PROJETO TSC03 / CURSO TÉCNICO EM SEGURANÇA CIBERNÉTICA

Aula 01 — Fundamentos das Redes sem Fio e Segurança WLAN

Do conceito de WLAN ao primeiro laboratório de conexão protegida no Cisco Packet Tracer.

MATERIAL DO ALUNO

IDENTIFICAÇÃO	INFORMAÇÕES
Unidade curricular	UC09 — Planejar e implementar a segurança em redes sem fio
Carga horária	36 horas | Aula 01 de 09 | Encontro de 4 horas (240 minutos)
Turma	TSC03
Professor	Msc Arlindo Batista Xavier Filho
Referência curricular	Plano de Curso Senac SP nº 316; Plano de Orientação para Oferta (PO)
Material	Edição de trabalho • outubro de 2026

Seu desafio da unidade curricular

Uma empresa de serviços denominada Centro Horizonte possui rede cabeada e deseja oferecer conexão Wi-Fi aos colaboradores e visitantes. A gestão teme exposição de informações e interrupções da operação. Sua equipe deverá planejar, configurar, testar e documentar uma rede sem fio segura ao longo da UC09. Nesta primeira aula, será construído e validado um protótipo de laboratório com autenticação.

Limite do laboratório Todas as redes, credenciais e endereços aqui apresentados são fictícios. Utilize exclusivamente o Cisco Packet Tracer ou equipamentos autorizados. Não realize testes em redes reais de terceiros.

O que você deverá conseguir fazer

- Explicar o funcionamento básico de uma WLAN e sua relação com a rede cabeada.
- Reconhecer as funções de access point, roteador wireless, interface de rede, SSID, canal e cliente.
- Distinguir WPAN, WLAN, WMAN e WWAN e diferenciar autenticação, criptografia e controle de acesso.
- Identificar riscos básicos de implantação e justificar escolhas iniciais de segurança.
- Montar uma WLAN simples no Packet Tracer, estabelecer conectividade e registrar evidências.

Roteiro dos 240 minutos

MOMENTO	TEMPO	ATIVIDADE
1. Acolhimento e contexto	20 min	Situação-problema, diagnóstico e critérios de sucesso.
2. Construção conceitual	40 min	Fundamentos wireless, equipamentos e ameaças.
3. Experimentação orientada	90 min	Laboratório no Packet Tracer e testes controlados.
4. Desafio aplicado	70 min	Plano inicial de WLAN para o Centro Horizonte.
5. Síntese e evidências	20 min	Quiz, relatório de aprendizado e entrega.

Os momentos podem ser redistribuídos conforme o ritmo da turma, sem alterar a carga total de 240 minutos. Intervalos institucionais devem seguir a orientação da unidade.

1. Redes sem fio: o que realmente muda?

Em uma rede cabeada, os dispositivos trocam quadros principalmente por um meio físico guiado, como cabos Ethernet. Em uma rede local sem fio, estações e pontos de acesso utilizam ondas de rádio. O Wi-Fi facilita mobilidade e expansão, mas exige cuidados com cobertura, interferência, autenticação e exposição do meio de transmissão.

O access point (AP) fornece acesso à WLAN e normalmente a conecta a uma rede de distribuição cabeada. Um roteador wireless doméstico pode reunir, em um mesmo equipamento, funções de AP, switch, roteador, NAT e servidor DHCP. Essas funções não são sinônimas; sua integração depende do modelo.

1.1 Vocabulário de operação

TERMO	SIGNIFICADO PRÁTICO
WLAN	Rede local sem fio; utiliza a família IEEE 802.11 em equipamentos Wi-Fi.
SSID	Identificador lógico da rede; é seu nome anunciado ou configurado.
BSSID	Identificador da célula de rádio, geralmente associado à interface do AP; não é o mesmo que SSID.
AP	Ponto de acesso que conecta clientes wireless ao ambiente de rede.
Cliente / STA	Dispositivo que se associa à infraestrutura wireless.
Canal	Parte do espectro de radiofrequências usada na comunicação.
DHCP	Serviço que pode fornecer IP, máscara, gateway e DNS aos clientes.
Gateway	Encaminha tráfego para outras redes; conexão Wi-Fi não significa acesso à Internet.
RSSI / SNR	Indicadores distintos: nível de sinal recebido / razão

	entre sinal e ruído.

1.2 Quatro escalas de comunicação

TIPO	ALCANCE / EXEMPLO	ATENÇÃO
WPAN	Dispositivos pessoais; Bluetooth entre periféricos.	Não confundir Bluetooth com WLAN Wi-Fi.
WLAN	Ambiente local; APs em residência ou escritório.	Principal foco da UC09.
WMAN	Abrangência metropolitana; soluções de acesso regional.	Não pressupõe uso de Wi-Fi doméstico.
WWAN	Rede celular de ampla abrangência.	Opera com tecnologias e modelos de serviço diferentes.

2. Segurança wireless começa no planejamento

Uma WLAN não é segura apenas porque “tem senha”. Segurança depende do conjunto: configuração de autenticação, criptografia adequada, atualização de firmware, senhas administrativas exclusivas, controle de acesso, segmentação, disponibilidade, documentação e monitoramento. A preocupação acompanha todo o ciclo da WLAN, desde o projeto até a manutenção.

2.1 Autenticação, confidencialidade e autorização

- Autenticação: verifica se o cliente pode ingressar na rede (por exemplo, por chave compartilhada ou credenciais corporativas).
- Criptografia: protege o tráfego de rádio contra leitura indevida conforme o protocolo e sua configuração.
- Autorização e segmentação: limitam os recursos que um cliente autenticado pode alcançar; acesso ao Wi-Fi não deve significar acesso irrestrito à LAN.
- Disponibilidade: depende de cobertura adequada, gerenciamento de canais, capacidade dos equipamentos e resposta a falhas.

2.2 Protocolos de proteção

TECNOLOGIA	USO DIDÁTICO / SITUAÇÃO
Aberta (sem proteção)	Não recomendada para a rede corporativa; presença de SSID não demonstra segurança.
WEP	Obsoleto e inseguro; estudar apenas como antecedente histórico.
WPA / TKIP	Legado; não adotar em implantação nova.
WPA2-Personal / AES	Proteção por senha compartilhada; utilizada no exercício do simulador.
WPA3-Personal / SAE	Alternativa atual quando suportada por AP e clientes; aprofundamento em aula futura.
WPA2/WPA3-Enterprise	Modelo empresarial com autenticação individual, normalmente associado a 802.1X/RADIUS; conteúdo

	posterior.

Importante O Cisco Packet Tracer pode oferecer apenas parte dos recursos dos equipamentos atuais. Nesta aula, a configuração prática usará WPA2-Personal/AES no equipamento WRT300N, quando disponível. WPA3 será abordado conceitualmente; não simularemos uma função inexistente.

2.3 Ameaças iniciais e medidas correspondentes

RISCO	MEDIDA DEFENSIVA INICIAL
Rede aberta ou senha previsível	Configurar proteção apropriada e senha forte e exclusiva.
AP não autorizado / rede de nome semelhante	Inventariar APs, orientar usuários e conferir identificação das redes.
Configuração administrativa padrão	Trocar senha de administração e desabilitar recursos desnecessários.
Visitantes alcançando sistemas internos	Planejar SSID e segmentação de convidados em etapas posteriores.
Cobertura inadequada / interferência	Realizar estudo básico de cobertura e testes; não presumir que mais potência resolve.

3. Laboratório guiado — sua primeira WLAN protegida

Duração de referência: 90 minutos. Execute somente em ambiente simulado. Este protótipo utiliza um roteador sem fio com DHCP integrado, duas estações Wi-Fi e uma estação cabeada. Não representa ainda a arquitetura corporativa completa do Centro Horizonte.

3.1 Inventário e endereçamento

ITEM	PARÂMETRO DE LABORATÓRIO
Simulador	Cisco Packet Tracer (versão disponível no laboratório).
Equipamentos	1 WRT300N (ou equivalente), 2 Laptop-PT com interface wireless e 1 PC-PT.
Cabo	Copper Straight-Through entre PC0 e uma porta LAN/Ethernet do WRT300N.
SSID	TSC03-LAB
Proteção	WPA2-Personal / AES, se a interface disponibilizar.
Senha de demonstração	TSC03-Lab-2026!WiFi (apenas rede simulada; nunca reutilizar em produção).
Rede IPv4	192.168.50.0/24
Gateway/LAN do roteador	192.168.50.1
DHCP	Habilitado; pool a partir de 192.168.50.100 (conforme campos disponíveis).

Esquema lógico: [Laptop0]))) [WRT300N] ((([Laptop1] | [WRT300N] ---- Ethernet ---- [PC0].

3.2 Etapas de montagem

1. Abra o Packet Tracer. Em Network Devices > Wireless Devices, insira um roteador WRT300N ou equivalente. Inclua Laptop0, Laptop1 e PC0.
2. Conecte PC0 a uma porta Ethernet/LAN do roteador usando cabo Copper Straight-Through. Não utilize a porta Internet/WAN para este teste local.
3. Verifique se Laptop0 e Laptop1 têm interfaces sem fio. Se necessário, na guia Physical desligue o laptop, substitua a interface pelo módulo WPC300N compatível e religue o dispositivo.
4. No roteador, abra GUI > Setup/Basic Setup (os nomes variam por versão). Defina endereço LAN 192.168.50.1 e máscara 255.255.255.0; ative o servidor DHCP e, se disponível, configure o início do pool em 192.168.50.100. Salve.
5. Abra GUI > Wireless/Basic Wireless Settings. Altere o SSID para TSC03-LAB. Salve as configurações.
6. Abra Wireless/Wireless Security, escolha WPA2 Personal, AES se houver essa opção, e configure a senha temporária da tabela. Salve.
7. Nos laptops, abra Desktop > PC Wireless ou Config > Wireless, conforme a interface existente. Selecione TSC03-LAB, forneça a chave correta e conecte.
8. Abra Desktop > IP Configuration nos três computadores e selecione DHCP. Se a associação ou a atribuição não ocorrer, verifique primeiro a configuração WLAN, depois o DHCP.
9. No Command Prompt de cada cliente, execute ipconfig. Depois execute ping 192.168.50.1; registre os resultados. Entre dois clientes, realize ping ao IP obtido, se permitido pela configuração do simulador.
10. Salve seu arquivo como TSC03_UC09_A01_EquipeXX.pkt e anote configurações, testes e ocorrências em uma tabela de evidências.

3.3 Testes e interpretação

TESTE	ESPERADO	SE FALHAR, INVESTIGUE
SSID aparece ou pode ser selecionado	Cliente identifica a WLAN.	Interface wireless, SSID configurado e estado do rádio.
Autenticação da estação	Associação com senha correta.	Modo de segurança e chave digitada.
ipconfig	Endereço 192.168.50.x/24, sem duplicidade.	DHCP ativo, associação e pool configurado.
ping 192.168.50.1	Resposta do gateway LAN.	IP, rádio, conectividade e firewall de simulação.
Acesso à Internet	Não exigido nesta aula.	O cenário não contém enlace WAN nem serviço externo.

Dica de diagnóstico Um cliente com endereço 169.254.x.x indica que não obteve configuração IPv4 via DHCP. Isso não prova, sozinho, que a senha Wi-Fi está incorreta: verifique associação, DHCP e enlace.

3.4 Registro de evidências do laboratório

EVIDÊNCIA	REGISTRO DO GRUPO
Nome da equipe / integrantes	_____
Arquivo .pkt	_____
SSID, proteção e gateway	_____
IP obtido por Laptop0	_____
IP obtido por Laptop1	_____
IP obtido por PC0	_____
Resultado do ping ao gateway	_____
Falha encontrada e correção	_____

4. Desafio aplicado — o Centro Horizonte

Duração: 70 minutos. Em grupos, discutam a demanda do cliente e construam um plano inicial de expansão, sem realizar testes de intrusão. O protótipo da etapa anterior demonstrou uma conexão protegida, mas a empresa precisará de decisões adicionais de arquitetura e gestão.

4.1 Briefing do cliente

O Centro Horizonte possui uma recepção e três salas de atendimento. Há 12 computadores ligados à rede cabeada, oito colaboradores com notebooks e até 15 visitantes simultâneos. A empresa mantém arquivos administrativos sensíveis na LAN. Deseja Wi-Fi confiável para colaboradores e acesso de visitantes à Internet, sem permitir que convidados atinjam sistemas internos. A planta, a distância entre salas e os obstáculos ainda serão levantados.

4.2 Entregáveis da equipe

1. Liste pelo menos seis perguntas técnicas antes de escolher equipamentos: usuários simultâneos, planta, paredes, alimentação, Internet, política de acesso etc.
2. Desenhe um diagrama lógico inicial distinguindo rede cabeada, acesso de colaboradores e acesso de visitantes. Indique quais conexões ainda são apenas propostas.
3. Elabore uma tabela contendo cinco riscos e uma medida defensiva ou verificação para cada um.
4. Defina critérios mínimos de aceite: autenticação, IP válido, comunicação autorizada, isolamento de visitantes (a verificar nas próximas aulas) e documentação.
5. Explique em até oito linhas por que o sucesso de um ping não comprova a segurança completa de uma WLAN.
6. Produza uma síntese de uma página com as decisões, as pendências e a evidência técnica já coletada.

4.3 Matriz preliminar de riscos

RISCO IDENTIFICADO	PROBABILIDADE/IMPACTO	CONTROLE SUGERIDO
_____	_____	_____
_____	_____	_____

_____	_____	_____
_____	_____	_____
_____	_____	_____

4.4 Perguntas para discussão

- Por que duas redes que compartilham o mesmo meio físico podem precisar de regras lógicas diferentes?
- O que mudaria se a empresa autorizasse apenas WPA3, mas seu simulador não oferecesse essa opção?
- Por que esconder o SSID ou restringir MAC não substitui autenticação e criptografia?
- Como distinguir uma falha de rádio de uma falha de DHCP, de roteamento ou de acesso a sistemas?

5. Síntese e avaliação formativa

Tempo: 20 minutos. Individualmente, registre respostas breves às perguntas abaixo. Depois, em equipe, revise o arquivo .pkt e a ficha do cenário.

1. Qual a diferença entre um access point e um roteador wireless multifunção?
2. Defina SSID e explique por que seu nome não é uma credencial de autenticação.
3. Cite uma ameaça e duas medidas de proteção adequadas para o contexto empresarial.
4. Explique a diferença entre estar associado ao Wi-Fi e ter acesso a um serviço da rede.
5. O que você verificaria em um cliente que recebe IP 169.254.12.5?

Critérios de evidência nesta aula

CRITÉRIO	EVIDÊNCIA OBSERVÁVEL
Conceitos e análise de risco	Respostas técnicas e justificativa das escolhas.
Protótipo e configuração	Arquivo .pkt salvo, SSID e proteção configurados.
Diagnóstico inicial	Capturas ou registros de ipconfig e ping com interpretação.
Comunicação e documentação	Plano preliminar e relato de pendências.

Entregue no Teams

- Arquivo de simulação: TSC03_UC09_A01_EquipeXX.pkt.
- Ficha de evidências e análise do cenário, preferencialmente em PDF.
- Identificação da equipe e síntese individual de aprendizado.

Continuidade Na Aula 02, o projeto será aprofundado com padrões IEEE 802.11, bandas de frequência e escolha de tecnologias para a implantação.

Referências e aprofundamento

- SENAC SÃO PAULO. Plano de Curso nº 316: Técnico em Segurança Cibernética. 2023. Seção UC09.
- SENAC SÃO PAULO. Plano de Orientação para Oferta: Técnico em Segurança Cibernética. 2023. Seção UC09.
- NIST. Guidelines for Securing Wireless Local Area Networks (WLANs). SP 800-153. 2012. https://doi.org/10.6028/NIST.SP.800-153
- CISCO NETWORKING ACADEMY. Packet Tracer — Configure Wireless Security. Atividade de simulação. https://contenthub.netacad.com/legacy/I2IoT/2.0/en/course/files/5.1.2.6%20Packet%20Tracer%20-%20Configure%20Wireless%20Security.pdf

Ficha individual de revisão e continuidade

Use este espaço para identificar sua evolução técnica e planejar a próxima aula. Esta ficha pode ser impressa ou preenchida no arquivo editável.

PERGUNTA DE REFLEXÃO	SEU REGISTRO
Qual foi a etapa mais difícil do laboratório?	_____
Que evidência demonstra conectividade local?	_____
Que risco a equipe não conseguiu controlar hoje?	_____
Qual decisão depende da medição de cobertura?	_____
O que pretendo investigar na Aula 02?	_____