

TP3 - Arquitetura de Redes de Computadores



Esse é o terceiro teste de performance da disciplina Arquitetura de redes de computadores.



Aluno: Bruno Fernandes

Email: bruno.fernandes@al.infnet.edu.br

Prof: Prof. Adriano Saad

- Comente 3 funcionalidades que podem existir na camada de aplicação do modelo TCP/IP.

A camada mais próxima do usuário final, ela tem por função servir como terminal para as operações que ocorrem em uma rede.

Capacidade de identificar codificação de caracteres para a conversão adequada e fazer criptografia, define uma interface de comunicação entre os hosts, representação de estruturas, padronizadas neste nível, geralmente usando XML.

Quando alguém precisa requisitar algo que está em uma rede, é na camada de aplicação que irá ser feita a requisição ou recebimento de informações, fornecimento de serviços de rede "reais", ao usuário. A camada de aplicação é responsável por gerenciar e deixar disponível ao usuário, todos os sistemas e ferramentas a ele destinados.

- Considerando a requisição HTTP abaixo, identifique: o nome do servidor, a URL, o Browser, e qual usuário e senha foram utilizados para acessar o sistema.

Request

Raw

Hex

```
POST /index.php?acao=login HTTP/1.1
Host: exemplo.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 43
Cookie: JSESSIONID=0BCE9BACC18AEAAA0799E00F59DC976B
Connection: close

user=donald&password=alb2c3d4
```

Nome do servidor: exemplo.com

URL: exemplo.com/index.php?acao=login

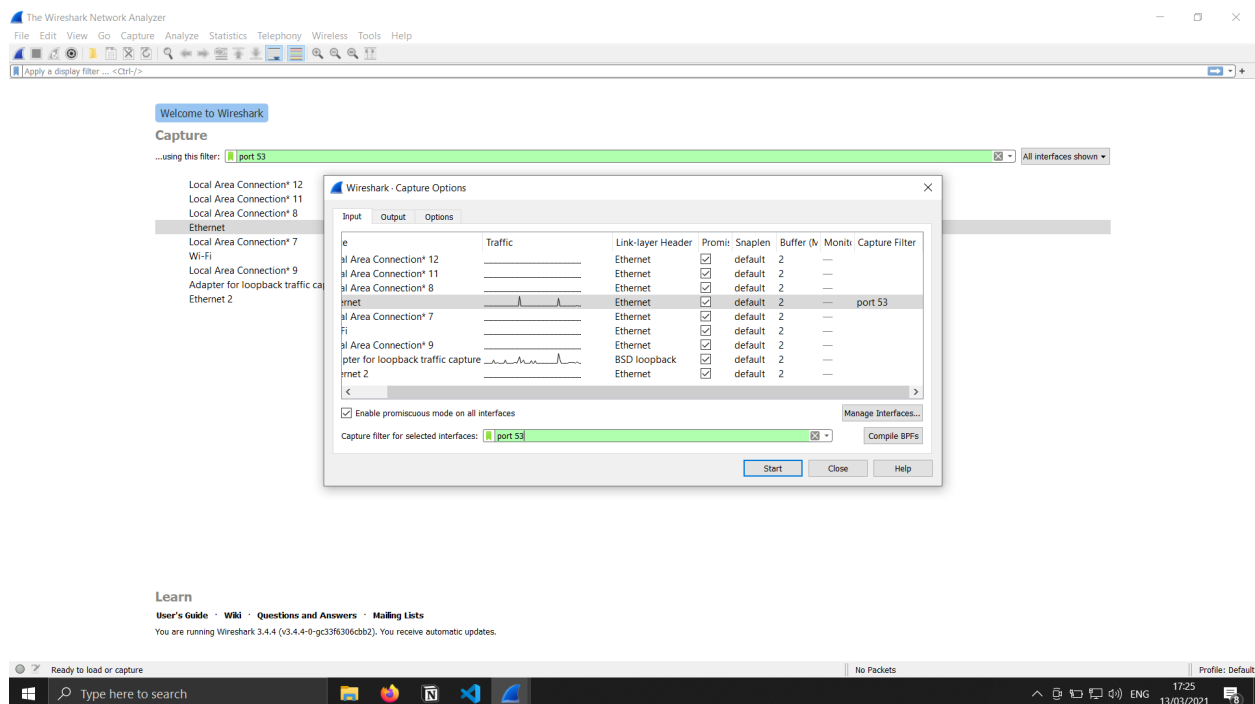
Browser: Mozilla Firefox

Usuário: donald

Senha: a1b2c3d4

- Faça uma captura utilizando o Wireshark de tráfego DNS (UDP porta 53). Você deve capturar a tela com o resultado dos testes e apontar com setas onde estão os pacotes relevantes. Observação: a captura da tela deve capturar a tela toda, inclusive com o horário e data na barra inferior para garantir a autenticidade da captura. Dica: Inicie a captura de pacotes com o wireshark, e só depois acesse algum site.

Antes da captura:



Iniciando a captura (Apenas o firefox, notion e kaspersky abertos):

Capturing from Ethernet (port 53)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|-----------------------|-----------------------|----------|--------|--|
| 5 | 9.524623 | 2804:14c:6581:7f1:1 | 2804:14d:1:0:181:21:1 | DNS | 103 | Standard query 0x7eed A youtube-ui.l.google.com |
| 6 | 9.539121 | 2804:14d:1:0:181:21:1 | 2804:14c:6581:7f1:1 | DNS | 463 | Standard query response 0x7eed A youtube-ui.l.google.com A 142.250.79.14 A 142.250.78.238 A 172.217.29.110 A 216.58.202.238 A 172... |
| 7 | 9.539747 | 2804:14c:6581:7f1:1 | 2804:14d:1:0:181:21:1 | DNS | 103 | Standard query 0x63c0 AAAA youtube-ui.l.google.com |
| 8 | 9.556079 | 2804:14d:1:0:181:21:1 | 2804:14c:6581:7f1:1 | DNS | 463 | Standard query response 0x63c0 AAAA youtube-ui.l.google.com AAAA 2800:3f0:4004:80b::200e AAAA 2800:3f0:4004:808::200e AAAA 2800:3... |
| 9 | 22.803497 | 192.168.0.11 | 181.213.132.3 | DNS | 90 | Standard query 0x2348 AAAA 30.ucp-ntfy.kaspersky-labs.com |
| 10 | 22.803638 | 192.168.0.11 | 181.213.132.3 | DNS | 90 | Standard query 0x2900 A 30.ucp-ntfy.kaspersky-labs.com |
| 11 | 22.803699 | 192.168.0.11 | 181.213.132.2 | DNS | 90 | Standard query 0x2348 AAAA 30.ucp-ntfy.kaspersky-labs.com |
| 12 | 22.803756 | 192.168.0.11 | 181.213.132.2 | DNS | 90 | Standard query 0x2900 A 30.ucp-ntfy.kaspersky-labs.com |
| 13 | 22.816499 | 181.213.132.3 | 192.168.0.11 | DNS | 172 | Standard query response 0x2348 AAAA 30.ucp-ntfy.kaspersky-labs.com SOA dnsmaster.kaspersky-labs.net |
| 14 | 22.822442 | 181.213.132.2 | 192.168.0.11 | DNS | 393 | Standard query response 0x2900 A 30.ucp-ntfy.kaspersky-labs.com A 62.67.238.211 A 62.67.238.208 A 62.67.238.205 A 62.67.238.214 A... |
| 15 | 22.823286 | 181.213.132.3 | 192.168.0.11 | DNS | 393 | Standard query response 0x2900 A 30.ucp-ntfy.kaspersky-labs.com A 62.67.238.202 A 62.67.238.205 A 62.67.238.211 A 62.67.238.208 A... |
| 16 | 22.824941 | 181.213.132.2 | 192.168.0.11 | DNS | 172 | Standard query response 0x2348 AAAA 30.ucp-ntfy.kaspersky-labs.com SOA dnsmaster.kaspersky-labs.net |

> Frame 1: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface \Device\NPF_{66001F06-792C-4432-A117-C33CB4F25CD}, id 0

> Ethernet II, Src: Dell0e:09:ee (e4:54:e8:0e:09:ee), Dst: ARRI5Go_d3:db:97 (bc:2e:48:d3:db:97)

> Internet Protocol Version 6, Src: 2804:14c:6581:7f1:11aa:f4c:fd81:4a30, Dst: 2804:14d:1:0:181:213:132:3

> User Datagram Protocol, Src Port: 53215, Dst Port: 53

> Domain Name System (query)

```

0000  bc 2e 48 d3 db 97 e4 54  e8 0e 09 ee 86 dd 60 00  ..H...T.....
0010  00 00 00 27 11 40 28 04  01 4c 65 81 07 f1 11 aa  ....@...Le....
0020  1f 4c fd 81 4a 30 28 04  01 4d 00 01 00 00 01 81  ..L..00...M....
0030  02 13 01 32 00 03 cf df  00 35 00 27 3d be ea 0e  ...2.....S'....
0040  01 00 00 01 00 00 00 00  00 00 03 77 77 77 06 6e  .........www.n
0050  6f 74 69 6f 6e 02 73 6f  00 00 1c 00 01          ..otion-so.....

```

Ethernet: <live capture in progress> Packets: 16 - Displayed: 16 (100.0%) Profile: Default

Final da captura (Ao acessar o site do LinkedIn):

Capturing from Ethernet (port 53)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|-----------------------|-----------------------|----------|--------|--|
| 233 | 70.477868 | 2804:14c:6581:7f1:1 | 2804:14d:1:0:181:21:1 | DNS | 105 | Standard query 0x2453 A pop-edc2.mix.linkedin.com |
| 234 | 70.496493 | 2804:14d:1:0:181:21:1 | 2804:14c:6581:7f1:1 | DNS | 453 | Standard query response 0x2453 A pop-edc2.mix.linkedin.com A 108.174.11.85 NS dns3.p09.nsone.net NS dns1.p09.nsone.net NS ns2.p43... |
| 235 | 70.497240 | 2804:14c:6581:7f1:1 | 2804:14d:1:0:181:21:1 | DNS | 105 | Standard query 0xd3f8 AAAA pop-edc2.mix.linkedin.com |
| 236 | 70.509439 | 2804:14d:1:0:181:21:1 | 2804:14c:6581:7f1:1 | DNS | 481 | Standard query response 0xd3f8 AAAA pop-edc2.mix.linkedin.com AAAA 2620:119:50e4:101::6cae:b55 NS dns1.p09.nsone.net NS dns3.p09... |
| 237 | 71.123721 | 2804:14c:6581:7f1:1 | 2804:14d:1:0:181:21:1 | DNS | 97 | Standard query 0x7b8f A p.adsymptotic.com |
| 238 | 71.123945 | 2804:14c:6581:7f1:1 | 2804:14d:1:0:181:21:1 | DNS | 97 | Standard query 0x62cc AAAA p.adsymptotic.com |
| 239 | 71.139677 | 2804:14d:1:0:181:21:1 | 2804:14c:6581:7f1:1 | DNS | 497 | Standard query response 0x7b8f A p.adsymptotic.com A 104.18.100.194 A 104.18.99.194 A 104.18.102.194 A 104.18.101.194 A 104.18.98... |
| 240 | 71.141689 | 2804:14d:1:0:181:21:1 | 2804:14c:6581:7f1:1 | DNS | 157 | Standard query response 0x62cc AAAA p.adsymptotic.com SOA plato.ns.cloudflare.com |
| 241 | 71.143771 | 2804:14c:6581:7f1:1 | 2804:14d:1:0:181:21:1 | DNS | 97 | Standard query 0x84c4 A p.adsymptotic.com |
| 242 | 71.158675 | 2804:14d:1:0:181:21:1 | 2804:14c:6581:7f1:1 | DNS | 497 | Standard query response 0x84c4 A p.adsymptotic.com A 104.18.100.194 A 104.18.99.194 A 104.18.102.194 A 104.18.101.194 A 104.18.98... |
| 243 | 71.160267 | 2804:14c:6581:7f1:1 | 2804:14d:1:0:181:21:1 | DNS | 97 | Standard query 0xc845 AAAA p.adsymptotic.com |
| 244 | 71.183617 | 2804:14d:1:0:181:21:1 | 2804:14c:6581:7f1:1 | DNS | 157 | Standard query response 0xc845 AAAA p.adsymptotic.com SOA plato.ns.cloudflare.com |

> Frame 1: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface \Device\NPF_{66001F06-792C-4432-A117-C33CB4F25CD}, id 0

> Ethernet II, Src: Dell0e:09:ee (e4:54:e8:0e:09:ee), Dst: ARRI5Go_d3:db:97 (bc:2e:48:d3:db:97)

> Internet Protocol Version 6, Src: 2804:14c:6581:7f1:11aa:f4c:fd81:4a30, Dst: 2804:14d:1:0:181:213:132:3

> User Datagram Protocol, Src Port: 53215, Dst Port: 53

> Domain Name System (query)

```

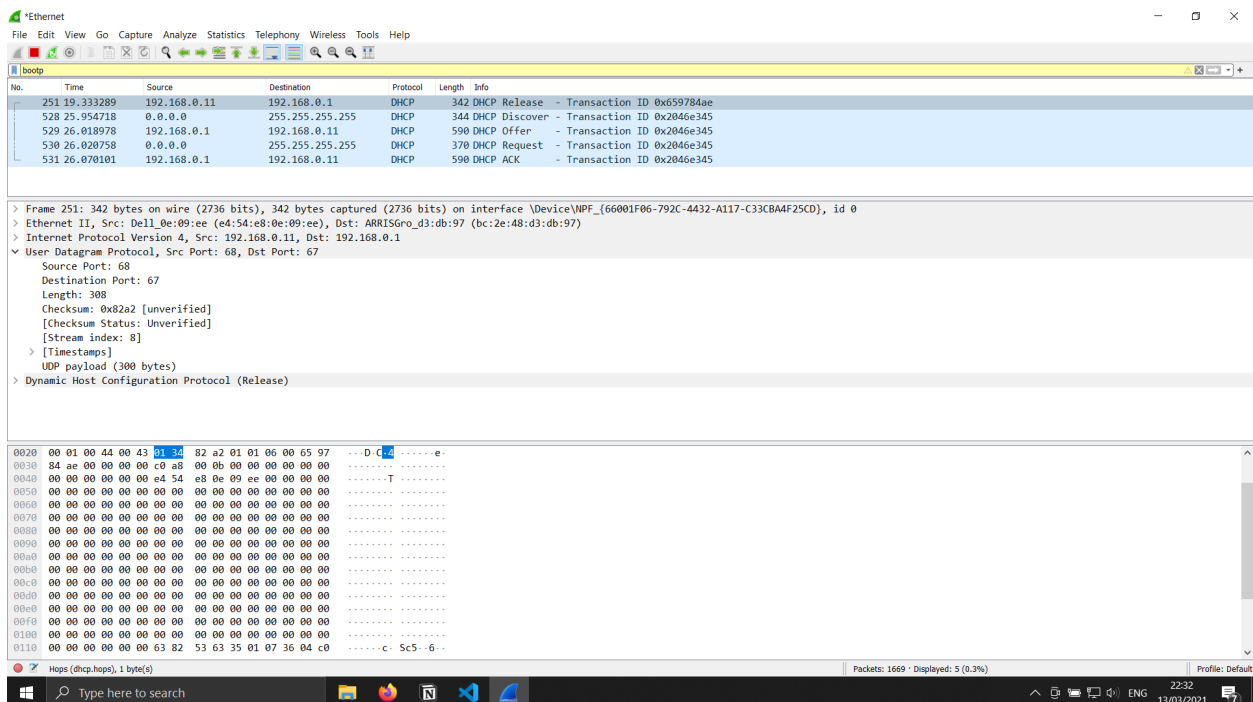
0000  bc 2e 48 d3 db 97 e4 54  e8 0e 09 ee 86 dd 60 00  ..H...T.....
0010  00 00 00 27 11 40 28 04  01 4c 65 81 07 f1 11 aa  ....@...Le....
0020  1f 4c fd 81 4a 30 28 04  01 4d 00 01 00 00 01 81  ..L..00...M....
0030  02 13 01 32 00 03 cf df  00 35 00 27 3d be ea 0e  ...2.....S'....
0040  01 00 00 01 00 00 00 00  00 00 03 77 77 77 06 6e  .........www.n
0050  6f 74 69 6f 6e 02 73 6f  00 00 1c 00 01          ..otion-so.....

```

Ethernet: <live capture in progress> Packets: 244 - Displayed: 244 (100.0%) Profile: Default

- Faça uma captura utilizando o Wireshark de tráfego DHCP (UDP porta 67 ou 68). Você deve capturar a tela com o resultado dos testes e apontar com setas onde estão os pacotes relevantes. Observação: a captura da tela deve capturar a tela toda, inclusive com o horário e data na barra inferior para garantir a autenticidade da captura. Dica: Inicie a captura de pacotes com o wireshark, e depois conecte e desconecte o cabo/placa de rede para ganhar um novo endereço IP.

A captura foi feita filtrando apenas os protocolos DHCP, portanto não foi necessário sinalizar os pacotes relevantes.



- Explique com suas próprias palavras os motivos pelos quais gerenciar uma rede é importante.

O gerenciamento de uma rede está associado a controlar os acessos, fazer com que a rede se mantenha estável, descongestionada, se possível melhorar a eficiência da rede, fazer com que a eficiência influencie em menores custos operacionais para a rede, manter a rede e as informações dela seguras, dentre outros motivos o gerenciamento de uma rede se faz tão importante. O gerenciamento de uma rede está associado ao controle de acessos,

documentação de funcionamento e configuração da rede, auxílio ao usuário, disponibilidade e desempenho, gerência de problemas na rede, controle de inventário e etc.

- Faça uma pesquisa na internet e liste pelo menos 3 softwares de monitoramento ou de gerência de redes.

Wireshark: É um software livre e de código livre para analisar pacotes, ele analisa o tráfego de uma rede e o disponibiliza em uma interface gráfica.

Nmap: É um software que faz port scan, utilizado para verificar a segurança de máquinas, descobrir serviços/servidores em uma rede. Dispõe uma interface gráfica e de console. O software Nmap faz a descoberta de hosts, scaneia portas(TCP e UDP), detecção de serviços para descobrir nome e versão, detecção de sistemas operacionais e dentre outras funcionalidades.

Pcap: É uma API que captura o tráfego de uma rede, softwares de monitoramento de redes utilizam as portabilidades atuais do Pcap (libpcap(Unix), Npcap(windows)) para fazer a captura de pacotes que trafegam na rede.

Spiceworks: É uma ferramenta de monitoramento de redes, com uma função de alerta em tempo real. É um Dashboard em tempo real, dá a possibilidade de monitorar os status de dispositivos e serviços, e alertando se valores específicos estão diferentes dos critérios prédefinidos.

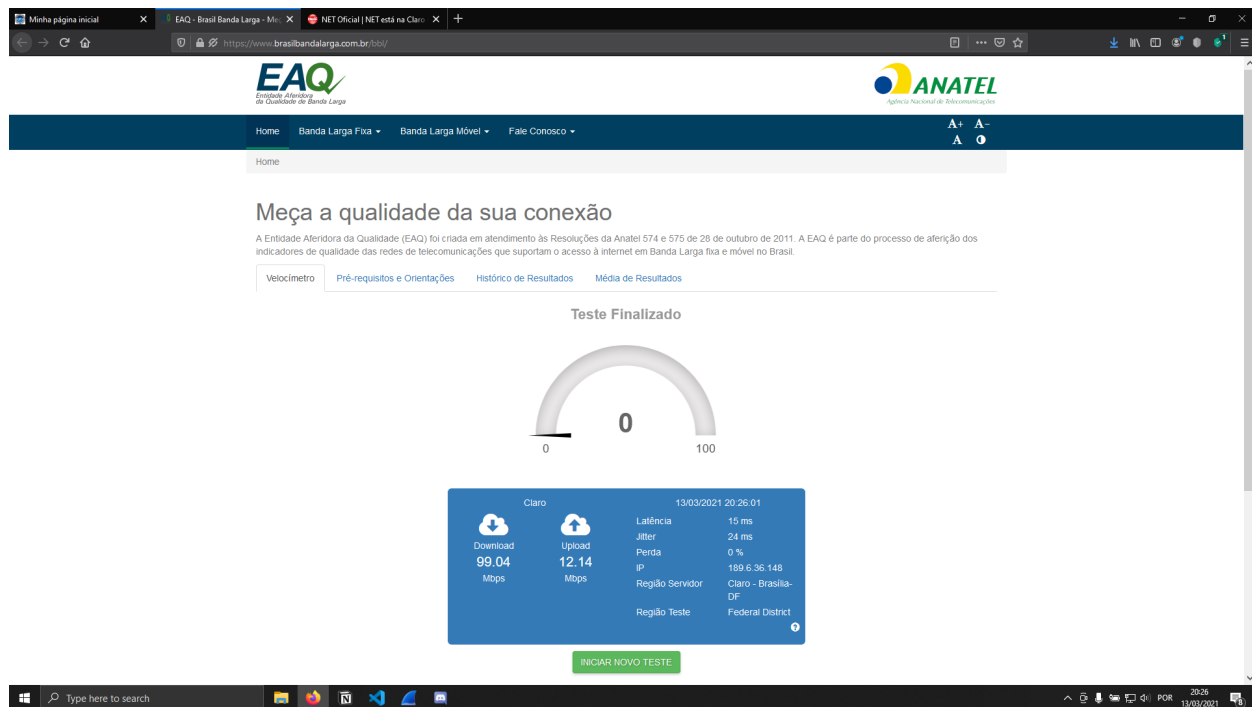
- Usuários ligaram para o suporte reclamando que não conseguiam imprimir seus arquivos na impressora da empresa. A primeira ação do funcionário do suporte foi executar um PING no endereço IP da impressora. Explique por que ele fez isso.

O PING pode ser usado para avaliar um sistema, ao fazer mudanças na rede, ou até a mesma apresentar problemas. Usando um tipo simples de pacote, temos uma resposta do subsistema de comunicação (TCP/IP) do sistema operacional, é bem simples de ser executado e rápido, para fazer uma verificação simples, avaliando a conexão e o tempo de comunicação com outro ponto. O funcionário

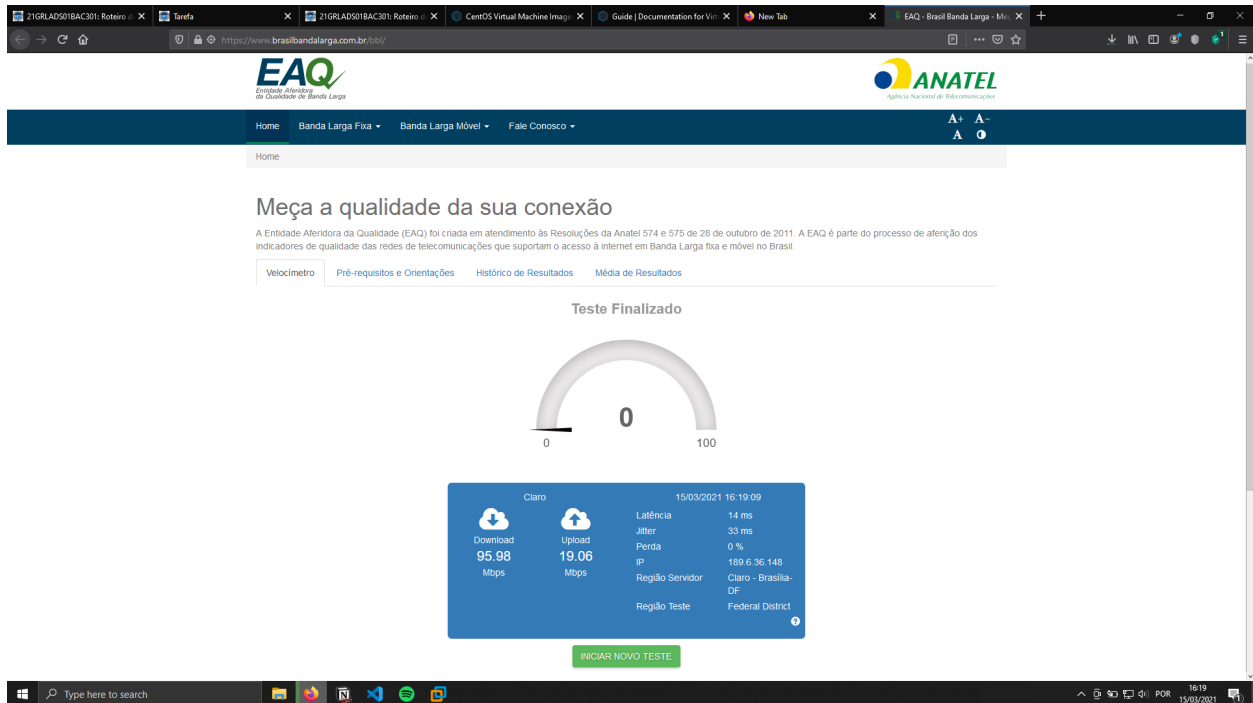
do suporte fez essa verificação com objetivo de verificar se a impressora estava conectada na rede.

- Acesse o site <http://www.brasilbandalarga.com.br/bbl> e faça, de sua residência ou de um local cuja velocidade contratada de serviço de internet você conheça, o teste de velocidade da internet em dois momentos diferentes, de preferência em horários bem distintos, como manhã e noite. Você deve capturar a tela com o resultado dos testes. Observação: a captura da tela deve capturar a tela toda, inclusive com o horário e data na barra inferior para garantir a autenticidade da captura.

captura 1:



captura 2:



- Com base no resultado do teste anterior, informe qual a velocidade do link de internet onde o teste foi feito e explique se o provedor está cumprindo com a velocidade mínima contratada.

A velocidade aproximada da internet que foi capturada chegou a 100 Mbps, porém a velocidade contratada é de 120 Mbps, isso se dá pelo cabo Ethernet usado ser Cat5, ou inferior, e não suportar velocidades superiores.

- Um administrador de rede executou um PING em um servidor interno e o resultado demonstrou que tudo estava correto. Logo depois, executou um PING em outro servidor interno, que estava no mesmo switch do primeiro servidor, e o resultado demonstrou que estava ocorrendo perda de pacotes. Liste pelo menos 3 problemas que poderiam causar esse tipo de perda de pacotes.

Erros no Hardware: Dispositivos ou peças do dispositivo também podem quebrar ou ter erros. Podemos ter sobrecargas no hardware, falhas de alimentação energética, dentre outras.

Sobrecarga no servidor: No segundo servidor, podemos estar tendo uma sobrecarga no tráfego da rede, levantando erros de transmissão e consequentemente ocasionando a perda de pacotes.

Erros de software: Diferenças de versão dos softwares e falta de algum pacote que seja de um servidor para o outro pode estar ocasionando perda de pacotes e diferenças entre os dois servidores internos.

Desempenho dos dispositivos: Os dois dispositivos são hardwares diferentes, ocasionando maior falta de desempenho de um em relação ao outro, ocasionando perda de pacotes de um lado.

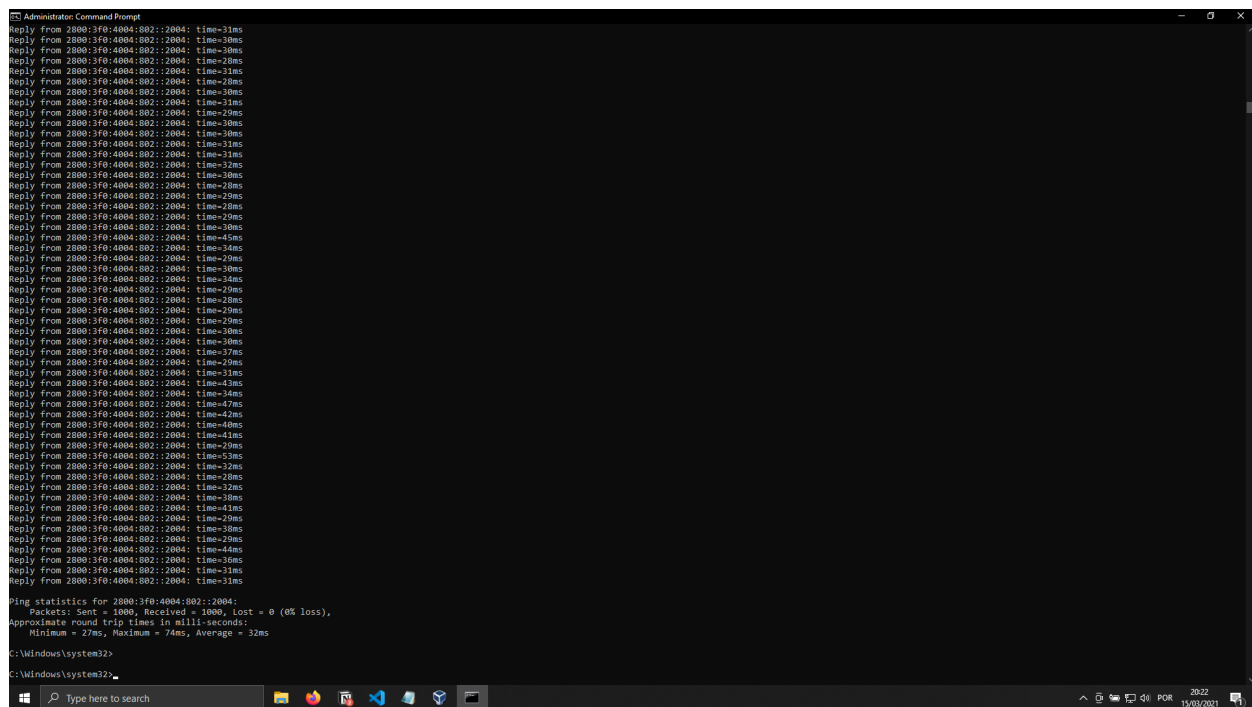
- Muitas empresas possuem redes wireless (wifi) dentro do ambiente corporativo. Faça uma pesquisa e liste pelo menos 3 critérios importantes para gerenciar redes wireless.

Deve ser feita uma configuração bem planejada e de forma correta da rede sem fio, com objetivo de cobrir todos os locais que devem ser servidos pela rede wi-fi, garantindo a qualidade de sinal, testando com um Site Survey para garantir a qualidade do sinal em cada ponto, portanto, disponibilidade é um critério importante. Deve ser controlado todos os acessos e monitoramento dos serviços usados na rede para garantir a segurança da rede, manter os dados sensíveis seguros e protegidos de possíveis acessos não autorizados, garantir a integridade dos dados, a segurança da rede é uma questão importante nos critérios de uma rede wireless. Podemos ter caso de uso de rede com servidores locais, onde é necessário ter backups e mais de um servidor para garantir disponibilidade, problemas como falha energética, dentre outros, podem afetar um servidor, portanto o outro mantém a rede estável e os dados seguros, em casos de utilização de nuvens de empresas terceirizadas (Amazon AWS, Google Cloud, Microsoft Azure e etc.), se faz necessária a contratação de funcionários que sejam especializados nesses serviços, para que seja configurada da forma mais otimizada para a empresa, de forma menos custosa e mais eficiente.

Qualidade da rede, disponibilidade e segurança são critérios importantes no gerenciamento das redes wireless.

- Execute o comando “**ping -n 1000 www.infnet.edu.br**”. Ao fim do programa, será exibido um resumo dos testes efetuados. Interprete os resultados de perda de pacotes e de atraso médio. Você deve capturar a tela com o resultado dos testes. Observação: a captura da tela deve capturar a tela toda, inclusive com o horário e data na barra inferior para garantir a autenticidade da captura.

O site www.infnet.edu.br não devolve qualquer resposta, provavelmente está com acesso bloqueado. Portanto foi feito o comando usando o site do google.com



```
Administrator: Command Prompt
Reply from 2800:3f0:4004:802::2004: time=31ms
Reply from 2800:3f0:4004:802::2004: time=30ms
Reply from 2800:3f0:4004:802::2004: time=28ms
Reply from 2800:3f0:4004:802::2004: time=28ms
Reply from 2800:3f0:4004:802::2004: time=31ms
Reply from 2800:3f0:4004:802::2004: time=28ms
Reply from 2800:3f0:4004:802::2004: time=30ms
Reply from 2800:3f0:4004:802::2004: time=28ms
Reply from 2800:3f0:4004:802::2004: time=31ms
Reply from 2800:3f0:4004:802::2004: time=32ms
Reply from 2800:3f0:4004:802::2004: time=30ms
Reply from 2800:3f0:4004:802::2004: time=31ms
Reply from 2800:3f0:4004:802::2004: time=28ms
Reply from 2800:3f0:4004:802::2004: time=29ms
Reply from 2800:3f0:4004:802::2004: time=28ms
Reply from 2800:3f0:4004:802::2004: time=29ms
Reply from 2800:3f0:4004:802::2004: time=30ms
Reply from 2800:3f0:4004:802::2004: time=34ms
Reply from 2800:3f0:4004:802::2004: time=30ms
Reply from 2800:3f0:4004:802::2004: time=30ms
Reply from 2800:3f0:4004:802::2004: time=34ms
Reply from 2800:3f0:4004:802::2004: time=29ms
Reply from 2800:3f0:4004:802::2004: time=28ms
Reply from 2800:3f0:4004:802::2004: time=29ms
Reply from 2800:3f0:4004:802::2004: time=30ms
Reply from 2800:3f0:4004:802::2004: time=30ms
Reply from 2800:3f0:4004:802::2004: time=27ms
Reply from 2800:3f0:4004:802::2004: time=29ms
Reply from 2800:3f0:4004:802::2004: time=31ms
Reply from 2800:3f0:4004:802::2004: time=33ms
Reply from 2800:3f0:4004:802::2004: time=34ms
Reply from 2800:3f0:4004:802::2004: time=7ms
Reply from 2800:3f0:4004:802::2004: time=42ms
Reply from 2800:3f0:4004:802::2004: time=40ms
Reply from 2800:3f0:4004:802::2004: time=41ms
Reply from 2800:3f0:4004:802::2004: time=29ms
Reply from 2800:3f0:4004:802::2004: time=33ms
Reply from 2800:3f0:4004:802::2004: time=22ms
Reply from 2800:3f0:4004:802::2004: time=28ms
Reply from 2800:3f0:4004:802::2004: time=32ms
Reply from 2800:3f0:4004:802::2004: time=30ms
Reply from 2800:3f0:4004:802::2004: time=41ms
Reply from 2800:3f0:4004:802::2004: time=29ms
Reply from 2800:3f0:4004:802::2004: time=30ms
Reply from 2800:3f0:4004:802::2004: time=44ms
Reply from 2800:3f0:4004:802::2004: time=36ms
Reply from 2800:3f0:4004:802::2004: time=31ms
Reply from 2800:3f0:4004:802::2004: time=31ms

Ping statistics for 2800:3f0:4004:802::2004:
    Packets: Sent = 1000, Received = 1000, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 27ms, Maximum = 74ms, Average = 32ms

C:\Windows\system32>
C:\Windows\system32>
```

Ping statistics for 2800:3f0:4004:802::2004:

Packets: Sent = 1000, Received = 1000, Lost = 0 (0% loss),

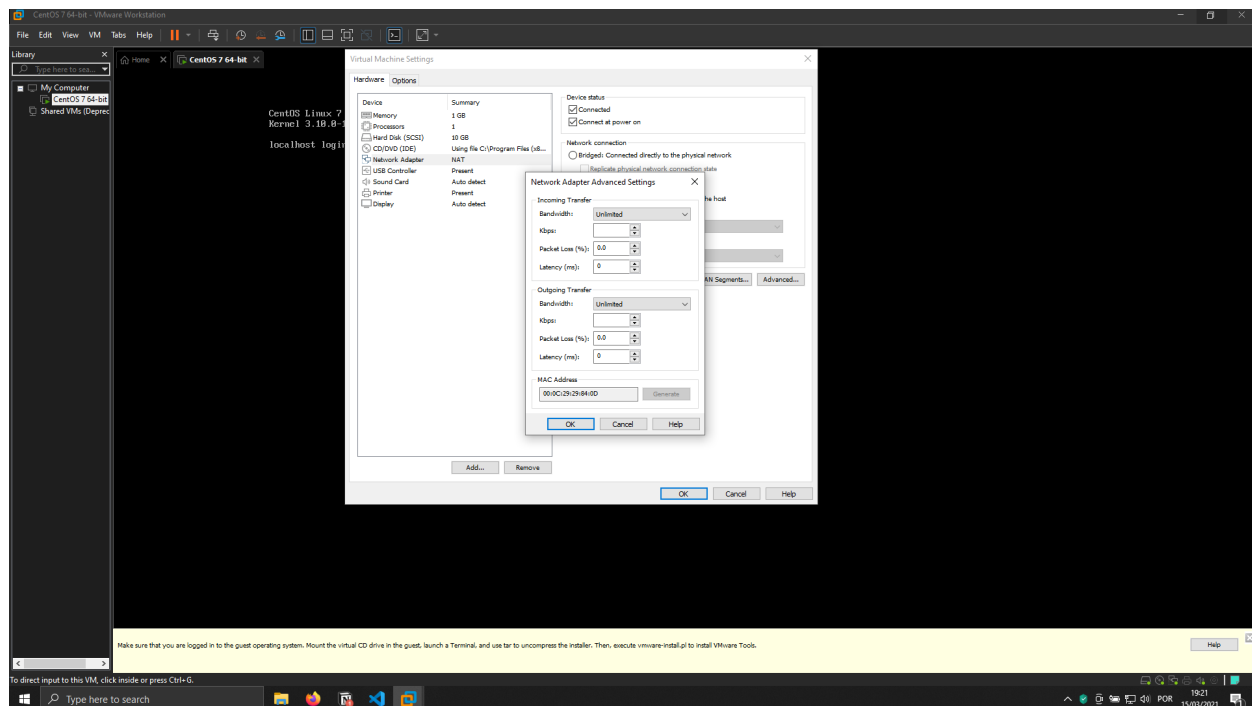
Approximate round trip times in milli-seconds:

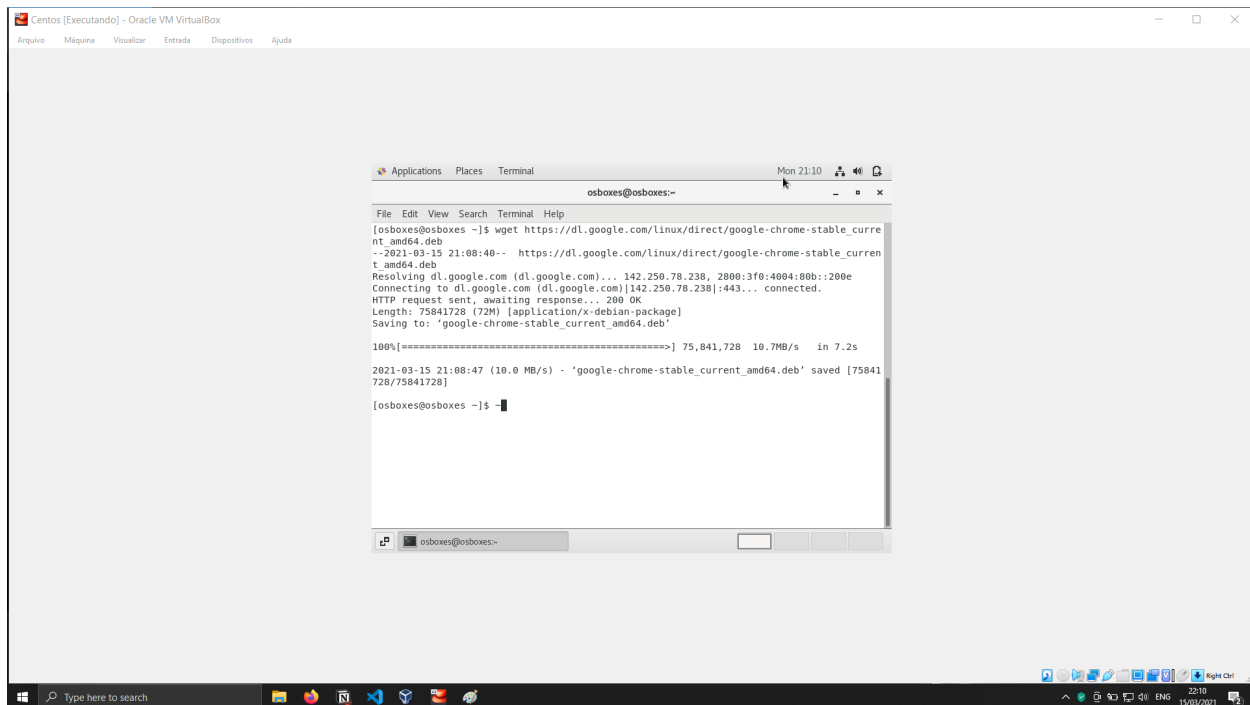
Minimum = 27ms, Maximum = 74ms, Average = 32ms

Podemos observar que a perda de pacotes foi 0 e o atraso médio do ping foi de 32ms.

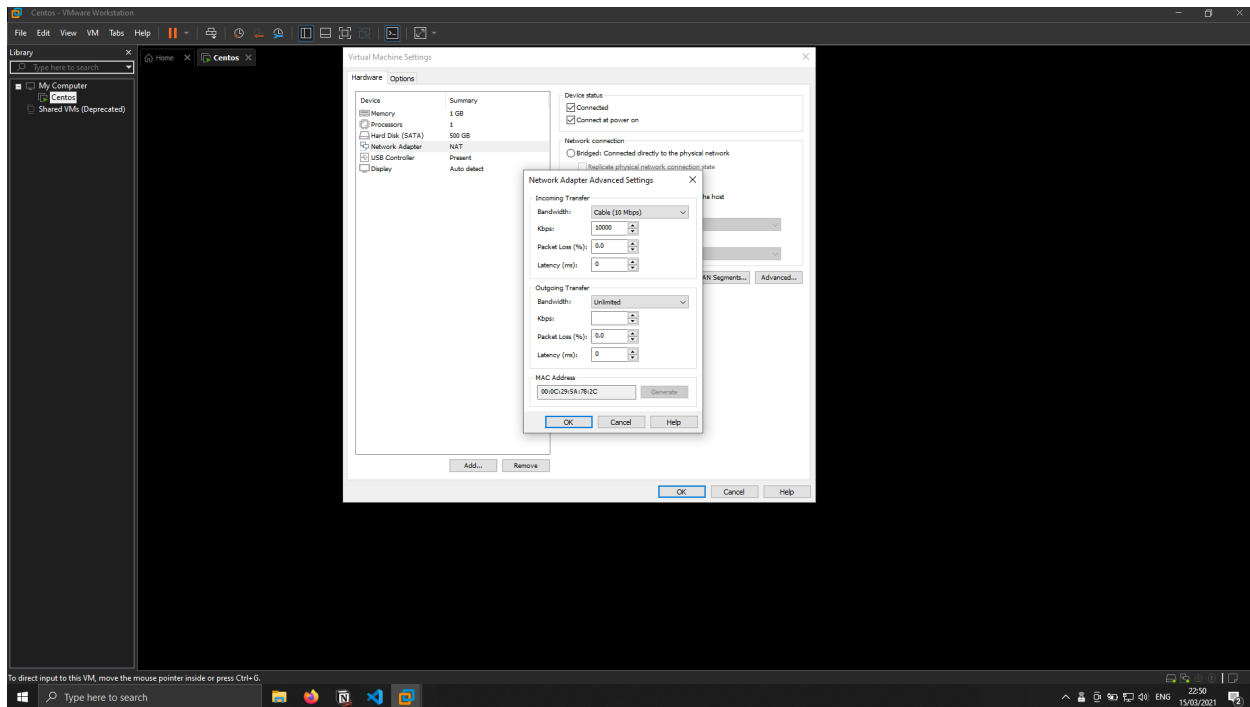
- Faça a instalação de uma máquina virtual conforme descrito na “**Etapas 6 - Prática - Como simular redes com velocidades menores e perda de pacotes**”. Carregue um servidor HTTP localmente no seu computador e disponibilize um arquivo entre 50Mbytes a 100Mbytes, ou escolha um arquivo de tamanho semelhante na internet para ser o arquivo de referência. Refaça o **Teste 1** você mesmo e apresente o resultado do teste. Você deve capturar a tela com o resultado dos testes. Observação: a captura da tela deve capturar a tela toda, inclusive com o horário e data na barra inferior para garantir a autenticidade da captura.

Iniciando o teste, verificando as configurações da máquina virtual:





- Seguindo a linha do exercício 13, refaça o **Teste 2** você mesmo e apresente o resultado do teste. Você deve capturar a tela com o resultado dos testes. Observação: a captura da tela deve capturar a tela toda, inclusive com o horário e data na barra inferior para garantir a autenticidade da captura.



- Seguindo a linha do exercício 13, refaça o **Teste 3** você mesmo e apresente o resultado do teste. Você deve capturar a tela com o resultado dos testes. Observação: a captura da tela deve capturar a tela toda, inclusive com o horário e data na barra inferior para garantir a autenticidade da captura.
- Seguindo a linha do exercício 13, refaça o **Teste 4** você mesmo e apresente o resultado do teste. Você deve capturar a tela com o resultado dos testes. Observação: a captura da tela deve capturar a tela toda, inclusive com o horário e data na barra inferior para garantir a autenticidade da captura.
- Foi estudado a aplicação de QoS para tráfego multimídia, como VOIP. Dê pelo menos 2 exemplos de outro tipo de tráfego que poderiam se beneficiar do QoS.

O QoS é interessante para quem quer prioridade de conexão na reprodução de vídeos, serviços de streaming, jogos online e etc. Empresas usam o QoS para seus serviços de VoIP para suporte ao usuário e sistema de vendas, porém, serviços os serviços de já mencionados anteriormente, comunicação em live, streaming, dentre outros podem ser serviços que podem se beneficiar do QoS.

- Explique com suas palavras porque não é possível priorizar um tráfego (QoS) fora dos limites da rede da empresa.

O protocolo IP trata todos os pacotes de forma igual, não garante todos os serviços nos roteadores, tudo isso pelo conceito do melhor esforço. O QoS é habilitado no roteador, portanto o serviço fora dos limites da empresa não tem como fazer esse QoS pelo fato de ser configurado no roteador.

- Veja novamente o item “Etapa 6 - Prática - Como esconder seu endereço real na internet”. Faça o teste de esconder o seu endereço IP (pode ser no computador ou no celular). Você deve capturar a tela com o resultado dos testes **antes e depois de mudar de endereço IP**. Observação: a captura da tela deve capturar a tela toda, inclusive com o horário e data na barra inferior para garantir a autenticidade da captura.

Antes da utilização de uma VPN:

The screenshot shows the MeuIP website interface. The main content area displays the IP address **Meu ip é 189.6.36.148** in orange. Below this, it shows "IP Reverso 189.6.36.148" and "Data 15h30min - 16/03/2021". There are two buttons: "Teste sua Velocidade Internet" (red) and "Veja a Localização" (green). A circular progress indicator is visible below the buttons. The left sidebar contains a list of tools: Calculadora IP, Email Checker, Gerador de Senha, Email Verify, Email Blacklist, Ferramentas de Rede, DNS Report, Medidor de Velocidade, GEO Localizador, Servidores, Switches, Roteadores, Redes sem fio, and Provedores & Cloud. The top navigation bar includes links for Blog, Contate-nos, and Facebook.

Ao utilizar a VPN do Kaspersky:

The screenshot shows the MeuIP website interface after using a VPN. The main content area displays the IP address **Meu ip é 177.54.147.19** in orange. Below this, it shows "IP Reverso 177-54-147-19.cust.hostzone.com.br" and "Data 15h32min - 16/03/2021". There are two buttons: "Teste sua Velocidade Internet" (red) and "Veja a Localização" (green). A circular progress indicator is visible below the buttons. Below the progress indicator, there is a section titled "Seu Histórico de IPs e Provedores" with a table showing the history of IP addresses and providers.

| Dia - Hora | seu IP | Provedor |
|-----------------------|---------------|------------------------------------|
| 16/03/2021 - 15:32:33 | 177.54.147.19 | 177-54-147-19.cust.hostzone.com.br |
| 16/03/2021 - 15:30:05 | 189.6.36.148 | 189.6.36.148 |

- Explique com suas palavras porque o Acordo de Nível de Serviço (SLA) é importante quando se contrata um link de internet, por exemplo.

Está relacionado com a garantia de prestação de serviços e aos níveis de qualidade que devem ser atendidos. É uma garantia para o usuário, empresa e o profissional que presta o serviço de TI, caso haja descumprimento do acordo o contratante ou empresa estarão resguardados, na questão financeira, porém não se faz desnecessário a busca de empresas que prestem serviços de qualidade.