Úloha 3: zabezpečenie siete proti prieniku pomocou služieb telefónu

V úlohe 3 sa povenujeme niektorým službám a nastaveniam telefónu, povieme si, ktoré je dobré vypnúť a v akých podmienkach.

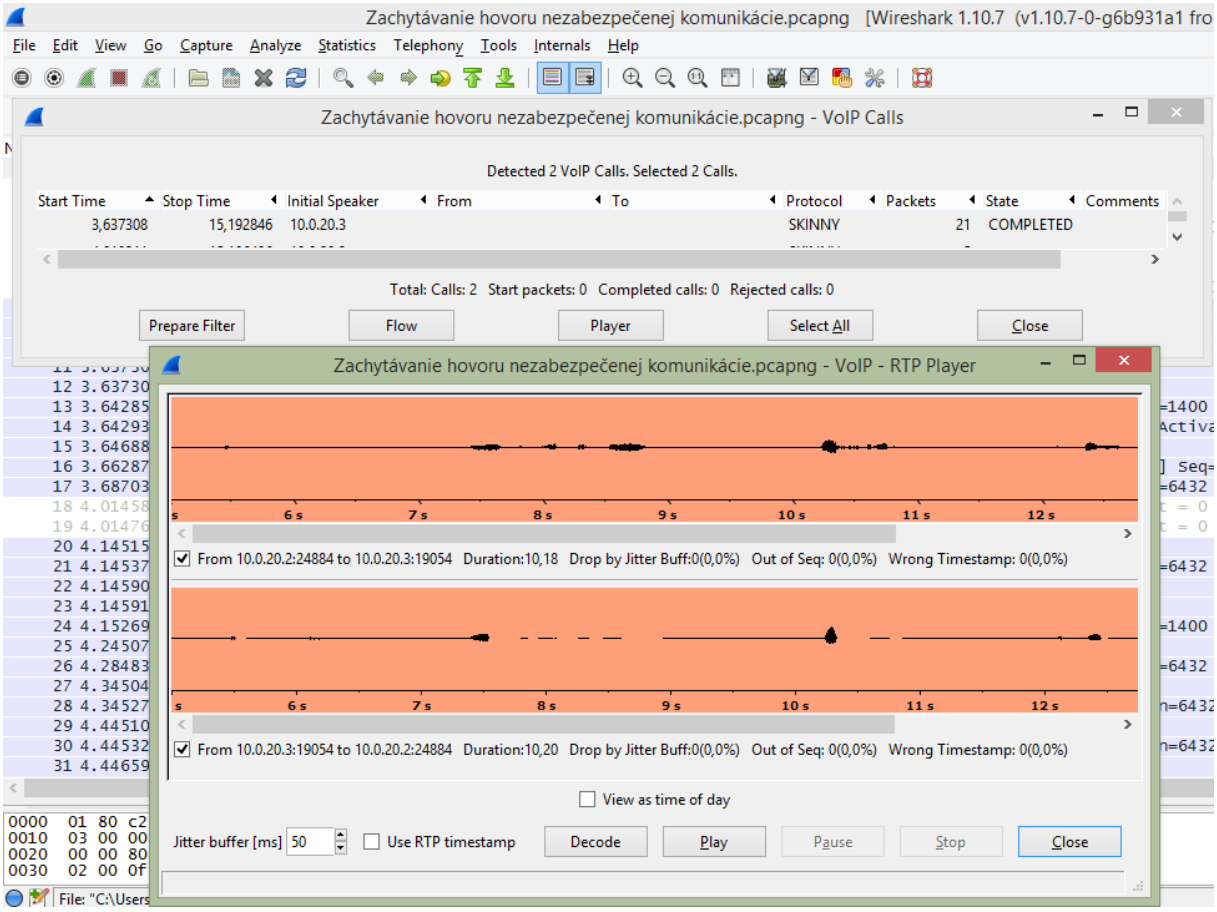
Všetky nastavenia prebiehajú v menu konkrétneho telefónu cez CUCM.

Device -> Phone a telefón ktorý chcete nastaviť. Nastavenia sa nachádzajú úplne dole, viď Obr.1.

Počítačový port

Pokiaľ máte IP telefón a prepínač nastavený pre fungovanie počítačového portu, môžete tento port na telefóne využiť a nepotrebujete viac LAN prípojok. Čo však pripojený počítač vidí, je všetka prichádzajúca a odchádzajúca komunikácia na telefóne. Je takto pripojený priamo do našej siete a vie odchytávať a nahrávať hovory, prípadne podstrčiť vlastné informácie. Niekedy je to vhodné, napríklad v Call centrách, kedy vedúci kontrolujú zamestnancov, ale vo väčšine prípadov je nepotrebný. Na miestach ako recepcia, kde nechceme pripájať ďalšie počítače je nechcený.

Otestujte sami odchytávanie hovoru, budete potrebovať voľne dostupný program Wireshark. Prepojte svoj počítač zo smerovača do počítačového portu a zmeňte svoju IP adresu na 10.0.10.X (Kde X predstavuje číslo 1 + číslo vašej skupiny). Vyberiete si sieťový adaptér ktorým ste pripojený k portu telefónu a spustíte zachytávanie. Z telefónu na ktorom sa nachádzate uskutočníte simulačný telefónny hovor s niekým zo skupiny a keď hovor skončíte, zastavíte odchytávanie. V menu programu Wireshark prejdete do **Telephony -> Voip Calls** zvolíte **Select All** a **Player**, následne **Decode** a môžete si vypočuť váš predošlý hovor (Obr.2).



Obr.1

Tlačidlo nastavenia

Tlačidlo nastavenia na telefóne má najmä informačnú funkciu, vidíme IP adresy sieťových prvkov, správy, ktoré telefón zobrazuje pokiaľ niečo nefunguje ako má a ďalšie, nastaviť sa dajú zvuky, jas a pá ďalších vecí. Nastavenia si môžete prejsť. Rovnako sú to veci, ktoré užívateľ za telefónom nutne nepotrebuje, vieme toto tlačidlo úplne vypnúť, alebo ponechať v obmedzenom režime, kedy má prístup práve k veciam ako hlasitosť, jas a nezobrazujú sa mu informácie o sieti. Obmedzené nastavenie je odporučené

Gratituos ARP (GARP, podvrhnuté/nechcenné ARP)

Samotné ARP správy slúžia na identifikáciu zariadenia podľa vlastnenej IP adresy. Chceme k nej zistiť prislúchajúcu MAC adresu. Podvrhnuté ARP správy sú také, ktoré sme si nevyžiadali. Je odporúčané GARP blokovať.

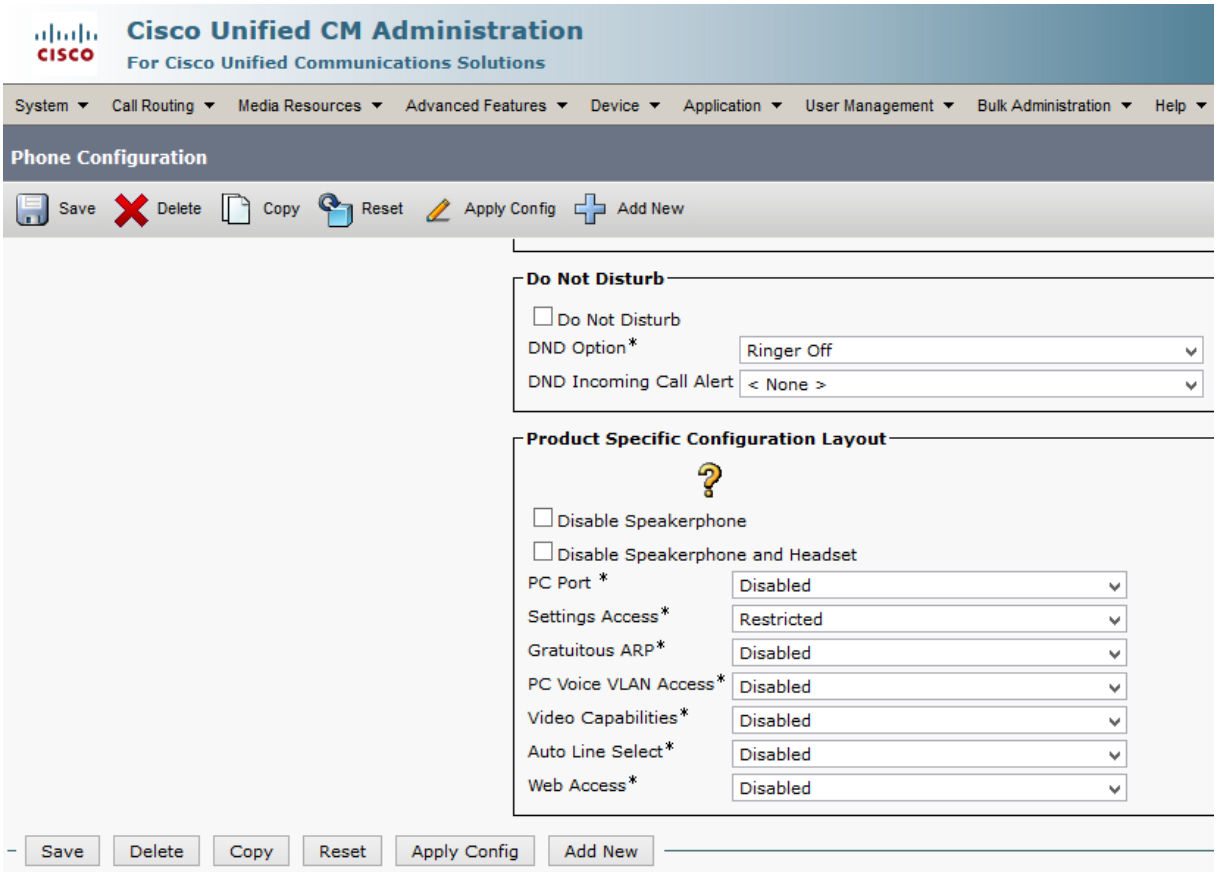
Prístup k hlasovej časti siete cez počítačový port

Pokiaľ máme počítačový port aktívny, nemusíme ho vypínať úplne, je možné vypnúť len prístup do hlasovej časti siete, v tomto prípade užívateľ nebude dostávať správy s príznakom

hlasovej komunikácie a nemôže tak komunikáciu odpočúvať. Otestujte jeho vypnutím a odpočúvaním prenosu. Wireshark vám teraz žiadny IP telefónny hovor nezaznamená.

Webové rozhranie telefónu

Rozhranie podobné tomu v ktorom sa práve nachádzate majú aj samotné telefóny. Tieto rozhrania sú dostupné po vložení ich IP adresy do webového prehliadača. Viete tu zistiť množstvo informácií o vašej sieti a vašom telefóne. Tieto informácie však bežný užívateľ vôbec nepotrebuje, naopak útočníkovi sa môžu hodiť. Preto je dobré webové rozhranie vypnúť, v prípade identifikácie chýb v sieti nie je problém ho znovu aktivovať.



Obr.2

Otestujte zadaním IP adresy do webového prehliadača, následným vypnutím znovu načítaním stránky.

Koniec Úlohy 3.