

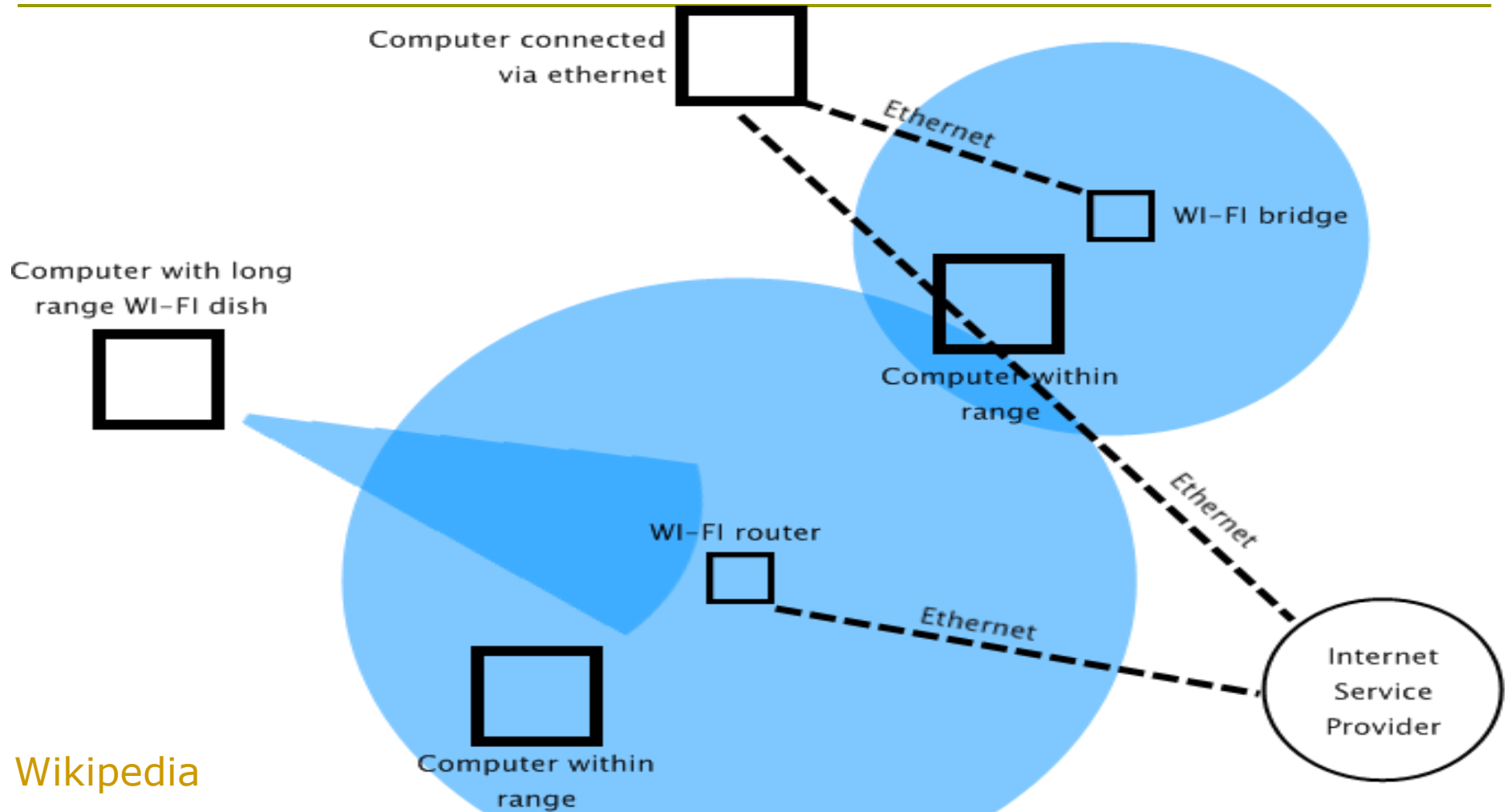
# WIRELESS SECURITY

---

M. Salahuddin

Id-SIRTII

# Common Topology



Wikipedia

4/20/2011

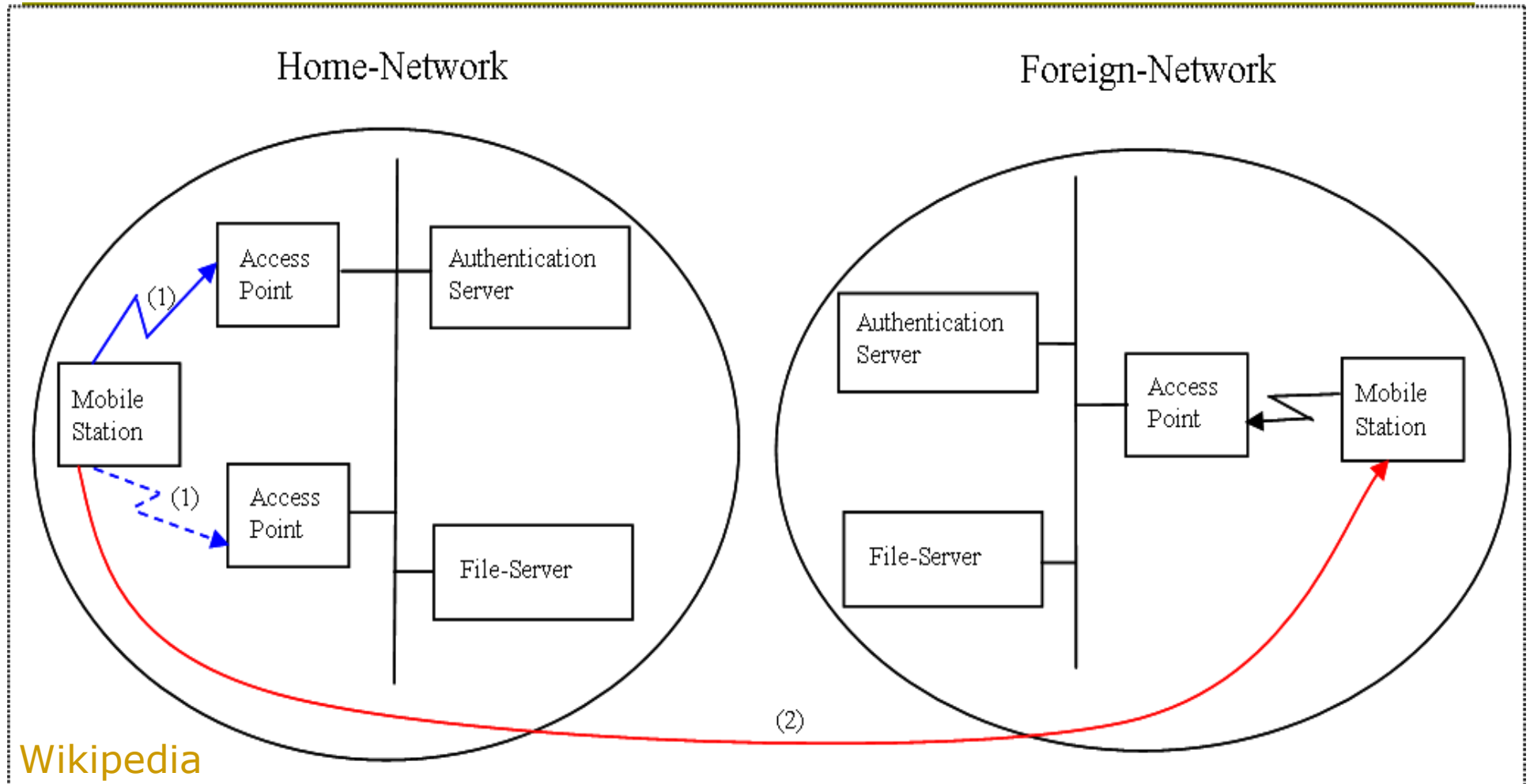
Wireless Security

# WLAN Types

---

- ❑ Peer to Peer / Ad Hoc mode, one to one connection
- ❑ Access Point / Infrastructure mode, star connection
- ❑ Bridge / Repeater mode, pass-through connection
- ❑ Mesh Network, every nodes can act as AP's chain
- ❑ Wireless Distribution System (WDS) mode, enable wireless interconnection between Access Point. Allow users to roam accross multiple Base Station

# WLAN Roaming



# Advantages

---

- ❑ Convenience, users can easily access at their primary networking environment (home or office)
- ❑ Mobility, access outside normal work environment
- ❑ Productivity, increase possibilities point of access
- ❑ Deployment, fast and less complex implementation
- ❑ Expandability, suddenly increase capacity & range
- ❑ Cost, low, affordable & modest comparing to wired
- ❑ Interoperability & easy integration to other network

# Disadvantages

---

- ❑ Security, less secure than wired network
- ❑ Range is limited, closed range up to 300 ft. only
- ❑ Reliability, subject to interference, multipath etc.
- ❑ Speed, older standards typically vary from 1 – 108 mbit/s. Newer standards (802.11n) support up to 200 mbit/s – 1 gbit/s throughput
- ❑ Radio frequencies are limited resource, possibilities on network saturation is high & it is not renewable

# Quick Facts

---

- ❑ Always use Encryption, WPA is better than WEP
- ❑ Always use Anti Virus, Anti Spyware, Firewall
- ❑ Change default identifier, turn off SSID broadcast
- ❑ Change default password, use strong combination
- ❑ Allow only specific trusted computer to access
- ❑ Never assume public hotspot are secure, they're not!
- ❑ Always turn off any wireless devices if not in use
- ❑ Careful, check twice before send or receive data, the real wireless security rely on Application Security

# Secure Application

---

- ❑ Try not to use untrusted public wireless network (i.e. HotSpots) if you have to access critical data and private services (i.e. online banking transaction etc.)
- ❑ If you have to do critical transaction, be sure to use proper encryption and extended secure application i.e. SSL (is a must on web transaction); PGP/GPG on mail send/receive; VPN/IPSec on remote application or services; SSH on remote login and etc.
- ❑ Make sure destination server is using valid certificate
- ❑ Make sure to disable shared access of your computer

# Securing HotSpot

---

- ❑ Limiting service coverage area, conservative power
- ❑ Hardening your captive portal security configuration
- ❑ Use double authentication RADIUS, LDAP and token
- ❑ Update with latest firmware and security patch
- ❑ Isolated network perimeter with DMZ and firewall
- ❑ Use different frequencies, channel, band if possible
- ❑ Disable remote administration (securing interface)
- ❑ Wireless Intrusion Prevention System WIPS, optional

# Good Password

---

- ❑ Combined character is more difficult to break
- ❑ Unusual phrase is better than common phrase
- ❑ Random long phrase is harder than short phrase
- ❑ WPA allows passwords as long as 63 characters
- ❑ Password is like shocks, better change them often
- ❑ Change all default password including SNMP's
- ❑ Memorize or put the password in secure place

# Common Attack 1

---

- ❑ Accidental Association, users accidentally connect to another wireless network that overlapping the existing official network. Can causing data leak or security breach into home network
- ❑ Malicious Association, attacker create fake AP's to "spoof" legitimate AP's to gain access to the users home network so he/she can steal passwords and any other private information and or launch attacks on the wired network and or plant virus/trojans
- ❑ Caffe Latte, using exploit to defeat WEP encryption

# Common Attack 2

---

- ❑ Add Hoc networks, because it has less protection
- ❑ MAC Spoofing, attacker can easily spoof MAC addr
- ❑ Man in The Middle, because of radio frequency use open air media, theoretically everybody can “hear” or sniff all of the communications / data flow / traffic
- ❑ Denial of Services, attacker continually bombards a targeted AP or network with in-appropriate data or other malicious commands. These are causing users not be able to get on the network and may crash the entire network (not only the wireless LAN)

# Post Audit

---

- ❑ Activate logs on any related equipment AP, Captive Portal, RADIUS, WIPS, Firewall, VPN Server etc.
- ❑ Register (record) / copy the user ID Card especially for public access providers (i.e. HotSpot) to prevent misuse by the (user) attacker
- ❑ Periodic analysis of logs and traffic pattern to know common and potential security threat on network
- ❑ Penetration test after hardening or update or patch network configuration and devices

# The Law

---

- ❑ ICT Minister Decree Number 26 of 2007, article 21: “Internet Cafe and HotSpot Providers must record users ID Card and access time (start/stop) and keep it for at least one (1) year, as a part of the operation procedures”
- ❑ Draft of ICT Minister Decree about the Wireless LAN Security Guidance