INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Professor: Macêdo Firmino
Disciplina: Arquitetura de Rede
Aula 10: Ferramentas de Teste no Windows e Camada de Transporte

O Windows possui algumas ferramentas que permitem configurar, monitorar e testar conexões de rede. Entre elas,temos o ipconfig, ping e tracert. Na sequência iremos apresenta-las.

ipconfig

O comando `ipconfig` é uma ferramenta de linha de comando do Windows. Ele exibe todos os valores de configuração de rede TCP/IP e atualiza as configurações do protocolo de configuração dinâmica de *hosts* (DHCP) e do sistema de nomes de domínios (DNS).

Quando usado sem parâmetros, o `ipconfig` exibe endereços IPv6 ou o endereço IPv4, a máscara da sub-rede e o *gateway* padrão para todos os adaptadores.

O mesmo também pode ser utilizado com os seguintes parâmetros:

***/all*:** Exibe todas as informações de configuração da interfaces de redes instaladas;

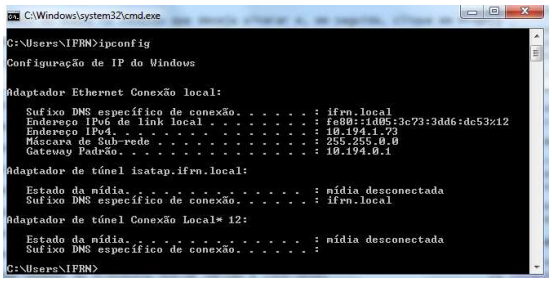
***/release*:** Libera o endereço ip do adaptador especificado;

***/renew*:** Renova o endereço ip para o adaptador especificado;

***/flushdns*:** Limpa o *cache* de resolução DNS;

***/displaydns*:** Exibe o conteúdo de *cache* de resolução de DNS.

Note que as opções */Release* e */Renew* apenas podem ser utilizadas se o sistema estiver configurado com DHCP.



Atividade

01. Digite "ipconfig /all" no Prompt de comando, e responda:

a) O enderço MAC;

b) O endereço IP;

c) A Máscara

d) O Gateway;

e) O Servidor DNS.

ping

A ferramenta `ping` verifica a conectividade de nível IP com outro computador TCP/IP através do envio de mensagens de solicitação de eco de protocolo ICMP. A confirmação das mensagens de resposta é exibida juntamente com o tempo de ida e volta.

O `ping` é o principal comando TCP/IP usado para testar problemas de conectividade, acesso e resolução de nomes. Você pode utilizar `ping` para testar tanto o nome do computador quanto seu endereço IP.

Por exemplo, o mesmo também pode ser utilizado com os seguintes parâmetros:

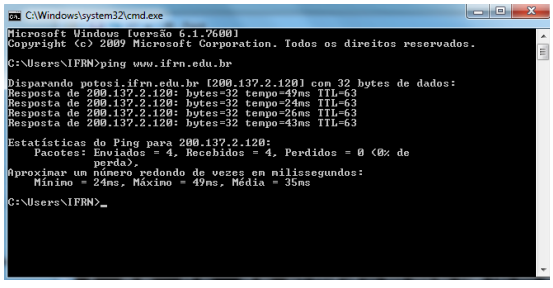
-t: Especifica que o `ping` continue enviando mensagens de solicitação de eco ao destino até que seja interrompido. Para interromper e sair do `ping`, pressione "CTRL+C".

-a: Especifica que a resolução inversa de nome seja realizada no endereço IP de destino. Se for bem-sucedida, o comando exibirá o nome do host correspondente.

-n: Determina o número de solicitações de eco enviadas. O padrão é 4.

-l: Especifica o comprimento, em *bytes*, do campo de dados nas solicitações de eco enviadas. O padrão é 32. O Tamanho máximo é 65.527.

-i: Especifica o valor do campo TTL no cabeçalho IP das solicitações de eco enviadas. O TTL máximo é 255.



Atividade

02. iremos utilizar o comando `ping` para testar o nossa conectividade. Para isso siga os passos:

a) Execute o `ping` no endereço de autoretorno digitando ping **127.0.0.1**. Escreva a resposta do comando.

b) Faça o `ping` no endereço IP do seu *gateway* padrão. Escreva a resposta do comando.

c) Execute um ping para o endereço portal.ifrn.edu.br. Escreva a resposta do comando.

d) Faça um comparativo apresentando as principais diferenças entre as respostas obtidas.

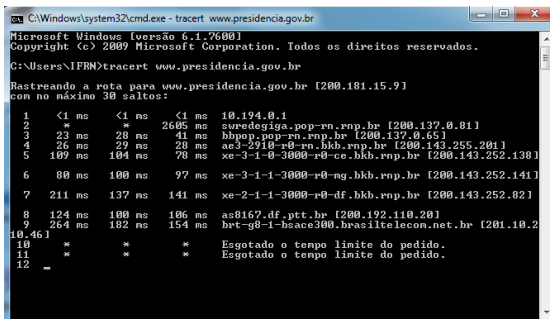
tracert

O utilitário de diagnóstico `tracert` determina a rota adotada até um destino. Para isso ele envia pacotes de eco ICMP (*Internet Control Message Protocol*) com diferentes valores de tempo de vida (TTL) do cabeçalho IP.

Lembrando que a função do campo TTL do IP é a contagem de saltos (roteadores) da origem ao destino. Cada roteador ao longo do caminho deverá diminuir o TTL do pacote em 1 antes de encaminhá-lo. Quando o TTL no pacote alcança 0, o roteador deve enviar uma mensagem de tempo excedido ICMP de volta para o computador de origem.

O `tracert` determina a rota enviando o primeiro pacote echo com TTL de 1 e incrementando o TTL de 1 em cada transmissão subseqüente, até que o destino responda ou o máximo de TTL. A rota é determinada examinando as mensagens ICMP de tempo excedido devolvidas por roteadores intermediários. Observe que alguns roteadores silenciosamente soltar pacotes com TTLs expirados e são invisíveis ao `tracert` .

Como resultado, o `tracert` imprime uma lista ordenada dos roteadores no caminho que retornaram a mensagem ICMP de tempo excedido.



Atividade

03. Iremos rastrear um caminho usando o tracert

a) Abra o Prompt de Comando e digite `tracertwww.presidencia.gov.br`. Escreva o resultado.

b) Quantos roteadores foram necessários passar para alcançar o destino? Quais os seus endereços IP ?

Camada de Transporte

O principal objetivo da camada de transporte é oferecer um serviço confiável, eficiente e econômico a seus usuários que, em geral, são processos presentes na camada de aplicação. Para atingir esse objetivo, a camada de transporte utiliza os serviços de transporte orientado à conexões e o serviço de transporte sem conexões.

Os dois principais protocolos da camada de transporte são: UDP (sem conexões) e TCP (orientado à conexões).

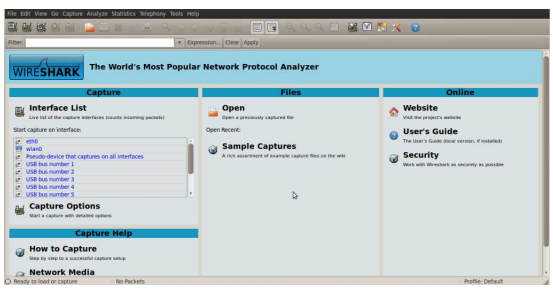
Para analisarmos protocolos de rede são utilizadas ferramentas chamadas de analisadores de tráfego. Na aula de hoje iremos utilizar um analisador de tráfego gratuito chamado de Wireshark. Com ele iremos visualizar o funcionamento dos protocolos TCP e UDP.

Wireshark

O Wireshark é um programa (conhecido como *sniffer*) que verifica os pacotes transmitidos pelo dispositivo de comunicação (placa de rede, placa de fax modem, etc.) do computador. O programa analisa o tráfego de entrada e saída e organiza-os por protocolo.

Exemplos de utilização do Wireshark:

- Administradores de rede utilizam para solucionar problemas de rede;
- Engenheiros de segurança de rede usá-lo para examinar problemas de segurança;
- Desenvolvedores utiliza para depurar implementações do protocolo;
- Pessoas que precisam aprender o protocolo de rede;



Para começar a capturar os pacotes, selecione a interface de rede. Para isso selecione no *menu*: "Capture/Interfaces". Irá aparecer uma janela que permitirá a seleção da interface. Além, das opções que podem ser configuradas para a interface. Selecione a interface Ethernet e clique em "*start*".

A janela principal será preenchida com uma lista dos pacotes capturados. A janela é dividida normalmente em três seções: uma seção mostra a lista de pacotes capturados, uma outra seção mostra uma árvore de protocolo de um pacote selecionado e a última mostra os *bytes* do pacote.

Para selecionar os pacotes baseados no protocolo, basta digitar o nome do protocolo no qual você está interessado no campo *Filter* (Filtro) e pressione o botão "Apply" (aplicar) para iniciar o filtro. A Figura abaixo mostra um exemplo de filtragem sobre o protocolo TCP.

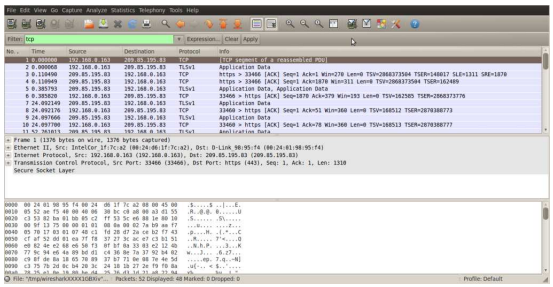


Figura 1: Exemplo de Capture de Tráfego TCP

Protocolo TCP

As principais funções do protocolo TCP são:

- Endereçamento;
- Controle de Conexão;
- Controle de Fluxo;
- Controle de Erro;
- Controle de Congestionamento.

Quando um processo de aplicação (por exemplo, um usuário) deseja estabelecer uma conexão com um processo de aplicação remoto, é necessário especificar a aplicação com a qual ele irá se conectar. Para isso são definidos endereços de transporte que os processos podem ouvir para receber solicitações de conexão. Estes endereços são chamados de portas e a este esquema é chamado de endereçamento.

O controle de conexão do TCP é formado por: estabelecimento da conexão, transferência dos dados e encerramento da conexão. Para estabelecer a conexão os dois *hosts* entram num processo de sincronização (conhecido como *Three-way Handshaking*). O processo de sincronização garante que os dois lados estão prontos para a transmissão dos dados e permite que os dispositivos determinem os números da sequência inicial. O estabelecimento da conexão é iniciado pelo cliente.

Após o estabelecimento da ligação virtual, o TCP aplica números de sequência aos segmentos de dados que está a transmitir, para que o receptor seja capaz de colocar adequadamente os *bytes* na ordem original. Além disso, os números de sequência também é utilizado para confirmação, ou seja, para que o receptor confirme o recebimento dos *bytes*. No TCP o número da confirmação refere-se ao próximo octeto esperado como parte da sessão TCP.

O TCP utiliza um mecanismo de janela deslizante para efetuar a função de controlo de fluxo. Este mecanismo permite determinar dinamicamente o tamanho da janela de transmissão. Os equipamentos negociam o tamanho de uma janela para permitir que um número máximo de *bytes* seja transmitido antes da confirmação.

Para controlar os erros na transmissão no TCP, quando é enviado um segmento, o transmissor também dispara um *timer*. Quando o segmento chega ao destino, a entidade TCP receptora retorna um segmento (com ou sem dados, de acordo com as circunstâncias) com um número de confirmação igual ao próximo número de seqüência que espera receber. Se o *timer* do transmissor expirar antes da confirmação ser recebida, o segmento será retransmitido. Além disso o TCP utiliza o *checksum* (para verificar erros em segmentos recebidos).

Quando a carga oferecida a qualquer rede é maior que sua capacidade, acontece um congestionamento. O TCP tenta controlar o congestionamento na rede manipulando dinamicamente o tamanho da janela de transmissão. Para isso é definido um algoritmo composto por três fases: aumento exponencial, aumento aditivo e diminuição multiplicativa. Este algoritmo irá dinamicamente evitar o congestionamento na rede.

Atividade

04. Agora iremos realizar uma Análise do protocolo TCP.

a) Começe a captura de tráfego na rede;

b) Utilize a Internet para acessar o site `www.ifrn.edu.br`);

c) Utilizando um filtro de forma a visualizar apenas os pacotes TCP do seu computador (ip.addr == "seu IP" and tcp);

d) Quais os campos existentes no cabeçalho de um segmento TCP?

e) Explique o funcionamento do *handshake* triplo com base nos tráfego que analisou na captura efetuada.

f) Apresente alguns valores de três segmentos TCP que você capturou: os números de sequência; tamanho das janelas e AKCs (confirmações). Explique qual a função de cada um destes parâmetros.

Protocolo UDP

Por outro lado, O Protocolo UDP (*User Datagram Protocol*) é o protocolo de transporte não orientado à conexão. O UDP é um protocolo simples que troca datagramas, sem confirmações nem entrega garantida. O processamento de erros e a retransmissão devem ser tratados por protocolos de camada superior.

O UDP recebe as mensagens do processo de aplicação, junta-lhe os campos de número de porta de origem e destino, adiciona dois outros campos, e passa o segmento resultante à camada de rede. De fato, o principal valor de se ter o UDP em relação ao uso do IP bruto é a adição das portas de origem e destino. Se o segmento chegar ao *host* de destino, o UDP usa os números da porta para o processo de aplicação correto.

Vale a pena mencionar explicitamente algumas ações que o UDP não realiza. Ele não realiza controle de fluxo, controle de erros ou retransmissão após a recepção de um segmento incorreto. O UDP apenas inicia a transferência de dados sem quaisquer preliminares formais. Assim o UDP não introduz qualquer atraso para estabelecer uma ligação. Desta forma, o UDP é utilizado em aplicações que podem tolerar uma pequena quantidade de perda de pacotes e são sensíveis à velocidade, por exemplo em aplicações multimídia, como telefone por Internet e videoconferência em tempo real.

Atividade

05. Agora iremos realizar uma Análise do protocolo UDP.

- **a)** Utilize a Internet normalmente (acesse sites, etc.);
- **b)** Aplique um filtro aos pacotes capturados de forma a visualizar apenas os pacotes UDP do seu computador (ip.addr == “seu IP“ and udp); Quais os campos existentes no cabeçalho de um segmento TCP e UDP?
- **c)** Escreve algumas portas UDP encontradas.
- **d)** Explique a diferença entre os protocolos TCP e UDP. E Indique as razões para uma aplicação utilizar do UDP em vez de TCP?