade de memória, a velocidade do processador e a taxa de transferência. (Capacidade de comutação do sistema, capacidade de débito do sistema).

Os cartões de rede são dispositivos que permitem a ligação de um anfitrião a uma rede informática. O parâmetro básico de uma placa de rede é a velocidade de envio e recepção de dados expressa em bits por segundo (100 Mbit/s, 1 Gbit/s, etc.). Ao ligar um anfitrião a um switch, é importante lembrar que o desempenho da rede será o do dispositivo com o débito mais baixo - o exemplo de um switch de 100 Mbps + placa de rede de 1000 Mbps dá um débito máximo de 100 Mbps.

15.4. Testes de desempenho da rede

Interferência na rede

A perda de dados devido a interferências electromagnéticas pode ocorrer tanto em redes sem fios como em redes que utilizam cabos de cobre. As redes eléctricas, dispositivos alimentados por altas correntes produzem radiação electromagnética.

Quando qualquer parte de uma rede WiFi está na proximidade de equipamento como um comboio de tracção eléctrica ou eléctrico, é de esperar interferência com a transmissão de dados.

Os cabos de rede feitos de cobre são afectados de forma semelhante pela radiação electromagnética. As redes onde os cabos UTP estão demasiado próximos de cabos eléctricos podem ser expostos a interferências electromagnéticas.

Se se espera interferência electromagnética num determinado local, usar fibra óptica como portador de dados; estes são resistentes à radiação electromagnética.

Testes de desempenho de redes informáticas

O desempenho de uma rede informática resume-se a determinar o rendimento, ou seja, a quantidade de informação que podemos enviar através da rede testada num determinado período de tempo. A forma mais simples de determinar o desempenho da rede é, portanto, descarregar/enviar uma certa quantidade de dados e medir o tempo que leva.

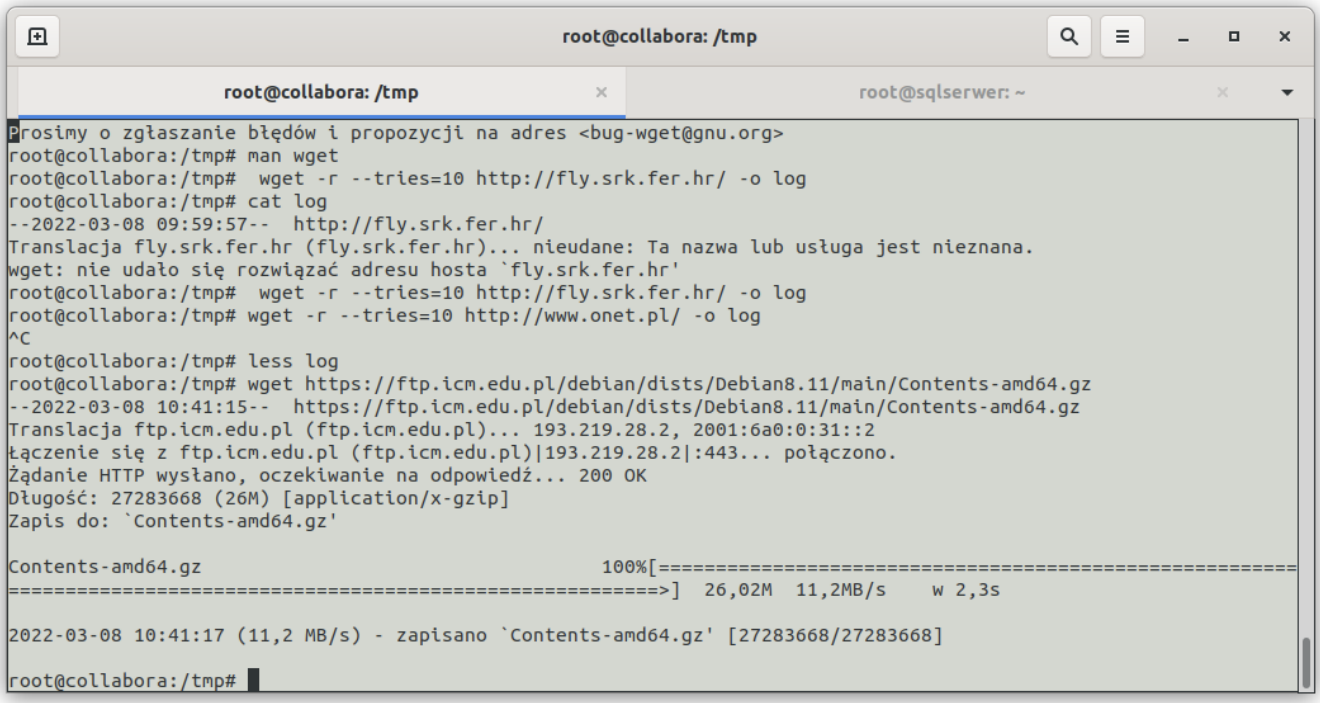
Os resultados de um teste de desempenho de rede podem ser distorcidos por outros factores que não fazem directamente parte da rede informática. Ao enviar ou descarregar dados, é importante lembrar que estes devem ser lidos e escritos em disco. Se o disco rígido do computador tiver uma velocidade máxima de leitura/gravação inferior à velocidade da rede, o resultado do teste de rendimento não mostrará o desempenho da rede, mas apenas o resultado da leitura/gravação dos dados no disco rígido. Neste caso, podemos dizer que o chamado "estrangulamento" do nosso sistema informático é o disco rígido. Outro factor comum que distorce o desempenho da rede são os limites de velocidade de descarga aplicados aos servidores de partilha de ficheiros. Uma vez que os fornecedores de download precisam de assegurar que o maior número possível de clientes tenha acesso aos ficheiros de download, não podem permitir que apenas um cliente atinja a velocidade máxima de download ao descarregar. Os servidores de ficheiros dividem a velocidade máxima de carregamento do servidor para o cliente pelo número esperado de clientes durante um determinado período de tempo, pelo que quando se descarrega um ficheiro pela Internet com um débito de, digamos, 300Mbps a transferência máxima é, por exemplo, de 10Mbps.

Para testar o rendimento da rede, podemos utilizar qualquer programa que descarregue/envie dados. No entanto, a fim de obter resultados fiáveis, estes devem ser repetidos muitas vezes em dias e horas diferentes. Podemos realizar um teste de desempenho utilizando programas tais como wget, ping ou utilizando websites dedicados para este fim: speeedtest.net, www.nperf.com.

wget

O programa wget é um programa de consola mais comummente utilizado no ambiente Linux. Nos sistemas operativos MS Windows a partir da versão 10, é fácil "instalar" Linux utilizando tecnologia WSL (Windows Subsystem for Linux). Para realizar um teste de largura de banda de rede utilizando o programa wget, emitir o seguinte comando na consola (terminal de texto): wget https://ftp.icm.edu.pl/debian/dists/Debian8.11/main/Contents- amd64.gz , este comando inicia o download a partir do endereço de Internet: https://ftp.icm.edu.pl/debian/dists/Debian8.11/main/Contents-amd64.gz.

Como podemos ver na imagem abaixo, obtemos a seguinte informação: 26 MB foram descarregados a uma velocidade de 11,2 MB/s em 2,3 segundos.



(Figura 1. teste de velocidade da rede usando o programa wget)

Podemos utilizar o programa wget para realizar múltiplos ensaios em simultâneo, por exemplo:

wget -r --tries=10 http://www.onet.pl/ -o log

Aqui realizamos um download recursivo (-r) do conteúdo de www.onet.pl , as tentativas de download são repetidas 10 vezes, os resultados são registados num ficheiro de registo. Os resultados armazenados no ficheiro de registo mostram o tempo e a velocidade da transferência dada a partir da página web.

ping

Outro programa de consola disponível em vários sistemas operativos é o ping.

Exemplo de teste de desempenho de rede usando ping:

ping wp.pl

PING wp.pl (212.77.98.9) 56(84) bytes de dados.

64 bytes de www.wp.pl (212.77.98.9): icmp_seq=1 ttl=55 tempo=16.0 ms 64 bytes de www.wp.pl (212.77.98.9): icmp_seq=2 ttl=55 tempo=15.3 ms 64 bytes de www.wp.pl (212.77.98.9): icmp_seq=3 ttl=55 tempo=15.2 ms 64 bytes de www.wp.pl (212.77.98.9): icmp_seq=4 ttl=55 time=15.3 ms 64 bytes de www.wp.pl (212.77.98.9): icmp_seq=5 ttl=55 time=15.2 ms 64 bytes de www.wp.pl (212.77.98.9): icmp_seq=6 ttl=55 time=15.2 ms 64 bytes de www.wp.pl (212.77.98.9): icmp_seq=6 ttl=55 time=15.2 ms 64 bytes de www.wp.pl (212.77.98.9): icmp_seq=7 ttl=55 hora=15,3 ms 64 bytes de www.wp.pl (212.77.98.9): icmp_seq=8 ttl=55 hora=15,3 ms 64 bytes de www.wp.pl (212.77.98.9): icmp_seq=9 ttl=55 hora=15,3 ms 64 bytes de www.wp.pl (212.77.98.9): icmp_seq=10 ttl=55 hora=15.3 ms 64 bytes de www.wp.pl (212.77.98.9): icmp_seq=11 ttl=55 time=15.2 ms 64 bytes de www.wp.pl (212.77.98.9): icmp_seq=12 ttl=55 time=15.2 ms 64 bytes de www.wp.pl (212.77.98.9): icmp_seq=13 ttl=55 time=15.2 ms

--- wp.pl ping statistics ---

13 pacotes transmitidos, 13 recebidos, 0% perda de pacotes, tempo 12015ms rtt min/avg/max/mdev = 15.185/15.307/16.032/0.212 ms

No exemplo acima, foi enviado para o servidor um pacote ICMP Echo Request com o endereço www.wp.pl 13 vezes e foi recebido o mesmo número de respostas (ICMP Echo Reply). A última linha do exemplo (min/avg/max/mdev = 15,185/15,307/16,032/0,212 ms) contém o resultado de um teste da velocidade de transmissão de um pacote através da rede - quanto menor o tempo de resposta, mais eficiente é a nossa rede.

teste de velocidade. rede

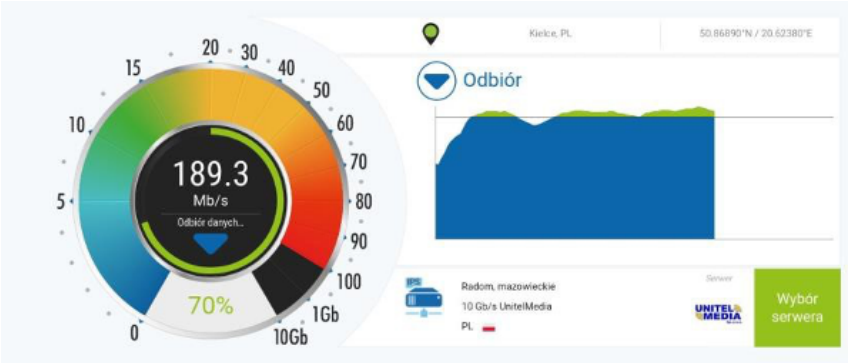
Existem também aplicações web para testar a velocidade de carregamento/transferência. Em https://www.speedtest.net podemos realizar um teste mostrando tanto o valor de PING como a velocidade de carregamento e descarregamento. As figuras abaixo mostram screenshots de um teste de carregamento da Internet entre uma rede em Kielce (Polónia) e uma rede em Praga (República Checa).

(Figura 2. teste de velocidade da rede usando o speedtest.net)

(Figura 3. resultado do teste da rede utilizando o speedtest.net)

[www. nperf.com](http://www.nperf.com)

A aplicação web npref.com é semelhante ao speedtes.net. Os resultados são também apresentados numa forma gráfica atractiva.



(Figura 4. Teste de velocidade da rede com www.nperf.com)

(Figura 5. Teste de velocidade da rede com www.nperf.com)

15.5. Limitação do tráfego de rede utilizando o exemplo de um router "casa"

O router liga a rede da casa (empresa) à Internet. No router, podemos limitar a velocidade, desactivar o acesso à Internet aos anfitriões locais. As exclusões e restrições de tráfego podem ser permanentes ou activadas durante um período de tempo específico.

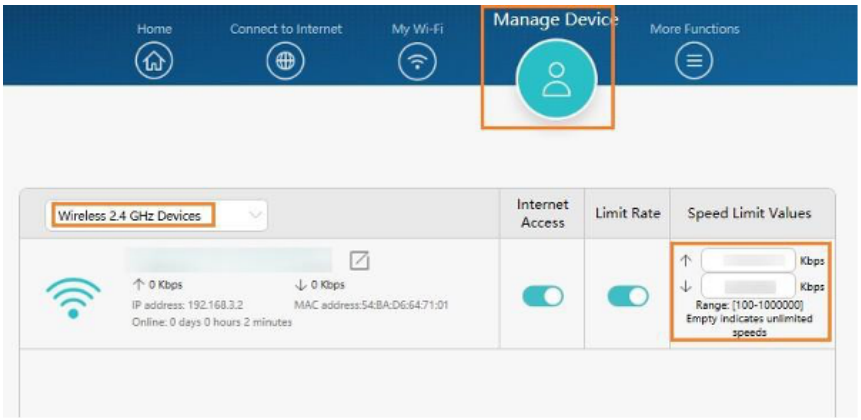
Num router "home", ou seja, um dispositivo barato concebido para servir uma rede constituída por várias a várias dezenas de hosts, podemos desactivar o acesso e limitar as velocidades de download e upload. As possibilidades de limitar o tráfego da rede dependem, evidentemente, do modelo de router.

O objectivo de introduzir uma limitação de velocidade de transferência é proteger contra uma queda na velocidade de download ou upload em hospedeiros chave na nossa rede doméstica. Por exemplo, se assumirmos que o nosso portátil, no qual estamos a fazer trabalho remoto, deve ter uma ligação estável à Internet durante uma teleconferência, introduziríamos limites de velocidade para todos os outros dispositivos.

Exemplo de permitir limites de velocidade num router Huawey Wi-Fi:

1. Ligue o seu computador/telefone ao router Wi-Fi (verifique a placa de nome na parte inferior do router para obter o nome Wi-Fi por defeito, sem palavra-passe) ou ligue o seu computador à porta LAN do router utilizando um cabo Ethernet. Introduza o endereço IP predefinido na barra de endereços do browser e inicie sessão na página de gestão baseada na web (verifique o endereço IP predefinido na placa de identificação na parte inferior do router).

2. Clique em Manage Device, seleccione o telefone ou computador para o qual deseja definir um limite, active a opção Limit Speed e clique no ícone sob Speed limit Values para definir a velocidade máxima de carregamento e descarregamento.



(Figura - Ecrã de configuração do dispositivo, fonte: https://consumer.huawei.com/en/support/content/en-us15806295/)

16. Testes básicos de redes informáticas

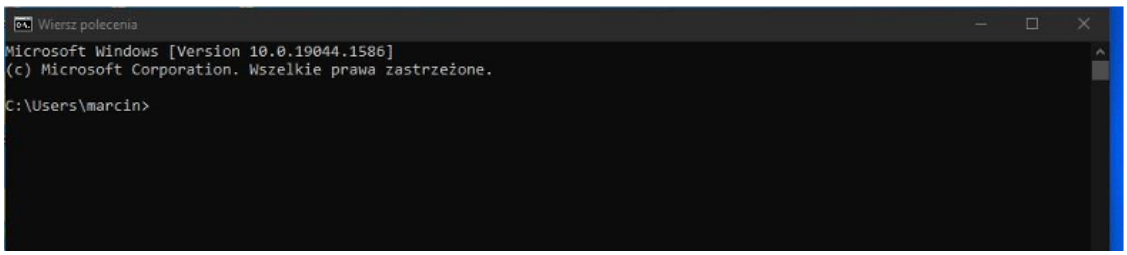
Testes de rede informática em ambientes MS Windows e UNIX-Like utilizando programas:

- ping
- tracert
- telnet
- nc
- wget

Todos os programas acima são iniciados digitando um comando no terminal / linha de comando.

Num sistema operativo Linux que execute o ambiente gráfico / macOS, será necessário iniciar um terminal para executar comandos digitados a partir do teclado. Os comandos são introduzidos numa janela de terminal.

No sistema operativo MS Windows, para executar um comando digitado a partir do teclado, é necessário iniciar a linha de comando. Para iniciar a linha de comando no Windows 10/11 clique em "Start" e na janela de pesquisa digite cmd .



16.1. ping

O programa ping é utilizado para diagnosticar as ligações de rede. Utilizamo-lo para verificar a qualidade da ligação entre os computadores que enviam os pedidos e que devolvem uma resposta.

Ping irá responder às seguintes perguntas:

Existe uma ligação entre os computadores?

Qual é o tempo de resposta de um pacote enviado?

Executar o programa na linha de comando do MS Windows (terminal Linux/Mac). No tipo de linha de comando: ping [IP ou nome] e confirmar pressionando Enter. Um exemplo de como o programa ping funciona em Linux:

ping 10.10.10.1

PING 10.10.10.1 (10.10.10.1) 56(84) bytes de dados.

64 bytes de 10.10.10.1: icmp_seq=1 ttl=64 tempo=0,364 ms 64 bytes de 10.10.10.1: icmp_seq=2 ttl=64 tempo=0,274 ms 64 bytes de 10.10.10.1: icmp_seq=3 ttl=64 tempo=0,433 ms 64 bytes de 10.10.10.1: icmp_seq=4 ttl=64 tempo=0.545 ms

64 bytes a partir de 10.10.10.1: icmp_seq=5 ttl=64 tempo=0.380 ms 64 bytes a partir de 10.10.10.1: icmp_seq=6 ttl=64 tempo=0.284 ms 64 bytes a partir de 10.10.10.1:

icmp_seq=7 ttl=64 tempo=0.477 ms 64 bytes a partir de 10.10.10.1: icmp_seq=8 ttl=64 tempo=0.257 ms

^C

--- 10.10.10.1 ping statistics ---

8 pacotes transmitidos, 8 recebidos, 0% perda de pacotes, tempo 7154ms rtt min/avg/max/mdev = 0.257/0.376/0.576/0.545/0.099 ms

No exemplo acima, foi enviado 8 vezes um pacote ICMP Echo Request e foi recebido o mesmo número de respostas (ICMP Echo Reply). Os pacotes foram enviados do computador com o IP 10.10.10.2 para o computador com o IP 10.10.10.1. O tempo médio de resposta é de 0,376 milissegundos.

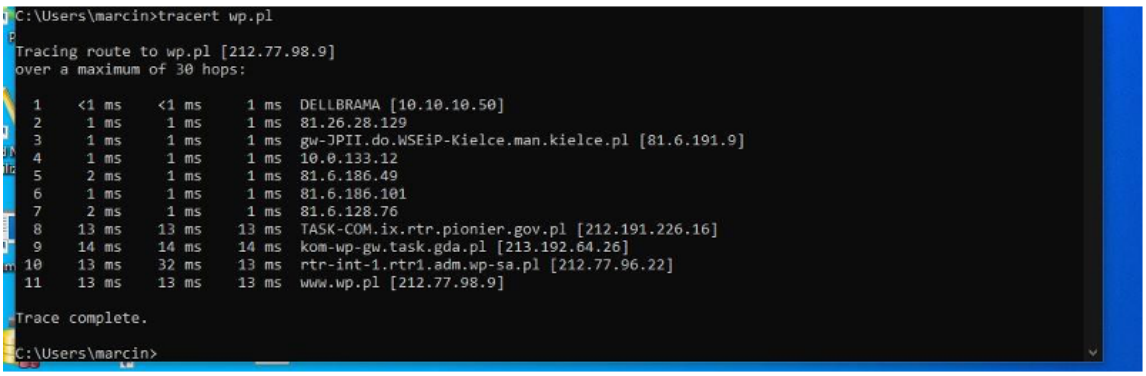
16.2. tracert

Tracert é um programa para determinar o encaminhamento (rota) de pacotes numa rede IP para traçar (MS Windows) / traceroute (Linux/macOS)

Tracert/traceroute devolve uma lista de routers consecutivos na rota para o computador alvo na rede.

Quanto maior for a rota - maior o número de routers - mais difícil é comunicar com o computador alvo na rede. Se houver um router mal configurado na nossa rota, teremos acesso difícil ao computador em questão (website de carregamento lento, erros ao descarregar ficheiros, má qualidade de rádio na Internet, etc.).

Exemplo de exame de uma rota das instalações da universidade para o servidor wp.pl:



No exemplo acima, vemos 11 nós (routers).

16.3. telnet

Telnet é o programa utilizado para se ligar a um servidor remoto. Telnet é instalado em computadores de classe de servidor, mas é também amplamente utilizado em todo o tipo de dispositivos de rede (por exemplo, switches, AccessPoint).

Pode utilizar o telnet para verificar se um determinado serviço, por exemplo SMTP, HTTP, está a funcionar no computador remoto. Para verificar a conectividade entre o computador cliente e o servidor na linha de comando (terminal), emitir o comando: telnet [endereço do servidor em teste] [porto de serviço especificado].

Se quiser verificar se existe um servidor STMP a funcionar no computador www.nasa.gov e poderá ligar-se a ele a partir do seu computador e enviar correio, emita o comando:

telnet www.nasa.gov 25

onde 25 é o número da porta TCP em que o serviço SMTP (envio de correio) ouve.

16.4. nc

Netcat (nc) é um comando executado num terminal. Está disponível em Linux e macOS Pode ser utilizado para testar o funcionamento de múltiplas portas TCP num servidor remoto em simultâneo.

Exemplo:

em Linux tipo trminal I:

nc -z -v 10.10.10.1 22

O comando devolve o resultado:

Ligação à porta 10.10.10.1 22 [tcp/ssh] bem sucedida!

Isto significa uma ligação bem sucedida ao anfitrião 10.10.10.1 na porta TCP 22

16.5. wget

Wget é um programa de consola que é utilizado para descarregar ficheiros. Wget devolve a velocidade de descarregamento para que possamos obter informações sobre o desempenho de descarregamento da nossa ligação à Internet.

Exemplo:

No terminal I, digite:

wget https://download. moodle. org/download. php/direct/stable311/moodle-latest-311.tgz -O moodle-latest-311.tgz

Isto significa que irei descarregar um ficheiro do servidor https://download. moodle. org, irei guardar o ficheiro descarregado sob o nome moodle- latest-311.tgz

Depois de emitir o comando no terminal, wget devolve o seguinte:

--2022-03-31 11:31:57-- https://download. moodle. org/download. php/direct/stable311/moodle-latest-311.tgz

Resolver download.moodle.org (download.moodle.org).... 104.22.64.81, 104.22.65.81, 172.67.26.233, ... Ligar a download.moodle.org (download.moodle.org)|104.22.64.81|:443..... ligado.

Pedido HTTP enviado, à espera de resposta 200 OK Comprimento: 60212386 (57M) [aplicação/g-zip].

Guardar para: Moodle-latest-311.tgz''.

moodle-latest-311.tgz 100%
[==========]
57,42M 11,0MB/s em 5,2s

2022-03-31 11:32:03 (11.1 MB/s) - 'moodle-latest-311.tgz' guardado [60212386/60212386].

Podemos ver a velocidade a que o ficheiro foi descarregado - 11.0 MB/s