Universidade Federal do ABC
Segurança de Redes

PARTE A – Análise de quadros IEEE 802.11 com Wireshark

Faça o download do arquivo de trace disponível no site da disciplina e use o Wireshark para analisar as informações.

1 – Selecione um pacote de **dados** e responda:

Qual o padrão utilizado (IEEE 802.11b, a, g, etc), frequência, taxa de dados e RSSI (*Received Signal Strength Indication*)?
Qual o BSSID, endereço de origem e endereço de destino? O que significam estes campos?
Frame check sequence: o pacote foi recebido corretamente?
Mecanismo de segurança: Identifique o flag que indica se o pacote está protegido ou não e qual mecanismo é utilizado (WEP, WPA).
Quais os parâmetros do mecanismo de segurança identificado? O que eles significam?

2 – Selecione um pacote do tipo **beacon** e responda:

Flag indicando se o pacote é protegido ou não. Qual o valor do bit?
Qual o SSID da rede?
Qual o intervalo em que são enviados os quadros beacon pelos APs (*Access Points*)?
Qual o endereço de destino do quadro?
Quais modos de segurança o AP suporta?

PARTE B – Packet tracer

1) Monte a rede conforme a figura e configure os equipamentos da rede.

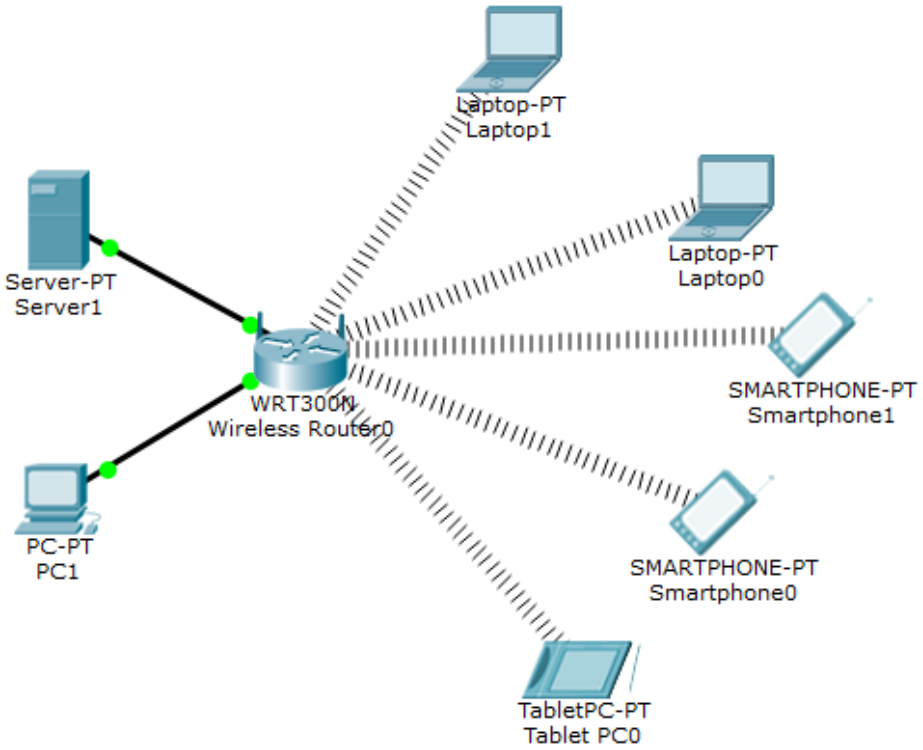
SSID: UFABC
Modo de segurança: WPA-2 PSK
Senha: escolha uma senha
Desabilite o broadcast de SSID no roteador sem fio
Habilite filtragem por endereço MAC no roteador e insira os endereços dos dispositivos permitidos
Endereços IP: estático ou por DHCP (habilite o servidor DHCP no roteador)
Verifique a conectividade da rede.

2) Configuração do firewall no servidor:

Habilite o serviço HTTP no servidor. Acesse a página pelos dispositivos da rede sem fio (laptops, tablet e smartphone) pelo Web Browser disponível na aba Desktop.

Configure regras no servidor para permitir acesso a página Web apenas dos laptops, bloqueando o acesso aos smartphones e tablets.
É preciso habilitar o firewall do servidor (*Desktop->Firewall*) e criar regras de permissão e negação de acesso.
Obs: na configuração do firewall é preciso inserir a "*wildcard mask*" (máscara curinga).
Ex: para uma regra referente à rede 192.168.1.0 a *wildcard mask* é 0.0.0.255. Para uma regra referente a um host específico (ex: 172.16.1.3) a *wildcard mask* é 0.0.0.0.

Teste a rede para ver se as configurações do firewall estão funcionando corretamente.



PARTE C – Políticas de segurança para redes sem fio

Veja os seguintes *templates* de política de segurança:

Wireless Communication Policy
Wireless Communication Standard

(estão disponíveis em https://www.sans.org/security-resources/policies)

1 – Qual o objetivo da política de segurança sem fio e do padrão de comunicação sem fio? Você acha que estas políticas são adequadas para serem aplicadas aos usuários da rede sem fio da UFABC?

2 – A política para redes sem fio se aplica a todos que utilizem uma rede sem fio da empresa. Segundo esta política, quais medidas a empresa pode tomar para verificar a conformidade com a política? Quais as medidas para um empregado que viole a política de segurança? Você alteraria algo neste item (Conformidade – *Policy Compliance*)?

3 – Quais os protocolos de autenticação permitidos pelos requisitos gerais do *Wireless Communication Standard*? E métodos de criptografia?

4 – O que é o SSID? Quais os requisitos dos dispositivos sem fio em relação ao SSID? O que significa desabilitar o broadcast de SSID?

5 – Por que nos requisitos de dispositivos sem fio "domésticos" de infraestrutura é permitido o método de autenticação WPA-PSK?