



Bezpečnostní aspekty konfigurace sítového prostředí pro IP telefonii

Seminář IP telefonie a videokonferencí 1.12.2009

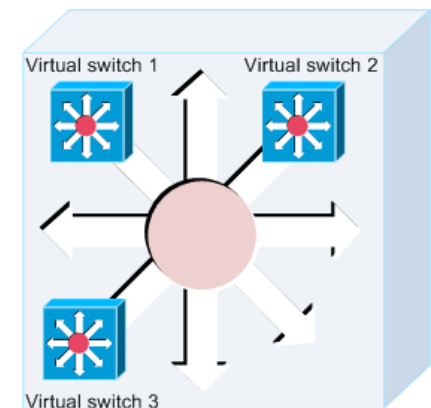
Michal Petrovič
petrovic@civ.zcu.cz

Obsah

- **Speciální infrastruktura pouze pro VoIP (VRF-lite)**
- **Omezení počtu MAC adres na portu**
- **Voice VLAN**
- **DHCP snooping**
- **Dynamic ARP Inspection**
- **IP Source Guard**
- **FW ASA**

Infrastruktura pouze pro VoIP I

- VRF-lite - Virtual Routing a Forwarding - lite
- Podpora na Cisco 3550, 3560, 4900M, 6500...
- Vlastní logická síť včetně směrovačů
- Vlastní směrování a podsítě
- Podsítě pouze pro IP telefony, SIP servery, GW...
- Řízené propojení do ostatních sítí (internetu)



Infrastruktura pouze pro VoIP II

```
ip vrf VoIP
```

```
description network for VoIP
```

```
interface vlan 800
```

```
description vlan for IPT
```

```
ip vrf forwarding VoIP
```

```
ip address 10.10.10.1 255.255.255.0
```

```
router ospf 1 vrf VoIP
```

```
router-id 10.10.1.1
```

```
log-adjacency-changes
```

```
network 10.10.0.0 0.0.255.255 area 0
```

```
default-information originate
```

Omezení počtu MAC adres na portu I

- **Konfigurace bezpečnosti na portu**
- **Ochrana proti přetečení CAM tabulky přepínače**

- **MAC Flooding**
 - Omezená paměť (tabulka) přepínače pro MAC adresy
 - Pokud není MAC v tabulce rozešle se na všechny porty

- **ARP Spoofing - ARP Poisoning Attack**
 - ARP pakety - podvodné adresy
 - adresát posílá útočnickovi, útočník přeposílá cíli
 - cíl odpovídá útočnickovi, útočník přeposílá adresátovi

Omezení počtu MAC adres na portu II

interface Fa0/1

switchport port-security	! zapnutí bezpečnosti
switchport port-security maximum 3	! 3 MAC adresy pro PC
switchport port-security violation restrict	! zahazuje pakety
switchport port-security aging time 2	! 2 minuty pro vypršení adresy
switchport port-security aging type inactivity	! pouze pokud je port neaktivní
switchport port-security maximum 1 vlan voice	! 1 MAC adresa pro IP telefon

Voice VLAN I

- **Speciální virtuální síť pouze pro IP telefony**
- **Oddělení datového provozu od telefonního**
- **Domluva pomocí CDP – Cisco Discovery Protocol**
- **Podpora QOS**
- **Konfigurace na portu přepínače**

Voice VLAN II

```
interface Fa0/1
```

```
switchport access vlan 10
```

```
switchport voice vlan 20
```

! konfigurace podsítě pro PC

! konfigurace podsítě pro IPT

DHCP snooping I

- Obrana proti „cizímu“ DHCP serveru
- Definice DHCP „důvěryhodných“ portů
- Vytváří tabulku s informacemi o přidělené IP
 - MAC adresa
 - IP adresa
 - čas zapůjčení IP adresy
 - VLAN
 - Port
 - způsob přidělení IP adresy (staticky/dynamicky)
- Tato tabulka se dále používá pro DAI

DHCP snooping II

```
ip dhcp snooping
```

```
ip dhcp snooping vlan 10
```

```
no ip dhcp snooping information option
```

```
int Gi0/4
```

! na trunk portech nastavit trust a počet DHCP dotazů

```
ip dhcp snooping trust
```

```
ip dhcp snooping limit rate 100
```

! default je neomezeno

DAI - Dynamic ARP Inspection I

- Zabraňuje útoku „man-in-the-middle“ a DoS
- Kontrola ARP paketů v síti
- Brání přeposílání podvodných ARP dotazů
- Kontroluje IP a MAC adresu podle „DHCP snooping binding“ tabulky pro všechny pakety
- Umožňuje nastavit omezení počtu ARP paketů
- Standardně je omezení na 15 ARP paketů/sec

Dynamic ARP Inspection

```
ip arp inspection vlan 10
```

```
ip arp inspection validate src-mac dst-mac ip
```

```
int Gi0/4                ! na trunk portech nastavit trust a počet ARP dotazů
```

```
ip arp inspection trust
```

```
ip arp inspection limit rate 50    ! default je 15 paketů/sec
```

IP Source Guard

- Podobné jako DHCP snooping
- Pro správnou funkčnost se používá společně!
- Při přidělení IP adresy klientovi se vytváří PVACL (per-port and VLAN Access Control List)
- Zabrání komunikaci nedůvěryhodným adresám
- Kontroluje IP a MAC adresu pro určitý port
- Zabráňuje převzetí IP adresy (volné nebo již přidělené)

IP Source Guard

```
interface Fa0/1
```

```
ip verify source port-security
```

```
ip verify source
```

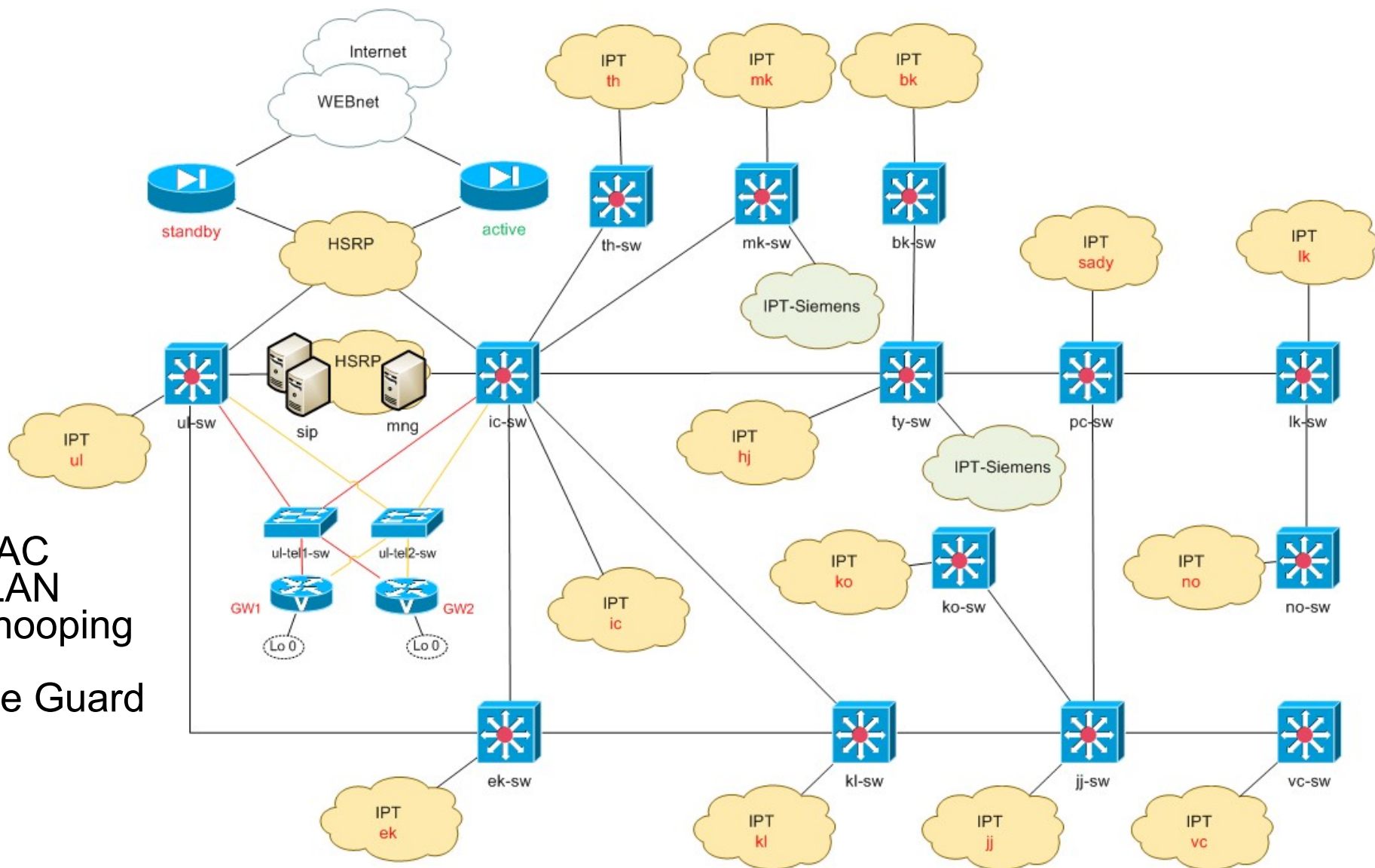
- **Zapnutí ukládání DHCP snooping tabulky na externí TFTP server**

```
ip dhcp snooping database tftp://IP_adresa/jméno_přepínače  
ip dhcp snooping database write-delay 15  
ip dhcp snooping database timeout 0
```

FW ASA

- **Firewall Cisco Adaptive Security Appliance**
- **Vhodný oddělovač virtuální VoIP sítě od ostatních sítí a internetu**
- **Možnost redundance**
- **Funkce:**
 - **Aplikační stavový firewall**
 - **VPN koncentrátor**
 - **Intrusion Protection systém**

VoIP infrastruktura



- VRF-lite
- Počet MAC
- Voice VLAN
- DHCP snooping
- DAI
- IP Source Guard
- FW ASA

Dotazy

???