Wireless Systems Security

EE/NiS/TM-584-A/WS

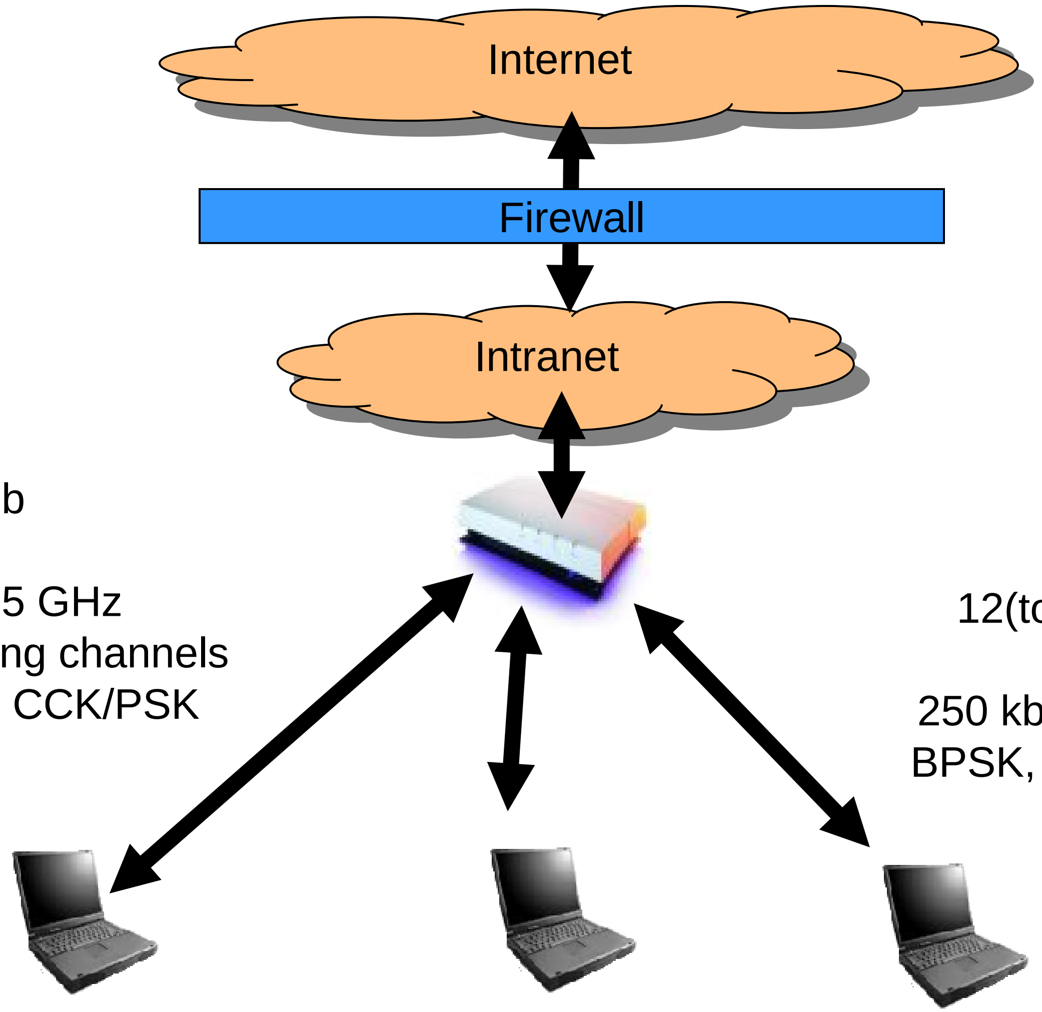
Bruce McNair

bmcnair@stevens.edu

Week 10

Case Study 6

Case 6 – Wireless LANs
802.11a, b, g



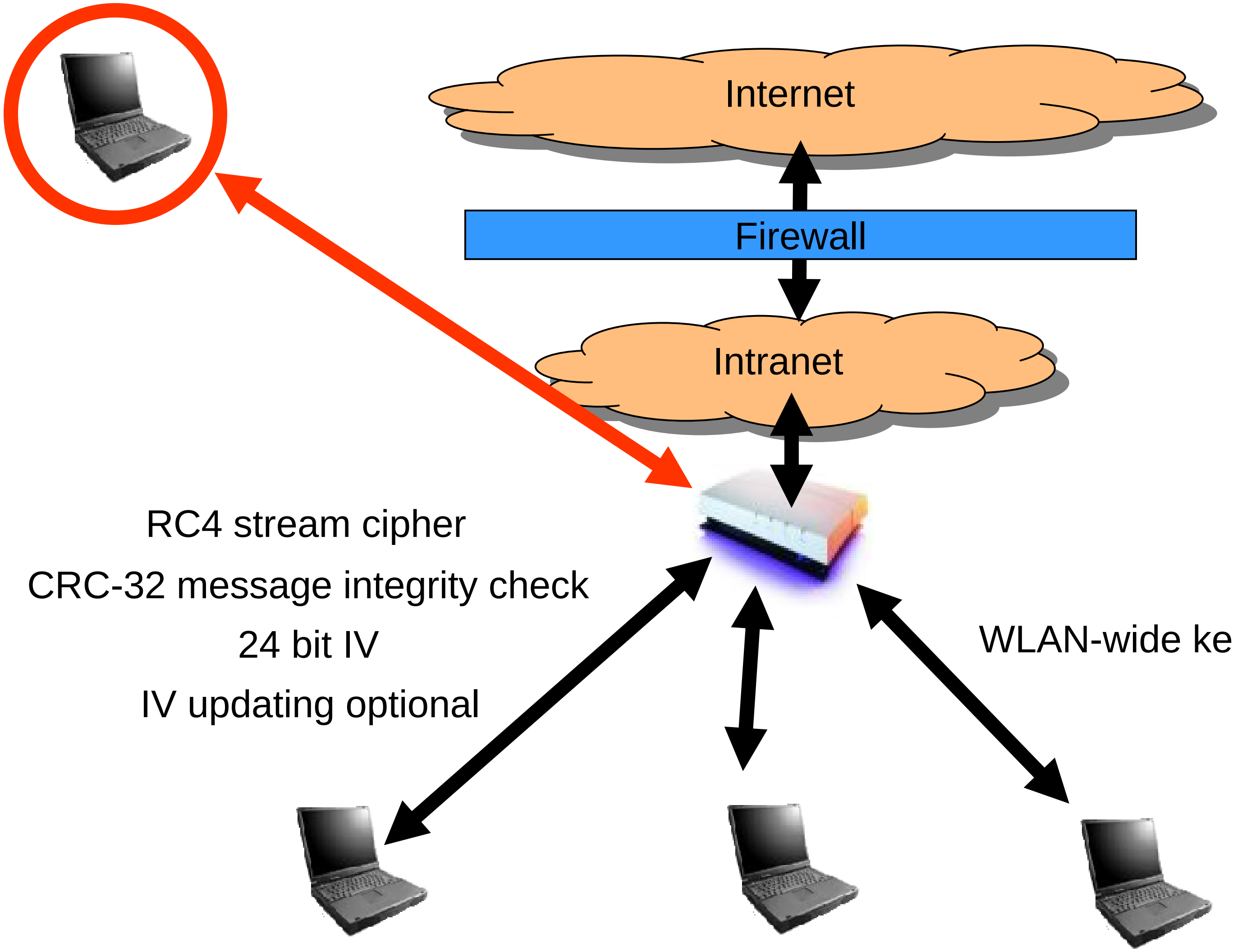
802.11b

2.400-2.4835 GHz
11 TDD overlapping channels
11 Mc/s DS-SS, CCK/PSK

802.11a

5.15-5.35 GHz,
5.725-5.825 GHz
12(to 20) non-overlapping
TDD channels
250 kbaud OFDM (52 carriers)
BPSK, QPSK, 16QAM, 64QAM
on each carrier

Case 6 – Wireless LANs 802.11a, b, g



RC4 stream cipher

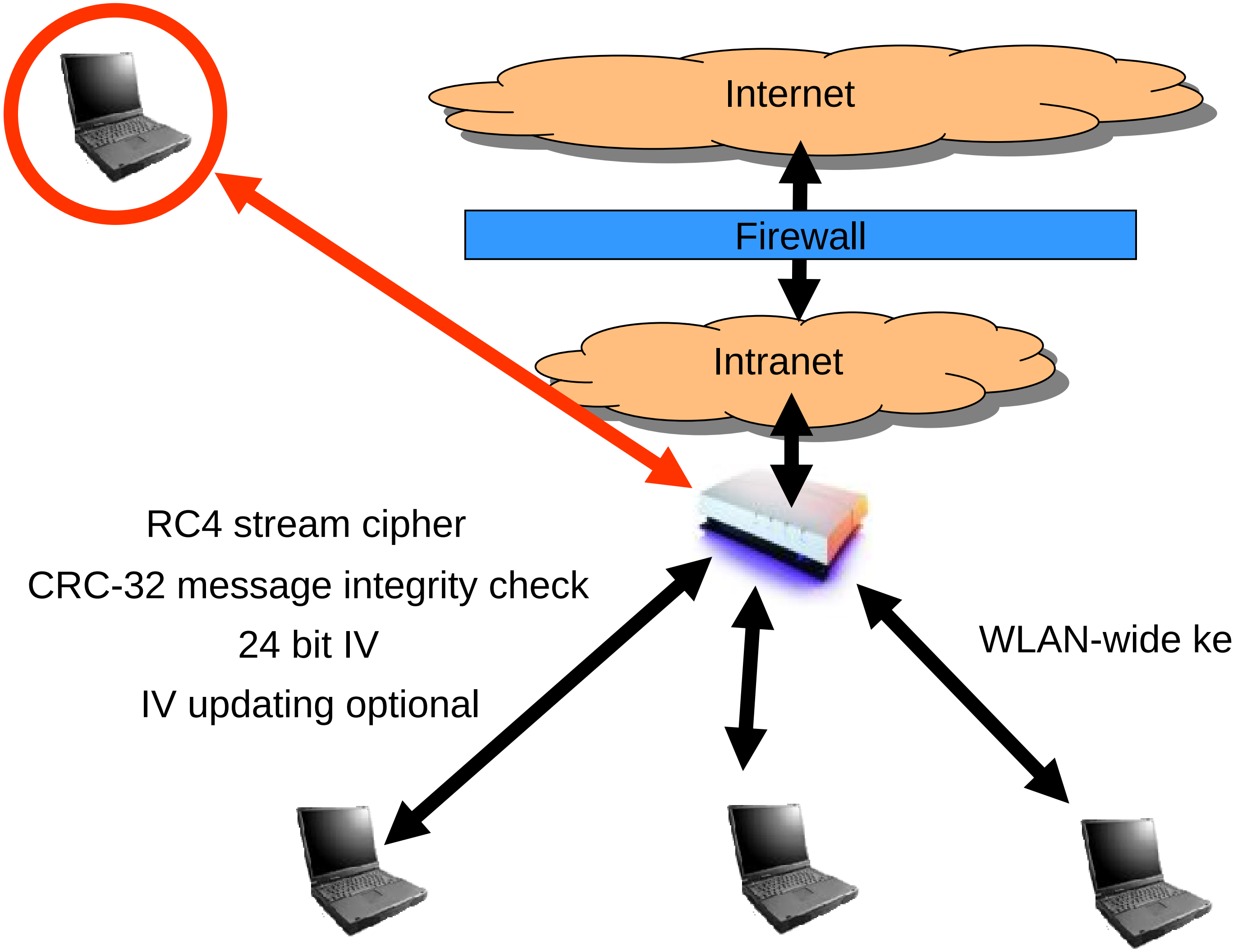
CRC-32 message integrity check

24 bit IV

IV updating optional

WLAN-wide key variable

Case 6 – Wireless LANs
802.11a, b, g



RC4 stream cipher

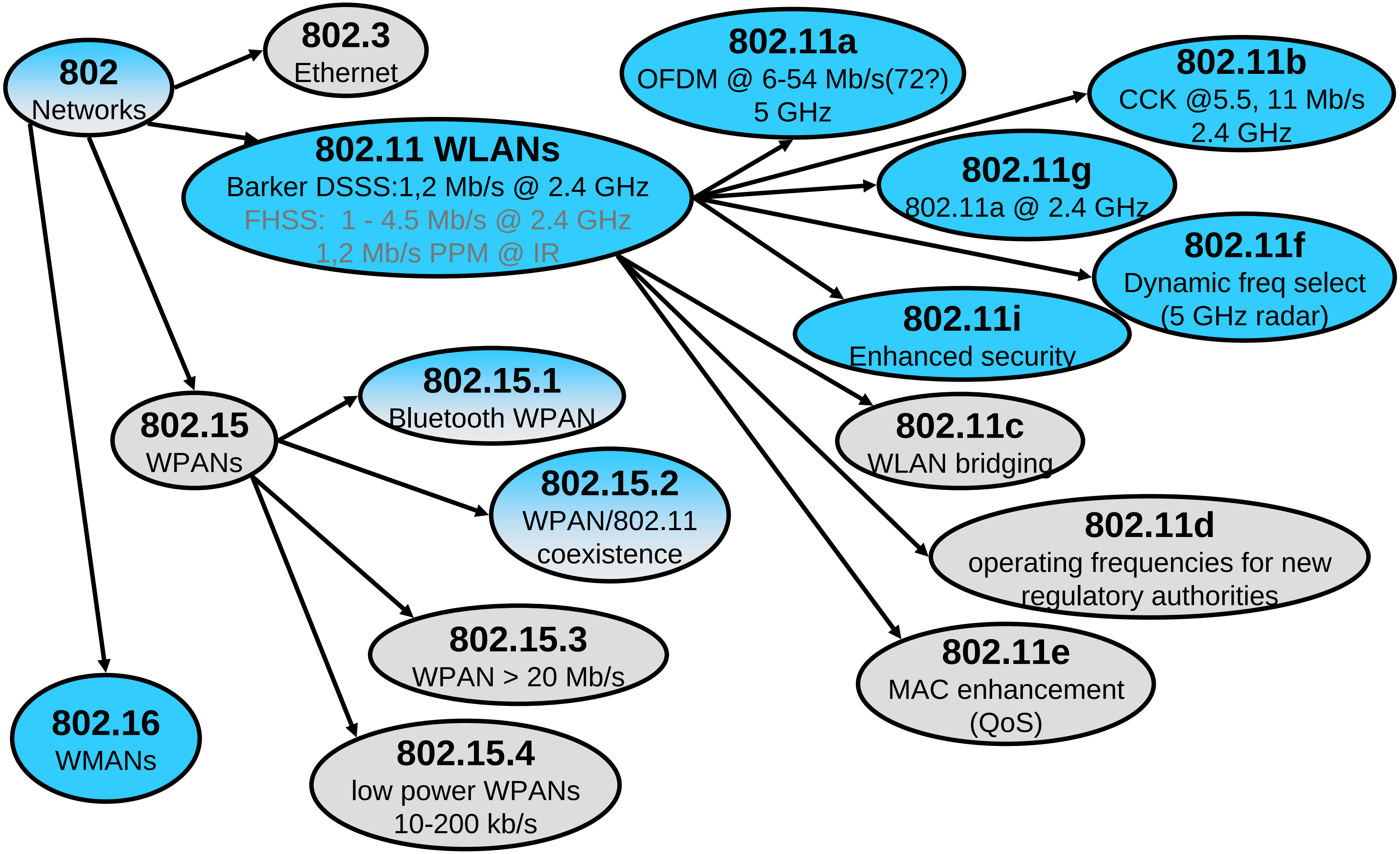
CRC-32 message integrity check

24 bit IV

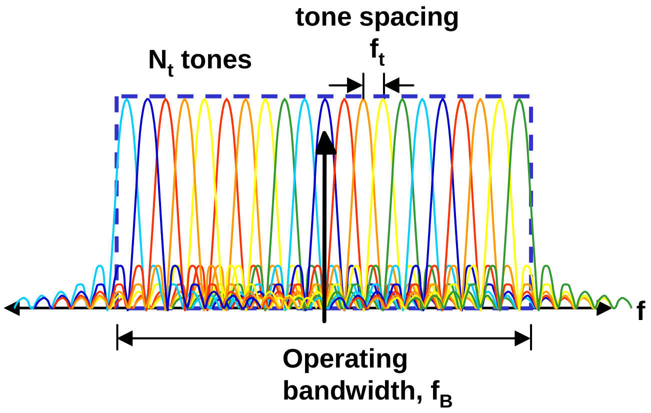
IV updating optional

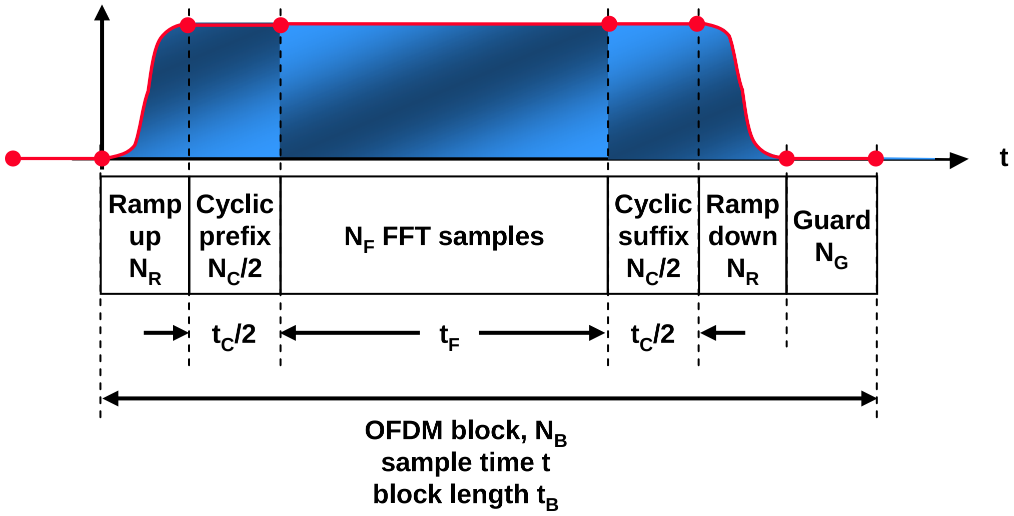
WLAN-wide key variable

IEEE 802 Standards (Alphabet Soup)



OFDM Basics





Ramp up N_R	Cyclic prefix $N_C/2$	N_F FFT samples	Cyclic suffix $N_C/2$	Ramp down N_R	Guard N_G

OFDM block, N_B
sample time t
block length t_B

Total bandwidth $f_B = N_t f_t$

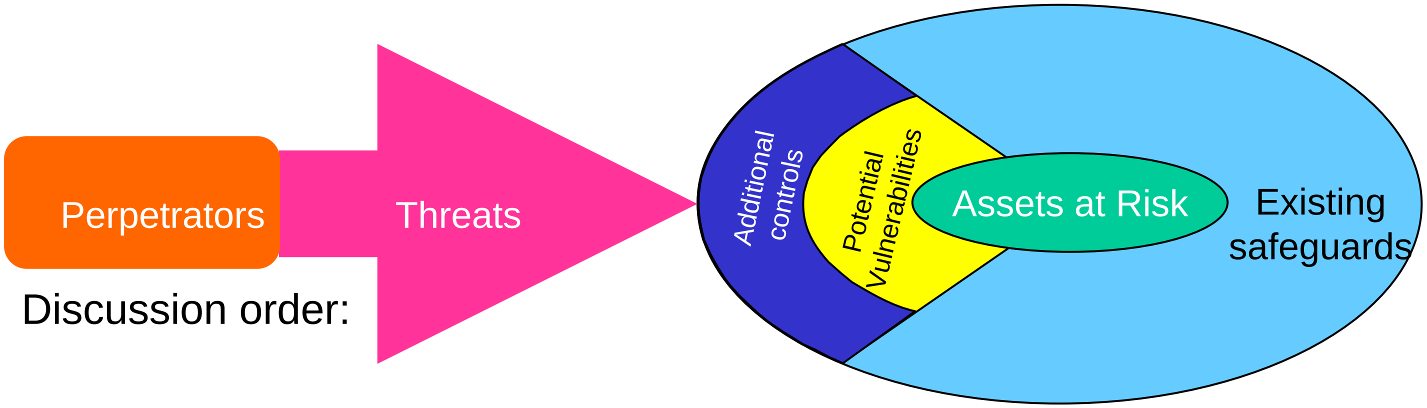
Tone spacing vs active block time $f_t = \frac{1}{t_F}$

$$N_B = 2N_R + N_C + N_G + N_F$$

Block efficiency $\eta = \frac{N_F}{N_B} = \frac{N_F}{N_F + N_C + 2N_R + N_G}$

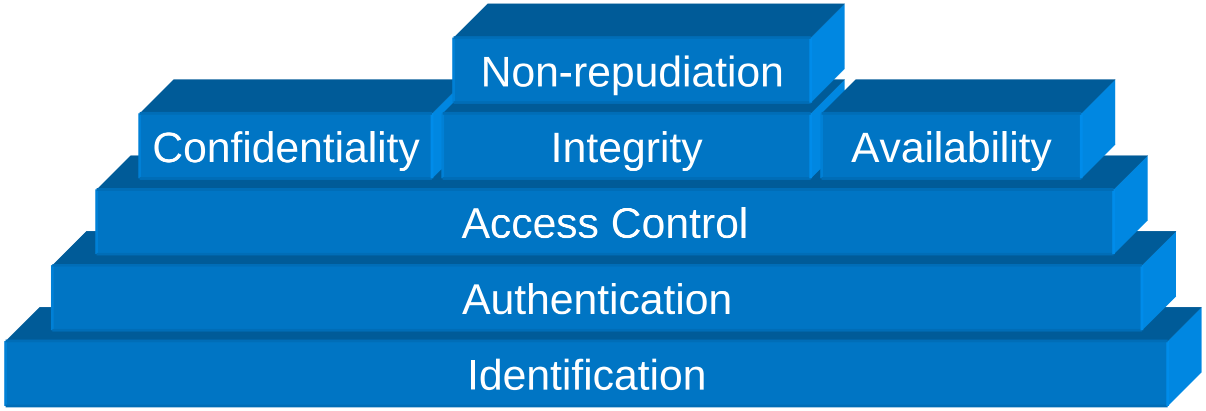
Tolerance to delay spread $\approx t_C \propto N_C$

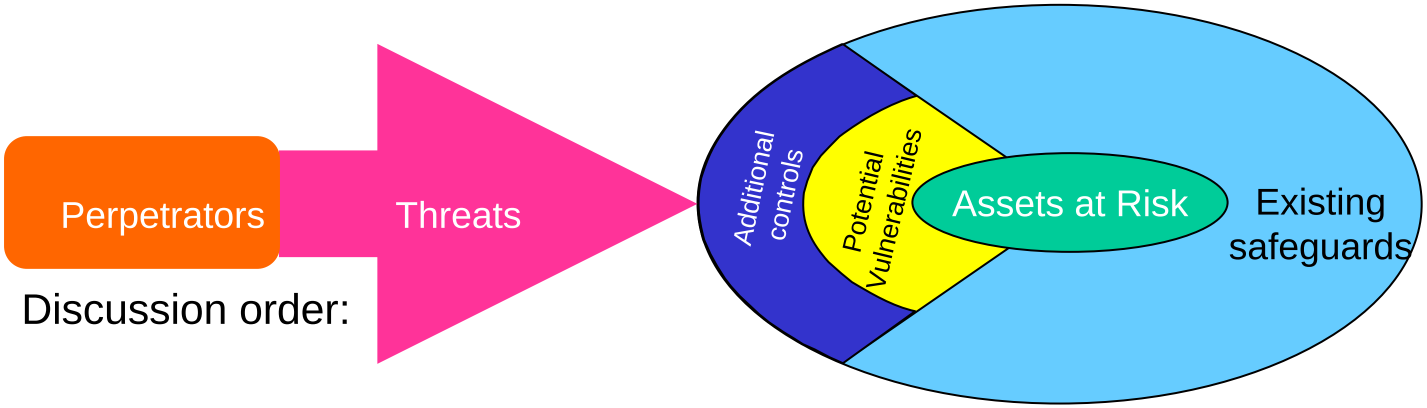
Raw capacity for M-ary tone modulation $N_t M$



Discussion order:

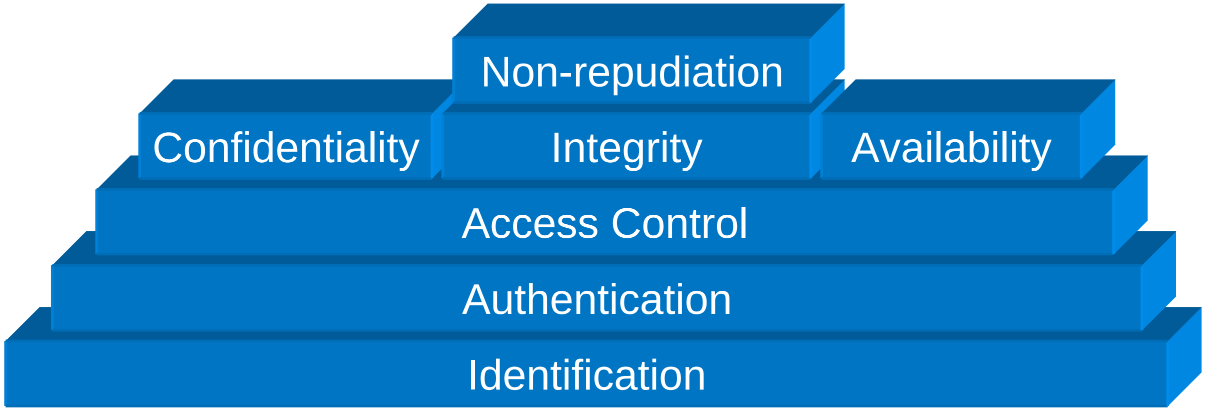
- Assets
- Perpetrators
- Threats
- Existing Safeguards
- Potential Vulnerabilities
- Additional Security Controls





Discussion order:

- Assets
- Perpetrators
- Threats
- Existing Safeguards
- Potential Vulnerabilities
- Additional Security Controls



Assets

- Access Point
  - Physical
  - Parameters
  - MAC address
- Initialization Vector
- Encryption key
- Channel bandwidth
- Data content
- User authentication over channel
- Access to intranet
- Capacity on wireless network
- Capacity on public internet (accessed via wireless network)
- Reputation
  - IP address of traffic originated through wireless network to intranet

Perpetrators

- War drivers
- Free riders
  - Your neighbors
- Mesh network users
- Hackers
- Competitive WLAN provider
- Curious eavesdroppers
- Competitors to user corporation
  - Corporate spies

Threats

Scan for open AP
Associate with open AP
Intercept/monitor data/interaction
Jam communications
Insert spurious traffic
- Hijack a session

Observe wireless MAC addresses
- Impersonate terminal

Guess default SSID
Guess common SSID
Monitor to learn SSID
attack WEP and break it
Denial of service
Theft of service
Engage in peer-peer communications
- Break into others' PCs

Vulnerabilities

- Misconfiguration of AP
  - AP bridging: broadcast Ethernet traffic
    - Overload wireless network
    - Compromise Ethernet traffic
- Lack of standards on key entry
- IV implementation
- Rogue APs are not authenticated as official ones are
  - Rogue DHCP servers
- WEP is broken
- Faulty AP design (e.g., Cisco association table overflow)
- Faulty implementation of SNMP
- No provision in 802.11a, b, or g for key variable change
  - Fixed, system wide key variable
- Powerful networking (plus) design flaws (plus) inexperienced network “administrators”
- Homogenous encryption standards/keys
  - Any valid user has wide access