## Introdução:

Esta é a décima primeira parte do Tutorial de TCP/IP. Na Parte 1 tratei dos aspectos básicos do protocolo TCP/IP. Na Parte 2falei sobre cálculos binários, um importante tópico para entender sobre redes, máscara de sub-rede e roteamento. Na Parte 3 falei sobre Classes de endereços, na Parte 4 fiz uma introdução ao roteamento e na Parte 5apresentei mais alguns exemplos e análises de como funciona o roteamento e na Parte 6 falei sobre a Tabela de Roteamento. Na Parte 7 tratei sobre a divisão de uma rede em sub-redes, conceito conhecido como subnetting. NaParte 8 fiz uma apresentação de um dos serviços mais utilizados pelo TCP/IP, que é o Domain Name System: DNS. O DNS é o serviço de resolução de nomes usado em todas as redes TCP/IP, inclusive pela Internet que, sem dúvidas, é a maior rede TCP/IP existente. Na Parte 9 fiz uma introdução ao serviço Dynamic Host Configuration Protocol – DHCP. Na Parte 10 fiz uma introdução ao serviço Windows Internet Name Services – WINS. Nesta décima primeira parte falarei sobre o conceito de portas de comunicação.

## Um pouco sobre Pacotes e sobre os protocolos de Transporte

O TCP/IP, na verdade, é formado por um grande conjunto de diferentes protocolos e serviços de rede. O nome TCP/IP deriva dos dois protocolos mais importantes e mais utilizados, que são os seguintes:

> **IP:** É um protocolo de endereçamento, um protocolo de rede. Eu me arriscaria a afirmar que as principais funções do protocolo IP são endereçamento e roteamento, ou de uma maneira mais simples, fornecer uma maneira para identificar unicamente cada máquina da rede (endereço IP) e uma maneira de encontrar um caminho entre a origem e o destino (Roteamento).
>
> **TCP:** O TCP é um protocolo de transporte e executa importantes funções para garantir que os dados sejam entregues de uma maneira confiável, ou seja, sem que os dados sejam corrompidos ou alterados.

Vamos imaginar uma situação prática, onde você deseja enviar um arquivo com cerca de 10 MB de um computador de origem para um computador de destino. Uma das primeiras coisas que tem que ser feitas é encontrar uma rota, um caminho entre a origem e o destino. Este é o papel do protocolo IP, mais especificamente da função de roteamento. Uma vez encontrado o caminho, o próximo passo é dividir o arquivo de 10 MB em pacotes de tamanhos menores, os quais possam ser enviados pelos equipamentos da rede. Além da divisão em pacotes menores, o TCP/IP tem que garantir que os pacotes sejam entregues sem erros e sem alterações. Pode também acontecer de os pacotes chegarem fora de ordem. O TCP/IP tem que ser capaz de identificar a ordem correta e entregar os pacotes para o programa de destino, na ordem correta. Por exemplo, pode acontecer de o pacote número 10 chegar antes do pacote número 9. Neste caso o TCP tem que aguardar a chegada do pacote número 9 e entregá-los na ordem correta. Pode também acontecer de serem perdidos pacotes durante o transporte. Neste caso, o TCP tem que informar à origem de que determinado pacote não foi recebido no tempo esperado e solicitar que este seja retransmitido. Todas estas funções – garantir a integridade, a seqüência correta e solicitar retransmissão – são exercidas pelo protocolo TCP – Transmission Control Protocol. Além do TCP existe também o UDP, o qual não faz todas estas verificaçõe e é utilizado por determinados serviços. A seguir apresento uma descrição dos protocolos TCP e UDP e um estudo comparativo.

## TCP – Uma Visão Geral

O Transmission Control Protocol (TCP) é, sem dúvidas, um dos mais importantes

protocolos da família TCP/IP. É um padrão definido na RFC 793, "Transmission Control Protocol (TCP)", que fornece um serviço de entrega de pacotes confiável e orientado por conexão. Ser orientado por conexão, significa que todos os aplicativos baseados em TCP como protocolo de transporte, antes de iniciar a troca de dados, precisam estabelecer uma conexão. Na conexão são fornecidas, normalmente, informações de logon, as quais identificam o usuário que está tentando estabelecer a conexão. Um exemplo típico são os aplicativos de FTP (Cute – FTP, ES-FTP e assim por diante). Para que você acesse um servidor de FTP, você deve fornecer um nome de usuário e senha. Estes dados são utilizados para identificar e autenticar o usuário. Após a identificação e autenticação, será estabelecida uma sessão entre o cliente de FTP e o servidor de FTP.

Algumas características do TCP:

**Garante a entrega de datagramas IP:** Esta talvez seja a principal função do TCP, ou seja, garantir que os pacotes sejam entregues sem alterações, sem terem sido corrompidos e na ordem correta. O TCP tem uma série de mecanismos para garantir esta entrega.

**Executa a segmentação e reagrupamento de grandes blocos de dados enviados pelos programas e Garante o seqüenciamento adequado e entrega ordenada de dados segmentados:** Esta característica refere-se a função de dividir grandes arquivos em pacotes menores e transmitir cada pacote separadamente. Os pacotes podem ser enviados por caminhos diferentes e chegar fora de ordem. O TCP tem mecanismos para garantir que, no destino, os pacotes sejam ordenados corretamente, antes de serem entregues ao programa de destino.

**Verifica a integridade dos dados transmitidos usando cálculos de soma de verificação:** O TCP faz verificações para garantir que os dados não foram alterados ou corrompidos durante o transporte entre a origem e o destino.

**Envia mensagens positivas dependendo do recebimento bem-sucedido dos dados. Ao usar confirmações seletivas, também são enviadas confirmações negativas para os dados que não foram recebidos**: No destino, o TCP recebe os pacotes, verifica se estão OK e, em caso afirmativo, envia uma mensagem para a origem, confirmando cada pacote que foi recebido corretamente. Caso um pacote não tenha sido recebido ou tenha sido recebido com problemas, o TCP envia uma mensagem ao computador de origem, solicitando uma retransmissão do pacote. Com esse mecanismo, apenas pacotes com problemas terão que ser reenviados, o que reduz o tráfego na rede e agiliza o envio dos pacotes.

**Oferece um método preferencial de transporte de programas que devem usar transmissão confiável de dados baseada em sessões, como bancos de dados cliente/servidor e programas de correio eletrônico:** Ou seja, o TCP é muito mais confiável do que o UDP (conforme mostrarei mais adiante) e é indicado para programas e serviços que dependam de uma entrega confiável de dados.

## Funcionamento do TCP

O TCP baseia-se na comunicação ponto a ponto entre dois hosts de rede. O TCP recebe os dados de programas e processa esses dados como um fluxo de bytes. Os bytes são agrupados em segmentos que o TCP numera e seqüência para entrega. Estes segmentos são mais conhecidos como "***Pacotes***".

Antes que dois hosts TCP possam trocar dados, devem primeiro estabelecer uma sessão entre si. Uma sessão TCP é inicializada através de um processo conhecido como um tree-way handshake (algo como Um Aperto de Mão Triplo). Esse processo sincroniza os números de seqüência e oferece informações de controle necessárias para estabelecer uma conexão virtual entre os dois hosts.

De uma maneira simplificada, o processo de tree-way handshake, pode ser descrito através dos seguintes passos:

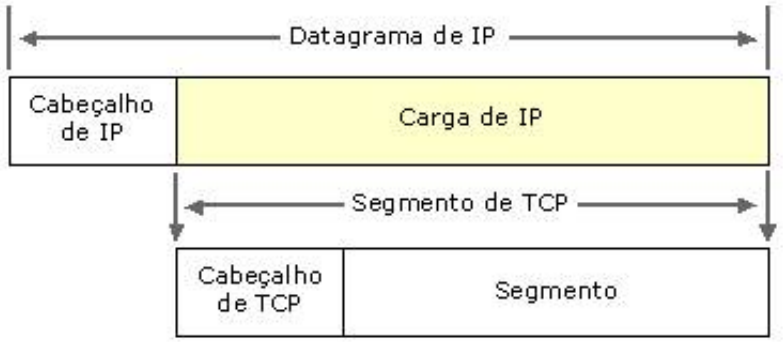
**O computador de origem solicita o estabelecimento de uma sessão com o computador de destino:** Por exemplo, você utiliza um programa de FTP (origem) para estabelecer uma sessão com um servidor de FTP (destino).

O computador de destino recebe a requisição, verifica as credenciais enviadas (tais como as informações de logon e senha) e envia de volta para o cliente, informações que serão utilizadas pelo cliente, para estabelecer efetivamente a sessão. As informações enviadas nesta etapa são importantes, pois é através destas informações que o servidor irá identificar o cliente e liberar ou não o acesso.

O computador de origem recebe as informações de confirmação enviadas pelo servidor e envia estas confirmações de volta ao servidor. O servidor recebe as informações, verifica que elas estão corretas e estabelece a sessão. A partir deste momento, origem e destino estão autenticados e aptos a trocar informações usando o protocolo TCP. Se por algum motivo, as informações enviadas pela origem não estiverem corretas, a sessão não será estabelecida e uma mensagem de erro será enviada de volta ao computador de origem.

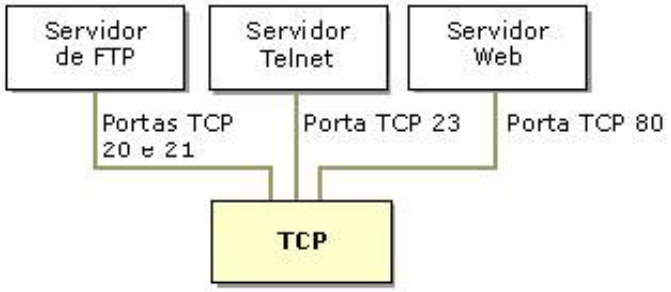
Depois de concluído o tree-way handshake inicial, os segmentos são enviados e confirmados de forma seqüencial entre os hosts remetente e destinatário. Um processo de handshake semelhante é usado pelo TCP antes de fechar a conexão para verificar se os dois hosts acabaram de enviar e receber todos os dados.

Os segmentos TCP são encapsulados e enviados em datagramas IP, conforme apresentado na figura a seguir, obtida na ajuda do Windows 2000 Server:




## O conceito de Portas TCP

Os programas TCP usam números de porta reservados ou conhecidos, conforme apresentado na seguinte ilustração, da ajuda do Windows 2000 Server:




## O que é uma Porta TCP?

Bem, sem entrar em detalhes técnicos do TCP/IP, vou explicar, através de um exemplo prático, o conceito de porta. Vamos imaginar um usuário, utilizando um computador com conexão à Internet. Este usuário, pode, ao mesmo tempo, acessar um ou mais sites da Internet, usar o Outlook Express para ler suas mensagens de email, estar conectado a um servidor de FTP, usando um programa como o WS-FTP, para fazer download de um ou mais arquivos, estar jogando DOOM através da Internet e assim por diante.

Todas as informações que este usuário recebe estão chegando através de pacotes que

chegam até a placa de Modem ou até o Modem ADSL, no caso de uma conexão rápida. A pergunta que naturalmente surge é:

**Como o sistema sabe para qual dos programas se destina cada um dos pacotes que estão chegando no computador?**

Por exemplo, chega um determinado pacote. Este pacote é para uma das janelas do Navegador, é para o cliente de FTP, é um comando do DOOM, é referente a uma mensagem de email ou quem é o destinatário deste pacote? A resposta para esta questão é o mecanismo de portas utilizado pelo TCP/IP. Cada programa trabalha com um protocolo/serviço específico, ao qual está associado um número de porta. Por exemplo, o serviço de FTP, normalmente opera na porta 21 (na verdade usa duas portas, uma para controle e outra para o envio de dados). Todo pacote que for enviado do servidor FTP para o cliente, terá, além dos dados que estão sendo enviados, uma série de dados de controle, tais como o número do pacote, código de validação dos dados e também o número da porta. Quando o pacote chega no seu computador, o sistema lê no pacote o número da porta e sabe para quem encaminhar o pacote. Por exemplo, se você está utilizando um cliente de FTP para fazer um download, os pacotes que chegarem, com informação de Porta = 21, serão encaminhados para o cliente de FTP, o qual irá ler o pacote e dar o destino apropriado. Outro exemplo, o protocolo HTTP, utilizado para o transporte de informações de um servidor Web até o seu navegador, opera, por padrão, na porta 80. Os pacotes que chegarem, destinados à porta 80, serão encaminhados para o navegador. Se houver mais de uma janela do navegador aberta, cada uma acessando diferentes páginas, o sistema inclui informações, além da porta, capazes de identificar cada janela individualmente. Com isso, quando chega um pacote para a porta 80, o sistema identifica para qual das janelas do navegador se destina o referido pacote.

**Em resumo:** O uso do conceito de portas, permite que vários programas estejam em funcionamento, ao mesmo tempo, no mesmo computador, trocando informações com um ou mais serviços/servidores.

O lado do servidor de cada programa que usa portas TCP escuta as mensagens que chegam no seu número de porta conhecido. Todos os números de porta de servidor TCP menores que 1.024 (e alguns números mais altos) são reservados e registrados pela Internet Assigned Numbers Authority (IANA, autoridade de números atribuídos da Internet). Por exemplo, o serviço HTTP (servidor Web), instalado em um servidor, fica sempre "escutando" os pacotes que chegam ao servidor. Os pacotes destinados a porta 80, serão encaminhados pelo sistema operacional para processamento do servidor Web.

A tabela a seguir é uma lista parcial de algumas portas de servidor TCP conhecidas usadas por programas baseados em TCP padrão.

| Número de porta TCP | Descrição |
|---|---|
| 20 | Servidor FTP (File Transfer Protocol, protocolo de transferência de arquivo) (canal de dados) |
| 21 | Servidor FTP (canal de controle) |
| 23 | Servidor Telnet |
| 53 | Transferências de zona DNS (Domain Name System, sistema de nomes de domínios) |
| 80 | Servidor da Web (HTTP, Hypertext Transfer Protocol, protocolo de transferência de hipertexto) |
| 139 | Serviço de sessão de NetBIOS |

Para obter uma lista atualizada e completa de todas as portas TCP conhecidas e

registradas atualmente, consulte o seguinte endereço:

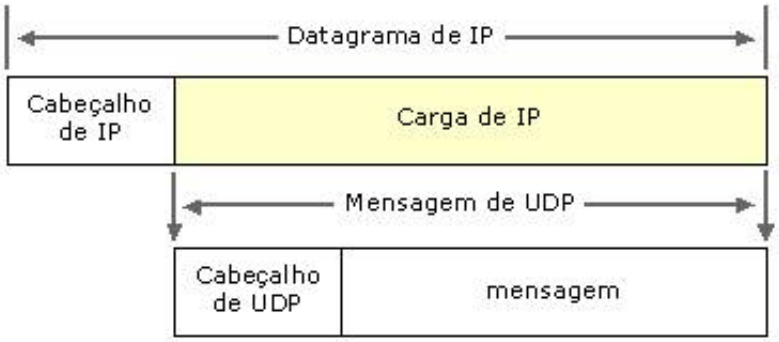
http://www.iana.org/assignments/port-numbers

### UDP – Uma Visão Geral

O User Datagram Protocol (UDP) é um padrão TCP/IP e está definido pela RFC 768, "User Datagram Protocol (UDP)." O UDP é usado por alguns programas em vez de TCP para o transporte rápido de dados entre hosts TCP/IP. Porém o UDP não fornece garantia de entrega e nem verificação de dados. De uma maneira simples, dizemos que o protocolo UDP manda os dados para o destino; se vai chegar ou se vai chegar corretamente, sem erros, só Deus sabe. Pode parecer estranho esta característica do UPD, porém você verá que em determinadas situações, o fato de o UDP ser muito mais rápido do que o TCP (por não fazer verificações e por não estabelecer sessões), o uso do UDP é recomendado.

O protocolo UDP fornece um serviço de pacotes **sem conexão** que oferece entrega com base no melhor esforço, ou seja, UDP não garante a entrega ou verifica o seqüenciamento para qualquer pacote. Um host de origem que precise de comunicação confiável deve usar TCP ou um programa que ofereça seus próprios serviços de seqüenciamento e confirmação.

As mensagens UDP são encapsuladas e enviadas em datagramas IP, conforme apresentado na seguinte ilustração, da ajuda do Windows 2000 Server:




### Portas UDP

O conceito de porta UDP é idêntico ao conceito de portas TCP, embora tecnicamente, existam diferenças na maneira como as portas são utilizadas em cada protocolo. A idéia é a mesma, por exemplo, se um usuário estiver utilizando vários programas baseados em UDP, ao mesmo tempo, no seu computador, é através do uso de portas, que o sistema operacional sabe a qual programa se destina cada pacote UDP que chega.

O lado do servidor de cada programa que usa UDP escuta as mensagens que chegam no seu número de porta conhecido. Todos os números de porta de servidor UDP menores que 1.024 (e alguns números mais altos) são reservados e registrados pela Internet Assigned Numbers Authority (IANA, autoridade de números atribuídos da Internet).

Cada porta de servidor UDP é identificada por um número de porta reservado ou conhecido. A tabela a seguir mostra uma lista parcial de algumas portas de servidor UDP conhecidas usadas por programas baseados em UDP padrão.

| Número de porta UDP | Descrição |
|---|---|
| 53 | Consultas de nomes DNS (Domain Name System, sistema de nomes de domínios) |
| 69 | Trivial File Transfer Protocol (TFTP) |
| 137 | Serviço de nomes de NetBIOS |
| 138 | Serviço de datagrama de NetBIOS |
| 161 | Simple Network Management Protocol (SNMP) |
| 520 | Routing Information Protocol (RIP, protocolo de informações de roteamento) |

Para obter uma lista atualizada e completa de todas as portas TCP conhecidas e registradas atualmente, consulte o seguinte endereço:

http://www.iana.org/assignments/port-numbers

## Comparando UDP e TCP:

Geralmente, as diferenças na maneira como UDP e TCP entregam os dados assemelham-se às diferenças entre um telefonema e um cartão postal. O TCP funciona como um telefonema, verificando se o destino está disponível e pronto para a comunicação. O UDP funciona como um cartão postal — as mensagens são pequenas e a entrega é provável, mas nem sempre garantida.

UDP é geralmente usado por programas que transmitem pequenas quantidades de dados ao mesmo tempo ou têm necessidades em tempo real. Nessas situações, a baixa sobrecarga do UDP (pois este não faz as verificações que são feitas pela TCP) e as capacidades de broadcast do UDP (por exemplo, um datagrama, vários destinatários) são mais adequadas do que o TCP.

O UDP contrasta diretamente com os serviços e recursos oferecidos por TCP. A tabela a seguir compara as diferenças em como a comunicação TCP/IP é tratada dependendo do uso de UDP ou TCP para o transporte de dados.

| UDP | TCP |
|---|---|
| Serviço sem conexão; nenhuma sessão é estabelecida entre os hosts. | Serviço orientado por conexão; uma sessão é estabelecida entre os hosts. |
| UDP não garante ou confirma a entrega ou seqüência os dados. | TCP garante a entrega através do uso de confirmações e entrega seqüenciada dos dados. |
| Os programas que usam UDP são responsáveis por oferecer a confiabilidade necessária ao transporte de dados. | Os programas que usam TCP têm garantia de transporte confiável de dados. |
| UDP é rápido, necessita de baixa sobrecarga e pode oferecer suporte à comunicação ponto a ponto e ponto a vários pontos. | TCP é mais lento, necessita de maior sobrecarga e pode oferecer suporte apenas à comunicação ponto a ponto. |

Tanto UDP quanto TCP usam portas para identificar as comunicações para cada programa TCP/IP, conforme descrito anteriormente.

## Conclusão

Nesta parte do tutorial fiz uma apresenta ção dos protocolos TCP e UDP, os quais são responsáveis pelo transporte de pacotes em redes baseadas no TCP/IP. Você também aprendeu sobre as diferenças entre os protocolos TCP e UDP e sobre o conceito de porta de comunicação.