

Aprendendo Wireless via Programação

Introdução a Redes de Computadores
prof. Ricardo Fabbri



2 de Dezembro de 2014



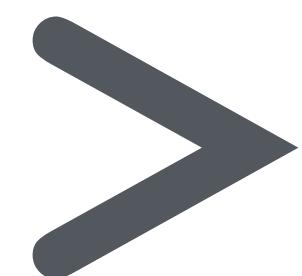
> Objetivos destas Aulas

- Aprender sobre Wifi através de programação voltada à segurança
- Consolidar conceitos de redes e programação
- Python como ferramenta prática para programação em redes
 - A ser usada junto à programação de redes em C vista nas últimas aulas
 - Python: facilita construir apps mais alto nível e complexas
- Fornecer alguma ajuda para trabalho sobre Botnets

> Direto ao ponto

- Vamos já começar com programação para ataques
- Ao longo dos ataques a teoria sobre Wifi será aprendida, sob demanda
- Linux é *o* OS mais poderoso para Wifi hacking!
 - Linux é feature-rich.. bate BSD nisto, de longe
 - Kernel: facilmente alterável para conter filtros, etc.
 - Sistema: ferramental sem fim..
 - Kali / backtrack facilita estas mudanças, mas qualquer linux serve

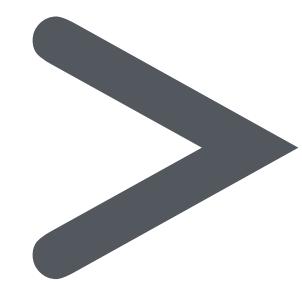




Wifi Sniffing

- `tcpdump`, `libpcap`, etc.. não muda
- Basta colocar no modo de monitoramento

```
root@linux# airmon-ng start wlan0
```

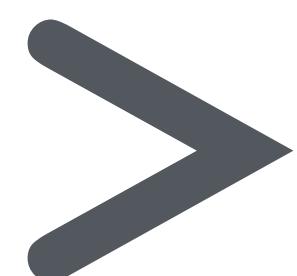


Wifi Sniffing

- **python 1-test-sniff.py**
- **python 2-creditSniff.py**
- **python sniffhidden.py**

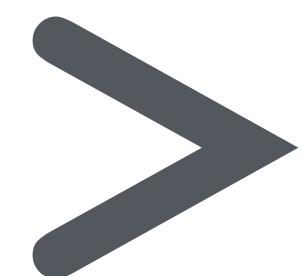
> Bluetooth IEEE 802.15.1

- Bluetooth - muito bom no livro **Violent Python**
- **btfind.py**
- **ver o resto**



Teoria

- 802.11: 802 = LAN , 11 = working group (wifi)
- 802.15 Bluetooth - PAN
- 802.16 Broadband wireless
- 802.11 LAN wireless



802.11x

- 802.11a 54Mbps@5GHz , nao ficou popular
- 802.11b 11MBps@2.4GHz , mais comum
 - WEP: ~dias para quebrar
- 802.11g melhoria no 11b, ficando mais comum
- 802.11i 11b mais seguro
- 802.11n 100Mbps , compativel com 11g e 11b

> Wifi 802.11

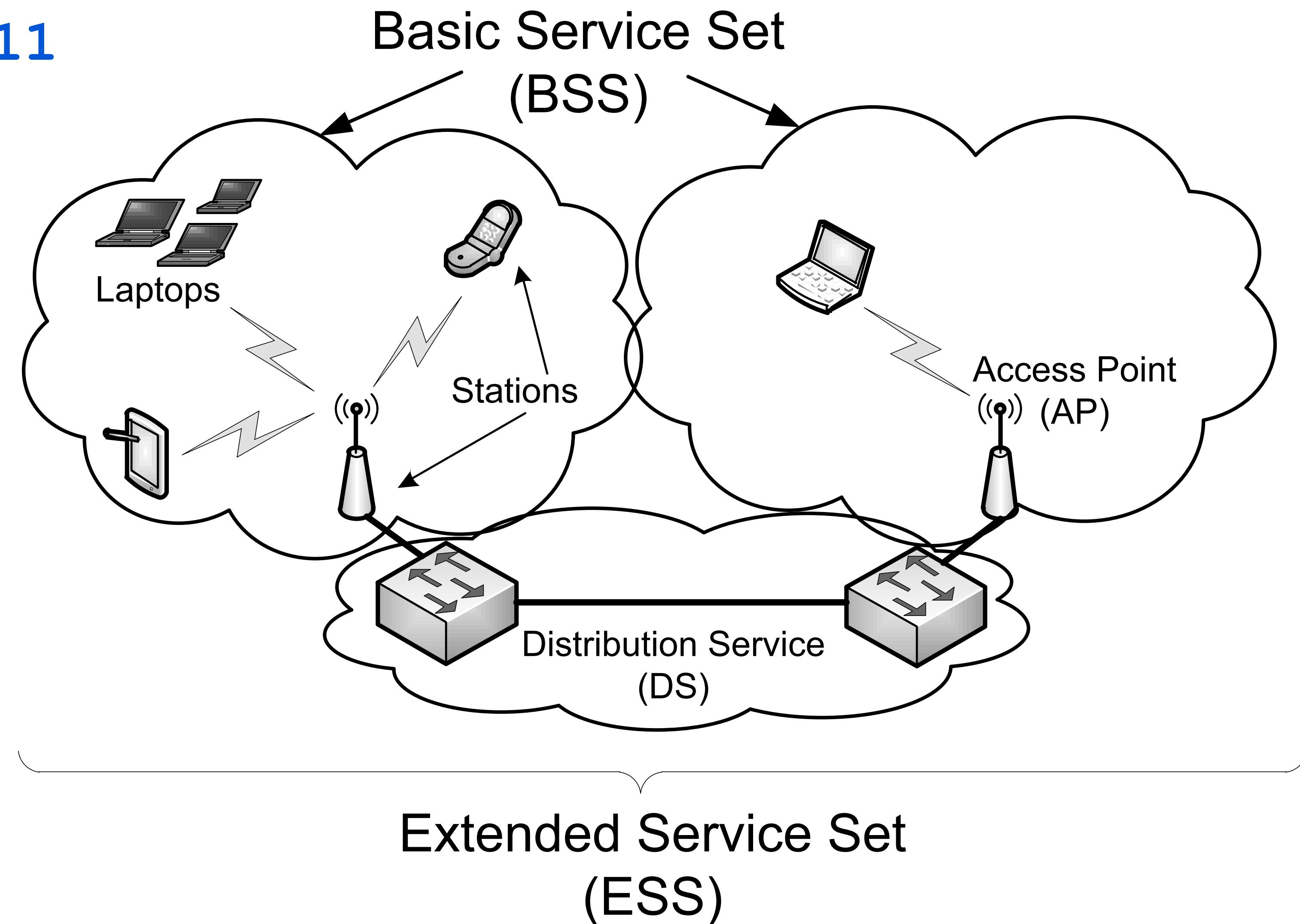
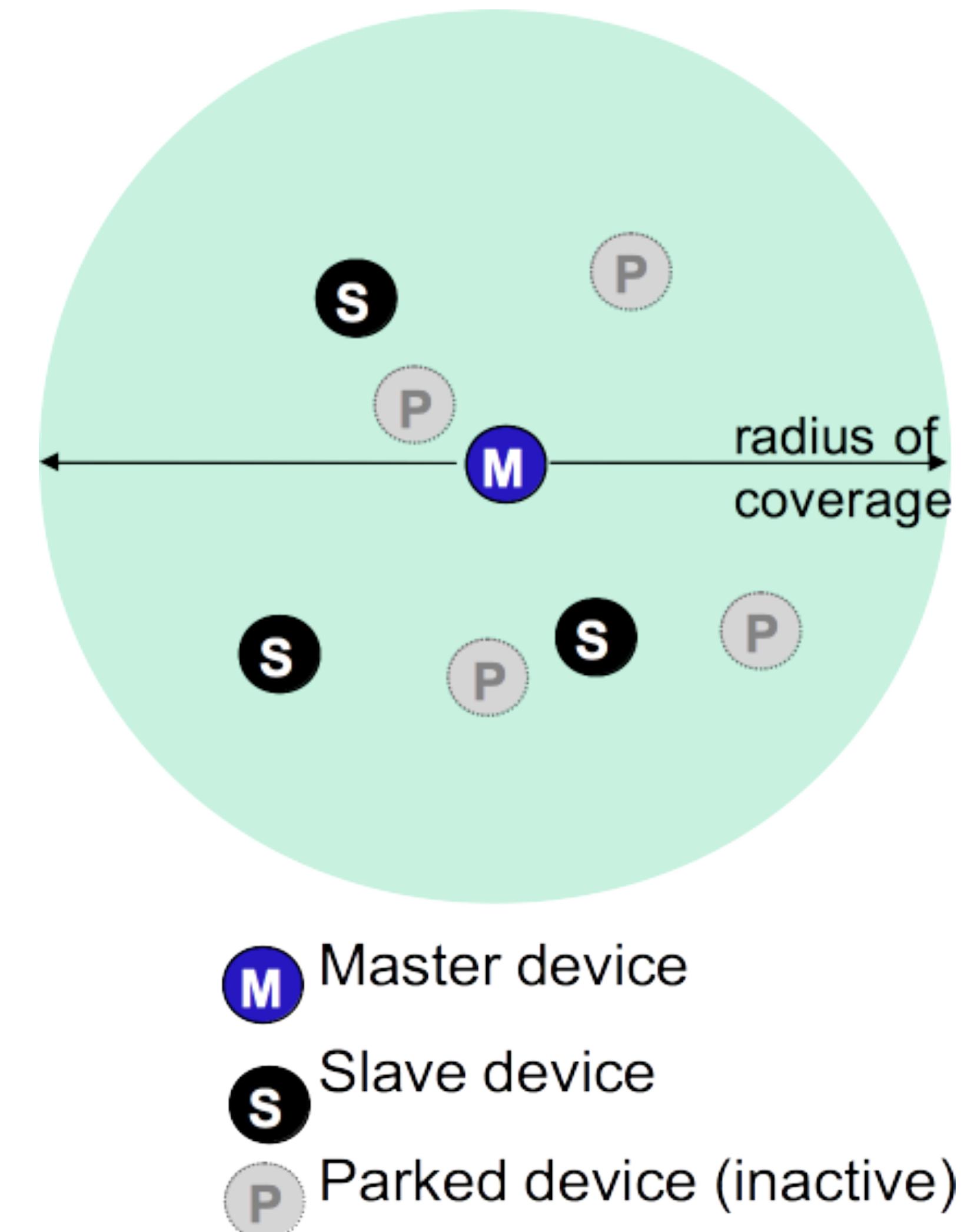


Figure 3-17 The IEEE 802.11 terminology for a wireless LAN. Access points (APs) can be connected using a distribution service (DS, a wireless or wired backbone) to form an extended WLAN (called an ESS). Stations include both APs and mobile devices communicating together that form a basic service set (BSS). Typically, an ESS has an assigned ESSID that functions as a name for the network.

> Bluetooth IEEE 802.15.1

- menos 10m diâmetro
- substitui cabo de pequenos dispositivos
- ad hoc: no infrastructure
- master/slaves:
 - slaves request permission to send (to master)
 - master grants requests



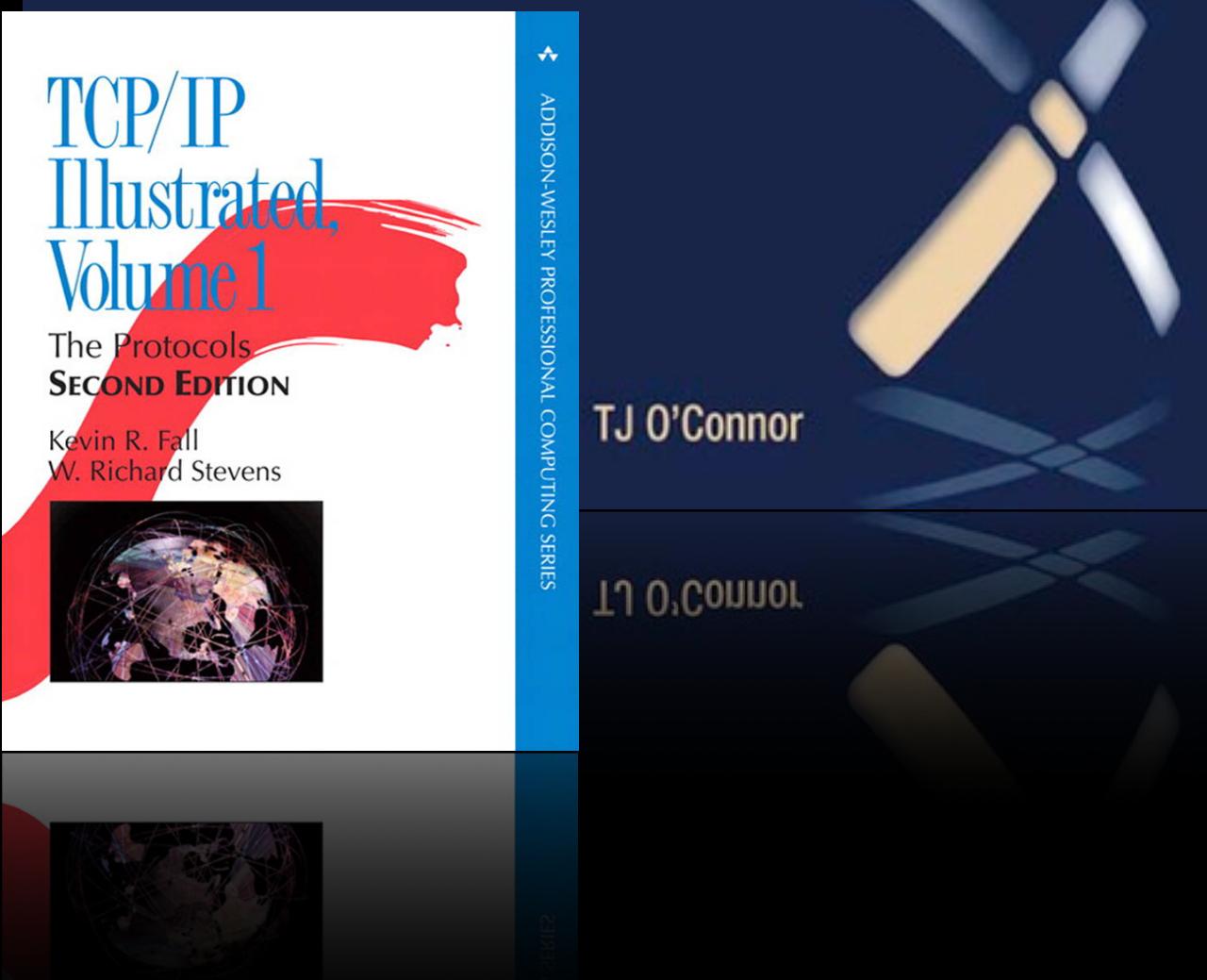
Bibliografia

O objetivo aqui foi estudar WiFi sob o ponto de vista de programação. Estudar:

VIOLENT PYTHON

A Cookbook for Hackers, Forensic Analysts,
Penetration Testers, and Security Engineers

Violent Python
cap 5 (principal)



TCP/IP Illustrated
Sec. 3.5 (funcionamento)

(comandos não são exigidos na P2 mas ajudam no entendimento e poderão valer ponto extra na prova)

>> Ver biblioteca no UERJ.tk
wiki.nosdigitais.teia.org.br/RC