Aula 08 | Monitoramento e diagnóstico WLAN

Da observação do sintoma ao teste de correção e ao relatório técnico

IDENTIFICAÇÃO	INFORMAÇÕES
Unidade curricular	UC09 — Planejar e implementar a segurança em redes sem fio
Turma / encontro	TSC03 · Aula 08 de 09 · 4 horas (240 minutos)
Material	Material do aluno · conteúdo, laboratório e evidências
Professor	Msc Arlindo Batista Xavier Filho

1. Situação-problema: Centro Horizonte

Após a segmentação da Aula 07, a WLAN do Centro Horizonte apresenta chamados de suporte: visitantes sem IP válido, falhas de associação, clientes na sub-rede errada e possível quebra da política de acesso ao servidor corporativo. Sua equipe deve atuar como suporte técnico, sem desmontar as configurações que funcionam.

Questão norteadora: como provar a causa de uma falha sem concluir, precipitadamente, que o problema está no Wi-Fi?

Objetivos e indicadores da UC09

- Identificar os níveis do diagnóstico: rádio/associação, autenticação, endereçamento, VLAN/trunk, roteamento/ACL e serviço.
- Coletar evidências com comandos e interfaces disponíveis no Cisco Packet Tracer, distinguindo simulação de medição real.
- Aplicar uma alteração de cada vez, testar novamente e registrar o resultado.
- Produzir relatório de incidente e matriz de aceitação para a Aula 09.

A atividade produz evidências principalmente para o indicador 4 (diagnóstico do funcionamento e conectividade) e retoma os indicadores 1, 2 e 3 (planejamento, interligação e configuração).

Organização do encontro — 240 minutos

MOMENTO	TEMPO	AÇÃO
Acolhimento e retomada	20 min	Relembrar topologia e estabelecer linha de base.
Diagnóstico por camadas	40 min	Relacionar sintomas, hipóteses, testes e ferramentas.
Laboratório guiado	90 min	Conferir a rede e diagnosticar quatro falhas controladas.
Desafio de suporte	70 min	Analisar incidentes e propor solução com evidências.
Síntese e registro	20 min	Quiz, relatório e preparação do projeto final.

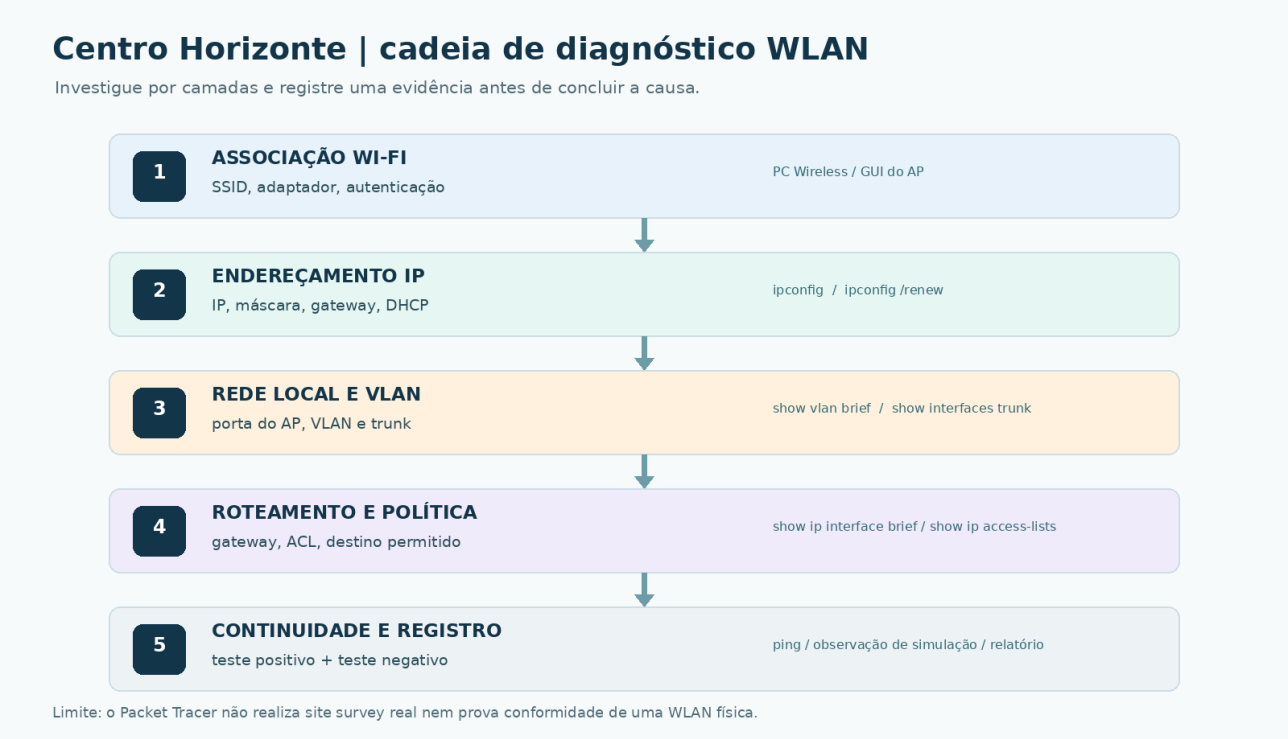
2. O que significa monitorar uma WLAN?

Monitoramento reúne observações contínuas ou periódicas que permitem perceber alterações de funcionamento, segurança e uso. Diagnóstico é a investigação de uma ocorrência: identifica um sintoma, testa hipóteses, encontra a causa provável e confirma a correção. Monitoramento não equivale, por si só, a auditoria completa ou detecção de todas as ameaças [1].

INDICADOR	PERGUNTA TÉCNICA	ONDE VERIFICAR
Associação / autenticação	Cliente encontra o SSID e associa?	PC Wireless e GUI Wireless do AP.
IP e gateway	Recebeu IP da VLAN esperada?	ipconfig; pools e bindings no R1.
Camada 2	AP está na VLAN correta?	show vlan brief e show interfaces trunk no SW1.
Roteamento e controle	Tráfego permitido/negado segue a política?	ping, ACL e interface de aplicação.

Radiofrequência real	Há baixa cobertura ou interferência?	Survey e ferramentas reais; não inferir pelo Packet Tracer.

3. Método: observar → hipotetizar → testar → corrigir → retestar



Importante: um ping que falhou não comprova a causa. Antes, verifique a associação, o endereço, o gateway e um teste positivo de referência. A configuração de ACL deve ser confrontada com o sentido de aplicação e a origem do teste.

4. Laboratório guiado no Packet Tracer — 90 minutos

Topologia herdada da Aula 07: SW1-2960 conectado ao roteador R1 por trunk, VLAN 10 corporativa (192.168.50.0/24), VLAN 20 visitantes (192.168.60.0/24), servidor em 192.168.50.10, AP1 e AP2 simplificados em portas access separadas. DHCP no R1; DHCP dos equipamentos wireless desativado; conexão ao switch pela porta LAN dos WRT300N. Nomes de interfaces podem variar por modelo.

Etapa A — preparar a linha de base (20 min)

1. Abra uma cópia do .pkt da Aula 07 e salve como TSC03_UC09_A08_EquipeXX.pkt.
2. Registre VLANs, portas, faixas IP e identificação dos dois SSIDs. Nunca inclua senhas reais nos relatórios.
3. Teste: corp → servidor 192.168.50.10 (deve funcionar); visitante → gateway 192.168.60.1 (deve funcionar); visitante → servidor (deve ser bloqueado).
4. Registre pelo menos um print da configuração e os resultados positivos e negativos.

Etapa B — comandos de diagnóstico (25 min)

```
Cliente (Desktop > Command Prompt):
ipconfig
ipconfig /renew
ping 192.168.60.1
ping 192.168.50.10

SW1 (CLI):
show vlan brief
show interfaces trunk
show interfaces fa0/3 switchport

R1 (CLI):
show ip interface brief
show ip dhcp binding
show ip dhcp pool
show ip access-lists
show ip interface gigabitEthernet0/0.20
```

No WRT300N, utilize as abas GUI/Config/Status oferecidas pela versão do simulador. Salve as alterações com Save Settings. Alguns comandos de switch/roteador podem variar ou não estar implementados no modelo escolhido.

Etapa C — diagnóstico de falhas controladas (45 min)

CASO	SINTOMA	SEU PRIMEIRO TESTE
C01	Cliente visitante sem endereço DHCP	DHCP / VLAN / caminho até servidor DHCP
C02	Cliente não se associa ao Wi-Fi	Autenticação / credencial
C03	Visitante obtém IP da rede corporativa	Porta access / VLAN incorreta
C04	Visitante chega ao servidor interno	ACL / local ou sentido de aplicação

O docente prepara as falhas ou fornece capturas/dados fictícios. Para cada caso: (1) registre o sintoma, (2) levante duas hipóteses, (3) selecione o teste, (4) aplique uma única correção em ambiente autorizado e (5) repita o teste de aceitação.

5. Desafio aplicado: central de suporte (70 minutos)

Cinco chamados foram registrados. Os casos C01–C04 podem ser reproduzidos na simulação; C05 contém valores sintéticos de radiofrequência para análise em papel. A equipe deve priorizar os riscos e justificar a ordem de atendimento.

ID	EVIDÊNCIA FORNECIDA	QUESTÃO A INVESTIGAR
C01	169.254.12.8; SSID associado; gateway vazio	DHCP / VLAN / caminho até servidor DHCP
C02	SSID visível; senha incompatível no cliente	Autenticação / credencial
C03	192.168.50.103 em vez de 192.168.60.x	Porta access / VLAN incorreta
C04	Ping a 192.168.50.10 responde; gateway 60.1 alcançável	ACL / local ou sentido de aplicação
C05	Dados fornecidos: RSSI -82 dBm; ruído -93 dBm; SNR 11 dB	Cobertura / interferência — estudo fictício

C05: RSSI = -82 dBm e ruído = -93 dBm; SNR = 11 dB (diferença em dB). Esses valores são dados de exercício, NÃO medições realizadas pelo Packet Tracer nem limites universais de aceitação. Uma decisão real depende da aplicação, equipamentos, taxa, canais e survey.

Matriz de testes e aceitação — WLAN Centro Horizonte

ORIGEM	DESTINO	RESULTADO-ALVO	EVIDÊNCIA
Visitante VLAN 20	Gateway 192.168.60.1	**Permitido**	IP + ping
Visitante VLAN 20	Servidor 192.168.50.10	**Bloqueado**	ping + ACL
Corporativo VLAN 10	Servidor 192.168.50.10	**Permitido**	ping + IP
Visitante VLAN 20	Outro visitante	**Não garantido**	Requer isolamento no AP
Equipamento de Wi-Fi	DHCP servidor R1	**Deve funcionar**	binding DHCP + IP
Cliente Wi-Fi	SSID e autenticação	**Associado**	GUI / PC Wireless

Teste bloqueado isolado NÃO comprova ACL: combine conectividade de referência, configuração e reteste.

6. Ficha para evidências e entrega

CAMPO	REGISTRO DA EQUIPE
ID do chamado / prioridade	_____
Sintoma e cenário inicial	_____
Hipótese e teste selecionado	_____

Resultado e evidência coletada	_____
Correção executada e justificativa	_____
Reteste / situação final	_____
Risco residual / pendência	_____

Entrega no Teams: arquivo .pkt gerado pela equipe, relatório de um incidente com evidências, matriz dos cinco chamados, linha de base dos testes e lista de pendências para a Aula 09. Sem senhas reais, dados pessoais ou imagens de redes de terceiros.

7. Autoavaliação e preparação da Aula 09

- Expliquei por que falha de ping, isoladamente, não determina uma causa?
- Consegui diferenciar problema de associação, DHCP, VLAN e ACL?
- Produzi evidência antes e depois da correção?
- Quais testes ainda precisam ser completados no projeto final?

8. Oficina de registro: um exemplo analisado

Exemplo C03 — A equipe observou que o notebook de visitantes recebeu 192.168.50.103. A hipótese inicial foi associação do AP2 à VLAN corporativa; o técnico verificou no SW1 a configuração da Fa0/3, confirmou VLAN 10 e corrigiu apenas essa porta para VLAN 20. Após renovar DHCP, o cliente recebeu endereço 192.168.60.x. O registro só é considerado concluído após confirmar acesso ao gateway 60.1 e bloqueio ao servidor 50.10, mantendo o tráfego corporativo permitido.

9. Checklist de passagem para a Aula 09

EVIDÊNCIA A CONSOLIDAR	SITUAÇÃO
Topologia e endereços finais	[ ] Confirmada [ ] Pendente
AP corporativo e de visitantes	[ ] Confirmada [ ] Pendente
DHCP por VLAN	[ ] Confirmada [ ] Pendente
Regra de isolamento aplicada	[ ] Confirmada [ ] Pendente
Testes permitidos / negados	[ ] Confirmada [ ] Pendente
Riscos residuais e limitações	[ ] Documentados [ ] Pendentes
Relatório e arquivo .pkt identificados	[ ] Concluídos [ ] Pendentes

Pense: quais resultados são demonstráveis no simulador e quais exigem um access point real, uma ferramenta de survey ou um controlador corporativo? Essa distinção será parte da defesa do projeto final.

Referências técnicas e aprofundamento

[1] NIST. Guidelines for Securing Wireless Local Area Networks (WLANs). SP 800-153. 2012. Disponível em: https://csrc.nist.gov/pubs/sp/800/153/final. Acesso em: 1 nov. 2026.

[2] CISCO. Packet Tracer: WRT300N GUI — configurações, Status e rede sem fio. Disponível em: https://tutorials.ptnetacad.net/help/default/GUI_wrt300n.htm. Acesso em: 1 nov. 2026.

[3] CISCO NETWORKING ACADEMY. Referência didática de verificação de VLANs: show vlan brief e interfaces. Disponível em: https://community.cisco.com/kxiwq67737/attachments/kxiwq67737/writ_brtkb-board/46/1/CCNA_WRIT_SWRE_Mo%CC%81dulo_1%20ao%2016.pdf. Acesso em: 1 nov. 2026.