MATERIAL DO ALUNO • TEAMS

# Aula 25 — Monitoramento e Diagnóstico Operacional de Redes Locais

*UC01 • Planejar e executar a instalação de redes locais | Aula 25 de 27 | 3h30 | Turma TR5 | Prof.: Msc Arlindo Batista Xavier Filho*

## Objetivos de aprendizagem

- Diferenciar disponibilidade, latência (RTT), perda de pacotes, erros de interface e funcionamento de serviços.
- Coletar indicadores com ferramentas de observação no Windows, Debian e/ou simulação autorizada.
- Interpretar dados em contexto e distinguir indício, hipótese e causa comprovada.
- Elaborar registro de incidente com horário, fonte, teste, evidência, ação recomendada e reteste.

## 1. Situação-problema: por que a rede está lenta?

Na Escola Horizonte, funcionários relatam lentidão intermitente no acesso ao servidor de arquivos. O equipamento liga e responde a alguns testes, mas isso não comprova estabilidade. O técnico precisa definir o objeto monitorado, criar uma referência inicial e coletar evidências em intervalos controlados, sem sobrecarregar a rede.

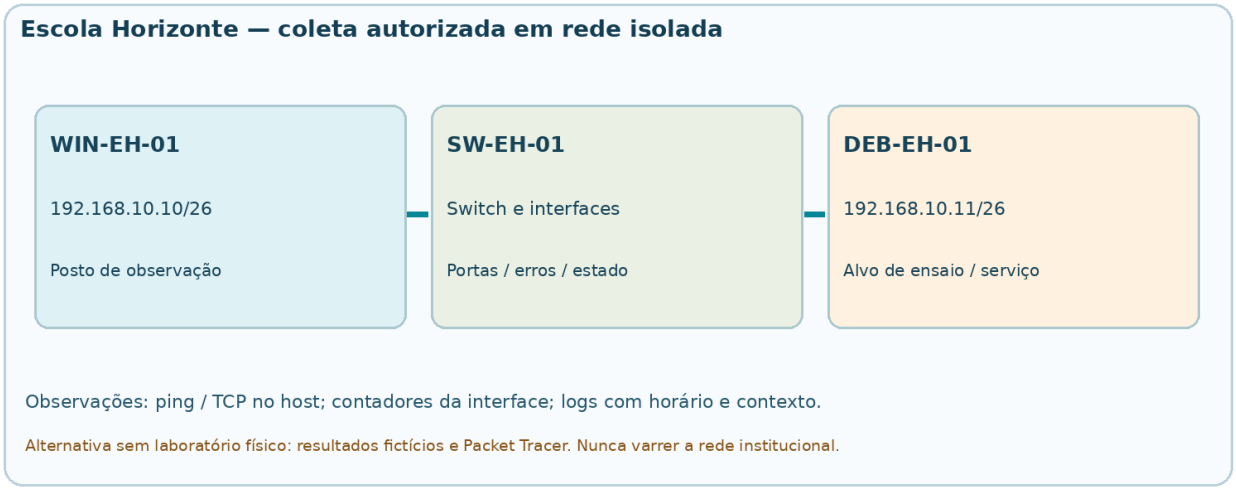



Figura 25.1 — Ambiente didático de coleta. Os endereços são simulados; o gateway e o acesso à Internet não são necessários para o teste entre hosts da mesma /26.

## 2. O que medir, como interpretar

| Indicador | O que revela | Limitação importante |
|---|---|---|
| **Disponibilidade** | Serviço respondeu na janela observada | Amostra curta não comprova uptime mensal. |
| **RTT / latência** | Tempo entre solicitação e resposta | Depende do teste, rota e processamento. |
| **Perda de pacotes** | Solicitações sem resposta na amostra | ICMP pode ser filtrado ou limitado. |
| **Erros de interface** | Contadores de erros e descartes | Precisam de comparação por intervalo. |
| **Porta / serviço** | Conexão TCP estabelecida | Não prova login, autorização nem uso da aplicação. |
| **Eventos / logs** | Alterações e falhas registradas | Horário, origem e contexto importam. |

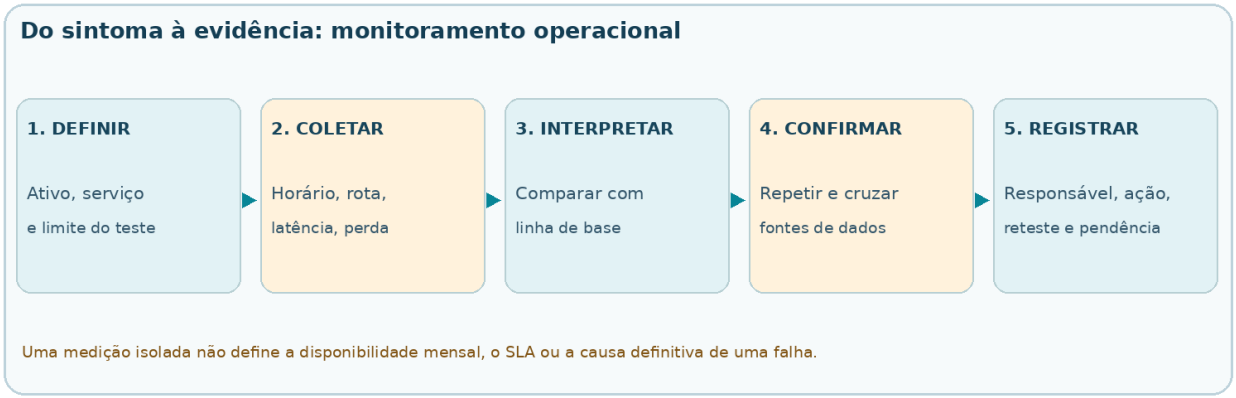



Figura 25.2 — Fluxo profissional: delimitar, coletar, comparar, confirmar e registrar.

## 3. Métricas com dados fictícios

Considere 8 tentativas de ping, 7 respostas e uma ausência de resposta. A perda observada foi 1/8 × 100 = 12,5%. Essa amostra não comprova que o serviço tenha indisponibilidade de 12,5% durante o mês, nem que houve perda de pacotes TCP. Se as respostas apresentarem RTT de 3, 8 e 11 ms, a média desses três valores será aproximadamente 7,3 ms; a medição deve informar quantas respostas foram consideradas.

**Atenção na interpretação** O ping utiliza mensagens ICMP e pode ser bloqueado ou priorizado de forma diferente de tráfego real de aplicação. Ping positivo não garante acesso ao compartilhamento SMB; ping sem resposta não é, por si só, prova de host desligado.

## 4. Comandos de consulta — Windows

```
Get-NetAdapter | Select-Object Name, Status, LinkSpeed
Get-NetAdapterStatistics | Select-Object Name, ReceivedBytes, SentBytes
ipconfig /all
ping -n 8 192.168.10.11
tracert -d 192.168.10.11
Test-NetConnection -ComputerName 192.168.10.11 -Port 445
Get-WinEvent -LogName System -MaxEvents 10
```

O resultado TCP 445 somente é esperado quando o compartilhamento SMB está ativo e acessível na VM autorizada. Se Get-WinEvent não estiver acessível, registre a limitação. Capture o horário e evite registrar dados pessoais.

## 5. Comandos de consulta — Debian

```
date -Is
ip -br link
ip -s link
ip -br address
ip route
ping -c 8 192.168.10.10
ss -lnt
journalctl -b -n 20 --no-pager
```

A leitura de logs pode ser restrita; não aumente privilégios sem autorização. A variação dos contadores de interface entre duas observações é mais informativa do que um número absoluto isolado. O comando ping -c 8 limita a amostra a oito solicitações; não execute monitoramento contínuo indiscriminado.

## 6. Oficina prática — Central de Monitoramento da Escola Horizonte

1. Em dupla, escolha um par Windows/Debian em rede isolada ou use os cartões com dados simulados fornecidos pelo professor.
2. Preencha o inventário: host, endereço, interface, serviço esperado, horário e responsável fictício.

3. Colete duas observações de estado da interface, contadores e ping controlado. Anote número de pacotes transmitidos, respostas, perda e RTT quando disponível.
4. Teste uma porta TCP de um serviço previamente autorizado. Compare resultado TCP com o resultado ICMP.
5. Investigue dois incidentes: um de conectividade/intermitência e outro de serviço ou registro de eventos. Descreva hipóteses alternativas.
6. Proponha ação corretiva que exija o mínimo de alteração. Registre autorização, critérios de aceite e reteste hipotético ou realizado em VM.
7. Entregue o relatório técnico, a ficha de laboratório e uma breve conclusão no Teams.

## 7. Casos para análise

| Código | Evidência fictícia | Investigue antes de concluir |
|---|---|---|
| **M1** | 8 ecos; 7 respostas; RTT variável | Verificar repetição e outras métricas. A causa não está confirmada. |
| **M2** | Interface Up, porém sem rota para outra sub-rede | Conferir prefixo, gateway e topologia. |
| **M3** | Ping ao servidor responde; TCP 445 falha | Verificar serviço SMB, escuta e políticas. |
| **M4** | IP responde; nome arquivos.escolahorizonte.test falha | Verificar servidor DNS, registro e cliente. |
| **M5** | Log indica reinício no horário relatado | Correlacionar tempo, serviço e outras evidências. |

## 8. Entrega e autoavaliação

- Preencha a ficha com dois ciclos de observação, dois incidentes e um plano de reteste.
- Não inclua credenciais, IPs públicos reais, nomes de alunos ou arquivos privados nos registros.
- Avalie sua capacidade de selecionar testes, interpretar números, justificar hipóteses e documentar resultados.

## Referências técnicas


MICROSOFT. Test-NetConnection (NetTCPIP). Disponível em: https://learn.microsoft.com/en-us/powershell/module/nettcpip/test-netconnection. Acesso em: 31 out. 2026.

MICROSOFT. Get-NetAdapterStatistics (NetAdapter). Disponível em: https://learn.microsoft.com/en-us/powershell/module/netadapter/get-netadapterstatistics. Acesso em: 31 out. 2026.

MICROSOFT. Get-WinEvent (Microsoft.PowerShell.Diagnostics). Disponível em: https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.diagnostics/get-winevent. Acesso em: 31 out. 2026.

DEBIAN. iproute2: ip-link(8) e ss(8). Disponível em: https://manpages.debian.org/. Acesso em: 31 out. 2026.

FREEDESKTOP. journalctl(1) — systemd. Disponível em: https://www.freedesktop.org/software/systemd/man/latest/journalctl.html. Acesso em: 31 out. 2026.

IETF. RFC 7276 — An Overview of Operations, Administration, and Maintenance Tools. Disponível em: https://www.rfc-editor.org/rfc/rfc7276. Acesso em: 31 out. 2026.