

ATIVIDADES TEÓRICA

Aluno: Wallan Oliveira da Silva, 3º Período

1) Cite quatro protocolos da camada de Internet da arquitetura TCP/IP e comente sobre cada um deles.

IP (Internet Protocol): O protocolo IP essencialmente define a camada Internet no modelo DoD. Os outros protocolos nesta camada existem apenas para suportá-lo. O protocolo IP efetua uma análise dos endereço para cada pacote de dados que recebe. Em seguida, utilizando uma tabela de roteamento (routing table), ele decide para onde o pacote deve ser enviado, selecionando a melhor rota (que nem sempre é a mais curta! Veremos isso mais adiante).

ICMP (Internet Control Message Protocol): O protocolo ICMP (Internet Control Message Protocol) é definido na camada Internet e é usado pelo protocolo IP. O ICMP é um protocolo gerenciador, agindo também como um "mensageiro" para o protocolo IP. Suas mensagens são transportadas como datagramas IPs. O ICMP também é usado na descoberta de rotas para gateways. Periodicamente, anúncios (advertisements) de routers são transmitidos pela rede, contendo os endereços IPs de suas interfaces ativas. Os dispositivos de rede analisam esses pacotes e atualizam as informações sobre rotas.

ARP (Address Resolution Protocol): O protocolo ARP (Protocolo de Resolução de Endereço) é responsável por localizar o endereço de hardware de um dispositivo a partir de seu endereço IP conhecido.

RARP (Reverse Address Resolution Protocol): O protocolo RARP (Protocolo de Resolução de Endereço Reverso) se encarrega de descobrir o endereço IP de uma máquina sem disco enviando mensagens de broadcast que contêm seu endereço MAC e uma requisição de endereço IP designado para aquele endereço MAC específico.

2) Quais são os campos do cabeçalho IP e suas respectivas finalidades.

Version: Número da versão do protocolo (atualmente 4);

HLEN: Comprimento do cabeçalho;

Priority ou ToS (Type of Service): Indica como o datagrama deve ser manipulado. Os primeiros 3 bits definem a prioridade;

Total Length: Comprimento total do pacote, incluindo o cabeçalho;

Identification: Valor único para identificação do pacote;

Flags: Especifica se a fragmentação deve ou não ocorrer;

Frag offset: Provê fragmentação e remontagem se um pacote de dados for muito extenso para ser colocado em um frame. Também permite diferentes unidades máximas de transmissão (Maximum Transmission Units - MTUs) na Internet;

TTL (T im e To L ive/Tem po de V ida): O valor TTL é estabelecido quando um pacote é originalmente gerado. Ele estabelece o tempo de vida do pacote através de diferentes métricas (número de saltos, tempo etc.). Se o pacote não atingir seu destino antes de o timer TTL expirar, ele é descartado. Isso impede pacotes IPs de circularem continuamente pela Internet, gerando loopings;

Protocol: Número da porta lógica do protocolo de camada superior (Transporte). A porta TCP é 6 e a UDP é 17, em hexadecimal (note que aqui falamos de portas lógicas utilizadas pelo protocolo IP. Apesar de o conceito ser parecido, não deve ser confundido com o que vimos na camada de Transporte (TCP e UDP));

Header Checksum: Checagem de redundância (aplicada ao cabeçalho, apenas);

Source IP address: Endereço IP de origem (32-bits);

Destination IP address: Endereço IP de destino (32-bits);

IP option: Campo utilizado em testes de rede (debugging);

Data: Dados enviados pela camada superior (Transporte)

3) Explique sobre as Portas Lógicas IP.

A porta lógica, é o dado capaz de identificar e individualizar o usuário que acessa a rede, sendo que tanto os provedores de conexão quanto os de aplicação, possuem informações sobre as portas lógicas, na medida em que registram essas informações quando os usuários navegam por suas plataformas.

4) Explique o que é:

a) Endereço de Broadcast

Endereço usado por aplicações e dispositivos para o envio de mensagens a todos os dispositivos de uma rede, simultaneamente (1-toall). Pode-se fazer aqui uma analogia ao sistema aberto de televisão. Todos com um aparelho de TV conseguem captar o sinal de uma TV aberta (ex. TV Cultura), pois o sinal é enviado de um ponto (antena transmissora) para todas as TVs em uma região

b) Endereço unicast

Comunicação de uma máquina para apenas outra máquina (1-to-1). A analogia aqui seria o pay-per-view . Somente o assinante que solicitou o programa (e pagou por ele, no caso) o receberá.

c) Endereço multicast

Endereço usado por apenas uma máquina para alcançar um grupo definido de máquinas (1-to-many). A analogia que cabe aqui é o sistema fechado de televisão (TV por assinatura). Apenas um grupo específico de usuários recebe o seu sinal (os assinantes);

3) Para as classes A, B, C e D, identifique quais partes identificam a parte de rede e a parte de host.

Classe A: rede.host.host.host

Classe B: rede.rede.host.host

Classe C: rede.rede.rede.host

Classe D: Classe reservada para endereços multicast

4) Qual a faixa de endereços IP que identifica um endereço classe A, B, C.

Classe A: 0-127

Classe B: 128-191

Classe C: 192-223

5) O que são os endereços reservados e qual a faixa para endereços classe A, B e C?

10.0.0.0 a 10.255.255.255 - 1 rede Classe A

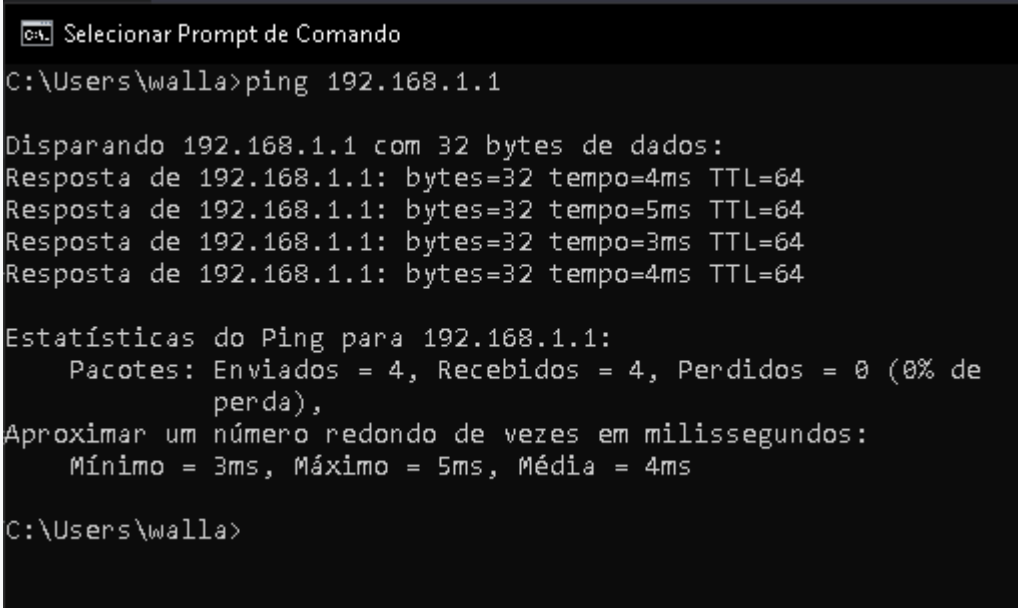
172.16.0.0 a 172.31.255.255 - 16 redes Classe B

192.168.0.0 a 192.168.255.255 - 255 redes Classe C

6) Quais as máscaras de rede padrão para classe A, B e C?

ATIVIDADE PRÁTICA

1) Utilizar o comando ping para testes na área de redes. Deverá ser utilizado o ping com quatro opções de parâmetros. Explicar o resultado dos testes do comando ping.



```
Selecionar Prompt de Comando
C:\Users\walla>ping 192.168.1.1

Disparando 192.168.1.1 com 32 bytes de dados:
Resposta de 192.168.1.1: bytes=32 tempo=4ms TTL=64
Resposta de 192.168.1.1: bytes=32 tempo=5ms TTL=64
Resposta de 192.168.1.1: bytes=32 tempo=3ms TTL=64
Resposta de 192.168.1.1: bytes=32 tempo=4ms TTL=64

Estatísticas do Ping para 192.168.1.1:
    Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de
        perda),
Aproximar um número redondo de vezes em milissegundos:
    Mínimo = 3ms, Máximo = 5ms, Média = 4ms

C:\Users\walla>
```

O comando "ping 192.168.1.1" é utilizado para testar a conectividade com o endereço IP 192.168.1.1. Esse endereço IP é um exemplo comum de um endereço utilizado em redes locais. O comando envia pacotes de dados para esse endereço IP e aguarda por respostas, permitindo verificar se o dispositivo associado a esse IP está ativo e respondendo na rede.

O resultado do comando mostrará informações sobre os pacotes enviados, recebidos e o tempo que leva para a resposta ocorrer. Isso pode ajudar a diagnosticar problemas de conectividade em uma rede local. Se tentar pingar em um dispositivo ou roteador na sua própria rede local, a resposta deverá ser rápida. Se estiver pingando um endereço fora da sua rede local, como um site na internet, os tempos de resposta podem variar dependendo da latência da conexão.

```
Selecionar Prompt de Comando
C:\Users\walla>ping -a 192.168.1.36

Disparando DESKTOP-G8IV1VS.hgu_lan [192.168.1.36] com 32 bytes de dados:
Resposta de 192.168.1.36: bytes=32 tempo<1ms TTL=128
Resposta de 192.168.1.36: bytes=32 tempo<1ms TTL=128
Resposta de 192.168.1.36: bytes=32 tempo<1ms TTL=128
Resposta de 192.168.1.36: bytes=32 tempo<1ms TTL=128

Estatísticas do Ping para 192.168.1.36:
    Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de
        perda),
Aproximar um número redondo de vezes em milissegundos:
    Mínimo = 0ms, Máximo = 0ms, Média = 0ms

C:\Users\walla>
```

O comando "ping -a 192.168.1.1" é utilizado para fazer um teste de conectividade com um endereço IP (neste caso, 192.168.1.1) e obter o nome de host correspondente, se possível. A opção "-a" é usada para realizar uma consulta reversa de DNS, ou seja, tenta encontrar o nome de host associado ao endereço IP fornecido.


```
Selecionar Administrador: Prompt de Comando
C:\Windows\system32>ping

Uso: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
        [-r count] [-s count] [[-j host-list] | [-k host-list]]
        [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
        [-4] [-6] target_name

Opções:
    -t           Executa ping no host especificado até ser parado.
                  Para ver as estatísticas e continuar, pressione
                  Control-Break;
                  Para parar, pressione Control-C.
    -a           Resolve os endereços para nomes de host.
    -n count     Número de solicitações de eco a serem enviadas.
    -l size      Envia o tamanho de buffer.
    -f           Define o sinalizador Não Fragmentar no pacote
                  (somente IPv4).
    -i TTL       Vida útil.
    -v TOS       Tipo de Serviço (somente IPv4. Essa configuração
                  foi preterida e não afeta o tipo de campo de serviço
                  no Cabeçalho IP).
    -r count     Registra a rota de saltos de contagem (somente IPv4).
    -s count     Carimbo de data/hora para saltos de contagem (somente IPv4).
    -j host-list Rota de origem flexível em host-list (somente IPv4).
    -k host-list Rota de origem rígida em host-list (somente IPv4).
    -w timeout   Tempo limite em milissegundos de espera por cada resposta.
    -R           Usa o cabeçalho de roteamento para testar também a rota
                  inversa (somente IPv6). Conforme RFC 5095, o uso desse
                  cabeçalho de roteamento foi preterido. Alguns sistemas podem
                  remover solicitações de eco se esse cabeçalho for usado.
    -S srcaddr   Endereço de origem a ser usado.
    -c compartment Identificador de compartimento de roteamento.
    -p           Executa ping em um endereço de provedor de Virtualização
                  de Rede Hyper-V.
    -4           Força o uso de IPv4.
    -6           Força o uso de IPv6.

C:\Windows\system32>
```

O comando `ping` é uma ferramenta de linha de comando que possui várias opções para testar a conectividade de rede e diagnosticar problemas de conexão. Aqui estão algumas das principais funções e opções do comando `ping`:

1. Testar Conectividade Básica:

O uso mais comum do comando `ping` é testar se um dispositivo ou host remoto está acessível na rede. Ele envia pacotes de teste (pings) para o destino especificado e aguarda por respostas. Isso verifica se o host está ativo e responde.

2. Número de Pacotes:

A opção `-n` permite especificar o número de pacotes de ping a serem enviados.

3. Intervalo entre Pacotes:

A opção `-w` permite definir um intervalo em milissegundos entre os pacotes de ping

4. Tamanho do Pacote:

A opção `-l` permite definir o tamanho em bytes dos pacotes de ping enviados.

5. Timeout:

A opção `-w` também pode ser usada para definir o tempo limite em milissegundos para aguardar por uma resposta.

6. Exibição de Resultados Contínuos:

A opção `-t` faz com que o comando `ping` continue a enviar pacotes de ping indefinidamente até ser interrompido manualmente (pressionando `Ctrl + C`).

7. Modo IPv6:

Para testar a conectividade usando o IPv6, você pode usar a opção `-6`.

8. Ajuda:

Para ver todas as opções disponíveis do comando `ping`, você pode usar a opção `-help`.

2) Utilizar o comando `tracert` para testes na área de redes. Deverá ser utilizado com quatro opções de parâmetros. Explicar o resultado dos testes do comando `tracert`.


```
Administrador: Prompt de Comando

C:\Windows\system32>tracert

Uso: tracert [-d] [-h nmax_saltos] [-j lst_hosts] [-w tempo_limite]
          [-R] [-S srcaddr] [-4] [-6] destino

Opções:
-d          Não resolver endereços para nomes de hosts.
-h nmax_saltos  Número máximo de saltos para a procura do destino.
-j lst_hosts  Rota ampliada de origens usada com a lista lst_hosts
              (só IPv4).
-w tempo_limite  Tempo de espera em milissegundos para cada resposta.
-R          Traça caminho de transmissão e retransmissão (só IPv6).
-S srcaddr  Endereço de origem para uso só (IPv6).
-4          Força usando IPv4.
-6          Força usando IPv6.

C:\Windows\system32>
```

O comando tracert (rastreamento de rota) é uma ferramenta de linha de comando presente no Windows que é usada para rastrear a rota que os pacotes de dados seguem de um computador para um destino na rede, como um site na internet ou outro host. Isso pode ajudar a identificar onde ocorrem possíveis atrasos ou problemas de conexão ao longo do caminho.

```
Administrador: Prompt de Comando

C:\Windows\system32>tracert 182.168.1.36

Rastreando a rota para fpb6a80124.ap.nuro.jp [182.168.1.36]
com no máximo 30 saltos:

 1    3 ms    3 ms    2 ms  192.168.1.1
 2    5 ms    4 ms    4 ms  10.255.255.200
 3   740 ms   4 ms    3 ms  10.200.0.10
 4    38 ms   6 ms    5 ms  160-238-162-1.pelikan.net.br [160.238.162.1]
 5    47 ms   5 ms   13 ms  100.101.69.9
 6     8 ms    9 ms    9 ms  189.42.111.65
 7    56 ms  332 ms   39 ms  200.244.67.251
 8   173 ms  173 ms  176 ms  ebt-B16122-intl02.nyk.embratel.net.br [200.230.220.190]
 9   185 ms  181 ms  182 ms  ebt-B101-intl01.nyk.embratel.net.br [200.230.252.197]
10   607 ms  165 ms  166 ms  ae11.cr1-nyc2.ip4.gtt.net [209.120.132.221]
11   225 ms  196 ms  930 ms  ae15.cr3-nyc6.ip4.gtt.net [89.149.186.217]
12   190 ms   *      *      63-220-192-118.static.pccwglobal.net [63.220.192.118]
13   490 ms  364 ms  610 ms  BE42.br01.osa02.pccwbtn.net [63.218.8.82]
14   380 ms  363 ms   ^C

C:\Windows\system32>
```

O comando tracert 182.168.1.36 será executado para rastrear a rota dos pacotes até o endereço IP 182.168.1.36. Isso pode fornecer informações sobre os roteadores intermediários que os pacotes passam antes de alcançar esse destino.

```
CA: Administrador: Prompt de Comando

C:\Windows\system32>tracert -d 182.168.1.36

Rastreando a rota para 182.168.1.36 com no máximo 30 saltos

 1    82 ms    4 ms    4 ms    192.168.1.1
 2   223 ms   105 ms   238 ms   10.255.255.200
 3    5 ms    21 ms    13 ms   10.200.0.10
 4    5 ms    10 ms    5 ms   160.238.162.1
 5   14 ms    11 ms    22 ms   100.101.69.9
 6    8 ms     9 ms    10 ms   189.42.111.65
 7   38 ms    37 ms    39 ms   200.244.67.251
 8   175 ms   183 ms   172 ms   200.230.220.190
 9   188 ms   181 ms   198 ms   200.230.252.197
10   174 ms   175 ms   175 ms   209.120.132.221
11   180 ms   200 ms   187 ms   213.200.119.186
12   174 ms    *    174 ms   63.220.192.118
13   350 ms    *   362 ms   63.218.8.82
14   344 ms   376 ms   388 ms   63.222.100.10
15   366 ms   426 ms   330 ms   219.98.228.145
16   362 ms   361 ms   356 ms   120.74.58.186
17   364 ms   386 ms   348 ms   152.165.182.209
18   355 ms   353 ms   350 ms   182.168.1.36

Rastreamento concluído.

C:\Windows\system32>
```

O comando `tracert -d 182.168.1.36` seria usado para rastrear a rota dos pacotes até o endereço IP 182.168.1.36, com a opção `-d` desativando a resolução de DNS.

```
CA: Administrador: Prompt de Comando

C:\Windows\system32>tracert -j 182.168.1.36

Rastreando a rota para fpb6a80124.ap.nuro.jp [182.168.1.36]
com no máximo 30 saltos:

 1    *      *      *      Esgotado o tempo limite do pedido.
 2    6 ms    6 ms    6 ms    10.255.255.50
 3   11 ms    9 ms    5 ms    10.200.0.29
 4    *      *      *      Esgotado o tempo limite do pedido.
 5    *      *      *      Esgotado o tempo limite do pedido.
 6    *      *      *      Esgotado o tempo limite do pedido.
 7    *      *      *      Esgotado o tempo limite do pedido.
 8    *      *      *      Esgotado o tempo limite do pedido.
 9    *      *      *      Esgotado o tempo limite do pedido.
10    *      *      *      Esgotado o tempo limite do pedido.
11  ^C

C:\Windows\system32>
```

O comando `tracert -j 192.168.1.36` é usado para realizar um rastreamento de rota usando um salto inicial especificado. Nesse caso, o endereço IP 192.168.1.36 é usado como o primeiro salto na rota.

3) Utilizar o comando ARP para testes na área de redes. Explicar o resultado dos testes do comando ARP.

```
Administrador: Prompt de Comando

C:\Windows\system32>arp

Exibe e modifica as tabelas de conversão de endereços IP para endereços físicos usadas pelo protocolo de resolução de endereços (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

-a          Exibe entradas ARP atuais interrogando os dados de protocolo atuais. Se inet_addr for especificado, somente os endereços IP e físicos do computador especificado serão exibidos. Se mais de uma interface de rede usar ARP, serão exibidas as entradas para cada tabela ARP.
-g          O mesmo que -a.
-v          Exibe as entradas ARP atuais no modo detalhado. Todas as entradas inválidas e entradas na interface de loopback serão mostradas.
inet_addr   Especifica um endereço Internet.
-N if_addr  Exibe as entradas ARP para cada interface de rede especificada por if_addr.
-d          Exclui o host especificado por inet_addr. O inet_addr pode ser marcado com o caractere * para exclusão de todos os hosts.
-s          Adiciona o host e associa o endereço Internet inet_addr ao Endereço físico eth_addr. O Endereço físico é passado como 6 bytes hexadecimais separados por hífens. A entrada é permanente.
eth_addr    Especifica um endereço físico.
if_addr     Caso esteja presente, especifica o endereço Internet da interface cuja tabela de conversão de endereços deve ser modificada.
            Caso contrário, é usada a primeira interface aplicável.

Exemplo:
> arp -s 157.55.85.212 00-aa-00-62-c6-09 .... Adiciona uma entrada estática.
> arp -a          .... Exibe a tabela ARP.
```

O comando "arp" (Address Resolution Protocol) é uma ferramenta de linha de comando que permite visualizar e gerenciar a tabela ARP de um sistema. A tabela ARP é usada para associar endereços IP a endereços MAC em uma rede local.

```
CA Administrator: Prompt de Comando

C:\Windows\system32>arp -a

Interface: 192.168.1.36 --- 0x8
    Endereço IP      Endereço físico      Tipo
    192.168.1.1      80-07-1b-1f-d5-70    dinâmico
    192.168.1.37      10-77-17-b8-64-8c    dinâmico
    192.168.1.255     ff-ff-ff-ff-ff-ff    estático
    224.0.0.22        01-00-5e-00-00-16    estático
    224.0.0.251       01-00-5e-00-00-fb    estático
    224.0.0.252       01-00-5e-00-00-fc    estático
    239.255.255.250   01-00-5e-7f-ff-fa    estático
    255.255.255.255   ff-ff-ff-ff-ff-ff    estático

Interface: 192.168.56.1 --- 0x11
    Endereço IP      Endereço físico      Tipo
    192.168.56.255   ff-ff-ff-ff-ff-ff    estático
    224.0.0.22        01-00-5e-00-00-16    estático
    224.0.0.251       01-00-5e-00-00-fb    estático
    224.0.0.252       01-00-5e-00-00-fc    estático
    239.255.255.250   01-00-5e-7f-ff-fa    estático

C:\Windows\system32>
```

O comando "arp -a" exibe a tabela ARP completa, mostrando as associações entre endereços IP e endereços MAC dos dispositivos na rede local.