

Security Considerations in IP Telephony Network Configuration

Abstract

This Technical Report deals with fundamental security settings in networks to provide secure VoIP services. Example configurations of Cisco devices are included as well.

Keywords: security, VoIP, SIP, IP telephony, SER, OpenSER, Asterisk, Linksys, Cisco, VRF-lite, ARP Spoofing, ARP Cache Poisoning, DHCP Spoofing, ICMP Redirect,, MAC Flooding, Port Security, DAI, DHCP Snooping IP Source Guard

Separate VoIP Infrastructure

For improved security, VoIP networks should be separated from other networks, especially data transfer networks as those typically include end-user PCs, which are easily abused by attackers to disrupt or eavesdrop on VoIP communications.

VRF-Lite technology (Virtual Routing and Forwarding - Lite) – supported by a wide range of devices such as Cisco Catalyst 3550, Catalyst 3560, Catalyst 4900M, Catalyst 6500, 3Com S7900E, S7500E, Juniper J4300 and many others – may be used to achieve network separation.

VFR typically relies on MLPS (Multiprotocol Label Switching) networks, encapsulating data transfers to separate them from those of other subscribers. However, VRF-Lite technology is not dependent on MPLS and can be used of its own.

Figure 1 gives an example of a configuration comprising of two routers and two switches. Blue lines represent links used by computers and red lines represent links dedicated to IP telephony. Both subnets are physically separated.

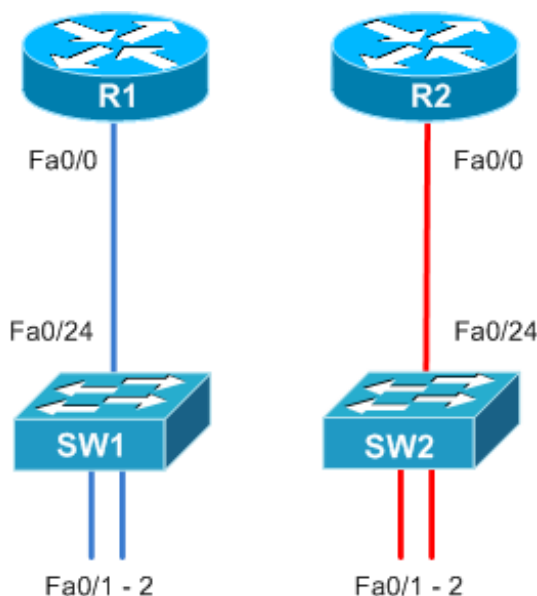


Fig. 1 – Two physically separated subnets

Configuration Example:

R1:

```
interface FastEthernet0/0
description PC_network
ip address 192.168.1.1 255.255.255.0
```

R2:

```
interface FastEthernet0/0
description VoIP_network
ip address 192.168.2.1 255.255.255.0
```

SW1:

```
interface range FastEthernet0/1 - 2
description PC_network
switchport mode access
!
interface FastEthernet0/24
description PC_network
switchport mode access
```

SW2:

```
interface range FastEthernet0/1 - 2
description VoIP_network
switchport mode access
!
interface FastEthernet0/24
description VoIP_network
switchport mode access
```

Figure 2 shows two physically separated routers, one used by the computer network and another one used by IP phones. The switch is shared by both subnets, which are still logically separated through VLAN (Virtual LAN) technology. The switch maintains VLAN 10 for computers and VLAN 20 for IP phones.

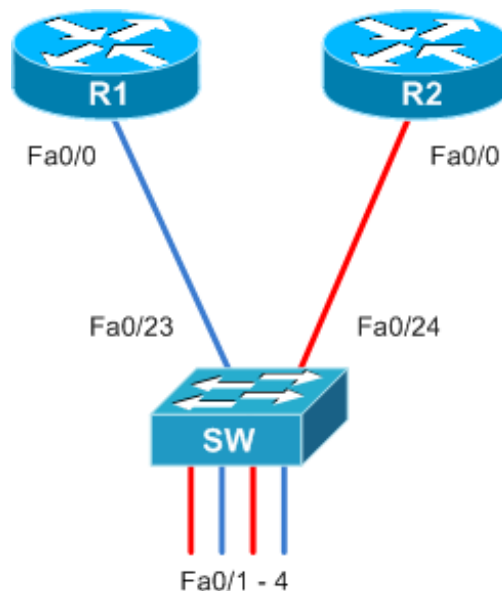


Fig. 2 – Two subnets with physically separated routers and logical separation in a switch

Configuration Example:

R1:

```
interface FastEthernet0/0
description PC_network
ip address 192.168.1.1 255.255.255.0
```

R2:

```
interface FastEthernet0/0
description VoIP_network
ip address 192.168.2.1 255.255.255.0
```

SW:

```
interface range FastEthernet0/1 , FastEthernet0/3
description PC_network
switchport access vlan 10
switchport mode access
!
interface range FastEthernet0/2 , FastEthernet0/4
description VoIP_network
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/23
description PC_network
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/24
description VoIP_network
switchport access vlan 20
switchport mode access
```

Figure 3 shows a single physical router comprising two virtual routers, and a single switch achieving logical separation through the VLAN technology. Logical separation of data and telephony networks, including their respective routing tables and protocols, has been achieved by establishing two virtual routers enclosed in a single physical device but acting independently. The router and switch must be connected by a line in TRUNK mode to allow transmission of data originating from multiple subnets through a single link.

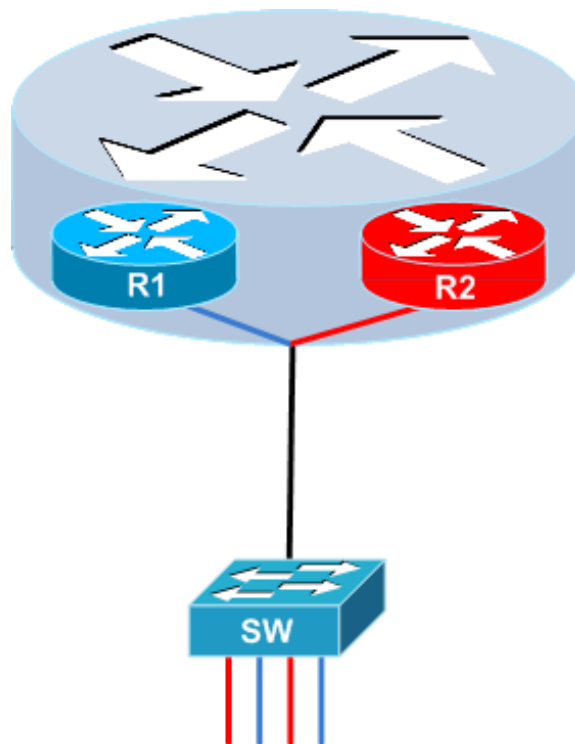


Fig. 3 – Two logically separated subnets sharing a single router and a single switch

Configuration Example:

R:

```
ip vrf VoIP
  description network for VoIP
!
ip vrf PC
  description network for PC

interface FastEthernet0/0.10
  description PC_network
  encapsulation dot1Q 10
  ip vrf forwarding PC
  ip address 192.168.1.1 255.255.255.0
!
interface FastEthernet0/0.20
  description VoIP_network
  encapsulation dot1Q 20
  ip vrf forwarding VoIP
  ip address 192.168.2.1 255.255.255.0
```

SW:

```
interface range FastEthernet0/1 , FastEthernet0/3
  description PC_network
  switchport access vlan 10
  switchport mode access
!
interface range FastEthernet0/2 , FastEthernet0/4
  description VoIP_network
  switchport access vlan 20
  switchport mode access
!
interface FastEthernet0/24
  description trunk_connection_to_router
  switchport trunk encapsulation dot1q
  switchport mode trunk
```

Limiting the Number of MAC Addressed at a Port

Limiting the number of individual network device addresses (so called MAC addresses) that can be connected to a single port in a switch is an essential security measure. Each switch maintains a CAM (Content Addressable Memory) table, keeping records of MAC addresses and ports they are connected to. This allows the switch to forward packets to the correct port instead of sending copies of the packet to all ports.

Limiting the number of MAC addressed at each port prevents “MAC Flooding” attacks, which exploit the limited capacity of the CAM table by overfilling it and causing the switch to send packets intended for the target device to all ports rather than just the one the target device is connected to. With the CAM table full, the switch treats any new address as unknown. The attack starts by generating a large number of MAC addresses and sending them to a port of the switch, filling up the CAM table and forcing the switch to start sending packets intended for other devices to all ports, where they are easily eavesdropped.

Unlimited number of MAC addresses at a port may also be exploited in another kind of attack, so called “ARP Spoofing” or “ARP Cache Poisoning.” This method relies on sending fake ARP (Address Resolution Protocol) queries, usually serving to translate IP addresses to MAC addresses. The attacker may pose as target and eavesdrop on the communication.

Configuration Example:

```
interface FastEthernet0/1
  switchport port-security          ! turn on security
  switchport port-security maximum 1 ! 1 MAC address for a PC
  switchport port-security violation restrict ! drop packets
  switchport port-security aging time 2 ! address expires in 2 minutes
  switchport port-security aging type inactivity ! only if the port is inactive
  switchport port-security maximum 1 vlan voice ! 1 MAC address for an IP phone
```

Voice VLAN

The first chapter of this Technical Report has documented the importance of logical separation of subnets used by computers and IP phones. Many IP phone manufacturers, however, support connecting a computer to the network through an IP phone, limiting the number of ports occupied. Unfortunately, this brings computers and IP phones together in one network once again.

Voice VLAN is a special subnet intended only for IP phones. It may be connected up to a certain port in a manner similar to computer subnets. Ports may be configured for simultaneous use of the computer and IP phone subnets. Obviously, the IP phone must support VLAN to handle simultaneous communication over multiple subnets correctly. Voice data are tagged, while data originating from the computer network are sent untagged, enabling easy differentiation.

CDP (Cisco Discovery Protocol) is another IP phone feature required to support Voice VLAN functionality. This proprietary protocol is typically supported by Cisco and Linksys phones, allowing the phone to negotiate subnet numbers with the switch instead of having the number set as a fixed property of the phone. Application of CDP brings about yet another advantage. Unless the IP phone succeeds in negotiating the subnet number with the switch correctly, voice data are never forwarded to its port.

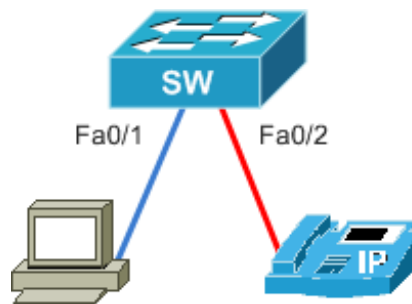


Fig. 4 – Connecting a PC and IP phone through their own links

Configuration Example:

```
interface FastEthernet0/1
  switchport access vlan 10          ! PC subnet configuration
  !
interface FastEthernet0/2
  switchport access vlan 20          ! IPT subnet configuration
```

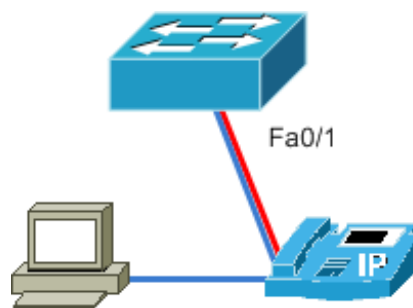


Fig 5 – Connecting a PC and IP phone through a common link

Configuration Example:

```
interface FastEthernet0/1
  switchport access vlan 10      ! PC subnet configuration
  switchport voice vlan 20      ! IPT subnet configuration
```

DHCP Snooping

Another protective measure used in computer networks is DHCP Snooping configuration. This allows administrators to declare individual ports “Trusted” or “Untrusted.” Untrusted ports block DHCP communication, preventing attackers' DHCP servers from providing IP addresses to computers and IP phones. If not prevented, attackers could modify DHCP configuration for other computers to regard their servers as default gateways, directing all communication to them and making it easy to eavesdrop. Administrators will prevent this by setting the uplink port and the port connecting their DHCP server to trusted, and even by limiting the number of DHCP requests and replies within a time frame to prevent flooding. Other ports connecting PCs and IP phones will be untrusted by default, blocking DHCP replies generated by possible attackers.

DHCP Snooping also allows administrators to maintain a table of MAC addresses, IP addresses issued by the DHCP server, and ports to which those addresses connect. The table may serve as an input for other tools such as Dynamic ARP Inspection or IP Source Guard.

An example of a “DHCP snooping binding” table:

MacAddress	IpAddress	Lease(sec)	Type	VLAN	Interface
00:01:01:01:01:01	192.168.1.10	2984	dhcp-snooping	10	FastEthernet0/1
00:02:02:02:02:02	192.168.2.10	3098	dhcp-snooping	20	FastEthernet0/2

Configuration Example:

```
ip dhcp snooping                ! Turn on DHCP Snooping
ip dhcp snooping vlan 10,20     ! Activate for selected VLANs
no ip dhcp snooping information option ! Don't modify DHCP packet with param 82

! Backups of the table will be stored on a TFTP server in case the
! switch restarts and computers or IP phones do not request new IP addresses

ip dhcp snooping database tftp://192.168.100.10/hostname
ip dhcp snooping database write-delay 15
ip dhcp snooping database timeout 0

interface FastEthernet0/24
  ip dhcp snooping trust        ! set TRUNK ports as trusted
  ip dhcp snooping limit rate 100 ! limit the number of DHCP queries
```

Dynamic ARP Inspection

Problems with fake ARP packets generated in ARP Cache Poisoning attacks are quite frequent. The basic principle has been described above, in the chapter dealing with limiting numbers of MAC addresses connected to a single port. The DAI (Dynamic ARP Inspection) technology allows us to monitor ARP packets and compare them to the DHCP Snooping Binding table. ARP packets arriving to any port are dropped unless they match the MAC/IP address combination issued by the DHCP server upon request. The standard limit is 15 ARP packets per second, preventing attackers from finding the correct combination by brute force.

Similar to DHCP Snooping technology, ports may be set as trusted or untrusted. TRUNK ports should be trusted. Attacks are not expected from that direction, the switch is not required to gather all information on communication through that port, and unintentional blocking of traffic will be prevented. There may be devices with static IP configuration within the network, some of them even incapable of requesting IP addresses from DHCP. Their ports may be set as trusted or, even better, appropriate static records may be entered into the DHCP Snooping Binding Table.

Configuration Example:

```
ip arp inspection vlan 10, 20          ! Turn on inspection in selected VLANs

! Turn on inspection of source and target MAC and IP addresses
ip arp inspection validate src-mac dst-mac ip

int FastEthernet0/24
  ip arp inspection trust              ! Set TRUNK port as trusted
  ip arp inspection limit rate 5      ! Limit the number of ARP requests
```

IP Source Guard

The IP Source Guard technology is similar to DHCP Snooping and cannot work without DHCP Snooping active and correctly configured. In case IP Source Guard is required to work without DHCP Snooping, static records must be entered in the DHCP Snooping Binding table.

Example static configurations of the DHCP Snooping Binding table:

```
ip source binding <mac-address> vlan <vlan-id> <ip-address> interface <interface-id>
```

With IP Source Guard active, switch port initially only allows DHCP packets and blocks other traffic. Once an IP address is issued to the client, a record is made in the PVACL (per-port and VLAN Access Control List), declaring on what conditions a packet is allowed to pass through a port. The switch verifies IP and MAC addresses arriving to any port with IP Source Guard configured, and compares them to records in the DHCP Snooping Binding table, including port numbers.

This is done to prevent ICMP Redirect attacks, the use of IP addresses issued to computers on different ports, and the use of unissued IP addresses.

Configuration Example:

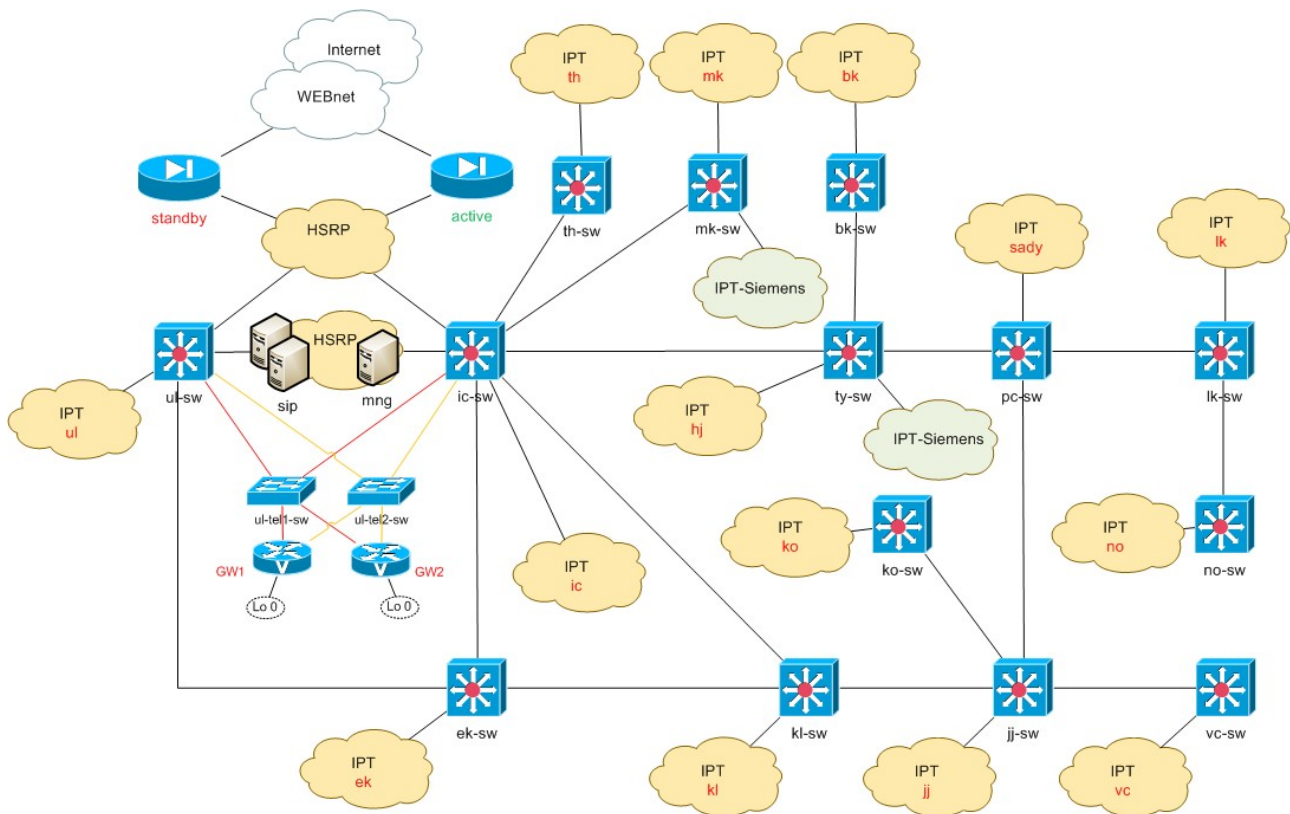
```
interface FastEthernet0/1
  ip verify source                    ! Activate IP Source Guard
```

FW ASA

The final step in VoIP security configuration consists in firewall setting. As explained above, there is a logically separated network used only by IP phones. However, such a network must be connected to other networks, including the Internet, in a safe fashion. That is why it needs to be protected at points implementing such connections.

There are multiple options available, one of them relying on Cisco ASA (Adaptive Security Appliance) firewall suitable to separate a VoIP network from other networks and the Internet. It may also serve as a VPN concentrator, providing secure remote access into the VoIP network. Cisco ASA also supports IPS (Intrusion Prevention System) consisting in in-depth inspection of all packets arriving to or from the VoIP network. Besides all that, Cisco ASA supports redundancy for uninterrupted operation.

An example of a dedicated VoIP network including virtual routers, voice gateways, SIP servers, and subnets with redundant connections to other networks through HSRP (Hot Standby Router Protocol):



Conclusion

The basic rule of security is preventing all known forms of attack, leaving nothing to chance. This is even more important in VoIP networks as their abuse may result in financial loss or compromising the reputation of a company or organization. More information including configuration example can be found at <http://sip.cesnet.cz>.