TÉCNICO EM SEGURANÇA CIBERNÉTICA · PLANO DE CURSO 316

Aula 06 | Autenticação e criptografia Wi-Fi

WPA2, WPA3, SAE, 802.1X e decisões para uma WLAN corporativa segura

UNIDADE CURRICULAR	UC09 — Segurança em redes sem fio
TURMA / AULA	TSC03 · Aula 06 de 09 · 240 minutos

Situação-problema do Centro Horizonte

A WLAN corporativa do Centro Horizonte já funciona na simulação da Aula 05. A equipe de TI deverá agora decidir como controlar a entrada de funcionários, visitantes e dispositivos legados sem confundir conectividade com segurança. O cliente solicita um parecer técnico que considere desempenho, compatibilidade, riscos e necessidade de isolamento.

Questão norteadora: uma rede aceita uma senha e permite ping. Isso é evidência suficiente de que está segura? Justifique.

Ao final deste encontro, você deverá ser capaz de

- Comparar WEP, WPA, WPA2 e WPA3 e reconhecer modos inadequados para novas implantações.
- Explicar a diferença entre credencial compartilhada (PSK/SAE) e autenticação empresarial (802.1X/EAP/RADIUS).
- Configurar e testar WPA2-Personal/AES no Packet Tracer, documentando uma tentativa de associação inválida em ambiente autorizado.
- Propor uma política de WLAN corporativa, convidados e dispositivos legados com justificativa e plano de migração.
- Produzir evidências de segurança sem compartilhar senhas de produção ou dados pessoais.

Roteiro do encontro (240 minutos)

Momento	Tempo	Evidência
1. Acolhimento e problema	20 min	Matriz inicial de riscos
2. Conceitos e demonstração	40 min	Comparação PSK/SAE/802.1X
3. Laboratório Packet Tracer	90 min	Arquivo .pkt e verificações
4. Desafio de arquitetura	70 min	Parecer técnico argumentado
5. Quiz e síntese	20 min	Registro de aprendizagem

1 | Quais mecanismos protegem uma WLAN?

Segurança wireless envolve autenticação (quem entra), criptografia (proteção dos dados no enlace), proteção de quadros de gerenciamento quando aplicável e controles de rede (o que o cliente pode acessar). Um único SSID ou uma senha longa não substituem essas camadas.

Modo	Situação atual e orientação didática
WEP / WPA original	Legados e inseguros; não adotar em novos projetos. TKIP também deve ser evitado.
WPA2-Personal (PSK)	Compartilha uma senha entre usuários; usar AES/CCMP, senha longa e acesso restrito quando WPA3 não for viável.
WPA3-Personal (SAE)	Autenticação baseada em SAE, mais resistente a ataques passivos de dicionário; compatibilidade de AP e clientes é requisito.
WPA2/3-Enterprise	Autenticação individual por 802.1X/EAP com servidor

	RADIUS; preferir métodos e validação de certificados adequados.
Aberta / Enhanced Open (OWE)	Rede aberta comum não autentica nem cifra o enlace; OWE cifra o tráfego por cliente, mas não comprova identidade.



Figura 1 — O Wi-Fi exige uma combinação de controles; esquema conceitual.

2 | Personal não é Enterprise

Em WPA2-Personal, vários clientes conhecem uma mesma senha. Quando a senha precisa ser revogada para um colaborador, a mudança pode afetar toda a equipe. O WPA3-Personal utiliza SAE, melhorando o processo de autenticação, mas não oferece por si só identidade e permissão individual por funcionário.

Em uma WLAN Enterprise, o equipamento do usuário atua como supplicant; o AP/controladora é o autenticador; e o servidor de autenticação geralmente usa RADIUS como transporte das decisões. A identidade pode ser baseada em credenciais individuais ou certificados, conforme o método EAP selecionado. A validação do certificado do servidor é essencial para reduzir riscos de redes falsas.

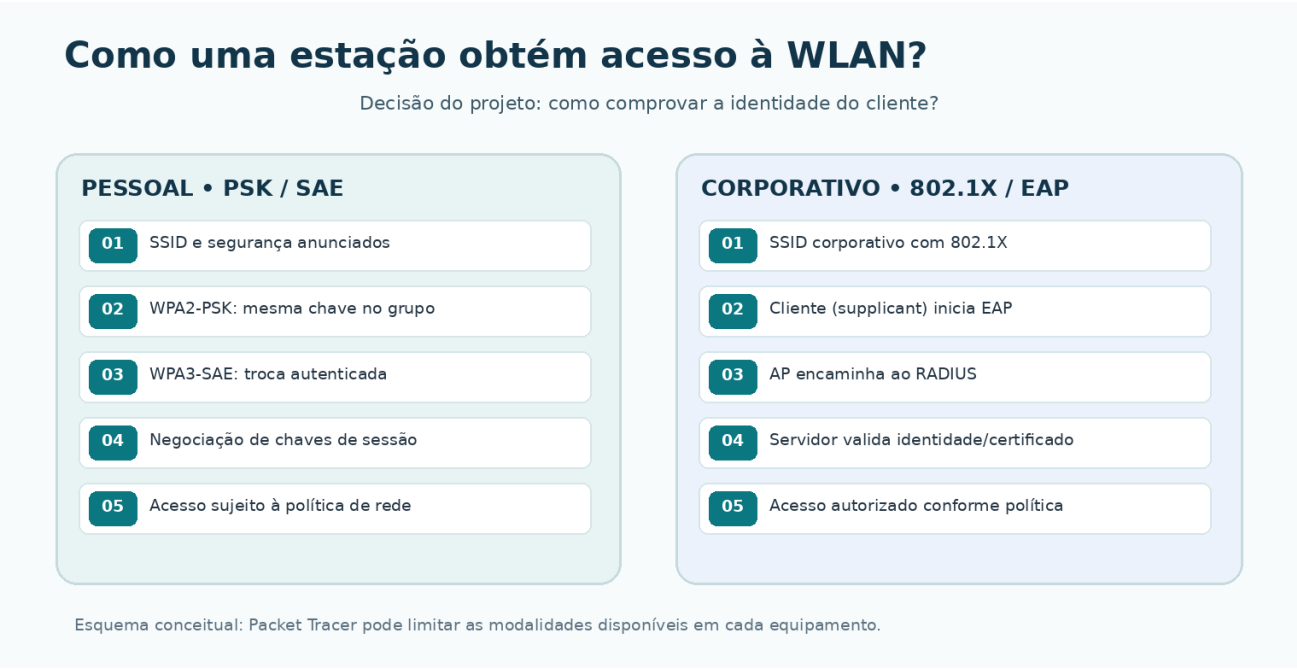


Figura 2 — Fluxo didático de autenticação pessoal e corporativa.

3 | PMF, WPS e modo de transição

- PMF (Protected Management Frames): protege determinados quadros robustos de gerenciamento; não significa que todo quadro de gerenciamento seja protegido. É exigido em WPA3 somente e nas operações de 6 GHz compatíveis.
- Modo de transição WPA2/WPA3: facilita coexistência de clientes antigos, mas preserva caminhos WPA2 e riscos associados. Defina prazo de retirada do legado.
- WPS: recomenda-se desabilitar, especialmente em redes corporativas, por ampliar a superfície de risco.
- SSID oculto e filtragem MAC: não substituem autenticação forte, segmentação e atualizações.

4 | Laboratório orientado — Packet Tracer (90 min)

Utilize o arquivo .pkt criado na Aula 05 ou refaça a topologia: R1 → switch → porta LAN do WRT300N, dois notebooks Wi-Fi e um PC cabeado. R1 = 192.168.50.1/24; AP = 192.168.50.2; DHCP no R1. O endereço e a senha abaixo são fictícios.

Item	Valor do laboratório
SSID	Horizonte-Lab
Segurança simulada	WPA2 Personal + AES (se disponível)
Senha temporária de treinamento	TSC03-Horizonte-2026!
Gateway/DHCP	192.168.50.1 · R1
AP simplificado	192.168.50.2 · DHCP desabilitado; porta LAN

1. 0–10 min | Abra uma cópia do .pkt da Aula 05 e salve como TSC03_UC09_A06_EquipeXX.pkt. Registre o estado inicial dos clientes.
2. 10–30 min | No WRT300N, use GUI → Wireless → Wireless Security (ou equivalente). Selecione WPA2 Personal e AES; configure a senha didática. Salve e confira SSID.
3. 30–45 min | Configure o Notebook A com a senha correta e obtenha IP via DHCP. Registre associação, ipconfig e ping para 192.168.50.1.
4. 45–60 min | No Notebook B, use intencionalmente uma senha incorreta e observe o erro. Não capture tráfego de terceiros nem realize desautenticação. Corrija e reteste.
5. 60–75 min | Verifique senha administrativa do AP, WPS (se existir), gerenciamento remoto e necessidade de atualização. Documente campos ausentes no modelo simulado.
6. 75–90 min | Salve o .pkt e colete evidências de configuração, falha controlada, correção e conectividade final.

Limite da ferramenta: a GUI e as opções variam conforme modelo e versão do Packet Tracer. Não apresentar WPA3/SAE/802.1X como configurados se o equipamento simulado não expuser essas opções. O exercício demonstra parâmetros e conectividade, não mede resistência criptográfica real.

Checklist de laboratório

[ ] .pkt original preservado e cópia identificada

[ ] WPA2 Personal/AES documentado com senha exclusivamente fictícia

[ ] Cliente A autenticado, recebeu IP e alcançou gateway

[ ] Falha de credencial do cliente B observada sem acesso indevido

[ ] Correção do cliente B e reteste registrados

[ ] Limitações da simulação descritas

5 | Desafio aplicado (70 min): arquiteto por um dia

A empresa possui 45 colaboradores, 25 visitantes diários e 12 dispositivos legados. Defina três perfis de acesso e proponha medidas para cada um. Não confunda a escolha do SSID com uma implementação comprovada de VLAN: o WRT300N básico pode não suportar todas as funções corporativas.

Perfil	Proposta de autenticação	Acesso autorizado
Funcionários	_____	_____
Visitantes	_____	_____
Legados/IoT	_____	_____

Sua equipe deverá registrar: (a) escolha do método e justificativa; (b) compatibilidade de clientes; (c) duas contramedidas adicionais; (d) quais configurações foram simuladas; (e) quais exigem equipamentos reais; (f) cronograma para retirada de WPA2/legados, se aplicável.

6 | Perguntas para reflexão e síntese (20 min)

7. Qual o ganho e o limite do WPA3-SAE diante de uma senha compartilhada?
8. O que muda ao usar 802.1X/EAP com RADIUS em vez de PSK?
9. Por que ocultar o SSID e filtrar MAC não constituem proteção suficiente?
10. Quais evidências comprovam o correto funcionamento do laboratório e quais não comprovam segurança real?

Evidências para entrega no Teams

- TSC03_UC09_A06_EquipeXX.pkt e três capturas comentadas.
- Relatório de testes (estado inicial → falha controlada → correção → reteste).
- Matriz de decisão da WLAN (funcionários, convidados e legados).
- Ressalva sobre limitações da simulação e próximos testes em campo.

Referências e fontes de aprofundamento

[1] CISCO NETWORKING ACADEMY. Packet Tracer - Configure Wireless Security (material didático). 2018. Disponível em: https://contenthub.netacad.com/legacy/I2IoT/2.0/en/course/files/5.1.2.6%20Packet%20Tracer%20-%20Configure%20Wireless%20Security.pdf. Acesso em: 1 nov. 2026.

[2] 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.

[3] CISCO. WPA3 Deployment Guide. Guia técnico. Disponível em: https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/technical-reference/wpa3-dg.pdf. Acesso em: 1 nov. 2026.

[4] HPE ARUBA NETWORKING. WPA3-Personal: transition mode. Documentação técnica. Disponível em: https://arubanetworking.hpe.com/techdocs/aos/wifi-design-deploy/security/modes/wpa3-personal/. Acesso em: 1 nov. 2026.