



<https://e-discovery.ng/>

INTERNAL NETWORK PENETRATION TESTING

Report for:

Date:

This document contains confidential information about IT systems and network infrastructure of the client, as well as information about potential vulnerabilities and methods of their exploitation. This confidential information is for internal use by the client only and shall not be disclosed to third parties.



Table of Contents

Table of Contents

Table of Contents	2
Executive Summary	3
Scope of Security Assessment	4
Methodology	6
Severity Definition	7
Summary of Findings	8
Key Findings	10
Possibility of MITM attack (Man in the middle)	10
Usage of the vulnerable Telnet Protocol	11
Unencrypted transmission over HTTP	12
Usage of weak login credentials to access the DB	13
No valid certificate	14
Data exchange between clients of the guest network	15
Weak MAC algorithms are used	16
Same passwords for Office and Management networks	17
Appendix A. Services and Open Network Ports	18
Appendix B. WiFi Testing	19
Networks for which handshake was intercepted	21
Appendix C. Testing Segmentation Tools	21



Executive Summary

E-Discovery (Consultant) was contracted by ____ (Client) to conduct the penetration testing of their internal network.

This report presents the findings of the security assessment of CLIENT's network conducted between February 04th, 2018 - February 22nd, 2018.

The main subject of the security assessment is CLIENT's internal network.

Penetration test has the following objectives:

- identify technical and functional vulnerabilities;
- estimate their severity level (ease of use, impact on information systems, etc);
- draw up a prioritized list of recommendations to address identified weaknesses.

According to our research after performing the penetration testing, security rating of CLIENT's infrastructure was identified as **Medium**.



Scope of Security Assessment

The testing area includes all client's systems located in the company's office.

Network segments, which are the entry point during testing, were agreed with the client. Based on existing documentation, the following network segments were selected: CLIENT11, CLIENT11, CLIENT11. During testing, an extension of the list of tested networks was agreed with the client and the following were added to it: CLIENT11, CLIENT11, CLIENT11. Wired and wireless WiFi connection can be used to connect to the network (SSIDs correspond to the names of the segments).

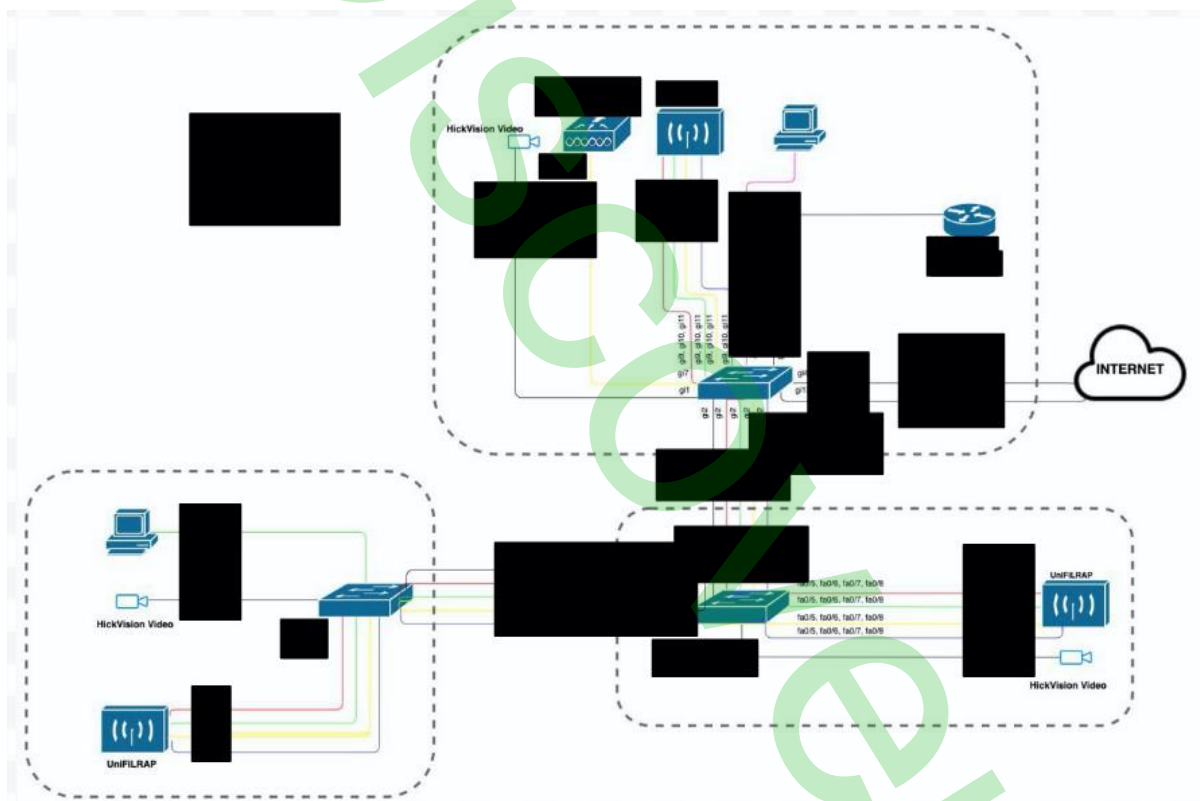


Figure 1 - Network diagram (provided by the client)



Table 1 - Subnet IP addresses (provided by the client)

vlan000	xxx.xxx.x.x
vlan000	xxx.xxx.x.x
vlan000	xxx.xxx.x.x
vlan000	xxx.xxx.x.x
vlan000	xxx.xxx.x.x
vlan000	xxx.xxx.x.x
vlan000	xxx.xxx.x.x

The network diagram and IP address table may differ from the actual network.



Methodology

The testing methodology is based on generally accepted industry-wide approaches to perform penetration testing for internal networks (NIST SP800-115, PTES, PCI Penetration Test Guidance).





Penetration tests include, at a minimum, checking for the following types of vulnerabilities:

- known vulnerabilities in operating systems and network components;
- using of insecure services;
- using of defaults credentials;
- vulnerable to MiTM components;
- testing to verify the effectiveness of segmentation tools;
- testing of WiFi network vulnerabilities.



Severity Definition

The level of criticality of each risk is determined based on the potential impact of loss from successful exploitation as well as ease of exploitation, existence of exploits in public access and other factors.

Severity	Description
High 	High-level vulnerabilities are easy to exploit and may provide an attacker with full control of the affected systems, also may lead to significant data loss or downtime. There are exploits or PoC available in public access.
Medium 	Medium-level vulnerabilities are much harder to exploit and may not provide the same access to affected systems. No exploits or PoCs available in public access. Exploitation provides only very limited access.
Low 	Low-level vulnerabilities provide an attacker with information that may assist them in conducting subsequent attacks against target information systems or against other information systems, which belong to an organization. Exploitation is extremely difficult, or impact is minimal.
Info 	These vulnerabilities are informational and can be ignored.

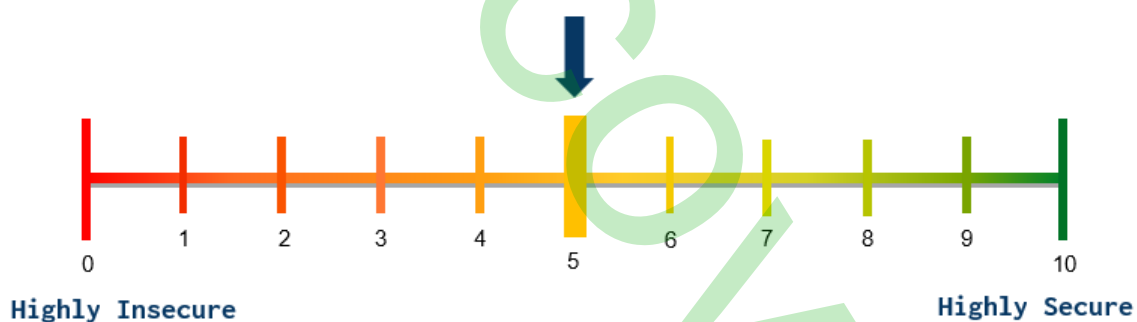


Summary of Findings

According to the following in-depth testing of the environment, CLIENT's infrastructure requires some improvements.

Value	Number of risks
High	3
Medium	1
Low	1
Info	3

Based on our understanding of the IT Infrastructure, as well as the nature of the vulnerabilities discovered, their exploitability, and the potential impact we have assessed the level of risk for your organization to be Medium.





Risk level	Vulnerabilities	Affected system	Recommendations
High	Possibility of MITM attack	All vlan	Use VPN and AV with arp-spoofing protection functionality
High	Usage of Telnet Protocol	xxx.xxx.x.x	Replace Telnet with SSH
High	Unencrypted transmission of information over HTTP	xxx.xxx.x.x xxx.xxx.x.x xxx.xxx.x.x xxx.xxx.x.x	Use HTTPS or SSH
Medium	Usage of weak login credentials to access the database	xxx.xxx.x.x	Change username and password. Enable Firewall for Developers' PCs
Low	No valid certificate	xxx.xxx.x.x xxx.xxx.x.x	Install a valid certificate
Info	Weak MAC algorithms are used	xxx.xxx.x.x	Disable weak MAC algorithms
Info	Same passwords for Office (network10) and Management (network12)	vlanxx, vlanxx	Change password for the network Management (network12)
Info	Successful interception of handshake from networks: "network101", "network10"	vlanxx, vlanxx	Use WPA2 Enterprise



Key Findings

■ ■ ■ ■ Possibility of MITM attack (Man in the middle)

#1	Description														
	MITM (man in the middle) - is a method of compromising a communication channel in which an attacker, having connected to the channel between contractors, interferes in the transmission protocol, deleting or distorting information.														
Evidence															
<table><tr><th>Client</th><th>Server</th><th>Protocol</th><th>Username</th><th>Password</th><th>Valid login</th><th>Login timestamp</th></tr><tr><td colspan="7"></td></tr></table> <p>0 hosts added to the hosts list...</p> <p>DHCP:</p> <p>ARP poisoning victims:</p> <p>GROUP 1 : ANY (all the hosts in the list)</p> <p>GROUP 2 : ANY (all the hosts in the list)</p> <p>HTTP:</p> <p>HTTP:</p> <p>HTTP:</p> <p>HTTP:</p>		Client	Server	Protocol	Username	Password	Valid login	Login timestamp							
Client	Server	Protocol	Username	Password	Valid login	Login timestamp									
Recommendations															
<ul style="list-style-type: none">• Use VPN and AV with arp-spoofing protection functionality															



■ ■ ■ ■ Usage of the vulnerable Telnet Protocol

#2Description


The Telnet service is launched on the remote host, which transmits the username and password in unencrypted form. An attacker could reveal login names and passwords by listening to traffic in the Telnet service.

Evidence


Location:

vlan00 -> ipv4:xxx.xxx.x.x, mac:xx:xx:xx:xx:xx:xx (Cisco Systems)

vlan00 -> ipv4:xxx.xxx.x.x, mac:xx:xx:xx:xx:xx:xx (Cisco Systems)



Result: Telnet Unencrypted Cleartext Login

Vulnerability	Severity	QoD	Host	Location	Actions
Telnet Unencrypted Cleartext Login	4.8 (Medium)	70%		23/tcp (IANA: telnet)	

Summary

The remote host is running a Telnet service that allows cleartext logins over unencrypted connections.


Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

An attacker can uncover login names and passwords by sniffing traffic to the Telnet service.

Solution

Solution type:  Mitigation

Replace Telnet with a protocol like SSH which supports encrypted connections.

Vulnerability Detection Method

Details: Telnet Unencrypted Cleartext Login








Version used: 2019-06-06T07:39:31+0000

Recommendations

- Replace Telnet with SSH, which supports encrypted connections.

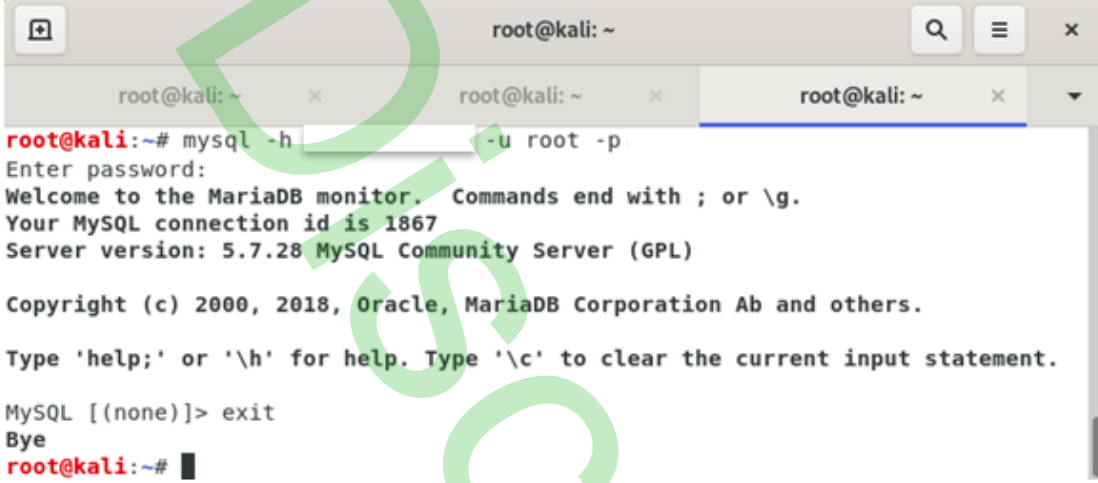


■ ■ ■ ■ Unencrypted transmission over HTTP

#3	Description												
<p>An attacker could use this situation to compromise or eavesdrop on an HTTP connection between a client and server using the man in the middle attack to gain access to sensitive data, such as usernames or passwords</p>													
<h4>Evidence</h4> <p>Location:</p> <pre>vlan00 -> ipv4:xxx.xxx.x.x, mac:xx:xx:xx:xx:xx:xx (Cisco Systems) vlan00 -> ipv4:xxx.xxx.x.x, mac:xx:xx:xx:xx:xx:xx (Cisco Systems) vlan00 -> ipv4:xxx.xxx.x.x, mac:xx:xx:xx:xx:xx:xx (D-Link) vlan00 -> ipv4:xxx.xxx.x.x, mac:xx:xx:xx:xx:xx:xx (DrayTek)</pre>													
<div>  Result: Cleartext Transmission of Sensitive Information via HTTP </div>													
<table border="1"> <thead> <tr> <th>Vulnerability</th> <th>Severity</th> <th>QoD</th> <th>Host</th> <th>Location</th> <th>Actions</th> </tr> </thead> <tbody> <tr> <td>Cleartext Transmission of Sensitive Information via HTTP</td> <td>4.8 (Medium)</td> <td>80%</td> <td></td> <td>80/tcp</td> <td> </td> </tr> </tbody> </table>		Vulnerability	Severity	QoD	Host	Location	Actions	Cleartext Transmission of Sensitive Information via HTTP	4.8 (Medium)	80%		80/tcp	 
Vulnerability	Severity	QoD	Host	Location	Actions								
Cleartext Transmission of Sensitive Information via HTTP	4.8 (Medium)	80%		80/tcp	 								
<p>Summary The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.</p>													
<p>Vulnerability Detection Result The following URLs requires Basic Authentication (URL:realm name): http:// /:"level 15 access"</p>													
<p>Links:</p>													
<h4>Recommendations</h4> <ul style="list-style-type: none"> Use encrypted HTTPS traffic or use SSH 													










Usage of weak login credentials to access the DB

#4	Description
	We managed to login as root with the password "123456".
	Evidence <p>Location: vlan00 -> ipv4:x.xx, mac:00:00:00:00:00:00 (Apple)</p>  <p>Recommendations</p> <ul style="list-style-type: none"> • Set a non-standard username and change password to strong one • Enable Firewall for Developers' PCs



■ ■ No valid certificate

#5	Description												
	The certificate has expired.												
Evidence Location: vlan00 -> ipv4:xx.x.xx.xx, mac:xx:xx:xx:xx:xx:xx (Ubiquiti Networks) vlan00 -> ipv4:xxx.xxx.x.xx, mac:xx:xx:xx:xx:xx:xx (Apple)													
 Result: SSL/TLS: Certificate Expired													
<table border="1"> <thead> <tr> <th>Vulnerability</th> <th>Severity</th> <th>QoD</th> <th>Host</th> <th>Location</th> <th>Actions</th> </tr> </thead> <tbody> <tr> <td>SSL/TLS: Certificate Expired</td> <td>5.0 (Medium)</td> <td>99%</td> <td></td> <td>443/tcp</td> <td> </td> </tr> </tbody> </table>	Vulnerability	Severity	QoD	Host	Location	Actions	SSL/TLS: Certificate Expired	5.0 (Medium)	99%		443/tcp	 	<p>Summary The remote server's SSL/TLS certificate has already expired.</p> <p>Vulnerability Detection Result The certificate of the remote service expired on 2020-01-02 00:03:10.</p> <p>Certificate details: subject ...: L=San Jose,ST=CA,C=US subject alternative names (SAN): None issued by .: serial: valid from : valid until: fingerprint fingerprint</p>
Vulnerability	Severity	QoD	Host	Location	Actions								
SSL/TLS: Certificate Expired	5.0 (Medium)	99%		443/tcp	 								
Recommendations <ul style="list-style-type: none"> Install a valid certificate 													










■ Data exchange between clients of the guest network

#6	Description
	Possibility of data exchange between clients of the guest network
	Evidence Location: vlan23 -> ipv4: <input type="text"/> , SSID: network101 <pre>root@kali:~# ping <input type="text"/></pre> <div style="border: 1px solid #ccc; height: 60px; margin: 5px 0;"></div> <pre>2 packets transmitted, 2 received, 0% packet loss, time 1001ms rtt min/avg/max/mdev = 160.071/174.265/188.460/14.194 ms root@kali:~# ping <input type="text"/></pre> <div style="border: 1px solid #ccc; height: 60px; margin: 5px 0;"></div> <pre>2 packets transmitted, 2 received, 0% packet loss, time 1002ms rtt min/avg/max/mdev = 44.588/55.741/66.894/11.153 ms</pre>
	Recommendations <ul style="list-style-type: none"> • Disable the Client <u>I</u>o Client Forwarding parameter in vlan00



■ Weak MAC algorithms are used

#7	Description												
	The following weak client-server MAC algorithms are supported by the remote service: HMAC-md0, HMAC-MD0-00, HMAC-SHA0-00.												
	Evidence Location: vlan00 -> ipv4:xx.x.xx.xxx, mac:xx:xx:xx:xx:xx:xx (D-Link International)												
	 Result: SSH Weak MAC Algorithms Supported												
	<table border="1"> <thead> <tr> <th>Vulnerability</th> <th>Severity</th> <th>QoD</th> <th>Host</th> <th>Location</th> <th>Actions</th> </tr> </thead> <tbody> <tr> <td>SSH Weak MAC Algorithms Supported</td> <td>2.6 (Low)</td> <td>95%</td> <td></td> <td>22/tcp</td> <td> </td> </tr> </tbody> </table>	Vulnerability	Severity	QoD	Host	Location	Actions	SSH Weak MAC Algorithms Supported	2.6 (Low)	95%		22/tcp	 
Vulnerability	Severity	QoD	Host	Location	Actions								
SSH Weak MAC Algorithms Supported	2.6 (Low)	95%		22/tcp	 								
	Summary The remote SSH server is configured to allow weak MD5 and/or 96-bit MAC algorithms.												
	Vulnerability Detection Result The following weak client-to-server MAC algorithms are supported by the remote service: hmac- <input type="text"/> hmac- <input type="text"/> hmac- <input type="text"/>												
	Links:												
	Recommendations <ul style="list-style-type: none"> • Disable weak MAC algorithms 												



■ Same passwords for Office and Management networks

#8	Description
	Same passwords for Office and Management networks
Evidence	
	Office and Management passwords
Recommendations	
	<ul style="list-style-type: none">• Change password for the network Management (network00)



Appendix A. Services and Open Network Ports

At the time of testing, the following services were available in the WAN:

IP Address	Description	Open Ports	Status	Services	Version
000.000.000 .000	WAN-port Cisco	22/tcp	open	ssh	Cisco SSH 1.25
		23/tcp	open	telnet	Cisco IOS telnet
		2001/tcp	open	telnet	Cisco router telnetd
		4001/tcp	open	tcpwrapped	

Identified services and open network ports in landscape orientation here.



Appendix B. WiFi Testing

SSID	MAC Address	WPA/WPA2	WPS	Vendor
network101	xx:xx:xx:xx:xx:xx	PSK-CCMP		Ubiquiti Networks Inc.
network	xx:xx:xx:xx:xx:xx	PSK-(TKIP CCMP) PSK-(TKIP CCMP)		Netcore Technology Inc.
network	xx:xx:xx:xx:xx:xx	PSK-CCMP		Ubiquiti Networks Inc.
network	xx:xx:xx:xx:xx:xx	PSK-(TKIP CCMP)	1.0	ALFA. INC.
network	xx:xx:xx:xx:xx:xx	PSK-CCMP PSK-CCMP		MERCURY COMMUNICATION TECHNOLOGIES CO.LTD.
network	xx:xx:xx:xx:xx:xx	PSK-(TKIP CCMP) PSK-(TKIP CCMP)		
[Hidden]	xx:xx:xx:xx:xx:xx	PSK-CCMP		Ubiquiti Networks Inc.
Vending	xx:xx:xx:xx:xx:xx	PSK-CCMP PSK-CCMP		
network	xx:xx:xx:xx:xx:xx	PSK-CCMP	1.0	Routerboard.com
network	xx:xx:xx:xx:xx:xx	PSK-(TKIP CCMP) PSK-(TKIP CCMP)		
network	xx:xx:xx:xx:xx:xx	PSK-CCMP	1.0	TP-LINK TECHNOLOGIES CO.LTD.
network	xx:xx:xx:xx:xx:xx	MGT-(TKIP CCMP) MGT-(TKIP CCMP)		TP-LINK TECHNOLOGIES CO.LTD.
network	xx:xx:xx:xx:xx:xx	PSK-CCMP		ASUSTek COMPUTER INC.
network	xx:xx:xx:xx:xx:xx	PSK-CCMP	1.0	ASUSTek COMPUTER INC.
network	xx:xx:xx:xx:xx:xx	PSK-CCMP PSK-CCMP		



SSID	MAC Address	WPA/WPA2	WPS	Vendor
[Hidden]	XX:XX:XX:XX:XX:XX	PSK-CCMP		
[Hidden]	XX:XX:XX:XX:XX:XX	PSK-CCMP		
network	XX:XX:XX:XX:XX:XX	PSK-CCMP		Ubiquiti Networks Inc.
[Hidden]	0E:EC:DA:XX:XX:XX	PSK-CCMP		
[Hidden]	B6:FB:E4:XX:XX:XX	PSK-CCMP		Ubiquiti Networks Inc.
[Hidden]	0E:EC:DA:XX:XX:XX	MGT-CCMP		
network101	78:8A:20:XX:XX:XX	MGT-CCMP		Ubiquiti Networks Inc.
network	FC:EC:DA:XX:XX:XX	PSK-(TKIP CCMP) PSK-(TKIP CCMP)		Ubiquiti Networks Inc.
[Hidden]	2E:EC:DA:XX:XX:XX	PSK-CCMP		
network101	74:83:C2:XX:XX:XX	PSK-CCMP		Ubiquiti Networks Inc.
[Hidden]	FC:EC:DA:XX:XX:XX	PSK-CCMP		
[Hidden]	76:83:C2:XX:XX:XX	PSK-CCMP		Ubiquiti Networks Inc.
[Hidden]	B6:FB:E4::XX:XX:XX	PSK-CCMP		Ubiquiti Networks Inc.
network	FE:EC:DA:XX:XX:XX	PSK-(TKIP CCMP) PSK-(TKIP CCMP)		Ubiquiti Networks Inc.
network	FE:EC:DA:XX:XX:XX	PSK-(TKIP CCMP) PSK-(TKIP CCMP)		Ubiquiti Networks Inc.



Networks for which handshake was intercepted

MAC Address	SSID	Пароль
XX:XX:XX:XX:XX:XX	network10	*****
XX:XX:XX:XX:XX:XX	network10	*****
XX:XX:XX:XX:XX:XX	network101	*****
XX:XX:XX:XX:XX:XX	network101	*****
XX:XX:XX:XX:XX:XX	network101	*****
XX:XX:XX:XX:XX:XX	network101	*****
XX:XX:XX:XX:XX:XX	network12	*****

Appendix C. Testing Segmentation Tools

The penetration testing verifies that segmentation controls/methods are operational and effective according to existing network diagram.

---	vlan00	vlan01	vlan02	vlan03	vlan04	vlan05
vlan00	+	-	-	+	-	-
vlan01	-	+	-	-	-	-
vlan02	+	+	+	+	+	+
vlan03	-	-	-	+	-	-