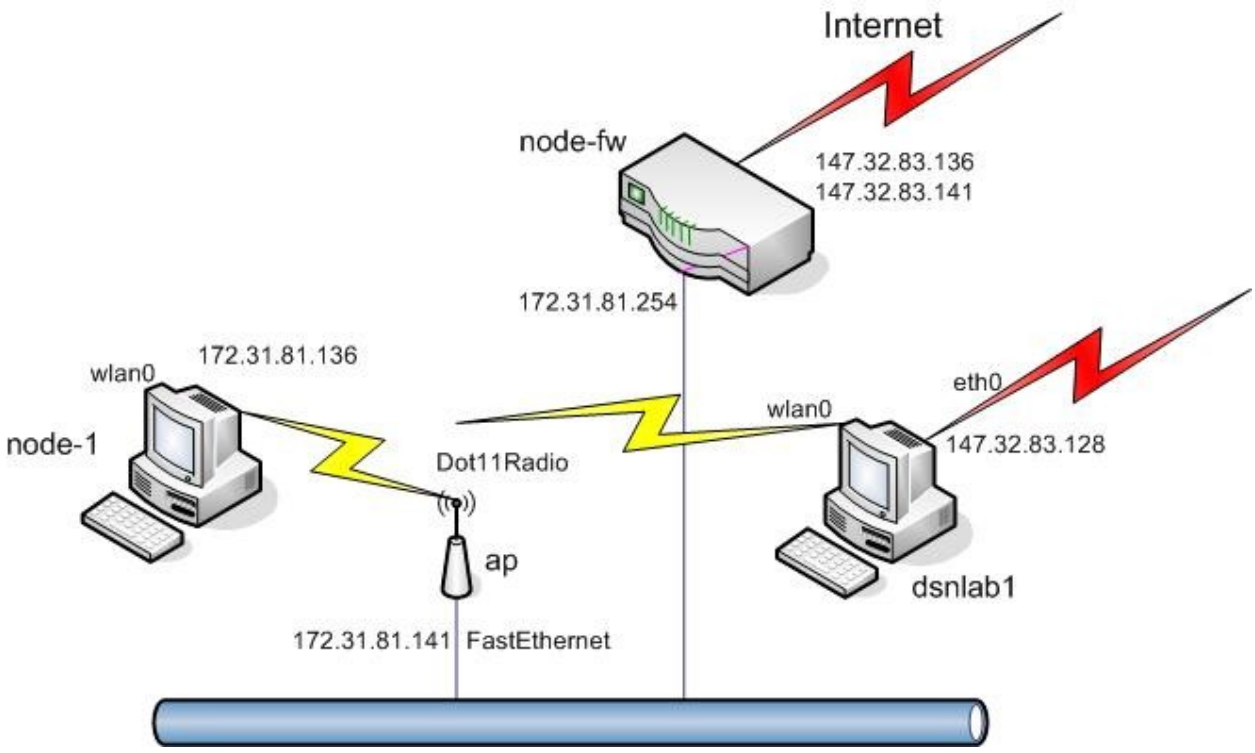
Praktikum – WIFI

Cíl cvičení:

V terminálovém režimu konfigurujte Access Point (AP) Cisco AiroNet 1230 a počítač s nainstalovaným bezdrátovým adaptérem, zapojené v síti podle obrázku a seznamte se s dalšími možnostmi správy:



Obrázek 1: Zapojení pracoviště

nastavte parametry FastEthernetového rozhraní na AP - IP adresa AP 172.31.81.141 s maskou 255.255.255.0, SNMP community name public,

- nakonfigurujte radiové rozhraní Dot11Radio0 AP,
- nakonfigurujte radiové rozhraní wlan0 počítače node-1, IP adresa node-2 172.31.81.136 s maskou 255.255.255.0,
- ověřte příkazem `route` nastavení směrovací tabulky počítače **node-1**,
- ověřte provozuschopnost celé konfigurace příkazy `ping` a `telnet`,
- monitorujte provoz bezdrátového spoje z počítače **dsnlab1**,
- překonfigurujte radiový spoj s využitím technologie WEP,
- přihlašte se prohlížečem WWW na IP adresu AP (147.32.83.141) a vyzkoušejte si možnosti správy v tomto režimu,
- odchytněte komunikaci pomocí programu kismet s i bez šifrování, data analyzujte.

Pokyny:

Access point **ap** (Cisco 1320) a počítač **node-1** jsou ovladatelné seriovou konzolí z počítače **dsnlab1**. K zařízením se připojujte programem `minicom` s parametrem označení terminálu (viz Tab.1).

```
minicom S1
```

Počítač	Port
node-1	S1
ap (cisco)	S11

Tabulka 1: Připojení seriových portů

Počítač **dsnlab1** je dostupný z libovolného pracoviště v laboratoři protokolem ssh pod adresou 147.32.83.128, uživatelský účet máte k dispozici pod jménem **dsy** a heslem **nod123**. Superuživatelský účet **root** na počítači **node-1** má heslo ***nod123***. AP je dostupný pod účtem **Cisco** s heslem **Cisco**. Pro vstup do privilegovaného režimu použijte heslo **Cisco**.

Upozornění!!!!

Pracoviště je umístěno za směrovačem s implementovaným překladem adres (NAT) a paketovým filtrem. Překlad adres překládá adresy ze sítě 147.32.83.0/24 na adresy sítě 172.31.81.0/24 v obou směrech. Paketový filtr propouští vše ze sítě 172.31.81.0/24 (směrem do internetu). Směrem ze sítě 147.32.83.0/24 (směrem z internetu) propouští pouze **icmp echo**, **tcp 22** a **tcp 80** (**ping**, **ssh**, **www**). Přidělené adresy jsou uvedeny v tabulce 2.

Vnější adresa	Vnitřní adresa
147.32.83.136	172.31.81.136
147.32.83.141	172.31.81.141

Tabulka 2: Adresní prostor - překlad adres

Vnitřní adresa tohoto směrovače (tedy **default gateway**) je **172.31.81.254**.

Start AP:

Po zapnutí AP odešlete z ovládacího terminálu znak `cr` (Enter), přepínač se na konzoli (terminálu nebo jeho emulátoru) ohlásí a (po zadání jména a hesla) přechází do příkazového módu s promptem

```
ap>
```

Pro vstup do privilegovaného režimu je třeba zadat příkaz enable a heslo (Cisco). Výsledkem je prompt:

```
ap#
```

Příkazový jazyk má kontextovou nápovědu, po stisknutí klávesy `?` nebo příkazu `help` dostaneme nabídku možných pokračování příkazu (při uvedení `?` nebo `help` na začátku řádky získáme seznam příkazů). Klávesou `Tab` si lze vyžádat doplnění jednoznačně určeného pokračování příkazu.

Při konfiguraci AP máme na výběr mezi řádkovými příkazy a WWW rozhraním.

Pro zpřístupnění AP prostřednictvím WWW rozhraní je třeba nastavit FastEthernet rozhraní a parametry TCP/IP stacku.

Do konfiguračního režimu přejděte zadáním:

```
ap#configure terminal
```

IP adresa se může nastavit pro virtuální rozhraní:

```
ap(config)#interface bvi 1
```

IP adresu nastavíte příkazem:

```
ap(config-if)#ip address 172.31.81.141 255.255.255.0
```
Adresu brány pak (v módu konfigurace):

```
ap(config)#ip default-gateway 172.31.81.254
```

FastEthernetové rozhraní je defaultně zapnuto, případné zapnutí provedete příkazy:

```
ap(config)#interface FastEthernet 0
ap(config-if)#no shutdown
```

Radiové rozhraní je defaultně zapnuto, případné zapnutí provedete příkazy:

```
ap(config)#interface dot11Radio 0
ap(config-if)#no shutdown
```

Pro radiové rozhraní je potřeba nastavit jeho roli:

```
ap(config-if)#station-role root
```

Dále je možné nastavit povolené rychlosti a výkony. Tyto hodnoty můžete ponechat v defaultním nastavení.

Důležité nastavení je číslo použitého kanálu (zadává se číslem kanálu, nebo hodnotou frekvence):

```
ap(config-if)#channel 3
```

Případně je možné nechat AP zvolit vhodný kanál automaticky:

```
ap(config-if)#channel least-congested
```

Nastavení WEP klíče:

```
ap(config-if)#encryption key 1 size 128bit 0 12345678901234567890123456
```

Zapnutí WEP:

```
ap(config-if)#encryption mode wep mandatory
```

Nastavení způsobu autentizace:

```
ap(config-if)#ssid tsunami
ap(config-if-ssid)#authentication shared
```

Konfigurace počítače

Pro zpřístupnění karty lze použít ovladač prism2_usb. Tento ovladač nahrajete příkazem

```
modprobe prism2_usb prism2_doreset=1
```

Konfigurace připojení:

```
wlanctl-ng wlan0 lnxreq_ifstate ifstate=enable
wlanctl-ng wlan0 lnxreq_autojoin ssid=tsunami authtype=opensystem
ifconfig wlan0 172.31.81.133 netmask 255.255.255.0
```

Nastavení šifrování pomocí WEP:

```
wlanctl-ng wlan0 lnxreq_hostwep decrypt=true encrypt=true
wlanctl-ng wlan0 dot11req_mibset mibattribute=dot11PrivacyInvoked=true
wlanctl-ng wlan0 dot11req_mibset mibattribute=dot11WEPDefaultKeyID=0
wlanctl-ng wlan0 dot11req_mibset mibattribute=dot11ExcludeUnencrypted=true
wlanctl-ng wlan0 dot11req_mibset \
mibattribute=dot11WEPDefaultKey0=12:34:56:78:90:12:34:56:78:90:12:34:56
```

Zachytávání bezdrátové komunikace:

Pro zachytávání bezdrátové komunikace použijeme program `kismet` (http://www.kismetwireless.net). Program musí být spuštěn s právy superuživatele:

sudo kismet

Program automaticky vyhledá dostupné bezdrátové sítě a vypíše je. Pro možnost práce s jednotlivými sítěmi je potřeba zapnout jiné řazení než autofit (s-s).
Nápovědu k programu získáte po stisku klávesy **h**. Kismet ukládá komunikaci do souboru ***.dump do adresáře /var/log/kismet. Tyto soubory je možné analyzovat pomocí programů `tcpdump` a `ethereal`.

Ověření činnosti:

Správné nastavení prvků sítě si ověříte příkazem `ping`. Možnosti správy a získávání informací o provozu AP prostřednictvím rozhraní WWW si ověříme přihlášením se (prohlížečem WWW) na IP adresu AP.