

COUNTY OF



ALLEGHENY

RICH FITZGERALD
COUNTY EXECUTIVE

January 23, March 6 & March 13, 2018 Special Elections Experience Report

Contributors:

Gwen Abramowitz

John O'Brien

Kristin Perkoski

Ashley Smith

Larry Szurley

David Voyer

Mark Wolosik

JERRY TYSKIEWICZ, DIRECTOR

DEPARTMENT OF ADMINISTRATIVE SERVICES – DIVISION OF ELECTIONS
604 COUNTY OFFICE BUILDING • 542 FORBES AVENUE • PITTSBURGH, PA 15219
PHONE (412) 350-4500 • FAX (412) 350-5697 • WWW.ALLEGHENYCOUNTY.US

January 23, 2018 Special Election to fill the vacancy in the 35th State House due to the resignation of Marc Gergely

Of the 40,813 registered voters in the 35th State House District, 4,382 – 10.74%, voted at the January 23, 2018 Special Election. This level of turnout is consistent with previous “stand-alone” special elections.

A total of 76 absentee ballots were issued and no provisional ballots were cast.

8,000 “emergency” paper ballots were supplied to the 84 polling places in the event that at least one-half of the voting machines in a precinct were non-functional. No emergency ballots were used.

2 candidates appeared on the ballot.

March 6, 2018 Special Election to fill the vacancy in the 8th Pittsburgh Council District due to the resignation of Dan Gilman

Of the 31,982 registered voters in the 8th Pittsburgh Council District, 4,961 – 15.51%, voted at the past March 6, 2018 Special Election. This level of turnout is consistent with previous “stand-alone” special elections.

A total of 413 absentee ballots were issued. Neither of the 2 provisional ballots cast were counted, as the provisional voter was not registered to vote in the 8th District.

Over 6,400 “emergency” paper ballots were supplied to the 34 polling places in the event that at least one-half of the voting machines in a precinct were non-functional. No emergency ballots were used.

4 candidates appeared on the ballot.

March 13, 2018 Special Election to fill the vacancy in the 18th Congressional District due to the resignation of Tim Murphy

Of the 214,772 registered voters in the 18th Congressional District, 103,198 – 48.05%, voted at the past March 13, 2018 Special Election. This level of turnout is significantly higher than previous “stand-alone” special elections.

A total of 4,041 absentee ballots were issued and 131 provisional ballots were cast. Of the provisional ballots, 14 were fully counted, 29 partially counted and 88 were not counted. The majority of those not counted were due to the fact that the provisional voter was not a registered voter or not registered in the 18th District.

Over 42,000 “emergency” paper ballots were supplied to the 253 polling places in the event that at least one-half of the voting machines in a precinct were non-functional. No emergency ballots were used.

3 candidates appeared on the ballot.

Accessibility

All 1,322 polling places in this County have been classified as “accessible” pursuant to the standards promulgated by the Secretary of the Commonwealth of Pennsylvania.

Firmware Verification

Allegheny County employed the services of “GRP Consulting Group, LLC” on to verify that the software resident on the iVotronic voting devices contain the “trusted build” version certified by the Pennsylvania Department of State. As has been the case since 2008, no instance of uncertified software has been detected. Copies of the reports prepared from the February 7, 2018 firmware verification are contained in this report.

Logic and Accuracy Testing – January 23, 2018 Special Election

Automated and manual Logic and Accuracy Testing (L&A) was performed. Automated L&A was performed on all 168 iVotronic voting machines deployed on January 23, 2018. Manual L&A was also performed on the Special Election ballot. Those parties and organizations permitted by Pennsylvania law to be present during this process were duly notified.

The “test deck” comprised of over 420 ballots, containing ballots for every candidate, was used to verify that the ES&S Model 650 high-speed ballot counters would accurately count the absentee, provisional and emergency optical scan paper ballots to be used at the special election. This test was conducted prior to Election day as well as before final certification of the election results. In both tests, the ballot scanners produced an accurate count. Public notice of the pre-election test was given, as required by law.

Logic and Accuracy Testing – March 6, 2018 Special Election

Automated and manual Logic and Accuracy Testing (L&A) was performed. Automated L&A was performed on all 92 iVotronic voting machines deployed on March 6, 2018. Manual L&A was also performed on the Special Election ballot. Those parties and organizations permitted by Pennsylvania law to be present during this process were duly notified.

The “test deck” comprised of over 408 ballots, containing ballots for every candidate, was used to verify that the ES&S Model 650 high-speed ballot counters would accurately count the absentee, provisional and emergency optical scan paper ballots to be used at the special election. This test was conducted prior to Election day as well as before final certification of the election results. In both tests, the ballot scanners produced an accurate count. Public notice of the pre-election test was given, as required by law

Logic and Accuracy Testing – March 13, 2018 Special Election

Automated and manual Logic and Accuracy Testing (L&A) was performed. Automated L&A was performed on all 673 iVotronic voting machines deployed on March 13, 2018. Manual L&A was also performed on the Special Election ballot. Those parties and organizations permitted by Pennsylvania law to be present during this process were duly notified.

The “test deck” comprised of over 1,265 ballots, containing ballots for every candidate, was used to verify that the ES&S Model 650 high-speed ballot counters would accurately count the absentee, provisional and emergency optical scan paper ballots to be used at the special election. This test was conducted prior to Election day as well as before final certification of the election results. In both tests, the ballot scanners produced an accurate count. Public notice of the pre-election test was given, as required by law

Network Security

Also following past practice, an independent third-party review was conducted both prior to and after each of the Special Elections to assure that our election network was isolated and not connected to any external network. Copies of the reports produced by “Solutions 4 Networks” are contained in this report.

Parallel Testing

Since the November 2006 Election, Allegheny County has employed a Certified Public Accounting firm to ensure that the functionality of the iVotronic voting machine devices have not been compromised. The parallel testing performed at each of the Special Elections indicated that the randomly-selected voting devices recorded and counted all votes completely and correctly. Copies of the reports issued by “Baker Tilly” are contained in this report.

GRP Consulting Group, LLC

4915 Twin Lakes Rd

Suite 15

Boulder, Colorado 80301

tel: 303/249-0445



GRP Consulting Group, LLC

***ALLEGHENY COUNTY PRE MARCH SPECIAL
ELECTIONS AND THE MAY 15, 2018 PRIMARY
ELECTION
ES&S IVOTRONICS FIRMWARE VERIFICATION
STUDY***

EXECUTIVE SUMMARY

Developed for:

***ALLEGHENY COUNTY
DIVISION OF ELECTIONS
STATE OF PENNSYLVANIA***

Document Number GCG-AC-iVo-FRPT-000236

TABLE OF CONTENTS

1. INTRODUCTION: ALLEGHENY COUNTY ES&S IVOTRONICS FIRMWARE VERIFICATION STUDY	2
1.1 APPROACH.....	2
1.1.1 <i>Study's Focus</i>	2
1.1.2 <i>Study's Concentration</i>	2
1.1.3 <i>Study's Phases</i>	2
2. FINDINGS	4

1. INTRODUCTION: ALLEGHENY COUNTY ES&S iVOTRONICS FIRMWARE VERIFICATION STUDY

The Allegheny County, Pennsylvania Division of Elections requested GRP Consulting Group to audit and verify the firmware source code on twenty (20) ES&S iVotronic DRE voting machines before conducting the March Special Elections and the May 15, 2018 Primary Election. The devices to be audited were randomly selected from the counties 4700 devices. The purpose was to verify that the samples have in residence on the U1 designated Electronic Erasable Programmable Read Only Memory (EEPROM) chip the firmware version 9.1.4.1 and that all applied firmware versions are accurate and true to the State of Pennsylvania's Trusted Build as held in escrow by the Secretary of State's Office in Harrisburg. The study was accomplished by applying the 'Allegheny County iVotronic Firmware Verification Protocol' and was performed on location at the Allegheny County Division of Elections warehouse; located at 901 Pennsylvania Ave., Pittsburgh, Pennsylvania. GRP Consulting Group and Allegheny County staff performed this firmware audit on February 7, 2018.

It is the finding of GRP Consulting Group that the firmware verification audit applied to the resident code on the sample population was found to be unaltered versions of the 9.1.4.1 firmware.

1.1 Approach

1.1.1 Study's Focus

The focus of the exercise was:

1. Implementation of a fair and statically correct random selection process.
2. Deploy the verification protocol, known as the 'Allegheny County iVotronic Firmware Verification Protocol', to verify on twenty (20) randomly chosen ES&S iVotronics DRE voting devices that they hold in residence on the U1 designated EEPROM chip the exact, true and unaltered version of the 9.1.4.1 certified firmware source code as held in escrow at the Secretary of State's office.

1.1.2 Study's Concentration

The GRP Consulting Group analyst was tasked to independently apply a repeatable and validated verification protocol to verify that the ES&S firmware version 9.1.4.1 that resides in escrow by the Secretary of State's office and is resident on the Allegheny County iVotronic Direct-Recording Entry (DRE) - touch screen voting devices – are exact, true and unaltered versions of the certified firmware source code.

1.1.3 Study's Phases

GRP Consulting Group organized the project primary phases, each incorporating the flexibility to accommodate additional requirements, as they may have become known. The general strategy employed was comprised of the following aspects:

1. Setup, configure and control the verification environment and the parameters associated with each verification cycle;
2. Apply the SHA256 algorithm to verify that before the March Special Elections and the May 15, 2018 Primary Election the 9.1.4.1 firmware on the iVotronic DREs is the true and certified version of the firmware and has not been altered;
3. Execute twenty (20) verification cycles;
4. Conduct reviews and analyses of all verification results and anomalies obtained during the twenty (20) verification execution cycles;
5. Advise the County on possible root cause(s) of any and all anomalies; and
6. Prepare and deliver a report of the verification activities, the results of all verification executions, and conclusions and recommendations in Executive Summary and Final Report formats.

2. FINDINGS

GRP Consulting Group was engaged by the Allegheny Division of Elections on site at 901 Pennsylvania Ave., Pittsburgh, PA on February 7, 2018; the purpose of the engagement was to apply the 'Allegheny County iVotronic Firmware Verification Protocol' to verify the ES&S iVotronic firmware version 9.1.4.1 is resident on the Allegheny County iVotronic population.

On February 7, 2018, the GRP Consulting Group analyst completed the verification process of the firmware on twenty (20) Allegheny County iVotronics chosen at random from the population of approximately 4700 machines. It is the findings of GRP Consulting Group that the firmware version 9.1.4.1 residing on the twenty (20) randomly chosen machines, do represent the population, and furthermore, that the firmware version as resident on the U1 designated Electronic Erasable Programmable Read Only Memory (EEPROM) chip is an exact, true, and unaltered version of the NVLAP federally certified trusted build as held in archive at SysTest Labs and in escrow by the Pennsylvania Secretary of State in Harrisburg, PA.

County of Allegheny

January 2018 Pre/**Post**-Election Air Gap Analysis of Election Tabulation Network

Research and Recommendations Provided by:



a network infrastructure company

Prepared by:
Jacob Winkle
Senior Consulting Engineer
jwinkle@s4nets.com
(412) 626-3147



Contents

Overview.....	2
Site Contacts	2
General Physical Security/Building Access	2
Physical Security/Building Access - No Issues Found	2
Election Tabulations Network.....	6
Network Overview.....	6
Network Overview - Logical	7
Network Overview - Physical	9
External Connections on Client Devices	81
No Wireless Adapters or Bluetooth Capability Found on Client Devices	82
No Wireless Keyboards and Mice.....	82
Network Air Gap Analysis	82
Air Gap Network Intact - Recommendations for Improvement	82
Client Operating Systems – Update the Clients to a supported OS.	83
Server Operating System – Update the Server Operating System.....	83
Remote Assistance Enabled.....	83
Remote Desktop is Enabled.	83
Windows Update Enabled/None Selected.....	83
Lock Physical Access to the Dell PowerConnect 2716.....	83
Remove the Default Gateway Option.....	83



Overview

The County of Allegheny has engaged solutions4networks to perform a network air gap analysis of their elections tabulation network located in Pittsburgh, PA. An **air gap, air wall** or **air gapping** is a network security measure employed on one or more computers to ensure that a secure computer network is physically isolated from unsecured networks, such as the public Internet or an unsecured local area network. solutions4networks has been tasked to verify the tabulation network is a stand-alone, isolated network and to assess the networks' vulnerability to external access and/or tampering. In addition to the network, solutions4network has been asked to assess and document the general physical security of the warehouse building.

A pre-election onsite visit was made Jacob Winkle of solutions4networks on January 22, 2018. The purpose of this document is to report the results of the assessment, identify security concerns and to make recommendations for the remediation of these concerns. A post-Election onsite visit was made on January 25, 2018. This report covers both the Pre-Election assessment and the **Post-Election review**. Post-Election Review updates will be noted in **red**.

Site Contacts

Elizabeth Dell
Elizabeth.Dell@AlleghenyCounty.US
412-350-6059

Robin Gigliotti
Robin.Gigliotti@AlleghenyCounty.US
412-350-6647

901 Pennsylvania Avenue
Pittsburgh, PA 15233

General Physical Security/Building Access

Physical Security/Building Access - No Issues Found

There are several suites within the warehouse and there were no outside signs, which identified that it was County of Allegheny building space. The building phone at the main entrance also did not have any entries to dial for the County of Allegheny.

Building Main Entrance:



Suite 901:



1/22/2018 - solutions4networks engineer, Jacob Winkle, was met at suite 901 by Elizabeth Dell and was asked to provide a valid driver's license as identification before access to the building was granted.



1/25/2018 - solutions4networks engineer, Jacob Winkle, was met at suite 901 by Elizabeth Dell and was asked to provide a driver's license identification before access to the building was granted.

Entrance from the street required badge card access or a key. The first door in the warehouse required a security code, but it was a physical, non-electronic lock.

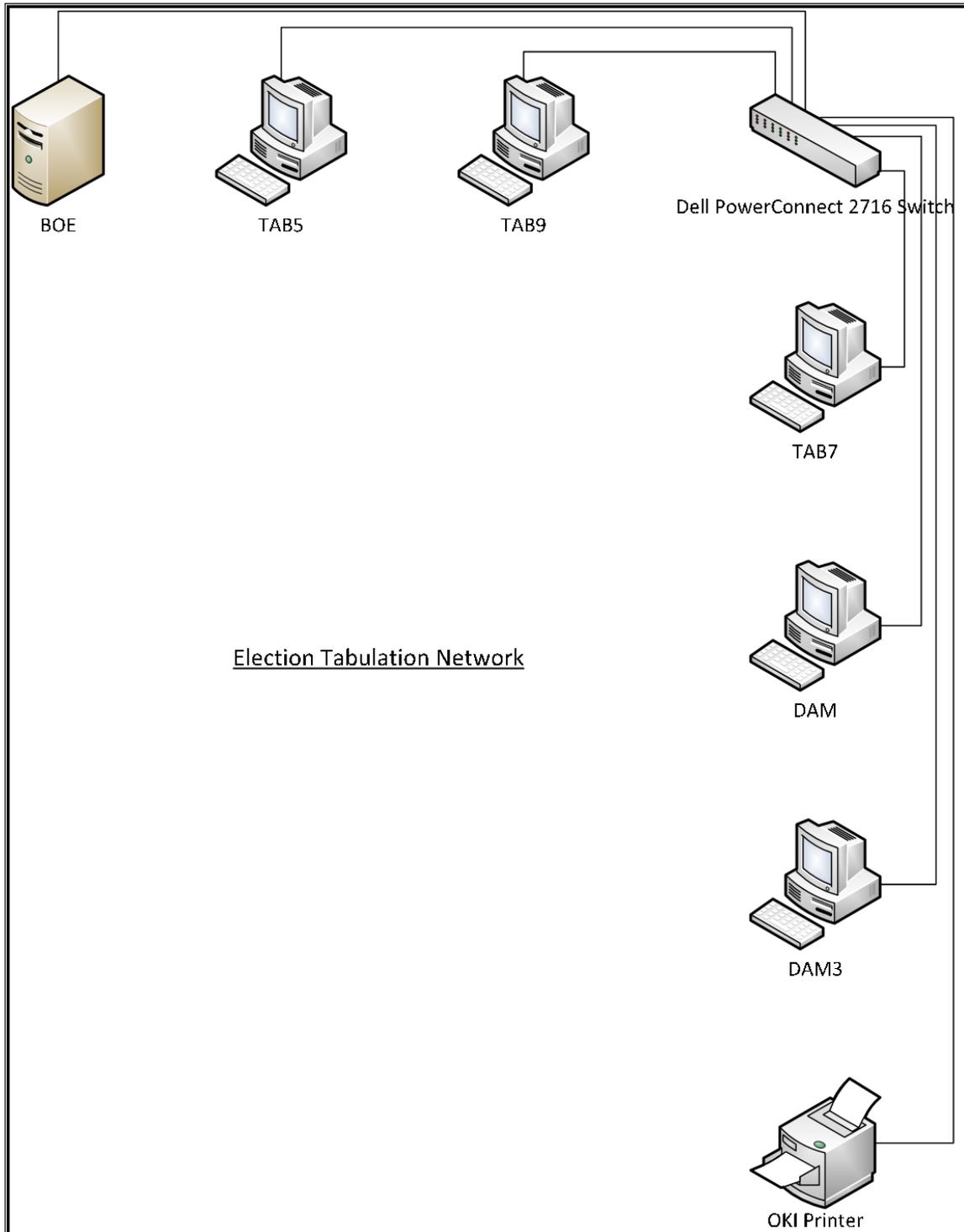
Security cameras were observed over the street entrance and inside the computer room. There is a sign in the tabulation network room that states "No Cell Phones are Permitted".

Physical Post-Election Review: All items indicated above remained the same.

Election Tabulations Network

Network Overview

The solutions4networks engineer created the following network drawing based off the observed finding from the onsite physical inspections performed during the air gap analysis.





The Election Tabulation Network consisted of the following devices:

- 1 Dell PowerConnect 2716 Ethernet Switch
- 1 Windows Server
- 5 Client PC's
 - Two DAM (Dial Access Modem) Servers
 - 3 Windows XP Clients
- 1 Printer

Network Overview - Logical

All the devices had an address from RFC1918 private network 192.168.1.0/24. The Windows Server with address 192.168.1.20 provided DHCP, DNS and WINS services. A default gateway of 192.168.1.1 was configured, but no such device was found on the network. All devices on the network could ping each other so the network was fully self-contained and each node was accessible to one another.

Post-Election Review: All items indicated above remained the same.

Dell Server PE-SC1420	Dell Optiplex 790	Dell Optiplex 790	Dell Optiplex 790	Dell Precision 890	Dell Optiplex 790	Okidata Printer B6300
BOE.elections.local	TAB5.elections.local	TAB9.elections.local	TAB7.elections.local	DAM.elections.local	DAM3.elections.local	
provides DHCP, WINS, DNS Services	DHCP enabled	DHCP enabled	DHCP enabled	static	DHCP enabled/	DHCP Reserved
Win2003 SP1	Win XP Pro ver 2002 SP3	Win XP Pro ver 2002 SP3	Win XP Pro ver 2002 SP3	WinXP SP3	WinXP SP3	
Dell Server PESC1420						
intel Xeon CPU 3.20 GHZ	Intel core i5-2400 CPU 3.1 GHz	Intel core i5-2400 CPU 3.1 GHz	Intel core i5-2400 CPU 3.1 GHz	Intel Xeon 5110@1.60GHz		
3.19 GHz 2.00 GB RAM	3.09 GHZ, 3.16 GB Ram	3.09 GHZ, 3.16 GB Ram	3.09 GHZ, 3.16 GB Ram	1.60 GHz, 2.00 GB Ram		
2GB Ram	4 GB Ram	4 GB Ram	4 GB Ram	2 GB Ram	2 GB Ram	
IP: 192.168.1.20 (static)	IP: 192.168.1.24	IP: 192.168.1.18	IP: 192.168.1.40	IP: 192.168.1.101	IP: 192.168.1.41	IP: 192.168.1.50
netmask: 255.255.255.0	netmask: 255.255.255.0	netmask: 255.255.255.0	netmask: 255.255.255.0	netmask: 255.255.255.0	netmask: 255.255.255.0	netmask: 255.255.255.0
gateway: 192.168.1.1	gateway: 192.168.1.1 (doesn't exist)	gateway: 192.168.1.1 (doesn't exist)	gateway: 192.168.1.1 (doesn't exist)		gateway: 192.168.1.1 (doesn't exist)	
DNS: 192.168.1.20	DHCP Server: 192.168.1.20	DHCP Server: 192.168.1.20	DHCP Server: 192.168.1.20		DHCP Server: 192.168.1.20	
WINS: 192.168.1.20	DNS Server: 192.168.1.20	DNS Server: 192.168.1.20	DNS Server: 192.168.1.20	DNS Server: 192.168.1.20	DNS Server: 192.168.1.20	
	Wins Server: 192.168.1.20	Wins Server: 192.168.1.20	Wins Server: 192.168.1.20			
Conexant 56k modem						
wired keyboard	wired keyboard	wired keyboard	wired keyboard	wired keyboard	wired keyboard	
wired mouse	wired mouse	wired mouse	wired mouse	wired mouse	wired mouse	
3.5 floppy disk						
cd drive	RW/DVD	RW/DVD	RW/DVD	RW/DVD	RW/DVD	
tape drive				lomega Zip 250		
com1/com2	com1/com3	com1/com3	com1/com3	com1-10	com1/com2	
Dell PowerVault 100T DAT72						
Intel Pro 1000 MT LAN connection	Gigabit LAN connection	Gigabit LAN connection	Gigabit LAN connection	Broadcom Gigabit Controller		
Remote Desktop Enabled. Allowed users ELECTIONS\SBS Remote Operators	Remote Assistance is enabled	Remote Assistance is enabled	Remote Assistance is enabled	Remote Assistance is enabled	Remote Assistance is enabled	
	RDP disabled	RDP disabled	RDP disabled	RDP disabled	RDP disabled	
	connected to printer	connected to printer	connected to printer	connected to printer		



Network Overview - Physical

Each device on the network was inspected Pre- and Post-election for physical attachments and are noted below.

BOE.elections.local

Front: 2 USB ports - empty

1 Tape Drive – empty

1 CD/RW – empty

Rear: 1 USB – empty

1 USB connection on rear has a connection to a USB Seagate backup portable drive

2 serial/com ports – empty

1 LPT port – empty

PS2 Mouse/Keyboard

VGA port to monitor

LAN connection to Dell Switch

Additional Information Collected from CLI:

C:\>hostname

BOE

C:\>whoami

elections\administrator

C:\>ipconfig /all

Windows IP Configuration

Host Name : BOE



Primary Dns Suffix : elections.local
Node Type : Hybrid
IP Routing Enabled. : No
WINS Proxy Enabled. : No
DNS Suffix Search List. : elections.local

Ethernet adapter Server LAN NIC:

Connection-specific DNS Suffix . :
Description : Intel(R) PRO/1000 MT Network Connection
Physical Address. : 00-14-22-60-3F-94
DHCP Enabled. : No
IP Address. : 192.168.1.20
Subnet Mask : 255.255.255.0
Default Gateway : 192.168.1.1
DNS Servers : 192.168.1.20
Primary WINS Server : 192.168.1.20

C:\>arp -a

No ARP Entries Found

C:\>netstat -rn

IPv4 Route Table

=====



Interface List

0x1 MS TCP Loopback interface

0x10003 ...00 14 22 60 3f 94 Intel(R) PRO/1000 MT Network Connection

=====
=====

Active Routes:

Network	Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.20	10
127.0.0.0	255.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
192.168.1.0	255.255.255.0	255.255.255.0	192.168.1.20	192.168.1.20	10
192.168.1.20	255.255.255.255	255.255.255.255	127.0.0.1	127.0.0.1	10
192.168.1.255	255.255.255.255	255.255.255.255	192.168.1.20	192.168.1.20	10
224.0.0.0	240.0.0.0	240.0.0.0	192.168.1.20	192.168.1.20	10
255.255.255.255	255.255.255.255	255.255.255.255	192.168.1.20	192.168.1.20	1

Default Gateway: 192.168.1.1

=====

Persistent Routes:

None

C:\>netstat -an

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:25	0.0.0.0:0	LISTENING



TCP	0.0.0.0:42	0.0.0.0:0	LISTENING
TCP	0.0.0.0:53	0.0.0.0:0	LISTENING
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING
TCP	0.0.0.0:88	0.0.0.0:0	LISTENING
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:389	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:464	0.0.0.0:0	LISTENING
TCP	0.0.0.0:593	0.0.0.0:0	LISTENING
TCP	0.0.0.0:636	0.0.0.0:0	LISTENING
TCP	0.0.0.0:691	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1026	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1027	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1068	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1074	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1075	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1076	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1078	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1081	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1097	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1100	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1142	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1171	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1173	0.0.0.0:0	LISTENING
TCP	0.0.0.0:2160	0.0.0.0:0	LISTENING



TCP	0.0.0.0:2161	0.0.0.0:0	LISTENING
TCP	0.0.0.0:2260	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3052	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3268	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3269	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3389	0.0.0.0:0	LISTENING
TCP	0.0.0.0:6001	0.0.0.0:0	LISTENING
TCP	0.0.0.0:6002	0.0.0.0:0	LISTENING
TCP	0.0.0.0:6004	0.0.0.0:0	LISTENING
TCP	0.0.0.0:6358	0.0.0.0:0	LISTENING
TCP	0.0.0.0:6548	0.0.0.0:0	LISTENING
TCP	0.0.0.0:8081	0.0.0.0:0	LISTENING
TCP	0.0.0.0:10000	0.0.0.0:0	LISTENING
TCP	0.0.0.0:34571	0.0.0.0:0	LISTENING
TCP	0.0.0.0:34572	0.0.0.0:0	LISTENING
TCP	0.0.0.0:34573	0.0.0.0:0	LISTENING
TCP	127.0.0.1:389	127.0.0.1:59187	ESTABLISHED
TCP	127.0.0.1:1090	127.0.0.1:389	CLOSE_WAIT
TCP	127.0.0.1:1109	127.0.0.1:389	CLOSE_WAIT
TCP	127.0.0.1:1158	127.0.0.1:389	CLOSE_WAIT
TCP	127.0.0.1:53851	127.0.0.1:389	CLOSE_WAIT
TCP	127.0.0.1:59187	127.0.0.1:389	ESTABLISHED
TCP	192.168.1.20:135	192.168.1.20:1175	ESTABLISHED
TCP	192.168.1.20:135	192.168.1.20:2420	ESTABLISHED
TCP	192.168.1.20:135	192.168.1.20:2422	ESTABLISHED



TCP	192.168.1.20:139	0.0.0.0	LISTENING
TCP	192.168.1.20:389	192.168.1.20:2166	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:2362	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:2379	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:2424	TIME_WAIT
TCP	192.168.1.20:389	192.168.1.20:2425	TIME_WAIT
TCP	192.168.1.20:389	192.168.1.20:2426	TIME_WAIT
TCP	192.168.1.20:389	192.168.1.20:2429	TIME_WAIT
TCP	192.168.1.20:389	192.168.1.20:2430	TIME_WAIT
TCP	192.168.1.20:389	192.168.1.20:59174	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:59175	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:59178	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:59179	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:59181	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:59182	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:59186	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:59192	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:59193	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:59194	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:59195	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:59196	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:59197	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:59198	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:59200	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:59201	ESTABLISHED



TCP	192.168.1.20:445	192.168.1.41:1081	ESTABLISHED
TCP	192.168.1.20:691	192.168.1.20:1112	ESTABLISHED
TCP	192.168.1.20:691	192.168.1.20:1169	ESTABLISHED
TCP	192.168.1.20:691	192.168.1.20:53854	ESTABLISHED
TCP	192.168.1.20:1026	192.168.1.20:1108	ESTABLISHED
TCP	192.168.1.20:1026	192.168.1.20:1206	ESTABLISHED
TCP	192.168.1.20:1026	192.168.1.20:1356	ESTABLISHED
TCP	192.168.1.20:1026	192.168.1.20:1365	ESTABLISHED
TCP	192.168.1.20:1026	192.168.1.20:2416	ESTABLISHED
TCP	192.168.1.20:1026	192.168.1.20:2423	ESTABLISHED
TCP	192.168.1.20:1093	192.168.1.20:389	CLOSE_WAIT
TCP	192.168.1.20:1108	192.168.1.20:1026	ESTABLISHED
TCP	192.168.1.20:1111	192.168.1.20:389	CLOSE_WAIT
TCP	192.168.1.20:1112	192.168.1.20:691	ESTABLISHED
TCP	192.168.1.20:1130	192.168.1.20:389	CLOSE_WAIT
TCP	192.168.1.20:1159	192.168.1.20:389	CLOSE_WAIT
TCP	192.168.1.20:1169	192.168.1.20:691	ESTABLISHED
TCP	192.168.1.20:1175	192.168.1.20:135	ESTABLISHED
TCP	192.168.1.20:1206	192.168.1.20:1026	ESTABLISHED
TCP	192.168.1.20:1356	192.168.1.20:1026	ESTABLISHED
TCP	192.168.1.20:1365	192.168.1.20:1026	ESTABLISHED
TCP	192.168.1.20:1899	192.168.1.20:389	CLOSE_WAIT
TCP	192.168.1.20:1914	192.168.1.20:389	CLOSE_WAIT
TCP	192.168.1.20:1917	192.168.1.20:3268	CLOSE_WAIT
TCP	192.168.1.20:2166	192.168.1.20:389	ESTABLISHED



TCP	192.168.1.20:2362	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:2379	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:2415	192.168.1.20:135	TIME_WAIT
TCP	192.168.1.20:2416	192.168.1.20:1026	ESTABLISHED
TCP	192.168.1.20:2420	192.168.1.20:135	ESTABLISHED
TCP	192.168.1.20:2421	192.168.1.20:135	TIME_WAIT
TCP	192.168.1.20:2422	192.168.1.20:135	ESTABLISHED
TCP	192.168.1.20:2423	192.168.1.20:1026	ESTABLISHED
TCP	192.168.1.20:2425	192.168.1.20:389	TIME_WAIT
TCP	192.168.1.20:2427	192.168.1.20:445	TIME_WAIT
TCP	192.168.1.20:2429	192.168.1.20:389	TIME_WAIT
TCP	192.168.1.20:2430	192.168.1.20:389	TIME_WAIT
TCP	192.168.1.20:3268	192.168.1.20:59180	ESTABLISHED
TCP	192.168.1.20:3268	192.168.1.20:59183	ESTABLISHED
TCP	192.168.1.20:3268	192.168.1.20:59184	ESTABLISHED
TCP	192.168.1.20:3268	192.168.1.20:59185	ESTABLISHED
TCP	192.168.1.20:43188	192.168.1.20:389	CLOSE_WAIT
TCP	192.168.1.20:43189	192.168.1.20:3268	CLOSE_WAIT
TCP	192.168.1.20:53854	192.168.1.20:691	ESTABLISHED
TCP	192.168.1.20:59174	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:59175	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:59176	192.168.1.20:389	CLOSE_WAIT
TCP	192.168.1.20:59178	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:59179	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:59180	192.168.1.20:3268	ESTABLISHED



TCP	192.168.1.20:59181	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:59182	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:59183	192.168.1.20:3268	ESTABLISHED
TCP	192.168.1.20:59184	192.168.1.20:3268	ESTABLISHED
TCP	192.168.1.20:59185	192.168.1.20:3268	ESTABLISHED
TCP	192.168.1.20:59186	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:59192	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:59193	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:59194	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:59195	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:59196	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:59197	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:59198	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:59200	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:59201	192.168.1.20:389	ESTABLISHED
UDP	0.0.0.0:42	*.*	
UDP	0.0.0.0:135	*.*	
UDP	0.0.0.0:445	*.*	
UDP	0.0.0.0:500	*.*	
UDP	0.0.0.0:1035	*.*	
UDP	0.0.0.0:1065	*.*	
UDP	0.0.0.0:1072	*.*	
UDP	0.0.0.0:1082	*.*	
UDP	0.0.0.0:1101	*.*	
UDP	0.0.0.0:1132	*.*	



UDP	0.0.0.0:1172	*.*
UDP	0.0.0.0:1207	*.*
UDP	0.0.0.0:1434	*.*
UDP	0.0.0.0:2160	*.*
UDP	0.0.0.0:2161	*.*
UDP	0.0.0.0:3456	*.*
UDP	0.0.0.0:3457	*.*
UDP	0.0.0.0:4500	*.*
UDP	0.0.0.0:7846	*.*
UDP	0.0.0.0:38293	*.*
UDP	127.0.0.1:53	*.*
UDP	127.0.0.1:123	*.*
UDP	127.0.0.1:1064	*.*
UDP	127.0.0.1:1066	*.*
UDP	127.0.0.1:1083	*.*
UDP	127.0.0.1:1092	*.*
UDP	127.0.0.1:1102	*.*
UDP	127.0.0.1:1105	*.*
UDP	127.0.0.1:1141	*.*
UDP	127.0.0.1:1156	*.*
UDP	127.0.0.1:1163	*.*
UDP	127.0.0.1:1176	*.*
UDP	127.0.0.1:1185	*.*
UDP	127.0.0.1:1191	*.*
UDP	127.0.0.1:1200	*.*



UDP 127.0.0.1:1358 *.*
UDP 127.0.0.1:3456 *.*
UDP 127.0.0.1:3457 *.*
UDP 127.0.0.1:3979 *.*
UDP 127.0.0.1:14786 *.*
UDP 192.168.1.20:53 *.*
UDP 192.168.1.20:67 *.*
UDP 192.168.1.20:68 *.*
UDP 192.168.1.20:88 *.*
UDP 192.168.1.20:123 *.*
UDP 192.168.1.20:137 *.*
UDP 192.168.1.20:138 *.*
UDP 192.168.1.20:389 *.*
UDP 192.168.1.20:464 *.*
UDP 192.168.1.20:2535 *.*

C:\>systeminfo

Host Name: BOE
OS Name: Microsoft(R) Windows(R) Server 2003 for Small Business Server
OS Version: 5.2.3790 Service Pack 1 Build 3790
OS Manufacturer: Microsoft Corporation
OS Configuration: Primary Domain Controller
OS Build Type: Multiprocessor Free
Registered Owner: Allegheny County, PA



Registered Organization: Board of Elections

Product ID: 74995-OEM-4211904-03020

Original Install Date: 5/8/2006, 1:24:53 PM

System Up Time: 122 Days, 2 Hours, 37 Minutes, 25 Seconds

System Manufacturer: Dell Inc.

System Model: PowerEdge SC1420

System Type: X86-based PC

Processor(s): 2 Processor(s) Installed.

[01]: x86 Family 15 Model 4 Stepping 3 GenuineIntel ~ 3192 Mhz

[02]: x86 Family 15 Model 4 Stepping 3 GenuineIntel ~ 3192 Mhz

BIOS Version: DELL - 7

Windows Directory: C:\WINDOWS

System Directory: C:\WINDOWS\system32

Boot Device: \Device\HarddiskVolume2

System Locale: en-us;English (United States)

Input Locale: en-us;English (United States)

Time Zone: (GMT-05:00) Eastern Time (US & Canada)

Total Physical Memory: 2,046 MB

Available Physical Memory: 836 MB

Page File: Max Size: 3,435 MB

Page File: Available: 2,145 MB

Page File: In Use: 1,290 MB

Page File Location(s): C:\pagefile.sys

Domain: elections.local

Logon Server: \\BOE



Hotfix(s): 19 Hotfix(s) Installed.

[01]: File 1

[02]: File 1

[03]: File 1

[04]: File 1

[05]: File 1

[06]: File 1

[07]: File 1

[08]: File 1

[09]: File 1

[10]: Q147222

[11]: KB896358 - Update

[12]: KB896422 - Update

[13]: KB896424 - Update

[14]: KB896688 - Update

[15]: KB901214 - Update

[16]: KB902400 - Update

[17]: KB904706 - Update

[18]: KB908519 - Update

[19]: KB912919 - Update

Network Card(s): 1 NIC(s) Installed.

[01]: Intel(R) PRO/1000 MT Network Connection

Connection Name: Server LAN NIC

DHCP Enabled: No

IP address(es)



[01]: 192.168.1.20

C:\Documents and Settings\Administrator>

Post-Election Review: No Change

TAB5.elections.local

Front: 4 USB ports – empty

CD/RW - empty

Rear: 3 USB ports – empty

USB Keyboard

USB Mouse

VGA Monitor

Serial/COM connection to tabulation cartridge voter device

USB cable not connected to anything

LAN connection to Dell Switch

Additional Information Collected from CLI:

C:\>hostname

TAB5

C:\>ipconfig /all

Windows IP Configuration

Host Name : TAB5

Primary Dns Suffix : elections.local

Node Type : Hybrid

IP Routing Enabled. : No



WINS Proxy Enabled. : No
DNS Suffix Search List. : elections.local
elections.local

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : elections.local
Description : Intel(R) 82579LM Gigabit Network Con

nection

Physical Address. : 18-03-73-14-1C-2C
Dhcp Enabled. : Yes
Autoconfiguration Enabled : Yes
IP Address. : 192.168.1.11
Subnet Mask : 255.255.255.0
Default Gateway : 192.168.1.1
DHCP Server : 192.168.1.20
DNS Servers : 192.168.1.20
Primary WINS Server : 192.168.1.20
Lease Obtained. : Wednesday, January 24, 2018 8:26:21 AM
Lease Expires : Thursday, February 01, 2018 8:26:21 AM



C:\>arp -a

Interface: 192.168.1.11 --- 0x2

Internet Address	Physical Address	Type
192.168.1.20	00-14-22-60-3f-94	dynamic

C:\>netstat -rn

Route Table

=====

Interface List

0x1 MS TCP Loopback interface

0x2 ...18 03 73 14 1c 2c Intel(R) 82579LM Gigabit Network Connection - Packet Scheduler Miniport

=====

=====

Active Routes:

Network Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.11	10
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
192.168.1.0	255.255.255.0	192.168.1.11	192.168.1.11	10
192.168.1.11	255.255.255.255	127.0.0.1	127.0.0.1	10
192.168.1.255	255.255.255.255	192.168.1.11	192.168.1.11	10
224.0.0.0	240.0.0.0	192.168.1.11	192.168.1.11	10
255.255.255.255	255.255.255.255	192.168.1.11	192.168.1.11	1

Default Gateway: 192.168.1.1



=====
Persistent Routes:

None

C:\>netstat -an

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3306	0.0.0.0:0	LISTENING
TCP	127.0.0.1:1036	127.0.0.1:1037	ESTABLISHED
TCP	127.0.0.1:1037	127.0.0.1:1036	ESTABLISHED
TCP	127.0.0.1:1050	0.0.0.0:0	LISTENING
TCP	127.0.0.1:1051	0.0.0.0:0	LISTENING
TCP	192.168.1.11:139	0.0.0.0:0	LISTENING
TCP	192.168.1.11:2221	192.168.1.20:445	TIME_WAIT
UDP	0.0.0.0:445	*.*	
UDP	0.0.0.0:500	*.*	
UDP	0.0.0.0:4500	*.*	
UDP	127.0.0.1:123	*.*	
UDP	127.0.0.1:1025	*.*	
UDP	127.0.0.1:1046	*.*	
UDP	127.0.0.1:1900	*.*	



UDP 127.0.0.1:2003 *.*
UDP 192.168.1.11:123 *.*
UDP 192.168.1.11:137 *.*
UDP 192.168.1.11:138 *.*
UDP 192.168.1.11:1900 *.*

C:\>systeminfo

Host Name: TAB5
OS Name: Microsoft Windows XP Professional
OS Version: 5.1.2600 Service Pack 3 Build 2600
OS Manufacturer: Microsoft Corporation
OS Configuration: Member Workstation
OS Build Type: Multiprocessor Free
Registered Owner: admin
Registered Organization:
Product ID: 76487-OEM-0060807-79698
Original Install Date: 8/2/2016, 6:04:17 PM
System Up Time: 1 Days, 0 Hours, 30 Minutes, 41 Seconds
System Manufacturer: Dell Inc.
System Model: OptiPlex 790
System type: X86-based PC
Processor(s): 1 Processor(s) Installed.

[01]: x86 Family 6 Model 42 Stepping 7 Genuine Intel ~ 3092 Mhz



BIOS Version: DELL - 6222004
Windows Directory: C:\WINDOWS
System Directory: C:\WINDOWS\system32
Boot Device: \Device\HarddiskVolume1
System Locale: en-us;English (United States)
Input Locale: en-us;English (United States)
Time Zone: (GMT-05:00) Eastern Time (US & Canada)
Total Physical Memory: 3,241 MB
Available Physical Memory: 2,784 MB
Virtual Memory: Max Size: 2,048 MB
Virtual Memory: Available: 2,008 MB
Virtual Memory: In Use: 40 MB
Page File Location(s): C:\pagefile.sys
Domain: elections.local
Logon Server: \\BOE
Hotfix(s): 250 Hotfix(s) Installed.

[01]: File 1

[02]: File 1

[03]: File 1

[04]: File 1

[05]: File 1

[06]: File 1

[07]: File 1

[08]: File 1

[09]: File 1



[10]: File 1

[11]: File 1

[12]: File 1

[13]: File 1

[14]: File 1

[15]: File 1

[16]: File 1

[17]: File 1

[18]: File 1

[19]: File 1

[20]: File 1

[21]: File 1

[22]: File 1

[23]: File 1

[24]: File 1

[25]: File 1

[26]: File 1

[27]: File 1

[28]: File 1

[29]: File 1

[30]: File 1

[31]: File 1

[32]: File 1

[33]: File 1

[34]: File 1



[35]: File 1

[36]: File 1

[37]: File 1

[38]: File 1

[39]: File 1

[40]: File 1

[41]: File 1

[42]: File 1

[43]: File 1

[44]: File 1

[45]: File 1

[46]: File 1

[47]: File 1

[48]: File 1

[49]: File 1

[50]: File 1

[51]: File 1

[52]: File 1

[53]: File 1

[54]: File 1

[55]: File 1

[56]: File 1

[57]: File 1

[58]: File 1

[59]: File 1



- [60]: File 1
- [61]: File 1
- [62]: File 1
- [63]: File 1
- [64]: File 1
- [65]: File 1
- [66]: File 1
- [67]: File 1
- [68]: File 1
- [69]: File 1
- [70]: File 1
- [71]: File 1
- [72]: File 1
- [73]: File 1
- [74]: File 1
- [75]: File 1
- [76]: File 1
- [77]: File 1
- [78]: File 1
- [79]: File 1
- [80]: File 1
- [81]: File 1
- [82]: File 1
- [83]: File 1
- [84]: File 1



[85]: File 1

[86]: File 1

[87]: File 1

[88]: File 1

[89]: File 1

[90]: File 1

[91]: File 1

[92]: File 1

[93]: File 1

[94]: File 1

[95]: File 1

[96]: File 1

[97]: File 1

[98]: File 1

[99]: File 1

[100]: File 1

[101]: File 1

[102]: File 1

[103]: File 1

[104]: File 1

[105]: File 1

[106]: File 1

[107]: File 1

[108]: File 1

[109]: File 1



- [110]: File 1
- [111]: File 1
- [112]: File 1
- [113]: File 1
- [114]: File 1
- [115]: File 1
- [116]: File 1
- [117]: File 1
- [118]: File 1
- [119]: File 1
- [120]: File 1
- [121]: File 1
- [122]: Q147222
- [123]: KB2378111_WM9
- [124]: KB2803821-v2_WM9
- [125]: KB952069_WM9
- [126]: KB954155_WM9
- [127]: KB973540_WM9
- [128]: KB975558_WM8
- [129]: KB978695_WM9
- [130]: KB2564958 - Update
- [131]: KB936929 - Service Pack
- [132]: KB2115168 - Update
- [133]: KB2229593 - Update
- [134]: KB2296011 - Update



- [135]: KB2347290 - Update
- [136]: KB2387149 - Update
- [137]: KB2393802 - Update
- [138]: KB2419632 - Update
- [139]: KB2423089 - Update
- [140]: KB2443105 - Update
- [141]: KB2478960 - Update
- [142]: KB2478971 - Update
- [143]: KB2479943 - Update
- [144]: KB2481109 - Update
- [145]: KB2483185 - Update
- [146]: KB2485663 - Update
- [147]: KB2506212 - Update
- [148]: KB2507938 - Update
- [149]: KB2508429 - Update
- [150]: KB2509553 - Update
- [151]: KB2510581 - Update
- [152]: KB2535512 - Update
- [153]: KB2536276-v2 - Update
- [154]: KB2544893-v2 - Update
- [155]: KB2566454 - Update
- [156]: KB2570947 - Update
- [157]: KB2584146 - Update
- [158]: KB2585542 - Update
- [159]: KB2592799 - Update



- [160]: KB2598479 - Update
- [161]: KB2603381 - Update
- [162]: KB2619339 - Update
- [163]: KB2620712 - Update
- [164]: KB2631813 - Update
- [165]: KB2653956 - Update
- [166]: KB2655992 - Update
- [167]: KB2659262 - Update
- [168]: KB2661637 - Update
- [169]: KB2676562 - Update
- [170]: KB2686509 - Update
- [171]: KB2691442 - Update
- [172]: KB2698365 - Update
- [173]: KB2705219-v2 - Update
- [174]: KB2712808 - Update
- [175]: KB2719985 - Update
- [176]: KB2723135-v2 - Update
- [177]: KB2727528 - Update
- [178]: KB2757638 - Update
- [179]: KB2770660 - Update
- [180]: KB2780091 - Update
- [181]: KB2802968 - Update
- [182]: KB2807986 - Update
- [183]: KB2813345 - Update
- [184]: KB2820917 - Update



- [185]: KB2834886 - Update
- [186]: KB2847311 - Update
- [187]: KB2850869 - Update
- [188]: KB2859537 - Update
- [189]: KB2862152 - Update
- [190]: KB2862330 - Update
- [191]: KB2862335 - Update
- [192]: KB2864063 - Update
- [193]: KB2868038 - Update
- [194]: KB2868626 - Update
- [195]: KB2876217 - Update
- [196]: KB2876331 - Update
- [197]: KB2884256 - Update
- [198]: KB2892075 - Update
- [199]: KB2893294 - Update
- [200]: KB2898715 - Update
- [201]: KB2900986 - Update
- [202]: KB2904266 - Update
- [203]: KB2909212 - Update
- [204]: KB2914368 - Update
- [205]: KB2916036 - Update
- [206]: KB2922229 - Update
- [207]: KB2929961 - Update
- [208]: KB2930275 - Update
- [209]: KB2936068 - Update



- [210]: KB2964358 - Update
- [211]: KB923561 - Update
- [212]: KB942288-v3 - Update
- [213]: KB946648 - Update
- [214]: KB950762 - Update
- [215]: KB950974 - Update
- [216]: KB951376-v2 - Update
- [217]: KB952004 - Update
- [218]: KB95

Network Card(s): 1 NIC(s) Installed.

[01]: Intel(R) 82579LM Gigabit Network Connection

Connection Name: Local Area Connection

DHCP Enabled: Yes

DHCP Server: 192.168.1.20

IP address(es)

[01]: 192.168.1.11

C:\Documents and Settings\administrator.ELECTIONS>

Post-Election Review: No Change

TAB9.elections.local

Front: 4 USB ports – empty

CD/RW – empty

Rear: 3 USB – empty

USB Keyboard

USB Mouse



VGA Monitor

Serial/COM connection to flatbed voter machine

USB connection to tabulation cartridge voter device

LAN connection to Dell Switch

Additional Information Collected from CLI:

C:\>hostname

TAB9

C:\>ipconfig /all

Windows IP Configuration

Host Name : TAB9
Primary Dns Suffix : elections.local
Node Type : Hybrid
IP Routing Enabled. : No
WINS Proxy Enabled. : No
DNS Suffix Search List. : elections.local
elections.local

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . . : elections.local
Description : Intel(R) 82579LM Gigabit Network Connection
Physical Address. : 18-03-73-15-97-68



Dhcp Enabled. : Yes
 Autoconfiguration Enabled : Yes
 IP Address. : 192.168.1.12
 Subnet Mask : 255.255.255.0
 Default Gateway : 192.168.1.1
 DHCP Server : 192.168.1.20
 DNS Servers : 192.168.1.20
 Primary WINS Server : 192.168.1.20
 Lease Obtained. : Thursday, January 25, 2018 8:36:12 AM
 Lease Expires : Friday, February 02, 2018 8:36:12 AM

C:\>arp -a

Interface: 192.168.1.12 --- 0x2

Internet Address	Physical Address	Type
192.168.1.20	00-14-22-60-3f-94	dynamic

C:\>netstat -rn

Route Table

=====

Interface List

0x1 MS TCP Loopback interface
 0x2 ...18 03 73 15 97 68 Intel(R) 82579LM Gigabit Network Connection - Packet Scheduler Miniport

=====



=====

Active Routes:

Network	Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.12	10
127.0.0.0	255.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
192.168.1.0	255.255.255.0	255.255.255.0	192.168.1.12	192.168.1.12	10
192.168.1.12	255.255.255.255	255.255.255.255	127.0.0.1	127.0.0.1	10
192.168.1.255	255.255.255.255	255.255.255.255	192.168.1.12	192.168.1.12	10
224.0.0.0	240.0.0.0	240.0.0.0	192.168.1.12	192.168.1.12	10
255.255.255.255	255.255.255.255	255.255.255.255	192.168.1.12	192.168.1.12	1

Default Gateway: 192.168.1.1

=====

Persistent Routes:

None

C:\>netstat -an

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3306	0.0.0.0:0	LISTENING
TCP	127.0.0.1:1036	127.0.0.1:1037	ESTABLISHED
TCP	127.0.0.1:1037	127.0.0.1:1036	ESTABLISHED



```
TCP 127.0.0.1:1043 0.0.0.0 LISTENING
TCP 127.0.0.1:1051 0.0.0.0 LISTENING
TCP 192.168.1.12:139 0.0.0.0 LISTENING
```

```
UDP 0.0.0.0:445 *.*
UDP 0.0.0.0:500 *.*
UDP 0.0.0.0:4500 *.*
UDP 127.0.0.1:123 *.*
UDP 127.0.0.1:1025 *.*
UDP 127.0.0.1:1047 *.*
UDP 127.0.0.1:1900 *.*
UDP 192.168.1.12:123 *.*
UDP 192.168.1.12:137 *.*
UDP 192.168.1.12:138 *.*
UDP 192.168.1.12:1900 *.*
```

C:\>systeminfo

```
Host Name:          TAB9
OS Name:            Microsoft Windows XP Professional
OS Version:        5.1.2600 Service Pack 3 Build 2600
OS Manufacturer:   Microsoft Corporation
OS Configuration: Member Workstation
OS Build Type:      Multiprocessor Free
Registered Owner:   admin
```



Registered Organization:

Product ID: 76487-OEM-0060807-79698

Original Install Date: 8/2/2016, 6:04:17 PM

System Up Time: 0 Days, 0 Hours, 26 Minutes, 41 Seconds

System Manufacturer: Dell Inc.

System Model: OptiPlex 790

System type: X86-based PC

Processor(s): 1 Processor(s) Installed.

[01]: x86 Family 6 Model 42 Stepping 7 Genuine Intel ~ 3093 Mhz

BIOS Version: DELL - 6222004

Windows Directory: C:\WINDOWS

System Directory: C:\WINDOWS\system32

Boot Device: \Device\HarddiskVolume1

System Locale: en-us;English (United States)

Input Locale: en-us;English (United States)

Time Zone: (GMT-05:00) Eastern Time (US & Canada)

Total Physical Memory: 3,241 MB

Available Physical Memory: 2,760 MB

Virtual Memory: Max Size: 2,048 MB

Virtual Memory: Available: 1,997 MB

Virtual Memory: In Use: 51 MB

Page File Location(s): C:\pagefile.sys

Domain: elections.local

Logon Server: \\BOE

Hotfix(s): 250 Hotfix(s) Installed.



- [01]: File 1
- [02]: File 1
- [03]: File 1
- [04]: File 1
- [05]: File 1
- [06]: File 1
- [07]: File 1
- [08]: File 1
- [09]: File 1
- [10]: File 1
- [11]: File 1
- [12]: File 1
- [13]: File 1
- [14]: File 1
- [15]: File 1
- [16]: File 1
- [17]: File 1
- [18]: File 1
- [19]: File 1
- [20]: File 1
- [21]: File 1
- [22]: File 1
- [23]: File 1
- [24]: File 1
- [25]: File 1



- [26]: File 1
- [27]: File 1
- [28]: File 1
- [29]: File 1
- [30]: File 1
- [31]: File 1
- [32]: File 1
- [33]: File 1
- [34]: File 1
- [35]: File 1
- [36]: File 1
- [37]: File 1
- [38]: File 1
- [39]: File 1
- [40]: File 1
- [41]: File 1
- [42]: File 1
- [43]: File 1
- [44]: File 1
- [45]: File 1
- [46]: File 1
- [47]: File 1
- [48]: File 1
- [49]: File 1
- [50]: File 1



- [51]: File 1
- [52]: File 1
- [53]: File 1
- [54]: File 1
- [55]: File 1
- [56]: File 1
- [57]: File 1
- [58]: File 1
- [59]: File 1
- [60]: File 1
- [61]: File 1
- [62]: File 1
- [63]: File 1
- [64]: File 1
- [65]: File 1
- [66]: File 1
- [67]: File 1
- [68]: File 1
- [69]: File 1
- [70]: File 1
- [71]: File 1
- [72]: File 1
- [73]: File 1
- [74]: File 1
- [75]: File 1



- [76]: File 1
- [77]: File 1
- [78]: File 1
- [79]: File 1
- [80]: File 1
- [81]: File 1
- [82]: File 1
- [83]: File 1
- [84]: File 1
- [85]: File 1
- [86]: File 1
- [87]: File 1
- [88]: File 1
- [89]: File 1
- [90]: File 1
- [91]: File 1
- [92]: File 1
- [93]: File 1
- [94]: File 1
- [95]: File 1
- [96]: File 1
- [97]: File 1
- [98]: File 1
- [99]: File 1
- [100]: File 1



- [101]: File 1
- [102]: File 1
- [103]: File 1
- [104]: File 1
- [105]: File 1
- [106]: File 1
- [107]: File 1
- [108]: File 1
- [109]: File 1
- [110]: File 1
- [111]: File 1
- [112]: File 1
- [113]: File 1
- [114]: File 1
- [115]: File 1
- [116]: File 1
- [117]: File 1
- [118]: File 1
- [119]: File 1
- [120]: File 1
- [121]: File 1
- [122]: Q147222
- [123]: KB2378111_WM9
- [124]: KB2803821-v2_WM9
- [125]: KB952069_WM9



- [126]: KB954155_WM9
- [127]: KB973540_WM9
- [128]: KB975558_WM8
- [129]: KB978695_WM9
- [130]: KB2564958 - Update
- [131]: KB936929 - Service Pack
- [132]: KB2115168 - Update
- [133]: KB2229593 - Update
- [134]: KB2296011 - Update
- [135]: KB2347290 - Update
- [136]: KB2387149 - Update
- [137]: KB2393802 - Update
- [138]: KB2419632 - Update
- [139]: KB2423089 - Update
- [140]: KB2443105 - Update
- [141]: KB2478960 - Update
- [142]: KB2478971 - Update
- [143]: KB2479943 - Update
- [144]: KB2481109 - Update
- [145]: KB2483185 - Update
- [146]: KB2485663 - Update
- [147]: KB2506212 - Update
- [148]: KB2507938 - Update
- [149]: KB2508429 - Update
- [150]: KB2509553 - Update



- [151]: KB2510581 - Update
- [152]: KB2535512 - Update
- [153]: KB2536276-v2 - Update
- [154]: KB2544893-v2 - Update
- [155]: KB2566454 - Update
- [156]: KB2570947 - Update
- [157]: KB2584146 - Update
- [158]: KB2585542 - Update
- [159]: KB2592799 - Update
- [160]: KB2598479 - Update
- [161]: KB2603381 - Update
- [162]: KB2619339 - Update
- [163]: KB2620712 - Update
- [164]: KB2631813 - Update
- [165]: KB2653956 - Update
- [166]: KB2655992 - Update
- [167]: KB2659262 - Update
- [168]: KB2661637 - Update
- [169]: KB2676562 - Update
- [170]: KB2686509 - Update
- [171]: KB2691442 - Update
- [172]: KB2698365 - Update
- [173]: KB2705219-v2 - Update
- [174]: KB2712808 - Update
- [175]: KB2719985 - Update



- [176]: KB2723135-v2 - Update
- [177]: KB2727528 - Update
- [178]: KB2757638 - Update
- [179]: KB2770660 - Update
- [180]: KB2780091 - Update
- [181]: KB2802968 - Update
- [182]: KB2807986 - Update
- [183]: KB2813345 - Update
- [184]: KB2820917 - Update
- [185]: KB2834886 - Update
- [186]: KB2847311 - Update
- [187]: KB2850869 - Update
- [188]: KB2859537 - Update
- [189]: KB2862152 - Update
- [190]: KB2862330 - Update
- [191]: KB2862335 - Update
- [192]: KB2864063 - Update
- [193]: KB2868038 - Update
- [194]: KB2868626 - Update
- [195]: KB2876217 - Update
- [196]: KB2876331 - Update
- [197]: KB2884256 - Update
- [198]: KB2892075 - Update
- [199]: KB2893294 - Update
- [200]: KB2898715 - Update



- [201]: KB2900986 - Update
- [202]: KB2904266 - Update
- [203]: KB2909212 - Update
- [204]: KB2914368 - Update
- [205]: KB2916036 - Update
- [206]: KB2922229 - Update
- [207]: KB2929961 - Update
- [208]: KB2930275 - Update
- [209]: KB2936068 - Update
- [210]: KB2964358 - Update
- [211]: KB923561 - Update
- [212]: KB942288-v3 - Update
- [213]: KB946648 - Update
- [214]: KB950762 - Update
- [215]: KB950974 - Update
- [216]: KB951376-v2 - Update
- [217]: KB952004 - Update
- [218]: KB95

NetWork Card(s): 1 NIC(s) Installed.

[01]: Intel(R) 82579LM Gigabit Network Connection

Connection Name: Local Area Connection

DHCP Enabled: Yes

DHCP Server: 192.168.1.20

IP address(es)



[01]: 192.168.1.12

Post-Election Review: No changes

TAB7.elections.local

Front: 4 USB ports – empty

CD/RW – empty

Rear: 3 USB – empty

USB Keyboard

USB Mouse

VGA Monitor

LAN connection to Dell Switch

Additional Information Collected from CLI:

C:\>hostname

TAB7

C:\>ipconfig /all

Windows IP Configuration

Host Name : TAB7
Primary Dns Suffix : elections.local
Node Type : Hybrid
IP Routing Enabled. : No
WINS Proxy Enabled. : No
DNS Suffix Search List. : elections.local
elections.local



Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : elections.local
Description : Intel(R) 82579LM Gigabit Network Connection
Physical Address. : 18-03-73-1B-CF-E2
Dhcp Enabled. : Yes
Autoconfiguration Enabled : Yes
IP Address. : 192.168.1.40
Subnet Mask : 255.255.255.0
Default Gateway : 192.168.1.1
DHCP Server : 192.168.1.20
DNS Servers : 192.168.1.20
Primary WINS Server : 192.168.1.20
Lease Obtained. : Monday, January 22, 2018 8:32:01 AM

Lease Expires : Tuesday, January 30, 2018 8:32:01 AM

C:\>arp -a

Interface: 192.168.1.40 --- 0x2

Internet Address	Physical Address	Type
192.168.1.20	00-14-22-60-3f-94	dynamic

C:\>netstat -rn



Route Table

=====

Interface List

0x1 MS TCP Loopback interface

0x2 ...18 03 73 1b cf e2 Intel(R) 82579LM Gigabit Network Connection - Packet Scheduler Miniport

=====

=====

Active Routes:

Network Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.40	10
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
192.168.1.0	255.255.255.0	192.168.1.40	192.168.1.40	10
192.168.1.40	255.255.255.255	127.0.0.1	127.0.0.1	10
192.168.1.255	255.255.255.255	192.168.1.40	192.168.1.40	10
224.0.0.0	240.0.0.0	192.168.1.40	192.168.1.40	10
255.255.255.255	255.255.255.255	192.168.1.40	192.168.1.40	1

Default Gateway: 192.168.1.1

=====

Persistent Routes:

None



C:\>netstat -an

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3306	0.0.0.0:0	LISTENING
TCP	127.0.0.1:1045	0.0.0.0:0	LISTENING
TCP	127.0.0.1:1048	127.0.0.1:1049	ESTABLISHED
TCP	127.0.0.1:1049	127.0.0.1:1048	ESTABLISHED
TCP	127.0.0.1:1055	0.0.0.0:0	LISTENING
TCP	192.168.1.40:139	0.0.0.0:0	LISTENING
TCP	192.168.1.40:2627	192.168.1.20:139	ESTABLISHED
TCP	192.168.1.40:2716	192.168.1.20:135	TIME_WAIT
UDP	0.0.0.0:445	*.*	
UDP	0.0.0.0:500	*.*	
UDP	0.0.0.0:4500	*.*	
UDP	127.0.0.1:123	*.*	
UDP	127.0.0.1:1025	*.*	
UDP	127.0.0.1:1041	*.*	
UDP	127.0.0.1:1900	*.*	
UDP	192.168.1.40:123	*.*	
UDP	192.168.1.40:137	*.*	



UDP 192.168.1.40:138 *.*

UDP 192.168.1.40:1900 *.*

C:\>systeminfo

Host Name: TAB7

OS Name: Microsoft Windows XP Professional

OS Version: 5.1.2600 Service Pack 3 Build 2600

OS Manufacturer: Microsoft Corporation

OS Configuration: Member Workstation

OS Build Type: Multiprocessor Free

Registered Owner: admin

Registered Organization:

Product ID: 76487-OEM-0060807-79698

Original Install Date: 8/2/2016, 6:04:17 PM

System Up Time: 0 Days, 0 Hours, 51 Minutes, 41 Seconds

System Manufacturer: Dell Inc.

System Model: OptiPlex 790

System type: X86-based PC

Processor(s): 1 Processor(s) Installed.

[01]: x86 Family 6 Model 42 Stepping 7 Genuine Intel ~ 3092 Mhz

BIOS Version: DELL - 6222004

Windows Directory: C:\WINDOWS

System Directory: C:\WINDOWS\system32



Boot Device: \Device\HarddiskVolume1
System Locale: en-us;English (United States)
Input Locale: en-us;English (United States)
Time Zone: (GMT-05:00) Eastern Time (US & Canada)

Total Physical Memory: 3,241 MB
Available Physical Memory: 2,858 MB
Virtual Memory: Max Size: 2,048 MB
Virtual Memory: Available: 2,008 MB
Virtual Memory: In Use: 40 MB

Page File Location(s): C:\pagefile.sys

Domain: elections.local

Logon Server: \\BOE

Hotfix(s): 250 Hotfix(s) Installed.

[01]: File 1

[02]: File 1

[03]: File 1

[04]: File 1

[05]: File 1

[06]: File 1

[07]: File 1

[08]: File 1

[09]: File 1

[10]: File 1

[11]: File 1

[12]: File 1



- [13]: File 1
- [14]: File 1
- [15]: File 1
- [16]: File 1
- [17]: File 1
- [18]: File 1
- [19]: File 1
- [20]: File 1
- [21]: File 1
- [22]: File 1
- [23]: File 1
- [24]: File 1
- [25]: File 1
- [26]: File 1
- [27]: File 1
- [28]: File 1
- [29]: File 1
- [30]: File 1
- [31]: File 1
- [32]: File 1
- [33]: File 1
- [34]: File 1
- [35]: File 1
- [36]: File 1
- [37]: File 1



- [38]: File 1
- [39]: File 1
- [40]: File 1
- [41]: File 1
- [42]: File 1
- [43]: File 1
- [44]: File 1
- [45]: File 1
- [46]: File 1
- [47]: File 1
- [48]: File 1
- [49]: File 1
- [50]: File 1
- [51]: File 1
- [52]: File 1
- [53]: File 1
- [54]: File 1
- [55]: File 1
- [56]: File 1
- [57]: File 1
- [58]: File 1
- [59]: File 1
- [60]: File 1
- [61]: File 1
- [62]: File 1



- [63]: File 1
- [64]: File 1
- [65]: File 1
- [66]: File 1
- [67]: File 1
- [68]: File 1
- [69]: File 1
- [70]: File 1
- [71]: File 1
- [72]: File 1
- [73]: File 1
- [74]: File 1
- [75]: File 1
- [76]: File 1
- [77]: File 1
- [78]: File 1
- [79]: File 1
- [80]: File 1
- [81]: File 1
- [82]: File 1
- [83]: File 1
- [84]: File 1
- [85]: File 1
- [86]: File 1
- [87]: File 1



[88]: File 1

[89]: File 1

[90]: File 1

[91]: File 1

[92]: File 1

[93]: File 1

[94]: File 1

[95]: File 1

[96]: File 1

[97]: File 1

[98]: File 1

[99]: File 1

[100]: File 1

[101]: File 1

[102]: File 1

[103]: File 1

[104]: File 1

[105]: File 1

[106]: File 1

[107]: File 1

[108]: File 1

[109]: File 1

[110]: File 1

[111]: File 1

[112]: File 1



- [113]: File 1
- [114]: File 1
- [115]: File 1
- [116]: File 1
- [117]: File 1
- [118]: File 1
- [119]: File 1
- [120]: File 1
- [121]: File 1
- [122]: Q147222
- [123]: KB2378111_WM9
- [124]: KB2803821-v2_WM9
- [125]: KB952069_WM9
- [126]: KB954155_WM9
- [127]: KB973540_WM9
- [128]: KB975558_WM8
- [129]: KB978695_WM9
- [130]: KB2564958 - Update
- [131]: KB936929 - Service Pack
- [132]: KB2115168 - Update
- [133]: KB2229593 - Update
- [134]: KB2296011 - Update
- [135]: KB2347290 - Update
- [136]: KB2387149 - Update
- [137]: KB2393802 - Update



- [138]: KB2419632 - Update
- [139]: KB2423089 - Update
- [140]: KB2443105 - Update
- [141]: KB2478960 - Update
- [142]: KB2478971 - Update
- [143]: KB2479943 - Update
- [144]: KB2481109 - Update
- [145]: KB2483185 - Update
- [146]: KB2485663 - Update
- [147]: KB2506212 - Update
- [148]: KB2507938 - Update
- [149]: KB2508429 - Update
- [150]: KB2509553 - Update
- [151]: KB2510581 - Update
- [152]: KB2535512 - Update
- [153]: KB2536276-v2 - Update
- [154]: KB2544893-v2 - Update
- [155]: KB2566454 - Update
- [156]: KB2570947 - Update
- [157]: KB2584146 - Update
- [158]: KB2585542 - Update
- [159]: KB2592799 - Update
- [160]: KB2598479 - Update
- [161]: KB2603381 - Update
- [162]: KB2619339 - Update



- [163]: KB2620712 - Update
- [164]: KB2631813 - Update
- [165]: KB2653956 - Update
- [166]: KB2655992 - Update
- [167]: KB2659262 - Update
- [168]: KB2661637 - Update
- [169]: KB2676562 - Update
- [170]: KB2686509 - Update
- [171]: KB2691442 - Update
- [172]: KB2698365 - Update
- [173]: KB2705219-v2 - Update
- [174]: KB2712808 - Update
- [175]: KB2719985 - Update
- [176]: KB2723135-v2 - Update
- [177]: KB2727528 - Update
- [178]: KB2757638 - Update
- [179]: KB2770660 - Update
- [180]: KB2780091 - Update
- [181]: KB2802968 - Update
- [182]: KB2807986 - Update
- [183]: KB2813345 - Update
- [184]: KB2820917 - Update
- [185]: KB2834886 - Update
- [186]: KB2847311 - Update
- [187]: KB2850869 - Update



- [188]: KB2859537 - Update
- [189]: KB2862152 - Update
- [190]: KB2862330 - Update
- [191]: KB2862335 - Update
- [192]: KB2864063 - Update
- [193]: KB2868038 - Update
- [194]: KB2868626 - Update
- [195]: KB2876217 - Update
- [196]: KB2876331 - Update
- [197]: KB2884256 - Update
- [198]: KB2892075 - Update
- [199]: KB2893294 - Update
- [200]: KB2898715 - Update
- [201]: KB2900986 - Update
- [202]: KB2904266 - Update
- [203]: KB2909212 - Update
- [204]: KB2914368 - Update
- [205]: KB2916036 - Update
- [206]: KB2922229 - Update
- [207]: KB2929961 - Update
- [208]: KB2930275 - Update
- [209]: KB2936068 - Update
- [210]: KB2964358 - Update
- [211]: KB923561 - Update
- [212]: KB942288-v3 - Update



[213]: KB946648 - Update

[214]: KB950762 - Update

[215]: KB950974 - Update

[216]: KB951376-v2 - Update

[217]: KB952004 - Update

[218]: KB95

Network Card(s): 1 NIC(s) Installed.

[01]: Intel(R) 82579LM Gigabit Network Connection

Connection Name: Local Area Connection

DHCP Enabled: Yes

DHCP Server: 192.168.1.20

IP address(es)

[01]: 192.168.1.40

Post-Election Review: No Changes.

DAM.elections.local

Front: 2 USB – empty

CD/RW - empty

Floppy – empty

Rear: Octal Serial Cable to Modem bank

USB Keyboard

USB Mouse

VGA Monitor

LAN connection to Dell Switch



Additional Information Collected from CLI:

C:\>hostname

DAM

C:\>ipconfig /all

Windows IP Configuration

Host Name : DAM
Primary Dns Suffix : elections.local
Node Type : Broadcast
IP Routing Enabled. : No
WINS Proxy Enabled. : No
DNS Suffix Search List. : elections.local

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . . :
Description : Broadcom NetXtreme 57xx Gigabit Controller
Physical Address. : 00-19-B9-1F-F2-17
Dhcp Enabled. : No
IP Address. : 192.168.1.101
Subnet Mask : 255.255.255.0
Default Gateway :
DNS Servers : 192.168.1.20



C:\>arp -a

Interface: 192.168.1.101 --- 0x2

Internet Address	Physical Address	Type
192.168.1.20	00-14-22-60-3f-94	dynamic

C:\>netstat -rn

Route Table

=====

Interface List

0x1 MS TCP Loopback interface

0x2 ...00 19 b9 1f f2 17 Broadcom NetXtreme 57xx Gigabit Controller - Packet Scheduler Miniport

=====

=====

Active Routes:

Network Destination	Netmask	Gateway	Interface	Metric
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
192.168.1.0	255.255.255.0	192.168.1.101	192.168.1.101	10
192.168.1.101	255.255.255.255	127.0.0.1	127.0.0.1	10
192.168.1.255	255.255.255.255	192.168.1.101	192.168.1.101	10
224.0.0.0	240.0.0.0	192.168.1.101	192.168.1.101	10
255.255.255.255	255.255.255.255	192.168.1.101	192.168.1.101	1



=====
Persistent Routes:

None

C:\>netstat -an

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3071	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49152	0.0.0.0:0	LISTENING
TCP	127.0.0.1:1040	0.0.0.0:0	LISTENING
TCP	192.168.1.101:139	0.0.0.0:0	LISTENING
UDP	0.0.0.0:445	*.*	
UDP	0.0.0.0:500	*.*	
UDP	0.0.0.0:1025	*.*	
UDP	0.0.0.0:1026	*.*	
UDP	0.0.0.0:4500	*.*	
UDP	127.0.0.1:123	*.*	
UDP	127.0.0.1:1027	*.*	
UDP	127.0.0.1:1044	*.*	
UDP	127.0.0.1:1900	*.*	



UDP 192.168.1.101:123 *.*
UDP 192.168.1.101:137 *.*
UDP 192.168.1.101:138 *.*
UDP 192.168.1.101:1900 *.*

C:\>systeminfo

Host Name: DAM
OS Name: Microsoft Windows XP Professional
OS Version: 5.1.2600 Service Pack 2 Build 2600
OS Manufacturer: Microsoft Corporation
OS Configuration: Member Workstation
OS Build Type: Multiprocessor Free
Registered Owner: damsw
Registered Organization:
Product ID: 76487-OEM-0011903-00102
Original Install Date: 7/25/2007, 9:15:46 AM
System Up Time: 0 Days, 0 Hours, 34 Minutes, 35 Seconds
System Manufacturer: Dell Inc.
System Model: Precision WorkStation 690
System type: X86-based PC
Processor(s): 2 Processor(s) Installed.
[01]: x86 Family 6 Model 15 Stepping 6 Genuine Intel ~ 1595 Mhz
[02]: x86 Family 6 Model 15 Stepping 6 Genuine Intel ~ 1595 Mhz
BIOS Version: DELL - d



Windows Directory: C:\WINDOWS
System Directory: C:\WINDOWS\system32
Boot Device: \Device\HarddiskVolume2
System Locale: en-us;English (United States)
Input Locale: en-us;English (United States)
Time Zone: (GMT-05:00) Eastern Time (US & Canada)
Total Physical Memory: 2,046 MB
Available Physical Memory: 1,736 MB
Virtual Memory: Max Size: 2,048 MB
Virtual Memory: Available: 2,008 MB
Virtual Memory: In Use: 40 MB
Page File Location(s): C:\pagefile.sys
Domain: elections.local
Logon Server: \\BOE
Hotfix(s): 94 Hotfix(s) Installed.

[01]: File 1

[02]: File 1

[03]: File 1

[04]: File 1

[05]: File 1

[06]: File 1

[07]: File 1

[08]: File 1

[09]: File 1

[10]: File 1



- [11]: File 1
- [12]: File 1
- [13]: File 1
- [14]: File 1
- [15]: File 1
- [16]: File 1
- [17]: File 1
- [18]: File 1
- [19]: File 1
- [20]: File 1
- [21]: File 1
- [22]: File 1
- [23]: File 1
- [24]: File 1
- [25]: File 1
- [26]: File 1
- [27]: File 1
- [28]: File 1
- [29]: File 1
- [30]: File 1
- [31]: File 1
- [32]: File 1
- [33]: File 1
- [34]: File 1
- [35]: File 1



- [36]: File 1
- [37]: File 1
- [38]: File 1
- [39]: File 1
- [40]: File 1
- [41]: File 1
- [42]: File 1
- [43]: File 1
- [44]: File 1
- [45]: File 1
- [46]: Q147222
- [47]: S867460 - Update
- [48]: KB925398_WMP64
- [49]: KB923689
- [50]: KB873339 - Update
- [51]: KB885250 - Update
- [52]: KB885835 - Update
- [53]: KB887472 - Update
- [54]: KB889673 - Update
- [55]: KB891781 - Update
- [56]: KB896256 - Update
- [57]: KB896358 - Update
- [58]: KB896423 - Update
- [59]: KB896424 - Update
- [60]: KB899588 - Update



- [61]: KB899591 - Update
- [62]: KB901214 - Update
- [63]: KB904706 - Update
- [64]: KB908519 - Update
- [65]: KB908531 - Update
- [66]: KB908673 - Update
- [67]: KB909095 - Update
- [68]: KB911562 - Update
- [69]: KB912919 - Update
- [70]: KB912945 - Update
- [71]: KB914388 - Update
- [72]: KB917344 - Update
- [73]: KB917422 - Update
- [74]: KB918439 - Update
- [75]: KB918899 - Update
- [76]: KB919007 - Update
- [77]: KB920213 - Update
- [78]: KB920670 - Update
- [79]: KB920683 - Update
- [80]: KB920685 - Update
- [81]: KB921398 - Update
- [82]: KB922616 - Update
- [83]: KB923191 - Update
- [84]: KB923414 - Update
- [85]: KB923694 - Update



- [86]: KB923980 - Update
- [87]: KB924191 - Update
- [88]: KB924270 - Update
- [89]: KB924496 - Update
- [90]: KB925454 - Update
- [91]: KB926255 - Update
- [92]: KB928388 - Update
- [93]: KB929969 - Update
- [94]: KB835221WXP - Update

Network Card(s): 2 NIC(s) Installed.

[01]: Broadcom NetXtreme 57xx Gigabit Controller

Connection Name: Local Area Connection

DHCP Enabled: No

IP address(es)

[01]: 192.168.1.101

[02]: 1394 Net Adapter

Connection Name: 1394 Connection

DHCP Enabled: Yes

DHCP Server: N/A

IP address(es)

Post-Election Review: No Changes.

DAM3.elections.local

Front: 4 USB Ports – empty

CD/DVD – empty

Rear: 2 USB connected to 2 Digi Rapidport /4 modems



USB Keyboard

USB Mouse

VGA Monitor

LAN Connection to Dell Switch

Additional Information Collected from CLI:

C:\>hostname

DAM3

C:\>ipconfig /all

Windows IP Configuration

Host Name : DAM3
Primary Dns Suffix : elections.local
Node Type : Hybrid
IP Routing Enabled. : No
WINS Proxy Enabled. : No
DNS Suffix Search List. : elections.local
elections.local

Ethernet adapter Local Area Connection 2:

Connection-specific DNS Suffix . . : elections.local
Description : Intel(R) 82579LM Gigabit Network Connection
Physical Address. : D4-BE-D9-A4-D1-C5



Dhcp Enabled. : Yes
 Autoconfiguration Enabled : Yes
 IP Address. : 192.168.1.41
 Subnet Mask : 255.255.255.0
 Default Gateway : 192.168.1.1
 DHCP Server : 192.168.1.20
 DNS Servers : 192.168.1.20
 Primary WINS Server : 192.168.1.20
 Lease Obtained. : Thursday, January 25, 2018 8:31:37 AM
 Lease Expires : Friday, February 02, 2018 8:31:37 AM

C:\>arp -a

Interface: 192.168.1.41 --- 0x2

Internet Address	Physical Address	Type
192.168.1.20	00-14-22-60-3f-94	dynamic

C:\>netstat -rn

Route Table

=====

Interface List

0x1 MS TCP Loopback interface
 0x2 ...d4 be d9 a4 d1 c5 Intel(R) 82579LM Gigabit Network Connection - Packet Scheduler Miniport



=====
=====
Active Routes:

Network	Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.41		10
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1		1
192.168.1.0	255.255.255.0	192.168.1.41	192.168.1.41		10
192.168.1.41	255.255.255.255	127.0.0.1	127.0.0.1		10
192.168.1.255	255.255.255.255	192.168.1.41	192.168.1.41		10
224.0.0.0	240.0.0.0	192.168.1.41	192.168.1.41		10
255.255.255.255	255.255.255.255	192.168.1.41	192.168.1.41		1

Default Gateway: 192.168.1.1
=====

Persistent Routes:

None

C:\>netstat -an

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	127.0.0.1:1045	127.0.0.1:1046	ESTABLISHED
TCP	127.0.0.1:1046	127.0.0.1:1045	ESTABLISHED
TCP	127.0.0.1:1054	0.0.0.0:0	LISTENING



```
TCP 127.0.0.1:1057 0.0.0.0 LISTENING
TCP 192.168.1.41:139 0.0.0.0 LISTENING

UDP 0.0.0.0:445 *.*
UDP 0.0.0.0:500 *.*
UDP 0.0.0.0:1025 *.*
UDP 0.0.0.0:1026 *.*
UDP 0.0.0.0:4500 *.*
UDP 127.0.0.1:123 *.*
UDP 127.0.0.1:1027 *.*
UDP 127.0.0.1:1043 *.*
UDP 127.0.0.1:1900 *.*
UDP 192.168.1.41:123 *.*
UDP 192.168.1.41:137 *.*
UDP 192.168.1.41:138 *.*
UDP 192.168.1.41:1900 *.*
```

C:\>systeminfo

```
Host Name: DAM3
OS Name: Microsoft Windows XP Professional
OS Version: 5.1.2600 Service Pack 3 Build 2600
OS Manufacturer: Microsoft Corporation
OS Configuration: Member Workstation
```



OS Build Type: Multiprocessor Free

Registered Owner: ess

Registered Organization:

Product ID: 76487-OEM-0060807-79692

Original Install Date: 3/30/2016, 10:52:49 AM

System Up Time: 0 Days, 0 Hours, 37 Minutes, 9 Seconds

System Manufacturer: Dell Inc.

System Model: OptiPlex 790

System type: X86-based PC

Processor(s): 1 Processor(s) Installed.

[01]: x86 Family 6 Model 42 Stepping 7 Genuine Intel ~3093 Mhz

BIOS Version: DELL - 6222004

Windows Directory: C:\WINDOWS

System Directory: C:\WINDOWS\system32

Boot Device: \Device\HarddiskVolume1

System Locale: en-us;English (United States)

Input Locale: en-us;English (United States)

Time Zone: (GMT-05:00) Eastern Time (US & Canada)

Total Physical Memory: 3,241 MB

Available Physical Memory: 2,919 MB

Virtual Memory: Max Size: 2,048 MB

Virtual Memory: Available: 2,008 MB

Virtual Memory: In Use: 40 MB

Page File Location(s): C:\pagefile.sys

Domain: elections.local



Logon Server: \\BOE

Hotfix(s): 10 Hotfix(s) Installed.

[01]: File 1

[02]: File 1

[03]: File 1

[04]: File 1

[05]: Q147222

[06]: KB936929 - Service Pack

[07]: KB942288-v3 - Update

[08]: KB953356 - Update

[09]: KB954550-v5 - Update

[10]: KB835221WXP - Update

Network Card(s): 1 NIC(s) Installed.

[01]: Intel(R) 82579LM Gigabit Network Connection

Connection Name: Local Area Connection 2

DHCP Enabled: Yes

DHCP Server: 192.168.1.20

IP address(es)

[01]: 192.168.1.41

Post-Election Review: No Change

External Connections on Client Devices

The only outside (external) connections found on the network were the dial-up modems on the 2 DAM servers which are part of the application and are outbound only. No other external connections were found on the network. Each server/workstation was tested and none of them had Internet access. The 7 Ethernet connections on the Dell 2716 switch were traced to valid devices. No other cables were connected to the Dell Switch and no loose cables were observed near the switch. The solutions4networks engineer asked if there was a valid login for the Dell 2716 switch but was told that no one was aware of one.





No Wireless Adapters or Bluetooth Capability Found on Client Devices

Each PC was physically inspected for the presence of a wireless adapter or Bluetooth adapter and none were found.

The Windows “Device Manager” of each device was also inspected for the presence of any wireless devices.

No Wireless Keyboards and Mice

The keyboards and mice all had physical wires connected to the computers.

Post-Election Review: All items indicated above remained the same.

Network Air Gap Analysis

No issues found.

Air Gap Network Intact - Recommendations for Improvement

solutions4networks did not find any problems with the Election Tabulation Network, but have these recommendations to improve security of the network:



Client Operating Systems – Update the Clients to a supported OS.

The client PC's were found to be running Windows XP which is no longer supported by Microsoft. These may be more vulnerable to attack if the network was ever compromised. The clients also had their internal Firewall disabled. They did have Symantec Anti-virus installed, but the definitions were out of date. If this remains a closed air gapped network this should be a viable OS.

Server Operating System – Update the Server Operating System.

The server operating system is running Windows Server 2003, which is end of life July 2015. Any OS that is end of life is more vulnerable to attack if the network is ever compromised as it is no longer updated with any security patches. If this remains a closed air gapped network this should be a viable OS.

Remote Assistance Enabled.

Remote Assistance is enabled on the 3 clients and 2 DAM servers. This serves no positive purpose in a closed network environment where each machine is physically accessible and should be disabled in the event the network is ever compromised.

Remote Desktop is Enabled.

Remoted Desktop is enabled on the BOE server. Once again, this does not serve any positive purpose in a closed local network and should be disabled in the event the network is ever compromised.

Windows Update Enabled/None Selected.

The two DAM servers are configured differently from the rest of the computers on the network. Consistency should be the norm. All other computers have Auto Updates turned off. DAM1 has nothing selected and DAM2 has Auto Updates enabled and set for 3:00AM. Since this is a closed network and the OSes that are running are end of life there isn't a need to have Windows Update enabled.

Lock Physical Access to the Dell PowerConnect 2716

The Dell switch is easily accessible on the countertop. A locked cabinet would make it more difficult to connect an external cable. It is also recommended to disable any unused ports on the Dell Switch or move the unused ports to a different VLAN from the production network, but since the login is unknown a locked cabinet would suffice. Since the password is currently unknown and this is a flat network for ease of networking on the Dell switch there is the ability to reset it to unmanaged mode which would put all ports in Vlan 1.

Remove the Default Gateway Option

The DHCP server is giving the clients a default gateway of 192.168.1.1 even though no device exists. Removing the default gateway completely would make it more difficult for the clients to communicate with external networks. There is some inconsistency on the network in that not all the clients are set up for DHCP. Either set them all up for DHCP or set them all up for Static. For a more secure environment it would be better to disable DHCP on the BOE server entirely and configure static IPs on all the clients that way if someone were to ever connect to the Dell switch they would never obtain a DHCP address but would have to know the network addressing to hard code their PC.

County of Allegheny

Pre/**Post**-Election Air Gap Analysis of the Tabulation Network

For the Special Election

06 March 2018

Research and Recommendations Provided by:



a network infrastructure company

Prepared by:
Frank Calderone
Network Security Practice Lead
fcalderone@s4nets.com
(412) 626-3132



Contents

Overview.....	2
Site Contacts.....	2
General Physical Security/Building Access	2
Physical Security/Building Access - No Issues Found	2
Election Tabulations Network	8
Network Overview.....	8
Network Overview - Logical.....	9
Network Overview - Physical.....	11
External Connections on Client Devices	99
No Wireless Adapters or Bluetooth Capability Found on Client Devices.....	100
No Wireless Keyboards and Mice.....	100
Network Air Gap Analysis	100
Air Gap Network Intact - Recommendations for Improvement.....	100
Client Operating Systems – Update the Clients to a supported OS.	100
Server Operating System – Update the Server Operating System.....	101
Remote Assistance Enabled.....	101
Remote Desktop is Enabled.....	101
Windows Update Enabled/None Selected.....	101
Lock Physical Access to the Dell PowerConnect 2716.....	101
Remove the Default Gateway Option	101



Overview

The County of Allegheny has engaged solutions4networks to perform a network air gap analysis of their elections tabulation network located in Pittsburgh, PA. An **air gap, air wall** or **air gapping** is a network security measure employed on one or more computers to ensure that a secure computer network is physically isolated from unsecured networks, such as the public Internet or an unsecured local area network. solutions4networks has been tasked to verify the tabulation network is a stand-alone, isolated network and to assess the networks' vulnerability to external access and/or tampering. In addition to the network, solutions4network has been asked to assess and document the general physical security of the warehouse building.

A pre-election onsite visit was made by Frank Calderone of solutions4networks on March 5, 2018. The purpose of this document is to report the results of the assessment, identify security concerns and to make recommendations for the remediation of these concerns. A post-Election onsite visit was made on March 8, 2018. This report covers both the Pre-Election assessment and the **Post-Election review**. Post-Election Review updates will be noted in **red**.

Site Contacts

Elizabeth Dell

Elizabeth.Dell@AlleghenyCounty.US

412-350-6059

Robin Gigliotti

Robin.Gigliotti@AlleghenyCounty.US

412-350-6647

901 Pennsylvania Avenue

Pittsburgh, PA 15233

General Physical Security/Building Access

Physical Security/Building Access - No Issues Found

There are several suites within the warehouse and there were no outside signs, which identified that it was County of Allegheny building space. The building phone at the main entrance also did not have any entries to dial for the County of Allegheny.

Building Main Entrance:



Suite 901:



03/05/2018 - solutions4networks engineer, Frank Calderone, was met at the street entrance of suite 901 by Robin Gigliotti and was asked to provide a valid driver's license as identification before access to the building was granted.

03/08/2018 - solutions4networks engineer, Frank Calderone, was met at the street entrance suite 901 by Elizabeth Dell and was asked to provide a driver's license identification before access to the building was granted.

Entrance from the street required badge card access or a key (as seen in the picture in the previous page). The first door in the warehouse required a security code, but it was a physical, non-electronic lock.



Entrance into the Computer Room also require a code or a physical key.



Entrance to the tabulation room also required an electronic badge or key.



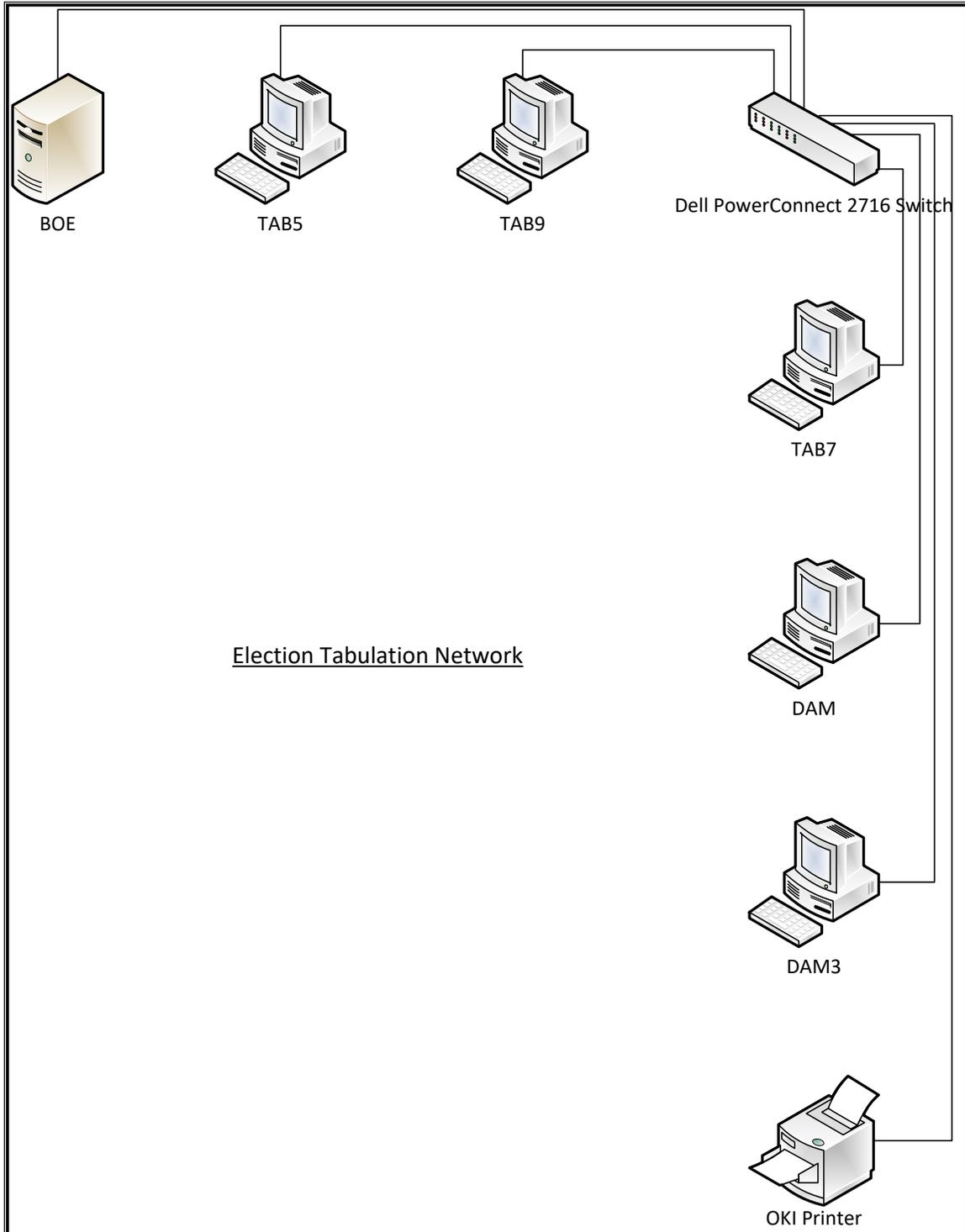
Security cameras were observed over the street entrance and inside the computer room. There is a sign in the tabulation network room that states “No Cell Phones are Permitted”.

Physical Post-Election Review: All items indicated above remained the same.

Election Tabulations Network

Network Overview

The solutions4networks engineer created the following network drawing based off the observed finding from the onsite physical inspections performed during the air gap analysis.





The Election Tabulation Network consisted of the following devices:

- 1 Dell PowerConnect 2716 Ethernet Switch
- 1 Windows Server
- 5 Client PC's
 - Two DAM (Dial Access Modem) Servers
 - 3 Windows XP Clients
- 1 Printer

Network Overview - Logical

All the devices had an address from RFC1918 private network 192.168.1.0/24. The Windows Server with address 192.168.1.20 provided DHCP, DNS and WINS services. A default gateway of 192.168.1.1 was configured, but no such device was found on the network. All devices on the network could ping each other so the network was fully self-contained and each node was accessible to one another.

Post-Election Review: All items indicated above remained the same.

Dell Server PE-SC1420	Dell Optiplex 790	Dell Optiplex 790	Dell Optiplex 790	Dell Precision 890	Dell Optiplex 790	Okidata Printer B6300
BOE.elections.local	TAB5.elections.local	TAB9.elections.local	TAB7.elections.local	DAM.elections.local	DAM3.elections.local	
provides DHCP, WINS, DNS Services	DHCP enabled	DHCP enabled	DHCP enabled	static	DHCP enabled/	DHCP Reserved
Win2003 SP1	Win XP Pro ver 2002 SP3	Win XP Pro ver 2002 SP3	Win XP Pro ver 2002 SP3	WinXP SP3	WinXP SP3	
Dell Server PESC1420						
intel Xeon CPU 3.20 GHZ	Intel core i5-2400 CPU 3.1 GHz	Intel core i5-2400 CPU 3.1 GHz	Intel core i5-2400 CPU 3.1 GHz	Intel Xeon 5110@1.60GHz		
3.19 GHz 2.00 GB RAM	3.09 GHZ, 3.16 GB Ram	3.09 GHZ, 3.16 GB Ram	3.09 GHZ, 3.16 GB Ram	1.60 GHz, 2.00 GB Ram		
2GB Ram	4 GB Ram	4 GB Ram	4 GB Ram	2 GB Ram	2 GB Ram	
IP: 192.168.1.20 (static)	IP: 192.168.1.11	IP: 192.168.1.12	IP: 192.168.1.40	IP: 192.168.1.101	IP: 192.168.1.41	IP: 192.168.1.50
netmask: 255.255.255.0	netmask: 255.255.255.0	netmask: 255.255.255.0	netmask: 255.255.255.0	netmask: 255.255.255.0	netmask: 255.255.255.0	netmask: 255.255.255.0
gateway: 192.168.1.1	gateway: 192.168.1.1 (doesn't exist)	gateway: 192.168.1.1 (doesn't exist)	gateway: 192.168.1.1 (doesn't exist)		gateway: 192.168.1.1 (doesn't exist)	
DNS: 192.168.1.20	DHCP Server: 192.168.1.20	DHCP Server: 192.168.1.20	DHCP Server: 192.168.1.20		DHCP Server: 192.168.1.20	
WINS: 192.168.1.20	DNS Server: 192.168.1.20	DNS Server: 192.168.1.20	DNS Server: 192.168.1.20	DNS Server: 192.168.1.20	DNS Server: 192.168.1.20	
	Wins Server: 192.168.1.20	Wins Server: 192.168.1.20	Wins Server: 192.168.1.20			
wired keyboard	wired keyboard	wired keyboard	wired keyboard	wired keyboard	wired keyboard	
wired mouse	wired mouse	wired mouse	wired mouse	wired mouse	wired mouse	
Intel Pro 1000 MT LAN connection	Gigabit LAN connection	Gigabit LAN connection	Gigabit LAN connection	Broadcom Gigabit Controller		

Network Overview - Physical

Each device on the network was inspected Pre- and Post-election for physical attachments and are noted below.

BOE.elections.local

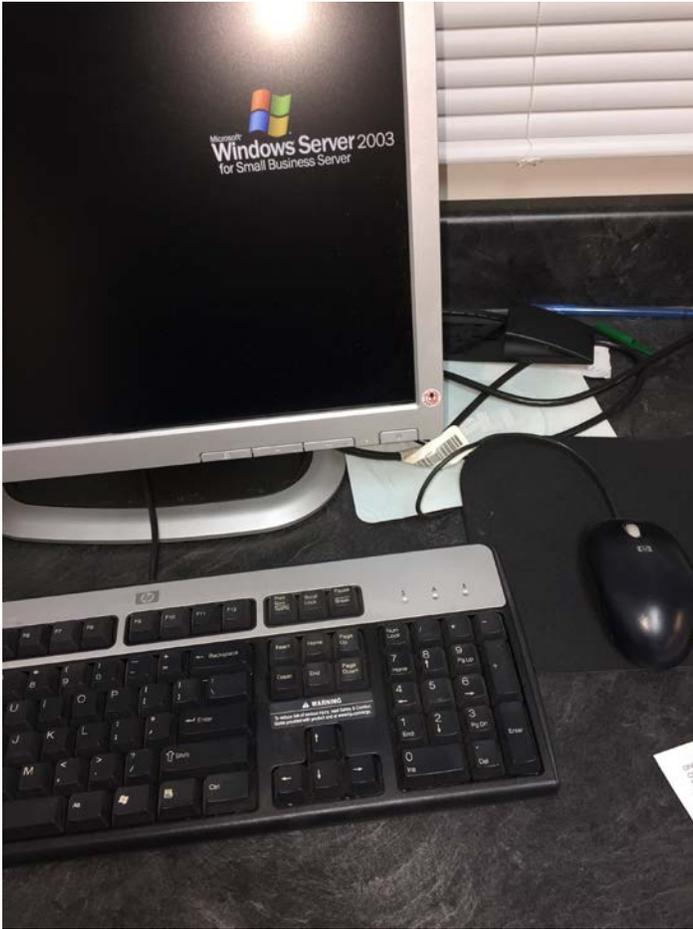
BOE Front



BOE Rear



BOE Desktop



Additional Information Collected from BOE CLI:

Microsoft Windows [Version 5.2.3790]

(C) Copyright 1985-2003 Microsoft Corp.

```
C:\Documents and Settings\Administrator>hostname
```

BOE

```
C:\Documents and Settings\Administrator>whoami
```

elections\administrator

```
C:\Documents and Settings\Administrator>ipconfig /all
```



Windows IP Configuration

Host Name : BOE
Primary Dns Suffix : elections.local
Node Type : Hybrid
IP Routing Enabled. : No
WINS Proxy Enabled. : No
DNS Suffix Search List. : elections.local

Ethernet adapter Server LAN NIC:

Connection-specific DNS Suffix . :
Description : Intel(R) PRO/1000 MT Network Connection
Physical Address. : 00-14-22-60-3F-94
DHCP Enabled. : No
IP Address. : 192.168.1.20
Subnet Mask : 255.255.255.0
Default Gateway : 192.168.1.1
DNS Servers : 192.168.1.20
Primary WINS Server : 192.168.1.20

C:\Documents and Settings\Administrator>

Microsoft Windows [Version 5.2.3790]

(C) Copyright 1985-2003 Microsoft Corp.



C:\Documents and Settings\Administrator>arp -a

Interface: 192.168.1.20 --- 0x10003

Internet Address	Physical Address	Type
192.168.1.11	18-03-73-14-1c-2c	dynamic
192.168.1.12	18-03-73-15-97-68	dynamic
192.168.1.101	00-19-b9-1f-f2-17	dynamic

C:\Documents and Settings\Administrator>netstat -rn

IPv4 Route Table

Interface List

```

0x1 ..... MS TCP Loopback interface
0x10003 ...00 14 22 60 3f 94 ..... Intel(R) PRO/1000 MT Network Connection

```

Active Routes:

Network Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.20	10
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
192.168.1.0	255.255.255.0	192.168.1.20	192.168.1.20	10
192.168.1.20	255.255.255.255	127.0.0.1	127.0.0.1	10
192.168.1.255	255.255.255.255	192.168.1.20	192.168.1.20	10



224.0.0.0 240.0.0.0 192.168.1.20 192.168.1.20 10

255.255.255.255 255.255.255.255 192.168.1.20 192.168.1.20 1

Default Gateway: 192.168.1.1

=====

Persistent Routes:

None

C:\Documents and Settings\Administrator>netstat -an

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:25	0.0.0.0:0	LISTENING
TCP	0.0.0.0:42	0.0.0.0:0	LISTENING
TCP	0.0.0.0:53	0.0.0.0:0	LISTENING
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING
TCP	0.0.0.0:88	0.0.0.0:0	LISTENING
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:389	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:464	0.0.0.0:0	LISTENING
TCP	0.0.0.0:593	0.0.0.0:0	LISTENING
TCP	0.0.0.0:636	0.0.0.0:0	LISTENING
TCP	0.0.0.0:691	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1026	0.0.0.0:0	LISTENING



TCP	0.0.0.0:1027	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1068	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1074	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1075	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1076	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1078	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1081	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1097	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1100	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1142	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1171	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1173	0.0.0.0:0	LISTENING
TCP	0.0.0.0:2160	0.0.0.0:0	LISTENING
TCP	0.0.0.0:2161	0.0.0.0:0	LISTENING
TCP	0.0.0.0:2260	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3052	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3268	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3269	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3389	0.0.0.0:0	LISTENING
TCP	0.0.0.0:6001	0.0.0.0:0	LISTENING
TCP	0.0.0.0:6002	0.0.0.0:0	LISTENING
TCP	0.0.0.0:6004	0.0.0.0:0	LISTENING
TCP	0.0.0.0:6358	0.0.0.0:0	LISTENING
TCP	0.0.0.0:6548	0.0.0.0:0	LISTENING
TCP	0.0.0.0:8081	0.0.0.0:0	LISTENING



TCP	0.0.0.0:10000	0.0.0.0:0	LISTENING
TCP	0.0.0.0:34571	0.0.0.0:0	LISTENING
TCP	0.0.0.0:34572	0.0.0.0:0	LISTENING
TCP	0.0.0.0:34573	0.0.0.0:0	LISTENING
TCP	127.0.0.1:389	127.0.0.1:45452	ESTABLISHED
TCP	127.0.0.1:1090	127.0.0.1:389	CLOSE_WAIT
TCP	127.0.0.1:1109	127.0.0.1:389	CLOSE_WAIT
TCP	127.0.0.1:1158	127.0.0.1:389	CLOSE_WAIT
TCP	127.0.0.1:43563	127.0.0.1:389	CLOSE_WAIT
TCP	127.0.0.1:45452	127.0.0.1:389	ESTABLISHED
TCP	192.168.1.20:135	192.168.1.20:1175	ESTABLISHED
TCP	192.168.1.20:135	192.168.1.20:47618	ESTABLISHED
TCP	192.168.1.20:135	192.168.1.101:1077	ESTABLISHED
TCP	192.168.1.20:139	0.0.0.0:0	LISTENING
TCP	192.168.1.20:139	192.168.1.12:2037	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:45429	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:45430	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:45431	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:45433	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:45435	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:45436	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:45438	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:45440	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:45441	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:45442	ESTABLISHED



TCP	192.168.1.20:389	192.168.1.20:45443	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:45444	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:45445	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:45447	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:45448	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:45451	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:45578	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:47544	FIN_WAIT_2
TCP	192.168.1.20:389	192.168.1.20:47607	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:47617	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:47621	TIME_WAIT
TCP	192.168.1.20:691	192.168.1.20:1112	ESTABLISHED
TCP	192.168.1.20:691	192.168.1.20:1169	ESTABLISHED
TCP	192.168.1.20:691	192.168.1.20:43565	ESTABLISHED
TCP	192.168.1.20:1026	192.168.1.20:1108	ESTABLISHED
TCP	192.168.1.20:1026	192.168.1.20:1206	ESTABLISHED
TCP	192.168.1.20:1026	192.168.1.20:1356	ESTABLISHED
TCP	192.168.1.20:1026	192.168.1.20:46982	ESTABLISHED
TCP	192.168.1.20:1093	192.168.1.20:389	CLOSE_WAIT
TCP	192.168.1.20:1108	192.168.1.20:1026	ESTABLISHED
TCP	192.168.1.20:1111	192.168.1.20:389	CLOSE_WAIT
TCP	192.168.1.20:1112	192.168.1.20:691	ESTABLISHED
TCP	192.168.1.20:1130	192.168.1.20:389	CLOSE_WAIT
TCP	192.168.1.20:1142	192.168.1.20:47619	ESTABLISHED
TCP	192.168.1.20:1159	192.168.1.20:389	CLOSE_WAIT



TCP	192.168.1.20:1169	192.168.1.20:691	ESTABLISHED
TCP	192.168.1.20:1175	192.168.1.20:135	ESTABLISHED
TCP	192.168.1.20:1206	192.168.1.20:1026	ESTABLISHED
TCP	192.168.1.20:1356	192.168.1.20:1026	ESTABLISHED
TCP	192.168.1.20:1914	192.168.1.20:389	CLOSE_WAIT
TCP	192.168.1.20:1917	192.168.1.20:3268	CLOSE_WAIT
TCP	192.168.1.20:3268	192.168.1.20:45427	ESTABLISHED
TCP	192.168.1.20:3268	192.168.1.20:45432	ESTABLISHED
TCP	192.168.1.20:3268	192.168.1.20:45434	ESTABLISHED
TCP	192.168.1.20:3268	192.168.1.20:45439	ESTABLISHED
TCP	192.168.1.20:41522	192.168.1.20:389	CLOSE_WAIT
TCP	192.168.1.20:41523	192.168.1.20:3268	CLOSE_WAIT
TCP	192.168.1.20:43565	192.168.1.20:691	ESTABLISHED
TCP	192.168.1.20:45427	192.168.1.20:3268	ESTABLISHED
TCP	192.168.1.20:45429	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:45430	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:45431	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:45432	192.168.1.20:3268	ESTABLISHED
TCP	192.168.1.20:45433	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:45434	192.168.1.20:3268	ESTABLISHED
TCP	192.168.1.20:45435	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:45436	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:45438	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:45439	192.168.1.20:3268	ESTABLISHED
TCP	192.168.1.20:45440	192.168.1.20:389	ESTABLISHED



TCP	192.168.1.20:45441	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:45442	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:45443	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:45444	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:45445	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:45447	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:45448	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:45449	192.168.1.20:389	CLOSE_WAIT
TCP	192.168.1.20:45451	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:45578	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:46982	192.168.1.20:1026	ESTABLISHED
TCP	192.168.1.20:47152	192.168.1.20:389	CLOSE_WAIT
TCP	192.168.1.20:47544	192.168.1.20:389	CLOSE_WAIT
TCP	192.168.1.20:47603	192.168.1.20:135	TIME_WAIT
TCP	192.168.1.20:47605	192.168.1.20:135	TIME_WAIT
TCP	192.168.1.20:47606	192.168.1.20:1026	TIME_WAIT
TCP	192.168.1.20:47607	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:47608	192.168.1.20:135	TIME_WAIT
TCP	192.168.1.20:47609	192.168.1.20:1026	TIME_WAIT
TCP	192.168.1.20:47617	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:47618	192.168.1.20:135	ESTABLISHED
TCP	192.168.1.20:47619	192.168.1.20:1142	ESTABLISHED
UDP	0.0.0.0:42	*.*	
UDP	0.0.0.0:135	*.*	
UDP	0.0.0.0:445	*.*	



UDP	0.0.0.0:500	*.*
UDP	0.0.0.0:1035	*.*
UDP	0.0.0.0:1065	*.*
UDP	0.0.0.0:1072	*.*
UDP	0.0.0.0:1082	*.*
UDP	0.0.0.0:1101	*.*
UDP	0.0.0.0:1132	*.*
UDP	0.0.0.0:1172	*.*
UDP	0.0.0.0:1207	*.*
UDP	0.0.0.0:1434	*.*
UDP	0.0.0.0:2160	*.*
UDP	0.0.0.0:2161	*.*
UDP	0.0.0.0:3456	*.*
UDP	0.0.0.0:3457	*.*
UDP	0.0.0.0:4500	*.*
UDP	0.0.0.0:7846	*.*
UDP	0.0.0.0:38293	*.*
UDP	127.0.0.1:53	*.*
UDP	127.0.0.1:123	*.*
UDP	127.0.0.1:1064	*.*
UDP	127.0.0.1:1066	*.*
UDP	127.0.0.1:1083	*.*
UDP	127.0.0.1:1092	*.*
UDP	127.0.0.1:1102	*.*
UDP	127.0.0.1:1105	*.*



UDP 127.0.0.1:1141 *.*
UDP 127.0.0.1:1156 *.*
UDP 127.0.0.1:1163 *.*
UDP 127.0.0.1:1176 *.*
UDP 127.0.0.1:1185 *.*
UDP 127.0.0.1:1191 *.*
UDP 127.0.0.1:1200 *.*
UDP 127.0.0.1:1358 *.*
UDP 127.0.0.1:3456 *.*
UDP 127.0.0.1:3457 *.*
UDP 127.0.0.1:3979 *.*
UDP 127.0.0.1:14786 *.*
UDP 192.168.1.20:53 *.*
UDP 192.168.1.20:67 *.*
UDP 192.168.1.20:68 *.*
UDP 192.168.1.20:88 *.*
UDP 192.168.1.20:123 *.*
UDP 192.168.1.20:137 *.*
UDP 192.168.1.20:138 *.*
UDP 192.168.1.20:389 *.*
UDP 192.168.1.20:464 *.*
UDP 192.168.1.20:2535 *.*

C:\Documents and Settings\Administrator>Microsoft Windows [Version 5.2.3790]

(C) Copyright 1985-2003 Microsoft Corp.



C:\Documents and Settings\Administrator>systeminfo

Host Name: BOE
OS Name: Microsoft(R) Windows(R) Server 2003 for Small Business Server
OS Version: 5.2.3790 Service Pack 1 Build 3790
OS Manufacturer: Microsoft Corporation
OS Configuration: Primary Domain Controller
OS Build Type: Multiprocessor Free
Registered Owner: Allegheny County, PA
Registered Organization: Board of Elections
Product ID: 74995-OEM-4211904-03020
Original Install Date: 5/8/2006, 1:24:53 PM
System Up Time: 164 Days, 2 Hours, 40 Minutes, 51 Seconds
System Manufacturer: Dell Inc.
System Model: PowerEdge SC1420
System Type: X86-based PC
Processor(s): 2 Processor(s) Installed.
 [01]: x86 Family 15 Model 4 Stepping 3 GenuineIntel ~
3192 Mhz
 [02]: x86 Family 15 Model 4 Stepping 3 GenuineIntel ~
3192 Mhz
BIOS Version: DELL - 7
Windows Directory: C:\WINDOWS



System Directory: C:\WINDOWS\system32
Boot Device: \Device\HarddiskVolume2
System Locale: en-us;English (United States)
Input Locale: en-us;English (United States)
Time Zone: (GMT-05:00) Eastern Time (US & Canada)
Total Physical Memory: 2,046 MB
Available Physical Memory: 671 MB
Page File: Max Size: 3,435 MB
Page File: Available: 2,056 MB
Page File: In Use: 1,379 MB
Page File Location(s): C:\pagefile.sys
Domain: elections.local
Logon Server: \\BOE
Hotfix(s): 19 Hotfix(s) Installed.
[01]: File 1
[02]: File 1
[03]: File 1
[04]: File 1
[05]: File 1
[06]: File 1
[07]: File 1
[08]: File 1
[09]: File 1
[10]: Q147222
[11]: KB896358 - Update



[12]: KB896422 - Update

[13]: KB896424 - Update

[14]: KB896688 - Update

[15]: KB901214 - Update

[16]: KB902400 - Update

[17]: KB904706 - Update

[18]: KB908519 - Update

[19]: KB912919 - Update

Network Card(s): 1 NIC(s) Installed.

[01]: Intel(R) PRO/1000 MT Network Connection

Connection Name: Server LAN NIC

DHCP Enabled: No

IP address(es)

[01]: 192.168.1.20

C:\Documents and Settings\Administrator>

Post-Election Review:

The same output was capture from the system at the CLI and a file diff was performed. Below are the differences.

Internet Address	Physical Address	Type
192.168.1.11	18-03-73-14-1c-2c	dynamic
192.168.1.12	18-03-73-15-97-68	dynamic
192.168.1.101	00-19-b9-1f-f2-17	dynamic

Internet Address	Physical Address	Type
192.168.1.1	00-00-00-00-00-00	invalid
192.168.1.11	18-03-73-14-1c-2c	dynamic
192.168.1.12	18-03-73-15-97-68	dynamic
192.168.1.40	18-03-73-1b-cf-e2	dynamic
192.168.1.41	d4-be-d9-a4-d1-c5	dynamic
192.168.1.50	08-00-37-17-6c-0b	dynamic
192.168.1.101	00-19-b9-1f-f2-17	dynamic



C:\Users\Frank\OneDrive - solutions4networks Inc\COA\Air Gap Analysis\airgap_06Mar2018\BOE-PRE-AG.txt				C:\Users\Frank\OneDrive - solutions4networks Inc\COA\Air Gap Analysis\airgap_06Mar2018\BOE-Post-AG.txt			
TCP	0.0.0.0:34573	0.0.0.0:0	LISTENING	TCP	0.0.0.0:34573	0.0.0.0:0	LISTENING
TCP	127.0.0.1:389	127.0.0.1:45452	ESTABLISHE	TCP	127.0.0.1:389	127.0.0.1:14039	ESTABLISHE
TCP	127.0.0.1:1090	127.0.0.1:389	CLOSE_WAIT	TCP	127.0.0.1:1090	127.0.0.1:389	CLOSE_WAIT
TCP	127.0.0.1:1109	127.0.0.1:389	CLOSE_WAIT	TCP	127.0.0.1:1109	127.0.0.1:389	CLOSE_WAIT
TCP	127.0.0.1:1158	127.0.0.1:389	CLOSE_WAIT	TCP	127.0.0.1:1158	127.0.0.1:389	CLOSE_WAIT
TCP	127.0.0.1:14039	127.0.0.1:389	ESTABLISHE	TCP	127.0.0.1:14039	127.0.0.1:389	ESTABLISHE
TCP	127.0.0.1:43563	127.0.0.1:389	CLOSE_WAIT	TCP	127.0.0.1:43563	127.0.0.1:389	CLOSE_WAIT
TCP	127.0.0.1:45452	127.0.0.1:389	ESTABLISHE	TCP	127.0.0.1:45452	127.0.0.1:389	ESTABLISHE
TCP	192.168.1.20:135	192.168.1.20:1175	ESTABLISHE	TCP	192.168.1.20:135	192.168.1.20:1175	ESTABLISHE
TCP	192.168.1.20:135	192.168.1.20:47618	ESTABLISHE	TCP	192.168.1.20:135	192.168.1.20:47618	ESTABLISHE
TCP	192.168.1.20:135	192.168.1.101:1077	ESTABLISHE	TCP	192.168.1.20:135	192.168.1.101:1077	ESTABLISHE
TCP	192.168.1.20:139	0.0.0.0:0	LISTENING	TCP	192.168.1.20:139	0.0.0.0:0	LISTENING
TCP	192.168.1.20:139	192.168.1.12:2037	ESTABLISHE	TCP	192.168.1.20:139	192.168.1.101:1072	ESTABLISHE
TCP	192.168.1.20:389	192.168.1.20:45429	ESTABLISHE	TCP	192.168.1.20:389	192.168.1.20:14022	ESTABLISHE
TCP	192.168.1.20:389	192.168.1.20:45430	ESTABLISHE	TCP	192.168.1.20:389	192.168.1.20:14025	ESTABLISHE
TCP	192.168.1.20:389	192.168.1.20:45431	ESTABLISHE	TCP	192.168.1.20:389	192.168.1.20:14027	ESTABLISHE
TCP	192.168.1.20:389	192.168.1.20:45433	ESTABLISHE	TCP	192.168.1.20:389	192.168.1.20:14028	ESTABLISHE
TCP	192.168.1.20:389	192.168.1.20:45435	ESTABLISHE	TCP	192.168.1.20:389	192.168.1.20:14029	ESTABLISHE
TCP	192.168.1.20:389	192.168.1.20:45436	ESTABLISHE	TCP	192.168.1.20:389	192.168.1.20:14031	ESTABLISHE
TCP	192.168.1.20:389	192.168.1.20:45438	ESTABLISHE	TCP	192.168.1.20:389	192.168.1.20:14032	ESTABLISHE
TCP	192.168.1.20:389	192.168.1.20:45440	ESTABLISHE	TCP	192.168.1.20:389	192.168.1.20:14034	ESTABLISHE
TCP	192.168.1.20:389	192.168.1.20:45441	ESTABLISHE	TCP	192.168.1.20:389	192.168.1.20:14035	ESTABLISHE
TCP	192.168.1.20:389	192.168.1.20:45442	ESTABLISHE	TCP	192.168.1.20:389	192.168.1.20:14036	ESTABLISHE
TCP	192.168.1.20:389	192.168.1.20:45443	ESTABLISHE	TCP	192.168.1.20:389	192.168.1.20:14037	ESTABLISHE
TCP	192.168.1.20:389	192.168.1.20:45444	ESTABLISHE	TCP	192.168.1.20:389	192.168.1.20:14038	ESTABLISHE
TCP	192.168.1.20:389	192.168.1.20:45445	ESTABLISHE	TCP	192.168.1.20:389	192.168.1.20:14039	ESTABLISHE
TCP	192.168.1.20:389	192.168.1.20:45447	ESTABLISHE	TCP	192.168.1.20:389	192.168.1.20:14040	ESTABLISHE
TCP	192.168.1.20:389	192.168.1.20:45448	ESTABLISHE	TCP	192.168.1.20:389	192.168.1.20:14041	ESTABLISHE
TCP	192.168.1.20:389	192.168.1.20:45451	ESTABLISHE	TCP	192.168.1.20:389	192.168.1.20:14042	ESTABLISHE
TCP	192.168.1.20:389	192.168.1.20:45578	ESTABLISHE	TCP	192.168.1.20:389	192.168.1.20:14043	ESTABLISHE
TCP	192.168.1.20:389	192.168.1.20:47544	FIN_WAIT_2	TCP	192.168.1.20:389	192.168.1.20:14044	ESTABLISHE
TCP	192.168.1.20:389	192.168.1.20:47607	ESTABLISHE	TCP	192.168.1.20:389	192.168.1.20:14045	ESTABLISHE
TCP	192.168.1.20:389	192.168.1.20:47617	ESTABLISHE	TCP	192.168.1.20:445	192.168.1.11:1101	ESTABLISHE
TCP	192.168.1.20:389	192.168.1.20:47621	TIME_WAIT	TCP	192.168.1.20:445	192.168.1.12:1121	ESTABLISHE
TCP	192.168.1.20:389	192.168.1.20:47621	TIME_WAIT	TCP	192.168.1.20:445	192.168.1.40:1098	ESTABLISHE

TCP	192.168.1.20:445	192.168.1.40:1098	ESTABLISHE
TCP	192.168.1.20:445	192.168.1.41:1081	ESTABLISHE

TCP	192.168.1.20:1026	192.168.1.20:46982	ESTABLISHE
TCP	192.168.1.20:1026	192.168.1.20:12782	ESTABLISHE

C:\Users\Frank\OneDrive - solutions4networks Inc\COA\Air Gap Analysis\airgap_06Mar2018\BOE-PRE-AG.txt				C:\Users\Frank\OneDrive - solutions4networks Inc\COA\Air Gap Analysis\airgap_06Mar2018\BOE-Post-AG.txt			
TCP	192.168.1.20:3268	192.168.1.20:45427	ESTABLISHE	TCP	192.168.1.20:3268	192.168.1.20:14023	ESTABLISHE
TCP	192.168.1.20:3268	192.168.1.20:45432	ESTABLISHE	TCP	192.168.1.20:3268	192.168.1.20:14026	ESTABLISHE
TCP	192.168.1.20:3268	192.168.1.20:45434	ESTABLISHE	TCP	192.168.1.20:3268	192.168.1.20:14033	ESTABLISHE
TCP	192.168.1.20:3268	192.168.1.20:45439	ESTABLISHE	TCP	192.168.1.20:3268	192.168.1.20:14038	ESTABLISHE
TCP	192.168.1.20:12782	192.168.1.20:1026	ESTABLISHE	TCP	192.168.1.20:12782	192.168.1.20:1026	ESTABLISHE
TCP	192.168.1.20:13664	192.168.1.20:389	CLOSE_WAIT	TCP	192.168.1.20:13664	192.168.1.20:389	CLOSE_WAIT
TCP	192.168.1.20:14022	192.168.1.20:389	ESTABLISHE	TCP	192.168.1.20:14022	192.168.1.20:389	ESTABLISHE
TCP	192.168.1.20:14023	192.168.1.20:3268	ESTABLISHE	TCP	192.168.1.20:14023	192.168.1.20:3268	ESTABLISHE
TCP	192.168.1.20:14025	192.168.1.20:389	ESTABLISHE	TCP	192.168.1.20:14025	192.168.1.20:389	ESTABLISHE
TCP	192.168.1.20:14026	192.168.1.20:3268	ESTABLISHE	TCP	192.168.1.20:14026	192.168.1.20:3268	ESTABLISHE
TCP	192.168.1.20:14027	192.168.1.20:389	ESTABLISHE	TCP	192.168.1.20:14027	192.168.1.20:389	ESTABLISHE
TCP	192.168.1.20:14028	192.168.1.20:389	ESTABLISHE	TCP	192.168.1.20:14028	192.168.1.20:389	ESTABLISHE
TCP	192.168.1.20:14029	192.168.1.20:389	ESTABLISHE	TCP	192.168.1.20:14029	192.168.1.20:389	ESTABLISHE
TCP	192.168.1.20:14030	192.168.1.20:389	CLOSE_WAIT	TCP	192.168.1.20:14030	192.168.1.20:389	CLOSE_WAIT
TCP	192.168.1.20:14031	192.168.1.20:389	ESTABLISHE	TCP	192.168.1.20:14031	192.168.1.20:389	ESTABLISHE
TCP	192.168.1.20:14032	192.168.1.20:389	ESTABLISHE	TCP	192.168.1.20:14032	192.168.1.20:389	ESTABLISHE
TCP	192.168.1.20:14033	192.168.1.20:3268	ESTABLISHE	TCP	192.168.1.20:14033	192.168.1.20:3268	ESTABLISHE
TCP	192.168.1.20:14034	192.168.1.20:389	ESTABLISHE	TCP	192.168.1.20:14034	192.168.1.20:389	ESTABLISHE
TCP	192.168.1.20:14035	192.168.1.20:389	ESTABLISHE	TCP	192.168.1.20:14035	192.168.1.20:389	ESTABLISHE
TCP	192.168.1.20:14036	192.168.1.20:389	ESTABLISHE	TCP	192.168.1.20:14036	192.168.1.20:389	ESTABLISHE
TCP	192.168.1.20:14037	192.168.1.20:389	ESTABLISHE	TCP	192.168.1.20:14037	192.168.1.20:389	ESTABLISHE
TCP	192.168.1.20:14038	192.168.1.20:3268	ESTABLISHE	TCP	192.168.1.20:14038	192.168.1.20:3268	ESTABLISHE
TCP	192.168.1.20:14040	192.168.1.20:389	ESTABLISHE	TCP	192.168.1.20:14040	192.168.1.20:389	ESTABLISHE
TCP	192.168.1.20:14041	192.168.1.20:389	ESTABLISHE	TCP	192.168.1.20:14041	192.168.1.20:389	ESTABLISHE
TCP	192.168.1.20:14042	192.168.1.20:389	ESTABLISHE	TCP	192.168.1.20:14042	192.168.1.20:389	ESTABLISHE
TCP	192.168.1.20:14043	192.168.1.20:389	ESTABLISHE	TCP	192.168.1.20:14043	192.168.1.20:389	ESTABLISHE
TCP	192.168.1.20:14044	192.168.1.20:389	ESTABLISHE	TCP	192.168.1.20:14044	192.168.1.20:389	ESTABLISHE
TCP	192.168.1.20:14045	192.168.1.20:389	ESTABLISHE	TCP	192.168.1.20:14045	192.168.1.20:389	ESTABLISHE
TCP	192.168.1.20:14190	192.168.1.20:389	ESTABLISHE	TCP	192.168.1.20:14190	192.168.1.20:389	ESTABLISHE
TCP	192.168.1.20:14204	192.168.1.20:389	ESTABLISHE	TCP	192.168.1.20:14204	192.168.1.20:389	ESTABLISHE
TCP	192.168.1.20:14231	192.168.1.20:135	TIME_WAIT	TCP	192.168.1.20:14231	192.168.1.20:135	TIME_WAIT



TCP	192.168.1.20:45427	192.168.1.20:3268	ESTABLISHE
TCP	192.168.1.20:45429	192.168.1.20:389	ESTABLISHE
TCP	192.168.1.20:45430	192.168.1.20:389	ESTABLISHE
TCP	192.168.1.20:45431	192.168.1.20:389	ESTABLISHE
TCP	192.168.1.20:45432	192.168.1.20:3268	ESTABLISHE
TCP	192.168.1.20:45433	192.168.1.20:389	ESTABLISHE
TCP	192.168.1.20:45434	192.168.1.20:3268	ESTABLISHE
TCP	192.168.1.20:45435	192.168.1.20:389	ESTABLISHE
TCP	192.168.1.20:45436	192.168.1.20:389	ESTABLISHE
TCP	192.168.1.20:45438	192.168.1.20:389	ESTABLISHE
TCP	192.168.1.20:45439	192.168.1.20:3268	ESTABLISHE
TCP	192.168.1.20:45440	192.168.1.20:389	ESTABLISHE
TCP	192.168.1.20:45441	192.168.1.20:389	ESTABLISHE
TCP	192.168.1.20:45442	192.168.1.20:389	ESTABLISHE
TCP	192.168.1.20:45443	192.168.1.20:389	ESTABLISHE
TCP	192.168.1.20:45444	192.168.1.20:389	ESTABLISHE
TCP	192.168.1.20:45445	192.168.1.20:389	ESTABLISHE
TCP	192.168.1.20:45447	192.168.1.20:389	ESTABLISHE
TCP	192.168.1.20:45448	192.168.1.20:389	ESTABLISHE
TCP	192.168.1.20:45449	192.168.1.20:389	CLOSE_WAIT
TCP	192.168.1.20:45451	192.168.1.20:389	ESTABLISHE
TCP	192.168.1.20:45578	192.168.1.20:389	ESTABLISHE
TCP	192.168.1.20:46982	192.168.1.20:1026	ESTABLISHE
TCP	192.168.1.20:47152	192.168.1.20:389	CLOSE_WAIT
TCP	192.168.1.20:47544	192.168.1.20:389	CLOSE_WAIT
TCP	192.168.1.20:47603	192.168.1.20:135	TIME_WAIT
TCP	192.168.1.20:47605	192.168.1.20:135	TIME_WAIT
TCP	192.168.1.20:47606	192.168.1.20:1026	TIME_WAIT
TCP	192.168.1.20:47607	192.168.1.20:389	ESTABLISHE
TCP	192.168.1.20:47608	192.168.1.20:135	TIME_WAIT
TCP	192.168.1.20:47609	192.168.1.20:1026	TIME_WAIT
TCP	192.168.1.20:47617	192.168.1.20:389	ESTABLISHE
TCP	192.168.1.20:47618	192.168.1.20:135	ESTABLISHE
TCP	192.168.1.20:47619	192.168.1.20:1142	ESTABLISHE

System Up Time: 164 Days, 2 Hours, 40 Minutes, 51 Seco | System Up Time: 167 Days, 2 Hours, 31 Minutes, 22 Seco

Available Physical Memory: 671 MB | Available Physical Memory: 661 MB

TAB5.elections.local

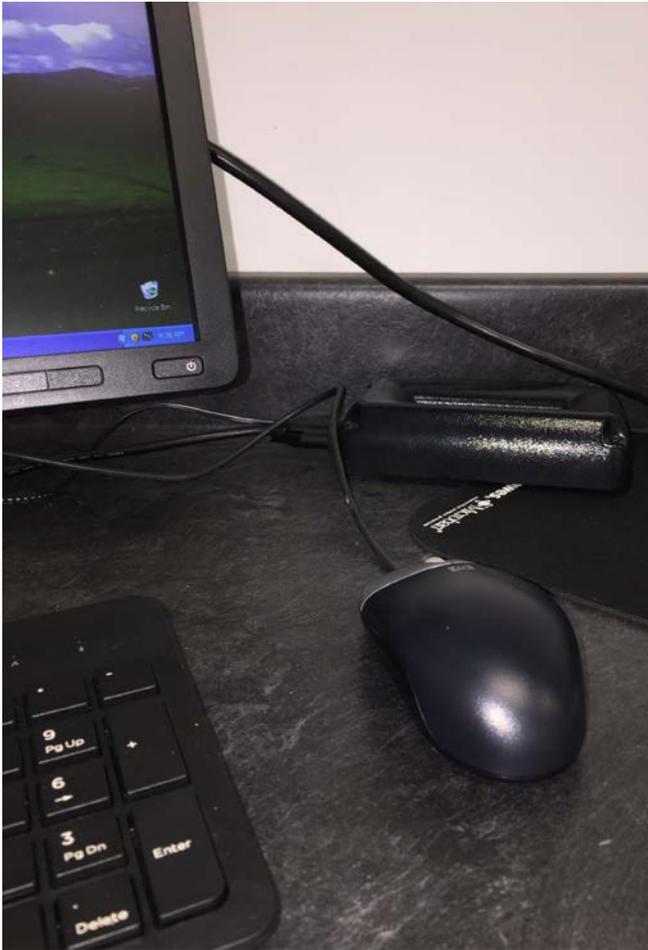
TAB5 Front



TAB5 Rear



TAB5 Desktop



Additional Information Collected from TAB5 CLI:

Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.

```
C:\Documents and Settings\administrator.ELECTIONS>hostname
```

TAB5

```
C:\Documents and Settings\administrator.ELECTIONS>whoami
```

'whoami' is not recognized as an internal or external command,
operable program or batch file.



DNS Servers : 192.168.1.20
 Primary WINS Server : 192.168.1.20
 Lease Obtained. : Sunday, March 04, 2018 9:03:16 AM
 Lease Expires : Monday, March 12, 2018 9:03:16 AM

C:\Documents and Settings\administrator.ELECTIONS>arp -a

Interface: 192.168.1.11 --- 0x2

Internet Address	Physical Address	Type
192.168.1.20	00-14-22-60-3f-94	dynamic

C:\Documents and Settings\administrator.ELECTIONS>Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\administrator.ELECTIONS>netstat -rn

Route Table

=====

Interface List

0x1 MS TCP Loopback interface
 0x2 ...18 03 73 14 1c 2c Intel(R) 82579LM Gigabit Network Connection - Pa
 cket Scheduler Miniport

=====

=====

Active Routes:



Network	Destination	Netmask	Gateway	Interface	Metric
	0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.11	10
	127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
	192.168.1.0	255.255.255.0	192.168.1.11	192.168.1.11	10
	192.168.1.11	255.255.255.255	127.0.0.1	127.0.0.1	10
	192.168.1.255	255.255.255.255	192.168.1.11	192.168.1.11	10
	224.0.0.0	240.0.0.0	192.168.1.11	192.168.1.11	10
	255.255.255.255	255.255.255.255	192.168.1.11	192.168.1.11	1

Default Gateway: 192.168.1.1

=====

Persistent Routes:

None

C:\Documents and Settings\administrator.ELECTIONS>netstat -an

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3306	0.0.0.0:0	LISTENING
TCP	127.0.0.1:1036	127.0.0.1:1037	ESTABLISHED
TCP	127.0.0.1:1037	127.0.0.1:1036	ESTABLISHED
TCP	127.0.0.1:1043	0.0.0.0:0	LISTENING
TCP	127.0.0.1:1044	0.0.0.0:0	LISTENING



```
TCP 192.168.1.11:139 0.0.0.0:0 LISTENING
TCP 192.168.1.11:2201 192.168.1.20:135 TIME_WAIT
TCP 192.168.1.11:2202 192.168.1.20:1026 TIME_WAIT
UDP 0.0.0.0:445 *.*
UDP 0.0.0.0:500 *.*
UDP 0.0.0.0:4500 *.*
UDP 127.0.0.1:123 *.*
UDP 127.0.0.1:1025 *.*
UDP 127.0.0.1:1048 *.*
UDP 127.0.0.1:1900 *.*
UDP 192.168.1.11:123 *.*
UDP 192.168.1.11:137 *.*
UDP 192.168.1.11:138 *.*
UDP 192.168.1.11:1900 *.*
```

C:\Documents and Settings\administrator.ELECTIONS>Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\administrator.ELECTIONS>systeminfo

```
Host Name:          TAB5
OS Name:            Microsoft Windows XP Professional
OS Version:        5.1.2600 Service Pack 3 Build 2600
OS Manufacturer:   Microsoft Corporation
OS Configuration:  Member Workstation
```



OS Build Type: Multiprocessor Free

Registered Owner: admin

Registered Organization:

Product ID: 76487-OEM-0060807-79698

Original Install Date: 8/2/2016, 6:04:17 PM

System Up Time: 5 Days, 0 Hours, 7 Minutes, 9 Seconds

System Manufacturer: Dell Inc.

System Model: OptiPlex 790

System type: X86-based PC

Processor(s): 1 Processor(s) Installed.

[01]: x86 Family 6 Model 42 Stepping 7 GenuineIntel ~
3092 Mhz

BIOS Version: DELL - 6222004

Windows Directory: C:\WINDOWS

System Directory: C:\WINDOWS\system32

Boot Device: \Device\HarddiskVolume1

System Locale: en-us;English (United States)

Input Locale: en-us;English (United States)

Time Zone: (GMT-05:00) Eastern Time (US & Canada)

Total Physical Memory: 3,241 MB

Available Physical Memory: 2,779 MB

Virtual Memory: Max Size: 2,048 MB

Virtual Memory: Available: 2,008 MB

Virtual Memory: In Use: 40 MB

Page File Location(s): C:\pagefile.sys



Domain: elections.local

Logon Server: \\BOE

Hotfix(s): 250 Hotfix(s) Installed.

[01]: File 1

[02]: File 1

[03]: File 1

[04]: File 1

[05]: File 1

[06]: File 1

[07]: File 1

[08]: File 1

[09]: File 1

[10]: File 1

[11]: File 1

[12]: File 1

[13]: File 1

[14]: File 1

[15]: File 1

[16]: File 1

[17]: File 1

[18]: File 1

[19]: File 1

[20]: File 1

[21]: File 1

[22]: File 1



[23]: File 1

[24]: File 1

[25]: File 1

[26]: File 1

[27]: File 1

[28]: File 1

[29]: File 1

[30]: File 1

[31]: File 1

[32]: File 1

[33]: File 1

[34]: File 1

[35]: File 1

[36]: File 1

[37]: File 1

[38]: File 1

[39]: File 1

[40]: File 1

[41]: File 1

[42]: File 1

[43]: File 1

[44]: File 1

[45]: File 1

[46]: File 1

[47]: File 1



[48]: File 1

[49]: File 1

[50]: File 1

[51]: File 1

[52]: File 1

[53]: File 1

[54]: File 1

[55]: File 1

[56]: File 1

[57]: File 1

[58]: File 1

[59]: File 1

[60]: File 1

[61]: File 1

[62]: File 1

[63]: File 1

[64]: File 1

[65]: File 1

[66]: File 1

[67]: File 1

[68]: File 1

[69]: File 1

[70]: File 1

[71]: File 1

[72]: File 1



[73]: File 1

[74]: File 1

[75]: File 1

[76]: File 1

[77]: File 1

[78]: File 1

[79]: File 1

[80]: File 1

[81]: File 1

[82]: File 1

[83]: File 1

[84]: File 1

[85]: File 1

[86]: File 1

[87]: File 1

[88]: File 1

[89]: File 1

[90]: File 1

[91]: File 1

[92]: File 1

[93]: File 1

[94]: File 1

[95]: File 1

[96]: File 1

[97]: File 1



- [98]: File 1
- [99]: File 1
- [100]: File 1
- [101]: File 1
- [102]: File 1
- [103]: File 1
- [104]: File 1
- [105]: File 1
- [106]: File 1
- [107]: File 1
- [108]: File 1
- [109]: File 1
- [110]: File 1
- [111]: File 1
- [112]: File 1
- [113]: File 1
- [114]: File 1
- [115]: File 1
- [116]: File 1
- [117]: File 1
- [118]: File 1
- [119]: File 1
- [120]: File 1
- [121]: File 1
- [122]: Q147222



- [123]: KB2378111_WM9
- [124]: KB2803821-v2_WM9
- [125]: KB952069_WM9
- [126]: KB954155_WM9
- [127]: KB973540_WM9
- [128]: KB975558_WM8
- [129]: KB978695_WM9
- [130]: KB2564958 - Update
- [131]: KB936929 - Service Pack
- [132]: KB2115168 - Update
- [133]: KB2229593 - Update
- [134]: KB2296011 - Update
- [135]: KB2347290 - Update
- [136]: KB2387149 - Update
- [137]: KB2393802 - Update
- [138]: KB2419632 - Update
- [139]: KB2423089 - Update
- [140]: KB2443105 - Update
- [141]: KB2478960 - Update
- [142]: KB2478971 - Update
- [143]: KB2479943 - Update
- [144]: KB2481109 - Update
- [145]: KB2483185 - Update
- [146]: KB2485663 - Update
- [147]: KB2506212 - Update



- [148]: KB2507938 - Update
- [149]: KB2508429 - Update
- [150]: KB2509553 - Update
- [151]: KB2510581 - Update
- [152]: KB2535512 - Update
- [153]: KB2536276-v2 - Update
- [154]: KB2544893-v2 - Update
- [155]: KB2566454 - Update
- [156]: KB2570947 - Update
- [157]: KB2584146 - Update
- [158]: KB2585542 - Update
- [159]: KB2592799 - Update
- [160]: KB2598479 - Update
- [161]: KB2603381 - Update
- [162]: KB2619339 - Update
- [163]: KB2620712 - Update
- [164]: KB2631813 - Update
- [165]: KB2653956 - Update
- [166]: KB2655992 - Update
- [167]: KB2659262 - Update
- [168]: KB2661637 - Update
- [169]: KB2676562 - Update
- [170]: KB2686509 - Update
- [171]: KB2691442 - Update
- [172]: KB2698365 - Update



- [173]: KB2705219-v2 - Update
- [174]: KB2712808 - Update
- [175]: KB2719985 - Update
- [176]: KB2723135-v2 - Update
- [177]: KB2727528 - Update
- [178]: KB2757638 - Update
- [179]: KB2770660 - Update
- [180]: KB2780091 - Update
- [181]: KB2802968 - Update
- [182]: KB2807986 - Update
- [183]: KB2813345 - Update
- [184]: KB2820917 - Update
- [185]: KB2834886 - Update
- [186]: KB2847311 - Update
- [187]: KB2850869 - Update
- [188]: KB2859537 - Update
- [189]: KB2862152 - Update
- [190]: KB2862330 - Update
- [191]: KB2862335 - Update
- [192]: KB2864063 - Update
- [193]: KB2868038 - Update
- [194]: KB2868626 - Update
- [195]: KB2876217 - Update
- [196]: KB2876331 - Update
- [197]: KB2884256 - Update



- [198]: KB2892075 - Update
- [199]: KB2893294 - Update
- [200]: KB2898715 - Update
- [201]: KB2900986 - Update
- [202]: KB2904266 - Update
- [203]: KB2909212 - Update
- [204]: KB2914368 - Update
- [205]: KB2916036 - Update
- [206]: KB2922229 - Update
- [207]: KB2929961 - Update
- [208]: KB2930275 - Update
- [209]: KB2936068 - Update
- [210]: KB2964358 - Update
- [211]: KB923561 - Update
- [212]: KB942288-v3 - Update
- [213]: KB946648 - Update
- [214]: KB950762 - Update
- [215]: KB950974 - Update
- [216]: KB951376-v2 - Update
- [217]: KB952004 - Update
- [218]: KB95

NetWork Card(s): 1 NIC(s) Installed.

[01]: Intel(R) 82579LM Gigabit Network Connection

Connection Name: Local Area Connection



DHCP Enabled: Yes
 DHCP Server: 192.168.1.20
 IP address(es)
 [01]: 192.168.1.11

C:\Documents and Settings\administrator.ELECTIONS>

Post-Election Review:

The same output was capture from the system at the CLI and a file diff was performed. Below are the differences.

```
Lease Obtained. . . . . : Sunday, March 04, 2018 9:03:11
Lease Expires . . . . . : Monday, March 12, 2018 9:03:11
Lease Obtained. . . . . : Thursday, March 08, 2018 8:44:00
Lease Expires . . . . . : Friday, March 16, 2018 8:44:00
```

C:\Users\Frank\OneDrive - solutions4networks Inc\COA\Air Gap Analysis\airgap_06Mar2018\TAB5-PRE-AG.txt	C:\Users\Frank\OneDrive - solutions4networks Inc\COA\Air Gap Analysis\airgap_06Mar2018\TAB5-Post-AG.txt
127.0.0.1:1037 127.0.0.1:1036 ESTABLISHED	127.0.0.1:1037 127.0.0.1:1036 ESTABLISHED
127.0.0.1:1043 0.0.0.0:0 LISTENING	127.0.0.1:1043 0.0.0.0:0 LISTENING
127.0.0.1:1044 0.0.0.0:0 LISTENING	127.0.0.1:1051 0.0.0.0:0 LISTENING
192.168.1.11:139 0.0.0.0:0 LISTENING	192.168.1.11:139 0.0.0.0:0 LISTENING
192.168.1.11:2201 192.168.1.20:135 TIME_WAIT	192.168.1.11:1101 192.168.1.20:445 ESTABLISHED
192.168.1.11:2202 192.168.1.20:1026 TIME_WAIT	
0.0.0.0:445 **:*	0.0.0.0:445 **:*
0.0.0.0:500 **:*	0.0.0.0:500 **:*
0.0.0.0:4500 **:*	0.0.0.0:4500 **:*
127.0.0.1:123 **:*	127.0.0.1:123 **:*
127.0.0.1:1025 **:*	127.0.0.1:1025 **:*
127.0.0.1:1048 **:*	127.0.0.1:1047 **:*

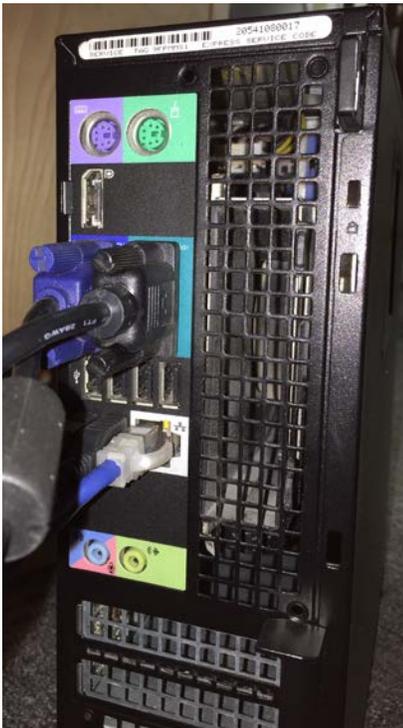
C:\Users\Frank\OneDrive - solutions4networks Inc\COA\Air Gap Analysis\airgap_06Mar2018\TAB5-PRE-AG.txt	C:\Users\Frank\OneDrive - solutions4networks Inc\COA\Air Gap Analysis\airgap_06Mar2018\TAB5-Post-AG.txt
Registered Organization:	Registered Organization:
Product ID: 76487-OEM-0060807-79698	Product ID: 76487-OEM-0060807-79698
Original Install Date: 8/2/2016, 6:04:17 PM	Original Install Date: 8/2/2016, 6:04:17 PM
System Up Time: 5 Days, 0 Hours, 7 Minutes, 9 Seconds	System Up Time: 0 Days, 0 Hours, 13 Minutes, 53 Second
System Manufacturer: Dell Inc.	System Manufacturer: Dell Inc.
System Model: OptiPlex 790	System Model: OptiPlex 790
System type: X86-based PC	System type: X86-based PC
Processor(s): 1 Processor(s) Installed.	Processor(s): 1 Processor(s) Installed.
[01]: x86 Family 6 Model 42 Stepping 7	[01]: x86 Family 6 Model 42 Stepping 7
3092 Mhz	3093 Mhz
BIOS Version: DELL - 6222004	BIOS Version: DELL - 6222004
Windows Directory: C:\WINDOWS	Windows Directory: C:\WINDOWS
System Directory: C:\WINDOWS\system32	System Directory: C:\WINDOWS\system32
Boot Device: \Device\HarddiskVolumel	Boot Device: \Device\HarddiskVolumel
System Locale: en-us;English (United States)	System Locale: en-us;English (United States)
Input Locale: en-us;English (United States)	Input Locale: en-us;English (United States)
Time Zone: (GMT-05:00) Eastern Time (US & Canada)	Time Zone: (GMT-05:00) Eastern Time (US & Canada)
Total Physical Memory: 3,241 MB	Total Physical Memory: 3,241 MB
Available Physical Memory: 2,779 MB	Available Physical Memory: 2,813 MB
Virtual Memory: Max Size: 2,048 MB	Virtual Memory: Max Size: 2,048 MB
Virtual Memory: Available: 2,008 MB	Virtual Memory: Available: 2,008 MB
Virtual Memory: In Use: 40 MB	Virtual Memory: In Use: 40 MB
Page File Location(s): C:\pagefile.sys	Page File Location(s): C:\pagefile.sys
Domain: elections.local	Domain: elections.local
Logon Server: \\BOE	Logon Server: \\BOE

TAB9.elections.local

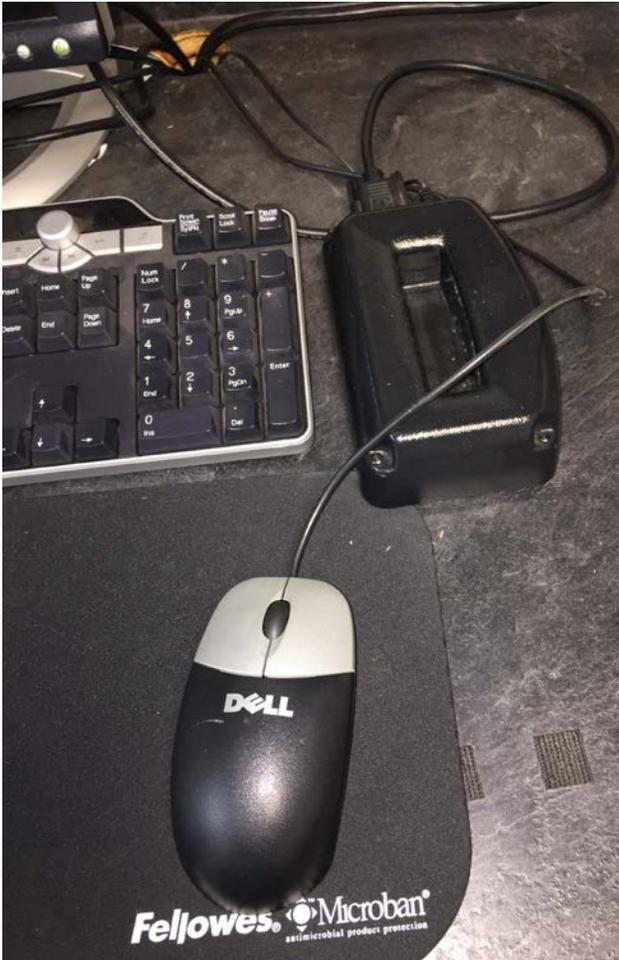
TAB9 Front



TAB9 Rear



TAB9 Desktop



Additional Information Collected from TAB9 CLI:

Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.

```
C:\Documents and Settings\Administrator.ELECTIONS>hostname
```

TAB9

```
C:\Documents and Settings\Administrator.ELECTIONS>whoami
```

'whoami' is not recognized as an internal or external command,



DHCP Server : 192.168.1.20
 DNS Servers : 192.168.1.20
 Primary WINS Server : 192.168.1.20
 Lease Obtained. : Sunday, March 04, 2018 9:02:34 AM
 Lease Expires : Monday, March 12, 2018 9:02:34 AM

C:\Documents and Settings\Administrator.ELECTIONS>arp -a

Interface: 192.168.1.12 --- 0x2

Internet Address	Physical Address	Type
192.168.1.20	00-14-22-60-3f-94	dynamic

C:\Documents and Settings\Administrator.ELECTIONS>Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator.ELECTIONS>netstat -rn

Route Table

=====

Interface List

0x1 MS TCP Loopback interface
 0x2 ...18 03 73 15 97 68 Intel(R) 82579LM Gigabit Network Connection - Pa
 cket Scheduler Miniport

=====

=====



Active Routes:

Network	Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.12		10
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1		1
192.168.1.0	255.255.255.0	192.168.1.12	192.168.1.12		10
192.168.1.12	255.255.255.255	127.0.0.1	127.0.0.1		10
192.168.1.255	255.255.255.255	192.168.1.12	192.168.1.12		10
224.0.0.0	240.0.0.0	192.168.1.12	192.168.1.12		10
255.255.255.255	255.255.255.255	192.168.1.12	192.168.1.12		1

Default Gateway: 192.168.1.1

=====

Persistent Routes:

None

C:\Documents and Settings\Administrator\ELECTIONS>netstat -an

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3306	0.0.0.0:0	LISTENING
TCP	127.0.0.1:1037	127.0.0.1:1038	ESTABLISHED
TCP	127.0.0.1:1038	127.0.0.1:1037	ESTABLISHED
TCP	127.0.0.1:1043	0.0.0.0:0	LISTENING



```
TCP 127.0.0.1:1044 0.0.0.0 LISTENING
TCP 192.168.1.12:139 0.0.0.0 LISTENING
TCP 192.168.1.12:2355 192.168.1.20:135 TIME_WAIT
TCP 192.168.1.12:2356 192.168.1.20:1026 TIME_WAIT
UDP 0.0.0.0:445 *.*
UDP 0.0.0.0:500 *.*
UDP 0.0.0.0:4500 *.*
UDP 127.0.0.1:123 *.*
UDP 127.0.0.1:1025 *.*
UDP 127.0.0.1:1048 *.*
UDP 127.0.0.1:1900 *.*
UDP 192.168.1.12:123 *.*
UDP 192.168.1.12:137 *.*
UDP 192.168.1.12:138 *.*
UDP 192.168.1.12:1900 *.*
```

C:\Documents and Settings\Administrator.ELECTIONS>Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator.ELECTIONS>systeminfo

```
Host Name:          TAB9
OS Name:            Microsoft Windows XP Professional
OS Version:        5.1.2600 Service Pack 3 Build 2600
OS Manufacturer:  Microsoft Corporation
```



OS Configuration: Member Workstation

OS Build Type: Multiprocessor Free

Registered Owner: admin

Registered Organization:

Product ID: 76487-OEM-0060807-79698

Original Install Date: 8/2/2016, 6:04:17 PM

System Up Time: 5 Days, 0 Hours, 13 Minutes, 38 Seconds

System Manufacturer: Dell Inc.

System Model: OptiPlex 790

System type: X86-based PC

Processor(s): 1 Processor(s) Installed.

[01]: x86 Family 6 Model 42 Stepping 7 GenuineIntel ~
3092 Mhz

BIOS Version: DELL - 6222004

Windows Directory: C:\WINDOWS

System Directory: C:\WINDOWS\system32

Boot Device: \Device\HarddiskVolume1

System Locale: en-us;English (United States)

Input Locale: en-us;English (United States)

Time Zone: (GMT-05:00) Eastern Time (US & Canada)

Total Physical Memory: 3,241 MB

Available Physical Memory: 2,746 MB

Virtual Memory: Max Size: 2,048 MB

Virtual Memory: Available: 1,996 MB

Virtual Memory: In Use: 52 MB



Page File Location(s): C:\pagefile.sys

Domain: elections.local

Logon Server: \\BOE

Hotfix(s): 250 Hotfix(s) Installed.

[01]: File 1

[02]: File 1

[03]: File 1

[04]: File 1

[05]: File 1

[06]: File 1

[07]: File 1

[08]: File 1

[09]: File 1

[10]: File 1

[11]: File 1

[12]: File 1

[13]: File 1

[14]: File 1

[15]: File 1

[16]: File 1

[17]: File 1

[18]: File 1

[19]: File 1

[20]: File 1

[21]: File 1



[22]: File 1

[23]: File 1

[24]: File 1

[25]: File 1

[26]: File 1

[27]: File 1

[28]: File 1

[29]: File 1

[30]: File 1

[31]: File 1

[32]: File 1

[33]: File 1

[34]: File 1

[35]: File 1

[36]: File 1

[37]: File 1

[38]: File 1

[39]: File 1

[40]: File 1

[41]: File 1

[42]: File 1

[43]: File 1

[44]: File 1

[45]: File 1

[46]: File 1



[47]: File 1

[48]: File 1

[49]: File 1

[50]: File 1

[51]: File 1

[52]: File 1

[53]: File 1

[54]: File 1

[55]: File 1

[56]: File 1

[57]: File 1

[58]: File 1

[59]: File 1

[60]: File 1

[61]: File 1

[62]: File 1

[63]: File 1

[64]: File 1

[65]: File 1

[66]: File 1

[67]: File 1

[68]: File 1

[69]: File 1

[70]: File 1

[71]: File 1



[72]: File 1

[73]: File 1

[74]: File 1

[75]: File 1

[76]: File 1

[77]: File 1

[78]: File 1

[79]: File 1

[80]: File 1

[81]: File 1

[82]: File 1

[83]: File 1

[84]: File 1

[85]: File 1

[86]: File 1

[87]: File 1

[88]: File 1

[89]: File 1

[90]: File 1

[91]: File 1

[92]: File 1

[93]: File 1

[94]: File 1

[95]: File 1

[96]: File 1



[97]: File 1

[98]: File 1

[99]: File 1

[100]: File 1

[101]: File 1

[102]: File 1

[103]: File 1

[104]: File 1

[105]: File 1

[106]: File 1

[107]: File 1

[108]: File 1

[109]: File 1

[110]: File 1

[111]: File 1

[112]: File 1

[113]: File 1

[114]: File 1

[115]: File 1

[116]: File 1

[117]: File 1

[118]: File 1

[119]: File 1

[120]: File 1

[121]: File 1



- [122]: Q147222
- [123]: KB2378111_WM9
- [124]: KB2803821-v2_WM9
- [125]: KB952069_WM9
- [126]: KB954155_WM9
- [127]: KB973540_WM9
- [128]: KB975558_WM8
- [129]: KB978695_WM9
- [130]: KB2564958 - Update
- [131]: KB936929 - Service Pack
- [132]: KB2115168 - Update
- [133]: KB2229593 - Update
- [134]: KB2296011 - Update
- [135]: KB2347290 - Update
- [136]: KB2387149 - Update
- [137]: KB2393802 - Update
- [138]: KB2419632 - Update
- [139]: KB2423089 - Update
- [140]: KB2443105 - Update
- [141]: KB2478960 - Update
- [142]: KB2478971 - Update
- [143]: KB2479943 - Update
- [144]: KB2481109 - Update
- [145]: KB2483185 - Update
- [146]: KB2485663 - Update



- [147]: KB2506212 - Update
- [148]: KB2507938 - Update
- [149]: KB2508429 - Update
- [150]: KB2509553 - Update
- [151]: KB2510581 - Update
- [152]: KB2535512 - Update
- [153]: KB2536276-v2 - Update
- [154]: KB2544893-v2 - Update
- [155]: KB2566454 - Update
- [156]: KB2570947 - Update
- [157]: KB2584146 - Update
- [158]: KB2585542 - Update
- [159]: KB2592799 - Update
- [160]: KB2598479 - Update
- [161]: KB2603381 - Update
- [162]: KB2619339 - Update
- [163]: KB2620712 - Update
- [164]: KB2631813 - Update
- [165]: KB2653956 - Update
- [166]: KB2655992 - Update
- [167]: KB2659262 - Update
- [168]: KB2661637 - Update
- [169]: KB2676562 - Update
- [170]: KB2686509 - Update
- [171]: KB2691442 - Update



- [172]: KB2698365 - Update
- [173]: KB2705219-v2 - Update
- [174]: KB2712808 - Update
- [175]: KB2719985 - Update
- [176]: KB2723135-v2 - Update
- [177]: KB2727528 - Update
- [178]: KB2757638 - Update
- [179]: KB2770660 - Update
- [180]: KB2780091 - Update
- [181]: KB2802968 - Update
- [182]: KB2807986 - Update
- [183]: KB2813345 - Update
- [184]: KB2820917 - Update
- [185]: KB2834886 - Update
- [186]: KB2847311 - Update
- [187]: KB2850869 - Update
- [188]: KB2859537 - Update
- [189]: KB2862152 - Update
- [190]: KB2862330 - Update
- [191]: KB2862335 - Update
- [192]: KB2864063 - Update
- [193]: KB2868038 - Update
- [194]: KB2868626 - Update
- [195]: KB2876217 - Update
- [196]: KB2876331 - Update



- [197]: KB2884256 - Update
- [198]: KB2892075 - Update
- [199]: KB2893294 - Update
- [200]: KB2898715 - Update
- [201]: KB2900986 - Update
- [202]: KB2904266 - Update
- [203]: KB2909212 - Update
- [204]: KB2914368 - Update
- [205]: KB2916036 - Update
- [206]: KB2922229 - Update
- [207]: KB2929961 - Update
- [208]: KB2930275 - Update
- [209]: KB2936068 - Update
- [210]: KB2964358 - Update
- [211]: KB923561 - Update
- [212]: KB942288-v3 - Update
- [213]: KB946648 - Update
- [214]: KB950762 - Update
- [215]: KB950974 - Update
- [216]: KB951376-v2 - Update
- [217]: KB952004 - Update
- [218]: KB95

NetWork Card(s): 1 NIC(s) Installed.

[01]: Intel(R) 82579LM Gigabit Network Connection



Connection Name: Local Area Connection

DHCP Enabled: Yes

DHCP Server: 192.168.1.20

IP address(es)

[01]: 192.168.1.12

C:\Documents and Settings\Administrator\ELECTIONS>

Post-Election Review:

The same output was capture from the system at the CLI and a file diff was performed. Below are the differences.

C:\Users\Frank\OneDrive - solutions4networks Inc\COA\Air Gap Analysis\airgap_06Mar2018\TAB9-PRE-AG.txt	C:\Users\Frank\OneDrive - solutions4networks Inc\COA\Air Gap Analysis\airgap_06Mar2018\TAB9-Post-AG.txt
Lease Obtained : Sunday, March 04, 2018 9:02:3	Lease Obtained : Thursday, March 08, 2018 8:48
Lease Expires : Monday, March 12, 2018 9:02:3	Lease Expires : Friday, March 16, 2018 8:48:5

C:\Users\Frank\OneDrive - solutions4networks Inc\COA\Air Gap Analysis\airgap_06Mar2018\TAB9-PRE-AG.txt	C:\Users\Frank\OneDrive - solutions4networks Inc\COA\Air Gap Analysis\airgap_06Mar2018\TAB9-Post-AG.txt
192.168.1.12:139 0.0.0.0:0 LISTENING	192.168.1.12:139 0.0.0.0:0 LISTENING
192.168.1.12:2355 192.168.1.20:135 TIME_WAIT	192.168.1.12:1121 192.168.1.20:445 ESTABLISHED
192.168.1.12:2356 192.168.1.20:1026 TIME_WAIT	

C:\Users\Frank\OneDrive - solutions4networks Inc\COA\Air Gap Analysis\airgap_06Mar2018\TAB9-PRE-AG.txt	C:\Users\Frank\OneDrive - solutions4networks Inc\COA\Air Gap Analysis\airgap_06Mar2018\TAB9-Post-AG.txt
Registered Organization:	Registered Organization:
Product ID: 76487-OEM-0060807-79698	Product ID: 76487-OEM-0060807-79698
Original Install Date: 8/2/2016, 6:04:17 PM	Original Install Date: 8/2/2016, 6:04:17 PM
System Up Time: 5 Days, 0 Hours, 13 Minutes, 38 Second	System Up Time: 0 Days, 0 Hours, 13 Minutes, 53 Second
System Manufacturer: Dell Inc.	System Manufacturer: Dell Inc.
System Model: OptiPlex 790	System Model: OptiPlex 790
System type: X86-based PC	System type: X86-based PC
Processor(s): 1 Processor(s) Installed. [01]: x86 Family 6 Model 42 Stepping 7	Processor(s): 1 Processor(s) Installed. [01]: x86 Family 6 Model 42 Stepping 7
3092 Mhz	3092 Mhz
BIOS Version: DELL - 6222004	BIOS Version: DELL - 6222004
Windows Directory: C:\WINDOWS	Windows Directory: C:\WINDOWS
System Directory: C:\WINDOWS\system32	System Directory: C:\WINDOWS\system32
Boot Device: \Device\HarddiskVolume1	Boot Device: \Device\HarddiskVolume1
System Locale: en-us:English (United States)	System Locale: en-us:English (United States)
Input Locale: en-us:English (United States)	Input Locale: en-us:English (United States)
Time Zone: (GMT-05:00) Eastern Time (US & Canada)	Time Zone: (GMT-05:00) Eastern Time (US & Canada)
Total Physical Memory: 3,241 MB	Total Physical Memory: 3,241 MB
Available Physical Memory: 2,746 MB	Available Physical Memory: 2,777 MB
Virtual Memory: Max Size: 2,048 MB	Virtual Memory: Max Size: 2,048 MB
Virtual Memory: Available: 1,996 MB	Virtual Memory: Available: 2,008 MB
Virtual Memory: In Use: 52 MB	Virtual Memory: In Use: 40 MB

TAB7.elections.local

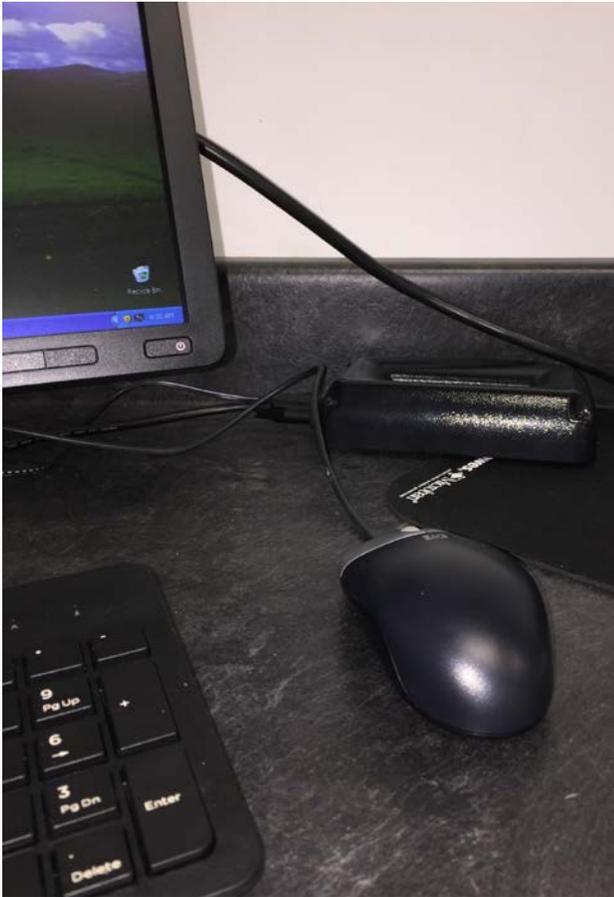
TAB7 Front



TAB7 Rear



TAB7 Desktop



Additional Information Collected from TAB7 CLI:

Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.

```
C:\Documents and Settings\Administrator.ELECTIONS>hostname
```

TAB7

```
C:\Documents and Settings\Administrator.ELECTIONS>whoami
```

'whoami' is not recognized as an internal or external command,
operable program or batch file.



DNS Servers : 192.168.1.20
Primary WINS Server : 192.168.1.20
Lease Obtained. : Monday, March 05, 2018 8:28:41 AM
Lease Expires : Tuesday, March 13, 2018 8:28:41 AM

C:\Documents and Settings\Administrator.ELECTIONS>arp -a

Interface: 192.168.1.40 --- 0x2

Internet Address	Physical Address	Type
192.168.1.20	00-14-22-60-3f-94	dynamic

C:\Documents and Settings\Administrator.ELECTIONS>Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator.ELECTIONS>netstat -rn

Route Table

=====

Interface List

0x1 MS TCP Loopback interface
0x2 ...18 03 73 1b cf e2 Intel(R) 82579LM Gigabit Network Connection - Pa
cket Scheduler Miniport

=====

=====

Active Routes:



Network	Destination	Netmask	Gateway	Interface	Metric
	0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.40	10
	127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
	192.168.1.0	255.255.255.0	192.168.1.40	192.168.1.40	10
	192.168.1.40	255.255.255.255	127.0.0.1	127.0.0.1	10
	192.168.1.255	255.255.255.255	192.168.1.40	192.168.1.40	10
	224.0.0.0	240.0.0.0	192.168.1.40	192.168.1.40	10
	255.255.255.255	255.255.255.255	192.168.1.40	192.168.1.40	1

Default Gateway: 192.168.1.1

=====

Persistent Routes:

None

C:\Documents and Settings\Administrator\ELECTIONS>netstat -an

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3306	0.0.0.0:0	LISTENING
TCP	127.0.0.1:1047	0.0.0.0:0	LISTENING
TCP	127.0.0.1:1048	127.0.0.1:1049	ESTABLISHED
TCP	127.0.0.1:1049	127.0.0.1:1048	ESTABLISHED
TCP	127.0.0.1:1055	0.0.0.0:0	LISTENING



TCP	192.168.1.40:139	0.0.0.0:0	LISTENING
TCP	192.168.1.40:2490	192.168.1.20:135	TIME_WAIT
TCP	192.168.1.40:2491	192.168.1.20:1026	TIME_WAIT
TCP	192.168.1.40:2494	192.168.1.20:445	ESTABLISHED
TCP	192.168.1.40:2496	192.168.1.20:1026	TIME_WAIT
TCP	192.168.1.40:2499	192.168.1.20:389	TIME_WAIT
TCP	192.168.1.40:2502	192.168.1.20:389	TIME_WAIT
TCP	192.168.1.40:2503	192.168.1.20:445	TIME_WAIT
TCP	192.168.1.40:2507	192.168.1.20:389	TIME_WAIT
TCP	192.168.1.40:2508	192.168.1.20:389	TIME_WAIT
TCP	192.168.1.40:2563	192.168.1.40:16992	ESTABLISHED
TCP	192.168.1.40:2566	192.168.1.40:16993	SYN_SENT
TCP	192.168.1.40:16992	192.168.1.40:2563	ESTABLISHED
UDP	0.0.0.0:445	*.*	
UDP	0.0.0.0:500	*.*	
UDP	0.0.0.0:4500	*.*	
UDP	127.0.0.1:123	*.*	
UDP	127.0.0.1:1025	*.*	
UDP	127.0.0.1:1041	*.*	
UDP	127.0.0.1:1900	*.*	
UDP	192.168.1.40:123	*.*	
UDP	192.168.1.40:137	*.*	
UDP	192.168.1.40:138	*.*	
UDP	192.168.1.40:1900	*.*	



C:\Documents and Settings\Administrator.ELECTIONS>Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator.ELECTIONS>systeminfo

Host Name: TAB7
OS Name: Microsoft Windows XP Professional
OS Version: 5.1.2600 Service Pack 3 Build 2600
OS Manufacturer: Microsoft Corporation
OS Configuration: Member Workstation
OS Build Type: Multiprocessor Free
Registered Owner: admin
Registered Organization:
Product ID: 76487-OEM-0060807-79698
Original Install Date: 8/2/2016, 6:04:17 PM
System Up Time: 0 Days, 0 Hours, 48 Minutes, 11 Seconds
System Manufacturer: Dell Inc.
System Model: OptiPlex 790
System type: X86-based PC
Processor(s): 1 Processor(s) Installed.
[01]: x86 Family 6 Model 42 Stepping 7 GenuineIntel ~
3092 Mhz
BIOS Version: DELL - 6222004
Windows Directory: C:\WINDOWS
System Directory: C:\WINDOWS\system32



Boot Device: \Device\HarddiskVolume1

System Locale: en-us;English (United States)

Input Locale: en-us;English (United States)

Time Zone: (GMT-05:00) Eastern Time (US & Canada)

Total Physical Memory: 3,241 MB

Available Physical Memory: 2,860 MB

Virtual Memory: Max Size: 2,048 MB

Virtual Memory: Available: 2,008 MB

Virtual Memory: In Use: 40 MB

Page File Location(s): C:\pagefile.sys

Domain: elections.local

Logon Server: \\BOE

Hotfix(s): 250 Hotfix(s) Installed.

 [01]: File 1

 [02]: File 1

 [03]: File 1

 [04]: File 1

 [05]: File 1

 [06]: File 1

 [07]: File 1

 [08]: File 1

 [09]: File 1

 [10]: File 1

 [11]: File 1

 [12]: File 1



[13]: File 1

[14]: File 1

[15]: File 1

[16]: File 1

[17]: File 1

[18]: File 1

[19]: File 1

[20]: File 1

[21]: File 1

[22]: File 1

[23]: File 1

[24]: File 1

[25]: File 1

[26]: File 1

[27]: File 1

[28]: File 1

[29]: File 1

[30]: File 1

[31]: File 1

[32]: File 1

[33]: File 1

[34]: File 1

[35]: File 1

[36]: File 1

[37]: File 1



[38]: File 1

[39]: File 1

[40]: File 1

[41]: File 1

[42]: File 1

[43]: File 1

[44]: File 1

[45]: File 1

[46]: File 1

[47]: File 1

[48]: File 1

[49]: File 1

[50]: File 1

[51]: File 1

[52]: File 1

[53]: File 1

[54]: File 1

[55]: File 1

[56]: File 1

[57]: File 1

[58]: File 1

[59]: File 1

[60]: File 1

[61]: File 1

[62]: File 1



[63]: File 1

[64]: File 1

[65]: File 1

[66]: File 1

[67]: File 1

[68]: File 1

[69]: File 1

[70]: File 1

[71]: File 1

[72]: File 1

[73]: File 1

[74]: File 1

[75]: File 1

[76]: File 1

[77]: File 1

[78]: File 1

[79]: File 1

[80]: File 1

[81]: File 1

[82]: File 1

[83]: File 1

[84]: File 1

[85]: File 1

[86]: File 1

[87]: File 1



[88]: File 1

[89]: File 1

[90]: File 1

[91]: File 1

[92]: File 1

[93]: File 1

[94]: File 1

[95]: File 1

[96]: File 1

[97]: File 1

[98]: File 1

[99]: File 1

[100]: File 1

[101]: File 1

[102]: File 1

[103]: File 1

[104]: File 1

[105]: File 1

[106]: File 1

[107]: File 1

[108]: File 1

[109]: File 1

[110]: File 1

[111]: File 1

[112]: File 1



- [113]: File 1
- [114]: File 1
- [115]: File 1
- [116]: File 1
- [117]: File 1
- [118]: File 1
- [119]: File 1
- [120]: File 1
- [121]: File 1
- [122]: Q147222
- [123]: KB2378111_WM9
- [124]: KB2803821-v2_WM9
- [125]: KB952069_WM9
- [126]: KB954155_WM9
- [127]: KB973540_WM9
- [128]: KB975558_WM8
- [129]: KB978695_WM9
- [130]: KB2564958 - Update
- [131]: KB936929 - Service Pack
- [132]: KB2115168 - Update
- [133]: KB2229593 - Update
- [134]: KB2296011 - Update
- [135]: KB2347290 - Update
- [136]: KB2387149 - Update
- [137]: KB2393802 - Update



- [138]: KB2419632 - Update
- [139]: KB2423089 - Update
- [140]: KB2443105 - Update
- [141]: KB2478960 - Update
- [142]: KB2478971 - Update
- [143]: KB2479943 - Update
- [144]: KB2481109 - Update
- [145]: KB2483185 - Update
- [146]: KB2485663 - Update
- [147]: KB2506212 - Update
- [148]: KB2507938 - Update
- [149]: KB2508429 - Update
- [150]: KB2509553 - Update
- [151]: KB2510581 - Update
- [152]: KB2535512 - Update
- [153]: KB2536276-v2 - Update
- [154]: KB2544893-v2 - Update
- [155]: KB2566454 - Update
- [156]: KB2570947 - Update
- [157]: KB2584146 - Update
- [158]: KB2585542 - Update
- [159]: KB2592799 - Update
- [160]: KB2598479 - Update
- [161]: KB2603381 - Update
- [162]: KB2619339 - Update



- [163]: KB2620712 - Update
- [164]: KB2631813 - Update
- [165]: KB2653956 - Update
- [166]: KB2655992 - Update
- [167]: KB2659262 - Update
- [168]: KB2661637 - Update
- [169]: KB2676562 - Update
- [170]: KB2686509 - Update
- [171]: KB2691442 - Update
- [172]: KB2698365 - Update
- [173]: KB2705219-v2 - Update
- [174]: KB2712808 - Update
- [175]: KB2719985 - Update
- [176]: KB2723135-v2 - Update
- [177]: KB2727528 - Update
- [178]: KB2757638 - Update
- [179]: KB2770660 - Update
- [180]: KB2780091 - Update
- [181]: KB2802968 - Update
- [182]: KB2807986 - Update
- [183]: KB2813345 - Update
- [184]: KB2820917 - Update
- [185]: KB2834886 - Update
- [186]: KB2847311 - Update
- [187]: KB2850869 - Update



- [188]: KB2859537 - Update
- [189]: KB2862152 - Update
- [190]: KB2862330 - Update
- [191]: KB2862335 - Update
- [192]: KB2864063 - Update
- [193]: KB2868038 - Update
- [194]: KB2868626 - Update
- [195]: KB2876217 - Update
- [196]: KB2876331 - Update
- [197]: KB2884256 - Update
- [198]: KB2892075 - Update
- [199]: KB2893294 - Update
- [200]: KB2898715 - Update
- [201]: KB2900986 - Update
- [202]: KB2904266 - Update
- [203]: KB2909212 - Update
- [204]: KB2914368 - Update
- [205]: KB2916036 - Update
- [206]: KB2922229 - Update
- [207]: KB2929961 - Update
- [208]: KB2930275 - Update
- [209]: KB2936068 - Update
- [210]: KB2964358 - Update
- [211]: KB923561 - Update
- [212]: KB942288-v3 - Update



- [213]: KB946648 - Update
- [214]: KB950762 - Update
- [215]: KB950974 - Update
- [216]: KB951376-v2 - Update
- [217]: KB952004 - Update
- [218]: KB95

NetWork Card(s): 1 NIC(s) Installed.

[01]: Intel(R) 82579LM Gigabit Network Connection

Connection Name: Local Area Connection

DHCP Enabled: Yes

DHCP Server: 192.168.1.20

IP address(es)

[01]: 192.168.1.40

C:\Documents and Settings\Administrator\ELECTIONS>

Post-Election Review:

The same output was capture from the system at the CLI and a file diff was performed. Below are the differences.

C:\Users\Frank\OneDrive - solutions4networks Inc\COA\Air Gap Analysis\airgap_06Mar2018\TAB7-PRE-AG.txt	C:\Users\Frank\OneDrive - solutions4networks Inc\COA\Air Gap Analysis\airgap_06Mar2018\TAB7-Post-AG.txt
Lease Obtained. : Monday, March 05, 2018 8:28:	Lease Obtained. : Thursday, March 08, 2018 8:4
Lease Expires : Tuesday, March 13, 2018 8:28	Lease Expires : Friday, March 16, 2018 8:43:



C:\Users\Frank\OneDrive - solutions4networks Inc\COA\Air Gap Analysis\airgap_06Mar2018\TAB7-PRE-AG.txt				C:\Users\Frank\OneDrive - solutions4networks Inc\COA\Air Gap Analysis\airgap_06Mar2018\TAB7-Post-AG.txt			
Proto	Local Address	Foreign Address	State	Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3306	0.0.0.0:0	LISTENING	TCP	0.0.0.0:3306	0.0.0.0:0	LISTENING
TCP	127.0.0.1:1047	0.0.0.0:0	LISTENING	TCP	127.0.0.1:1045	127.0.0.1:1046	ESTABLISHED
TCP	127.0.0.1:1048	127.0.0.1:1049	ESTABLISHED	TCP	127.0.0.1:1046	127.0.0.1:1045	ESTABLISHED
TCP	127.0.0.1:1049	127.0.0.1:1048	ESTABLISHED	TCP	127.0.0.1:1047	0.0.0.0:0	LISTENING
TCP	127.0.0.1:1055	0.0.0.0:0	LISTENING	TCP	127.0.0.1:1055	0.0.0.0:0	LISTENING
TCP	192.168.1.40:139	0.0.0.0:0	LISTENING	TCP	192.168.1.40:139	0.0.0.0:0	LISTENING
TCP	192.168.1.40:2490	192.168.1.20:135	TIME_WAIT				
TCP	192.168.1.40:2491	192.168.1.20:1026	TIME_WAIT				
TCP	192.168.1.40:2494	192.168.1.20:445	ESTABLISHED				
TCP	192.168.1.40:2496	192.168.1.20:1026	TIME_WAIT				
TCP	192.168.1.40:2499	192.168.1.20:389	TIME_WAIT				
TCP	192.168.1.40:2502	192.168.1.20:389	TIME_WAIT				
TCP	192.168.1.40:2503	192.168.1.20:445	TIME_WAIT				
TCP	192.168.1.40:2507	192.168.1.20:389	TIME_WAIT				
TCP	192.168.1.40:2508	192.168.1.20:389	TIME_WAIT				
TCP	192.168.1.40:2563	192.168.1.40:16992	ESTABLISHED				
TCP	192.168.1.40:2566	192.168.1.40:16993	SYN_SENT				
TCP	192.168.1.40:16992	192.168.1.40:2563	ESTABLISHED				

C:\Users\Frank\OneDrive - solutions4networks Inc\COA\Air Gap Analysis\airgap_06Mar2018\TAB7-PRE-AG.txt		C:\Users\Frank\OneDrive - solutions4networks Inc\COA\Air Gap Analysis\airgap_06Mar2018\TAB7-Post-AG.txt	
System Up Time:	0 Days, 0 Hours, 48 Minutes, 11 Seconds	System Up Time:	0 Days, 0 Hours, 18 Minutes, 58 Seconds
System Manufacturer:	Dell Inc.	System Manufacturer:	Dell Inc.
System Model:	OptiPlex 790	System Model:	OptiPlex 790
System type:	X86-based PC	System type:	X86-based PC
Processor(s):	1 Processor(s) Installed. [01]: x86 Family 6 Model 42 Stepping 7	Processor(s):	1 Processor(s) Installed. [01]: x86 Family 6 Model 42 Stepping 7
3092 Mhz		3093 Mhz	
BIOS Version:	DELL - 6222004	BIOS Version:	DELL - 6222004
Windows Directory:	C:\WINDOWS	Windows Directory:	C:\WINDOWS
System Directory:	C:\WINDOWS\system32	System Directory:	C:\WINDOWS\system32
Boot Device:	\Device\HarddiskVolume1	Boot Device:	\Device\HarddiskVolume1
System Locale:	en-us;English (United States)	System Locale:	en-us;English (United States)
Input Locale:	en-us;English (United States)	Input Locale:	en-us;English (United States)
Time Zone:	(GMT-05:00) Eastern Time (US & Canada)	Time Zone:	(GMT-05:00) Eastern Time (US & Canada)
Total Physical Memory:	3,241 MB	Total Physical Memory:	3,241 MB
Available Physical Memory:	2,860 MB	Available Physical Memory:	2,857 MB
Virtual Memory: Max Size:	2,048 MB	Virtual Memory: Max Size:	2,048 MB
Virtual Memory: Available:	2,008 MB	Virtual Memory: Available:	1,996 MB
Virtual Memory: In Use:	40 MB	Virtual Memory: In Use:	52 MB

DAM Front



DAM Rear





Additional Information Collected from DAM CLI:

Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.

```
C:\Documents and Settings\administrator.ELECTIONS>hostname
```

DAM

```
C:\Documents and Settings\administrator.ELECTIONS>whoami
```

'whoami' is not recognized as an internal or external command,
operable program or batch file.

```
C:\Documents and Settings\administrator.ELECTIONS>ipconfig /all
```

Windows IP Configuration

```
Host Name . . . . . : DAM
Primary Dns Suffix . . . . . : elections.local
Node Type . . . . . : Broadcast
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : elections.local
```

Ethernet adapter Local Area Connection:

```
Connection-specific DNS Suffix . :
```



Description : Broadcom NetXtreme 57xx Gigabit Cont
roller
Physical Address. : 00-19-B9-1F-F2-17
Dhcp Enabled. : No
IP Address. : 192.168.1.101
Subnet Mask : 255.255.255.0
Default Gateway :
DNS Servers : 192.168.1.20

C:\Documents and Settings\administrator.ELECTIONS>arp -a

Interface: 192.168.1.101 --- 0x2

Internet Address	Physical Address	Type
192.168.1.20	00-14-22-60-3f-94	dynamic

C:\Documents and Settings\administrator.ELECTIONS>Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\administrator.ELECTIONS>netstat -rn

Route Table

=====

Interface List

0x1 MS TCP Loopback interface
0x2 ...00 19 b9 1f f2 17 Broadcom NetXtreme 57xx Gigabit Controller - Pac



ket Scheduler Miniport

=====
=====

Active Routes:

Network	Destination	Netmask	Gateway	Interface	Metric
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1	
192.168.1.0	255.255.255.0	192.168.1.101	192.168.1.101	10	
192.168.1.101	255.255.255.255	127.0.0.1	127.0.0.1	10	
192.168.1.255	255.255.255.255	192.168.1.101	192.168.1.101	10	
224.0.0.0	240.0.0.0	192.168.1.101	192.168.1.101	10	
255.255.255.255	255.255.255.255	192.168.1.101	192.168.1.101	1	

=====

Persistent Routes:

None

C:\Documents and Settings\administrator.ELECTIONS>netstat -an

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3071	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49152	0.0.0.0:0	LISTENING
TCP	127.0.0.1:1039	0.0.0.0:0	LISTENING



```
TCP 192.168.1.101:139 0.0.0.0 LISTENING
TCP 192.168.1.101:1087 192.168.1.20:445 ESTABLISHED
UDP 0.0.0.0:445 *.*
UDP 0.0.0.0:500 *.*
UDP 0.0.0.0:1025 *.*
UDP 0.0.0.0:1026 *.*
UDP 0.0.0.0:4500 *.*
UDP 127.0.0.1:123 *.*
UDP 127.0.0.1:1027 *.*
UDP 127.0.0.1:1043 *.*
UDP 127.0.0.1:1900 *.*
UDP 192.168.1.101:123 *.*
UDP 192.168.1.101:137 *.*
UDP 192.168.1.101:138 *.*
UDP 192.168.1.101:1900 *.*
```

C:\Documents and Settings\administrator.ELECTIONS>Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\administrator.ELECTIONS>systeminfo

```
Host Name: DAM
OS Name: Microsoft Windows XP Professional
OS Version: 5.1.2600 Service Pack 2 Build 2600
OS Manufacturer: Microsoft Corporation
```



OS Configuration: Member Workstation

OS Build Type: Multiprocessor Free

Registered Owner: damsw

Registered Organization:

Product ID: 76487-OEM-0011903-00102

Original Install Date: 7/25/2007, 9:15:46 AM

System Up Time: 0 Days, 0 Hours, 51 Minutes, 51 Seconds

System Manufacturer: Dell Inc.

System Model: Precision WorkStation 690

System type: X86-based PC

Processor(s): 2 Processor(s) Installed.

[01]: x86 Family 6 Model 15 Stepping 6 GenuineIntel ~
1595 Mhz

[02]: x86 Family 6 Model 15 Stepping 6 GenuineIntel ~
1595 Mhz

BIOS Version: DELL - d

Windows Directory: C:\WINDOWS

System Directory: C:\WINDOWS\system32

Boot Device: \Device\HarddiskVolume2

System Locale: en-us;English (United States)

Input Locale: en-us;English (United States)

Time Zone: (GMT-05:00) Eastern Time (US & Canada)

Total Physical Memory: 2,046 MB

Available Physical Memory: 1,742 MB

Virtual Memory: Max Size: 2,048 MB



Virtual Memory: Available: 2,008 MB

Virtual Memory: In Use: 40 MB

Page File Location(s): C:\pagefile.sys

Domain: elections.local

Logon Server: \\BOE

Hotfix(s): 94 Hotfix(s) Installed.

[01]: File 1

[02]: File 1

[03]: File 1

[04]: File 1

[05]: File 1

[06]: File 1

[07]: File 1

[08]: File 1

[09]: File 1

[10]: File 1

[11]: File 1

[12]: File 1

[13]: File 1

[14]: File 1

[15]: File 1

[16]: File 1

[17]: File 1

[18]: File 1

[19]: File 1



[20]: File 1

[21]: File 1

[22]: File 1

[23]: File 1

[24]: File 1

[25]: File 1

[26]: File 1

[27]: File 1

[28]: File 1

[29]: File 1

[30]: File 1

[31]: File 1

[32]: File 1

[33]: File 1

[34]: File 1

[35]: File 1

[36]: File 1

[37]: File 1

[38]: File 1

[39]: File 1

[40]: File 1

[41]: File 1

[42]: File 1

[43]: File 1

[44]: File 1



- [45]: File 1
- [46]: Q147222
- [47]: S867460 - Update
- [48]: KB925398_WMP64
- [49]: KB923689
- [50]: KB873339 - Update
- [51]: KB885250 - Update
- [52]: KB885835 - Update
- [53]: KB887472 - Update
- [54]: KB889673 - Update
- [55]: KB891781 - Update
- [56]: KB896256 - Update
- [57]: KB896358 - Update
- [58]: KB896423 - Update
- [59]: KB896424 - Update
- [60]: KB899588 - Update
- [61]: KB899591 - Update
- [62]: KB901214 - Update
- [63]: KB904706 - Update
- [64]: KB908519 - Update
- [65]: KB908531 - Update
- [66]: KB908673 - Update
- [67]: KB909095 - Update
- [68]: KB911562 - Update
- [69]: KB912919 - Update



- [70]: KB912945 - Update
- [71]: KB914388 - Update
- [72]: KB917344 - Update
- [73]: KB917422 - Update
- [74]: KB918439 - Update
- [75]: KB918899 - Update
- [76]: KB919007 - Update
- [77]: KB920213 - Update
- [78]: KB920670 - Update
- [79]: KB920683 - Update
- [80]: KB920685 - Update
- [81]: KB921398 - Update
- [82]: KB922616 - Update
- [83]: KB923191 - Update
- [84]: KB923414 - Update
- [85]: KB923694 - Update
- [86]: KB923980 - Update
- [87]: KB924191 - Update
- [88]: KB924270 - Update
- [89]: KB924496 - Update
- [90]: KB925454 - Update
- [91]: KB926255 - Update
- [92]: KB928388 - Update
- [93]: KB929969 - Update
- [94]: KB835221WXP - Update



NetWork Card(s): 2 NIC(s) Installed.

[01]: Broadcom NetXtreme 57xx Gigabit Controller

Connection Name: Local Area Connection

DHCP Enabled: No

IP address(es)

[01]: 192.168.1.101

[02]: 1394 Net Adapter

Connection Name: 1394 Connection

DHCP Enabled: Yes

DHCP Server: N/A

IP address(es)

C:\Documents and Settings\administrator.ELECTIONS>

Post-Election Review:

The same output was capture from the system at the CLI and a file diff was performed. Below are the differences.

C:\Users\Frank\OneDrive - solutions4networks Inc\COA\Air Gap Analysis\airgap_06Mar2018\DAM-PRE-AG.txt	C:\Users\Frank\OneDrive - solutions4networks Inc\COA\Air Gap Analysis\airgap_06Mar2018\DAM-Post-AG.txt																																																												
Active Connections	Active Connections																																																												
<table border="1"> <thead> <tr> <th>Proto</th> <th>Local Address</th> <th>Foreign Address</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>TCP</td> <td>0.0.0.0:135</td> <td>0.0.0.0:0</td> <td>LISTENING</td> </tr> <tr> <td>TCP</td> <td>0.0.0.0:445</td> <td>0.0.0.0:0</td> <td>LISTENING</td> </tr> <tr> <td>TCP</td> <td>0.0.0.0:3071</td> <td>0.0.0.0:0</td> <td>LISTENING</td> </tr> <tr> <td>TCP</td> <td>0.0.0.0:49152</td> <td>0.0.0.0:0</td> <td>LISTENING</td> </tr> <tr> <td>TCP</td> <td>127.0.0.1:1039</td> <td>0.0.0.0:0</td> <td>LISTENING</td> </tr> <tr> <td>TCP</td> <td>192.168.1.101:139</td> <td>0.0.0.0:0</td> <td>LISTENING</td> </tr> <tr> <td>TCP</td> <td>192.168.1.101:1087</td> <td>192.168.1.20:445</td> <td>ESTABLISHED</td> </tr> </tbody> </table>	Proto	Local Address	Foreign Address	State	TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	TCP	0.0.0.0:3071	0.0.0.0:0	LISTENING	TCP	0.0.0.0:49152	0.0.0.0:0	LISTENING	TCP	127.0.0.1:1039	0.0.0.0:0	LISTENING	TCP	192.168.1.101:139	0.0.0.0:0	LISTENING	TCP	192.168.1.101:1087	192.168.1.20:445	ESTABLISHED	<table border="1"> <thead> <tr> <th>Proto</th> <th>Local Address</th> <th>Foreign Address</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>TCP</td> <td>0.0.0.0:135</td> <td>0.0.0.0:0</td> <td>LISTENING</td> </tr> <tr> <td>TCP</td> <td>0.0.0.0:445</td> <td>0.0.0.0:0</td> <td>LISTENING</td> </tr> <tr> <td>TCP</td> <td>0.0.0.0:3071</td> <td>0.0.0.0:0</td> <td>LISTENING</td> </tr> <tr> <td>TCP</td> <td>0.0.0.0:49152</td> <td>0.0.0.0:0</td> <td>LISTENING</td> </tr> <tr> <td>TCP</td> <td>127.0.0.1:1039</td> <td>0.0.0.0:0</td> <td>LISTENING</td> </tr> <tr> <td>TCP</td> <td>192.168.1.101:139</td> <td>0.0.0.0:0</td> <td>LISTENING</td> </tr> </tbody> </table>	Proto	Local Address	Foreign Address	State	TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	TCP	0.0.0.0:3071	0.0.0.0:0	LISTENING	TCP	0.0.0.0:49152	0.0.0.0:0	LISTENING	TCP	127.0.0.1:1039	0.0.0.0:0	LISTENING	TCP	192.168.1.101:139	0.0.0.0:0	LISTENING
Proto	Local Address	Foreign Address	State																																																										
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING																																																										
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING																																																										
TCP	0.0.0.0:3071	0.0.0.0:0	LISTENING																																																										
TCP	0.0.0.0:49152	0.0.0.0:0	LISTENING																																																										
TCP	127.0.0.1:1039	0.0.0.0:0	LISTENING																																																										
TCP	192.168.1.101:139	0.0.0.0:0	LISTENING																																																										
TCP	192.168.1.101:1087	192.168.1.20:445	ESTABLISHED																																																										
Proto	Local Address	Foreign Address	State																																																										
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING																																																										
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING																																																										
TCP	0.0.0.0:3071	0.0.0.0:0	LISTENING																																																										
TCP	0.0.0.0:49152	0.0.0.0:0	LISTENING																																																										
TCP	127.0.0.1:1039	0.0.0.0:0	LISTENING																																																										
TCP	192.168.1.101:139	0.0.0.0:0	LISTENING																																																										
<pre> System Up Time: 0 Days, 0 Hours, 51 Minutes, 51 Second System Manufacturer: Dell Inc. System Model: Precision WorkStation 690 System type: X86-based PC Processor(s): 2 Processor(s) Installed. [01]: x86 Family 6 Model 15 Stepping 6 1595 Mhz [02]: x86 Family 6 Model 15 Stepping 6 1595 Mhz BIOS Version: DELL - d Windows Directory: C:\WINDOWS System Directory: C:\WINDOWS\system32 Boot Device: \Device\HarddiskVolume2 System Locale: en-us;English (United States) Input Locale: en-us;English (United States) Time Zone: (GMT-05:00) Eastern Time (US & Canada) Total Physical Memory: 2,046 MB Available Physical Memory: 1,742 MB </pre>	<pre> System Up Time: 0 Days, 0 Hours, 21 Minutes, 52 Second System Manufacturer: Dell Inc. System Model: Precision WorkStation 690 System type: X86-based PC Processor(s): 2 Processor(s) Installed. [01]: x86 Family 6 Model 15 Stepping 6 1595 Mhz [02]: x86 Family 6 Model 15 Stepping 6 1595 Mhz BIOS Version: DELL - d Windows Directory: C:\WINDOWS System Directory: C:\WINDOWS\system32 Boot Device: \Device\HarddiskVolume2 System Locale: en-us;English (United States) Input Locale: en-us;English (United States) Time Zone: (GMT-05:00) Eastern Time (US & Canada) Total Physical Memory: 2,046 MB Available Physical Memory: 1,750 MB </pre>																																																												

DAM3.elections.local

DAM3 Front



DAM3 Rear



Additional Information Collected from DAM3 CLI:

Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.



```
C:\Documents and Settings\Administrator.ELECTIONS>hostname
```

DAM3

```
C:\Documents and Settings\Administrator.ELECTIONS>whoami
```

'whoami' is not recognized as an internal or external command,
operable program or batch file.

```
C:\Documents and Settings\Administrator.ELECTIONS>ipconfig /all
```

Windows IP Configuration

```
Host Name . . . . . : DAM3
Primary Dns Suffix . . . . . : elections.local
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : elections.local
                                elections.local
```

Ethernet adapter Local Area Connection 2:

```
Connection-specific DNS Suffix . : elections.local
Description . . . . . : Intel(R) 82579LM Gigabit Network Con
nection
Physical Address. . . . . : D4-BE-D9-A4-D1-C5
```



Dhcp Enabled : Yes
Autoconfiguration Enabled : Yes
IP Address : 192.168.1.41
Subnet Mask : 255.255.255.0
Default Gateway : 192.168.1.1
DHCP Server : 192.168.1.20
DNS Servers : 192.168.1.20
Primary WINS Server : 192.168.1.20
Lease Obtained : Monday, March 05, 2018 8:29:51 AM
Lease Expires : Tuesday, March 13, 2018 8:29:51 AM

C:\Documents and Settings\Administrator.ELECTIONS>arp -a

Interface: 192.168.1.41 --- 0x2

Internet Address	Physical Address	Type
192.168.1.20	00-14-22-60-3f-94	dynamic

C:\Documents and Settings\Administrator.ELECTIONS>Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator.ELECTIONS>netstat -rn

Route Table

=====

Interface List



0x1 MS TCP Loopback interface
 0x2 ...d4 be d9 a4 d1 c5 Intel(R) 82579LM Gigabit Network Connection - Pa
 cket Scheduler Miniport

=====
 =====

Active Routes:

Network	Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.41	10
127.0.0.0	255.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
192.168.1.0	255.255.255.0	255.255.255.0	192.168.1.41	192.168.1.41	10
192.168.1.41	255.255.255.255	255.255.255.255	127.0.0.1	127.0.0.1	10
192.168.1.255	255.255.255.255	255.255.255.255	192.168.1.41	192.168.1.41	10
224.0.0.0	240.0.0.0	240.0.0.0	192.168.1.41	192.168.1.41	10
255.255.255.255	255.255.255.255	255.255.255.255	192.168.1.41	192.168.1.41	1

Default Gateway: 192.168.1.1

=====

Persistent Routes:

None

C:\Documents and Settings\Administrator.ELECTIONS>netstat -an

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING



```
TCP 0.0.0.0:445      0.0.0.0:0      LISTENING
TCP 127.0.0.1:1040   127.0.0.1:1041 ESTABLISHED
TCP 127.0.0.1:1041   127.0.0.1:1040 ESTABLISHED
TCP 127.0.0.1:1055   0.0.0.0:0      LISTENING
TCP 127.0.0.1:1057   0.0.0.0:0      LISTENING
TCP 192.168.1.41:139 0.0.0.0:0      LISTENING
TCP 192.168.1.41:1093 192.168.1.20:445 ESTABLISHED
UDP 0.0.0.0:445      *.*
UDP 0.0.0.0:500      *.*
UDP 0.0.0.0:1025     *.*
UDP 0.0.0.0:1026     *.*
UDP 0.0.0.0:4500     *.*
UDP 127.0.0.1:123    *.*
UDP 127.0.0.1:1027   *.*
UDP 127.0.0.1:1048   *.*
UDP 127.0.0.1:1900   *.*
UDP 192.168.1.41:123 *.*
UDP 192.168.1.41:137 *.*
UDP 192.168.1.41:138 *.*
UDP 192.168.1.41:1900 *.*
```

C:\Documents and Settings\Administrator.ELECTIONS>Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator.ELECTIONS>systeminfo



Host Name: DAM3
OS Name: Microsoft Windows XP Professional
OS Version: 5.1.2600 Service Pack 3 Build 2600
OS Manufacturer: Microsoft Corporation
OS Configuration: Member Workstation
OS Build Type: Multiprocessor Free
Registered Owner: ess
Registered Organization:
Product ID: 76487-OEM-0060807-79692
Original Install Date: 3/30/2016, 10:52:49 AM
System Up Time: 0 Days, 0 Hours, 53 Minutes, 27 Seconds
System Manufacturer: Dell Inc.
System Model: OptiPlex 790
System type: X86-based PC
Processor(s): 1 Processor(s) Installed.
[01]: x86 Family 6 Model 42 Stepping 7 GenuineIntel ~
3092 Mhz
BIOS Version: DELL - 6222004
Windows Directory: C:\WINDOWS
System Directory: C:\WINDOWS\system32
Boot Device: \Device\HarddiskVolume1
System Locale: en-us;English (United States)
Input Locale: en-us;English (United States)
Time Zone: (GMT-05:00) Eastern Time (US & Canada)



Total Physical Memory: 3,241 MB

Available Physical Memory: 2,888 MB

Virtual Memory: Max Size: 2,048 MB

Virtual Memory: Available: 2,008 MB

Virtual Memory: In Use: 40 MB

Page File Location(s): C:\pagefile.sys

Domain: elections.local

Logon Server: \\BOE

Hotfix(s): 10 Hotfix(s) Installed.

[01]: File 1

[02]: File 1

[03]: File 1

[04]: File 1

[05]: Q147222

[06]: KB936929 - Service Pack

[07]: KB942288-v3 - Update

[08]: KB953356 - Update

[09]: KB954550-v5 - Update

[10]: KB835221WXP - Update

NetWork Card(s): 1 NIC(s) Installed.

[01]: Intel(R) 82579LM Gigabit Network Connection

Connection Name: Local Area Connection 2

DHCP Enabled: Yes

DHCP Server: 192.168.1.20

IP address(es)



[01]: 192.168.1.41

C:\Documents and Settings\Administrator\ELECTIONS>

Post-Election Review:

The same output was capture from the system at the CLI and a file diff was performed. Below are the differences.

C:\Users\Frank\OneDrive - solutions4networks Inc\COA\Air Gap Analysis\airgap_06Mar2018\DAM3-Pre-AG.txt	C:\Users\Frank\OneDrive - solutions4networks Inc\COA\Air Gap Analysis\airgap_06Mar2018\DAM3-Post-AG.txt
Lease Obtained : Monday, March 05, 2018 8:29:5	Lease Obtained : Thursday, March 08, 2018 8:44
Lease Expires : Tuesday, March 13, 2018 8:29:	Lease Expires : Friday, March 16, 2018 8:44:5
127.0.0.1:1040 127.0.0.1:1041 ESTABLISHED	127.0.0.1:1047 127.0.0.1:1048 ESTABLISHED
127.0.0.1:1041 127.0.0.1:1040 ESTABLISHED	127.0.0.1:1048 127.0.0.1:1047 ESTABLISHED
127.0.0.1:1055 0.0.0.0:0 LISTENING	127.0.0.1:1052 0.0.0.0:0 LISTENING
127.0.0.1:1057 0.0.0.0:0 LISTENING	127.0.0.1:1057 0.0.0.0:0 LISTENING
192.168.1.41:139 0.0.0.0:0 LISTENING	192.168.1.41:139 0.0.0.0:0 LISTENING
192.168.1.41:1093 192.168.1.20:445 ESTABLISHED	
0.0.0.0:445 **:*	0.0.0.0:445 **:*
0.0.0.0:500 **:*	0.0.0.0:500 **:*
0.0.0.0:1025 **:*	0.0.0.0:1025 **:*
0.0.0.0:1026 **:*	0.0.0.0:1026 **:*
0.0.0.0:4500 **:*	0.0.0.0:4500 **:*
127.0.0.1:123 **:*	127.0.0.1:123 **:*
127.0.0.1:1027 **:*	127.0.0.1:1027 **:*
127.0.0.1:1048 **:*	127.0.0.1:1043 **:*
System Up Time: 0 Days, 0 Hours, 53 Minutes, 27 Second	System Up Time: 0 Days, 0 Hours, 22 Minutes, 31 Second
System Manufacturer: Dell Inc.	System Manufacturer: Dell Inc.
System Model: OptiPlex 790	System Model: OptiPlex 790
System type: X86-based PC	System type: X86-based PC
Processor(s): 1 Processor(s) Installed.	Processor(s): 1 Processor(s) Installed.
[01]: x86 Family 6 Model 42 Stepping 7	[01]: x86 Family 6 Model 42 Stepping 7
3092 Mhz	3093 Mhz
BIOS Version: DELL - 6222004	BIOS Version: DELL - 6222004
Windows Directory: C:\WINDOWS	Windows Directory: C:\WINDOWS
System Directory: C:\WINDOWS\system32	System Directory: C:\WINDOWS\system32
Boot Device: \Device\HarddiskVolumel	Boot Device: \Device\HarddiskVolumel
System Locale: en-us:English (United States)	System Locale: en-us:English (United States)
Input Locale: en-us:English (United States)	Input Locale: en-us:English (United States)
Time Zone: (GMT-05:00) Eastern Time (US & Canada)	Time Zone: (GMT-05:00) Eastern Time (US & Canada)
Total Physical Memory: 3,241 MB	Total Physical Memory: 3,241 MB
Available Physical Memory: 2,888 MB	Available Physical Memory: 2,915 MB

External Connections on Client Devices

The only outside (external) connections found on the network were the dial-up modems on the 2 DAM servers which are part of the application and are outbound only. No other external connections were found on the network. Each server/workstation was tested and none of them had Internet access. The 7 Ethernet connections on the Dell 2716 switch were traced to valid devices. No other cables were connected to the Dell Switch and no loose cables were observed near the switch. The solutions4networks engineer asked if there was a valid login for the Dell 2716 switch but was told that no one was aware of one.

Modem Bank



Dell PowerConnect 2716



OKI B6300 Printer



No Wireless Adapters or Bluetooth Capability Found on Client Devices

Each PC was physically inspected for the presence of a wireless adapter or Bluetooth adapter and none were found.

The Windows “Device Manager” of each device was also inspected for the presence of any wireless devices.

No Wireless Keyboards and Mice

The keyboards and mice all had physical wires connected to the computers.

Post-Election Review: All items indicated above remained the same.

Network Air Gap Analysis

No issues found.

Air Gap Network Intact - Recommendations for Improvement

solutions4networks did not find any problems with the Election Tabulation Network, but have these recommendations to improve security of the network:

Client Operating Systems – Update the Clients to a supported OS.

The client PC’s were found to be running Windows XP which is no longer supported by Microsoft. These may be more vulnerable to attack if the network was ever compromised. The clients also had their internal Firewall



disabled. They did have Symantec Anti-virus installed, but the definitions were out of date. If this remains a closed air gapped network this should be a viable OS.

Server Operating System – Update the Server Operating System.

The server operating system is running Windows Server 2003, which is end of life July 2015. Any OS that is end of life is more vulnerable to attack if the network is ever compromised as it is no longer updated with any security patches. If this remains a closed air gapped network this should be a viable OS.

Remote Assistance Enabled.

Remote Assistance is enabled on the 3 clients and 2 DAM servers. This serves no positive purpose in a closed network environment where each machine is physically accessible and should be disabled in the event the network is ever compromised.

Remote Desktop is Enabled.

Remoted Desktop is enabled on the BOE server. Once again, this does not serve any positive purpose in a closed local network and should be disabled in the event the network is ever compromised.

Windows Update Enabled/None Selected.

The two DAM servers are configured differently from the rest of the computers on the network. Consistency should be the norm. All other computers have Auto Updates turned off. DAM1 has nothing selected and DAM2 has Auto Updates enabled and set for 3:00AM. Since this is a closed network and the OSes that are running are end of life there isn't a need to have Windows Update enabled.

Lock Physical Access to the Dell PowerConnect 2716

The Dell switch is easily accessible on the countertop. A locked cabinet would make it more difficult to connect an external cable. It is also recommended to disable any unused ports on the Dell Switch or move the unused ports to a different VLAN from the production network, but since the login is unknown a locked cabinet would suffice. Since the password is currently unknown and this is a flat network for ease of networking on the Dell switch there is the ability to reset it to unmanaged mode which would put all ports in Vlan 1.

Remove the Default Gateway Option

The DHCP server is giving the clients a default gateway of 192.168.1.1 even though no device exists. Removing the default gateway completely would make it more difficult for the clients to communicate with external networks. There is some inconsistency on the network in that not all the clients are set up for DHCP. Either set them all up for DHCP or set them all up for Static. For a more secure environment it would be better to disable DHCP on the BOE server entirely and configure static IPs on all the clients that way if someone were to ever connect to the Dell switch they would never obtain a DHCP address but would have to know the network addressing to hard code their PC.

County of Allegheny

Pre/**Post**-Election Air Gap Analysis of the Tabulation Network

For the Special Election

13 March 2018

Research and Recommendations Provided by:



a network infrastructure company

Prepared by:
Frank Calderone
Network Security Practice Lead
fcalderone@s4nets.com
(412) 626-3132



Contents

Overview.....	2
Site Contacts.....	2
General Physical Security/Building Access	2
Physical Security/Building Access - No Issues Found	2
Election Tabulations Network	8
Network Overview.....	8
Network Overview - Logical.....	9
Network Overview - Physical.....	11
External Connections on Client Devices	101
No Wireless Adapters or Bluetooth Capability Found on Client Devices.....	102
No Wireless Keyboards and Mice.....	102
Network Air Gap Analysis	102
Air Gap Network Intact - Recommendations for Improvement.....	102
Client Operating Systems – Update the Clients to a supported OS.	102
Server Operating System – Update the Server Operating System.....	103
Remote Assistance Enabled.....	103
Remote Desktop is Enabled.....	103
Windows Update Enabled/None Selected.....	103
Lock Physical Access to the Dell PowerConnect 2716.....	103
Remove the Default Gateway Option	103



Overview

The County of Allegheny has engaged solutions4networks to perform a network air gap analysis of their elections tabulation network located in Pittsburgh, PA. An **air gap, air wall or air gapping** is a network security measure employed on one or more computers to ensure that a secure computer network is physically isolated from unsecured networks, such as the public Internet or an unsecured local area network. solutions4networks has been tasked to verify the tabulation network is a stand-alone, isolated network and to assess the networks' vulnerability to external access and/or tampering. In addition to the network, solutions4network has been asked to assess and document the general physical security of the warehouse building.

A pre-election onsite visit was made by Frank Calderone of solutions4networks on March 12, 2018. The purpose of this document is to report the results of the assessment, identify security concerns and to make recommendations for the remediation of these concerns. A post-Election onsite visit was made on March 15, 2018. This report covers both the Pre-Election assessment and the **Post-Election review**. Post-Election Review updates will be noted in **red**.

Site Contacts

Elizabeth Dell

Elizabeth.Dell@AlleghenyCounty.US

412-350-6059

Robin Gigliotti

Robin.Gigliotti@AlleghenyCounty.US

412-350-6647

901 Pennsylvania Avenue

Pittsburgh, PA 15233

General Physical Security/Building Access

Physical Security/Building Access - No Issues Found

There are several suites within the warehouse and there were no outside signs, which identified that it was County of Allegheny building space. The building phone at the main entrance also did not have any entries to dial for the County of Allegheny.

Building Main Entrance:



Suite 901:



03/12/2018 - solutions4networks engineer, Frank Calderone, was met at the street entrance of suite 901 by Elizabeth Dell and was asked to provide a valid driver's license as identification before access to the building was granted.

03/15/2018 - solutions4networks engineer, Frank Calderone, was met at the street entrance suite 901 by Elizabeth Dell and was asked to provide a driver's license identification before access to the building was granted.

Entrance from the street required badge card access or a key (as seen in the picture in the previous page). The first door in the warehouse required a security code, but it was a physical, non-electronic lock.



Entrance into the Computer Room also require a code or a physical key.



Entrance to the tabulation room also required an electronic badge or key.



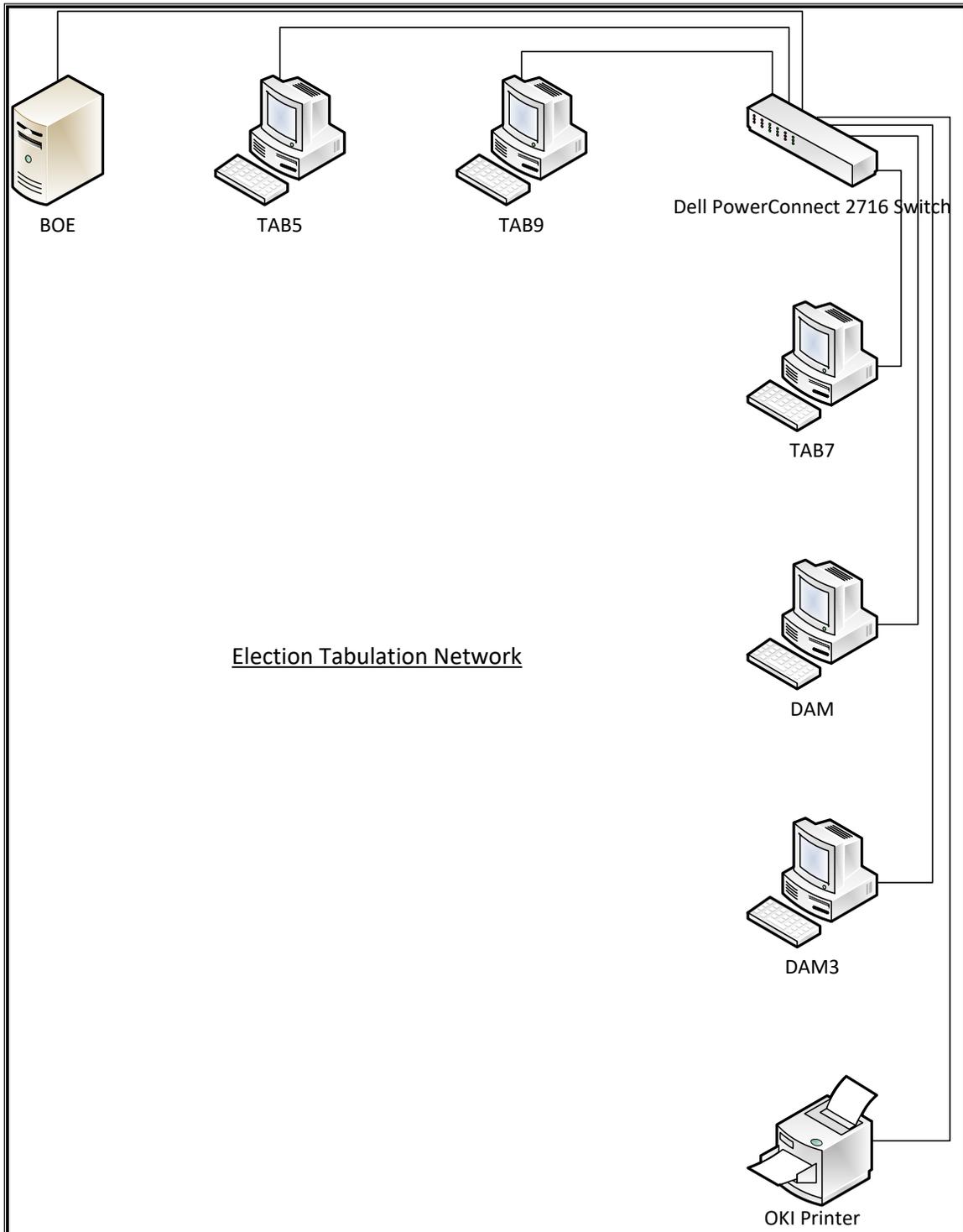
Security cameras were observed over the street entrance and inside the computer room. There is a sign in the tabulation network room that states “No Cell Phones are Permitted”.

Physical Post-Election Review: All items indicated above remained the same.

Election Tabulations Network

Network Overview

The solutions4networks engineer created the following network drawing based off the observed finding from the onsite physical inspections performed during the air gap analysis.





The Election Tabulation Network consisted of the following devices:

- 1 Dell PowerConnect 2716 Ethernet Switch
- 1 Windows Server
- 5 Client PC's
 - Two DAM (Dial Access Modem) Servers
 - 3 Windows XP Clients
- 1 Printer

Network Overview - Logical

All the devices had an address from RFC1918 private network 192.168.1.0/24. The Windows Server with address 192.168.1.20 provided DHCP, DNS and WINS services. A default gateway of 192.168.1.1 was configured, but no such device was found on the network. All devices on the network could ping each other so the network was fully self-contained and each node was accessible to one another.

Post-Election Review: All items indicated above remained the same.

Dell Server PE-SC1420	Dell Optiplex 790	Dell Optiplex 790	Dell Optiplex 790	Dell Precision 890	Dell Optiplex 790	Okidata Printer B6300
BOE.elections.local	TAB5.elections.local	TAB9.elections.local	TAB7.elections.local	DAM.elections.local	DAM3.elections.local	
provides DHCP, WINS, DNS Services	DHCP enabled	DHCP enabled	DHCP enabled	static	DHCP enabled/	DHCP Reserved
Win2003 SP1	Win XP Pro ver 2002 SP3	Win XP Pro ver 2002 SP3	Win XP Pro ver 2002 SP3	WinXP SP3	WinXP SP3	
Dell Server PESC1420						
intel Xeon CPU 3.20 GHZ	Intel core i5-2400 CPU 3.1 GHz	Intel core i5-2400 CPU 3.1 GHz	Intel core i5-2400 CPU 3.1 GHz	Intel Xeon 5110@1.60GHz		
3.19 GHz 2.00 GB RAM	3.09 GHZ, 3.16 GB Ram	3.09 GHZ, 3.16 GB Ram	3.09 GHZ, 3.16 GB Ram	1.60 GHz, 2.00 GB Ram		
2GB Ram	4 GB Ram	4 GB Ram	4 GB Ram	2 GB Ram	2 GB Ram	
IP: 192.168.1.20 (static)	IP: 192.168.1.11	IP: 192.168.1.12	IP: 192.168.1.40	IP: 192.168.1.101	IP: 192.168.1.41	IP: 192.168.1.50
netmask: 255.255.255.0	netmask: 255.255.255.0	netmask: 255.255.255.0	netmask: 255.255.255.0	netmask: 255.255.255.0	netmask: 255.255.255.0	netmask: 255.255.255.0
gateway: 192.168.1.1	gateway: 192.168.1.1 (doesn't exist)	gateway: 192.168.1.1 (doesn't exist)	gateway: 192.168.1.1 (doesn't exist)		gateway: 192.168.1.1 (doesn't exist)	
DNS: 192.168.1.20	DHCP Server: 192.168.1.20	DHCP Server: 192.168.1.20	DHCP Server: 192.168.1.20		DHCP Server: 192.168.1.20	
WINS: 192.168.1.20	DNS Server: 192.168.1.20	DNS Server: 192.168.1.20	DNS Server: 192.168.1.20	DNS Server: 192.168.1.20	DNS Server: 192.168.1.20	
	Wins Server: 192.168.1.20	Wins Server: 192.168.1.20	Wins Server: 192.168.1.20			
wired keyboard	wired keyboard	wired keyboard	wired keyboard	wired keyboard	wired keyboard	
wired mouse	wired mouse	wired mouse	wired mouse	wired mouse	wired mouse	
Intel Pro 1000 MT LAN connection	Gigabit LAN connection	Gigabit LAN connection	Gigabit LAN connection	Broadcom Gigabit Controller		

Network Overview - Physical

Each device on the network was inspected Pre- and Post-election for physical attachments and are noted below.

BOE.elections.local

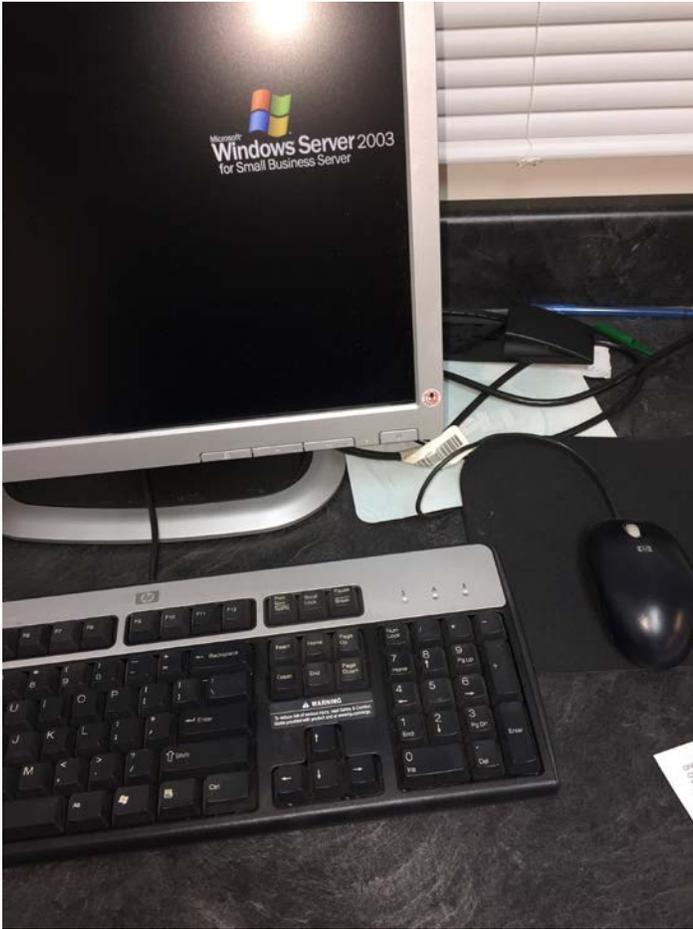
BOE Front



BOE Rear



BOE Desktop



Additional Information Collected from BOE CLI:

Microsoft Windows [Version 5.2.3790]

(C) Copyright 1985-2003 Microsoft Corp.

```
C:\Documents and Settings\Administrator>hostname
```

BOE

```
C:\Documents and Settings\Administrator>whoami
```

elections\administrator

```
C:\Documents and Settings\Administrator>ipconfig /all
```



Windows IP Configuration

Host Name : BOE
Primary Dns Suffix : elections.local
Node Type : Hybrid
IP Routing Enabled. : No
WINS Proxy Enabled. : No
DNS Suffix Search List. : elections.local

Ethernet adapter Server LAN NIC:

Connection-specific DNS Suffix . . :
Description : Intel(R) PRO/1000 MT Network Connection
Physical Address. : 00-14-22-60-3F-94
DHCP Enabled. : No
IP Address. : 192.168.1.20
Subnet Mask : 255.255.255.0
Default Gateway : 192.168.1.1
DNS Servers : 192.168.1.20
Primary WINS Server : 192.168.1.20

C:\Documents and Settings\Administrator>arp -a

Interface: 192.168.1.20 --- 0x10003



Internet Address	Physical Address	Type
192.168.1.11	18-03-73-14-1c-2c	dynamic
192.168.1.12	18-03-73-15-97-68	dynamic
192.168.1.40	18-03-73-1b-cf-e2	dynamic
192.168.1.41	d4-be-d9-a4-d1-c5	dynamic
192.168.1.101	00-19-b9-1f-f2-17	dynamic

C:\Documents and Settings\Administrator>Microsoft Windows [Version 5.2.3790]

(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>netstat -rn

IPv4 Route Table

=====

Interface List

0x1 MS TCP Loopback interface

0x10003 ...00 14 22 60 3f 94 Intel(R) PRO/1000 MT Network Connection

=====

=====

Active Routes:

Network Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.20	10
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
192.168.1.0	255.255.255.0	192.168.1.20	192.168.1.20	10
192.168.1.20	255.255.255.255	127.0.0.1	127.0.0.1	10



192.168.1.255 255.255.255.255 192.168.1.20 192.168.1.20 10

224.0.0.0 240.0.0.0 192.168.1.20 192.168.1.20 10

255.255.255.255 255.255.255.255 192.168.1.20 192.168.1.20 1

Default Gateway: 192.168.1.1

=====

Persistent Routes:

None

C:\Documents and Settings\Administrator>netstat -an

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:25	0.0.0.0:0	LISTENING
TCP	0.0.0.0:42	0.0.0.0:0	LISTENING
TCP	0.0.0.0:53	0.0.0.0:0	LISTENING
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING
TCP	0.0.0.0:88	0.0.0.0:0	LISTENING
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:389	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:464	0.0.0.0:0	LISTENING
TCP	0.0.0.0:593	0.0.0.0:0	LISTENING
TCP	0.0.0.0:636	0.0.0.0:0	LISTENING
TCP	0.0.0.0:691	0.0.0.0:0	LISTENING



TCP	0.0.0.0:1026	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1027	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1068	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1074	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1075	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1076	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1078	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1081	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1097	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1100	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1142	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1171	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1173	0.0.0.0:0	LISTENING
TCP	0.0.0.0:2160	0.0.0.0:0	LISTENING
TCP	0.0.0.0:2161	0.0.0.0:0	LISTENING
TCP	0.0.0.0:2260	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3052	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3268	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3269	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3389	0.0.0.0:0	LISTENING
TCP	0.0.0.0:6001	0.0.0.0:0	LISTENING
TCP	0.0.0.0:6002	0.0.0.0:0	LISTENING
TCP	0.0.0.0:6004	0.0.0.0:0	LISTENING
TCP	0.0.0.0:6358	0.0.0.0:0	LISTENING
TCP	0.0.0.0:6548	0.0.0.0:0	LISTENING



TCP	0.0.0.0:8081	0.0.0.0:0	LISTENING
TCP	0.0.0.0:10000	0.0.0.0:0	LISTENING
TCP	0.0.0.0:34571	0.0.0.0:0	LISTENING
TCP	0.0.0.0:34572	0.0.0.0:0	LISTENING
TCP	0.0.0.0:34573	0.0.0.0:0	LISTENING
TCP	127.0.0.1:389	127.0.0.1:46118	ESTABLISHED
TCP	127.0.0.1:1090	127.0.0.1:389	CLOSE_WAIT
TCP	127.0.0.1:1109	127.0.0.1:389	CLOSE_WAIT
TCP	127.0.0.1:1158	127.0.0.1:389	CLOSE_WAIT
TCP	127.0.0.1:43563	127.0.0.1:389	CLOSE_WAIT
TCP	127.0.0.1:46118	127.0.0.1:389	ESTABLISHED
TCP	192.168.1.20:135	192.168.1.20:1175	ESTABLISHED
TCP	192.168.1.20:135	192.168.1.20:48020	ESTABLISHED
TCP	192.168.1.20:135	192.168.1.20:48022	ESTABLISHED
TCP	192.168.1.20:139	0.0.0.0:0	LISTENING
TCP	192.168.1.20:389	192.168.1.20:46106	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:46108	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:46109	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:46111	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:46112	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:46114	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:46115	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:46119	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:46123	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:46124	ESTABLISHED



TCP	192.168.1.20:389	192.168.1.20:46125	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:46126	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:46127	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:46128	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:46155	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:46156	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:46157	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:47131	ESTABLISHED
TCP	192.168.1.20:389	192.168.1.20:47924	ESTABLISHED
TCP	192.168.1.20:445	192.168.1.11:1202	ESTABLISHED
TCP	192.168.1.20:445	192.168.1.12:1166	ESTABLISHED
TCP	192.168.1.20:445	192.168.1.40:1275	ESTABLISHED
TCP	192.168.1.20:445	192.168.1.41:1075	ESTABLISHED
TCP	192.168.1.20:445	192.168.1.101:1071	ESTABLISHED
TCP	192.168.1.20:691	192.168.1.20:1112	ESTABLISHED
TCP	192.168.1.20:691	192.168.1.20:1169	ESTABLISHED
TCP	192.168.1.20:691	192.168.1.20:43565	ESTABLISHED
TCP	192.168.1.20:1026	192.168.1.20:1108	ESTABLISHED
TCP	192.168.1.20:1026	192.168.1.20:1206	ESTABLISHED
TCP	192.168.1.20:1026	192.168.1.20:1356	ESTABLISHED
TCP	192.168.1.20:1026	192.168.1.20:36869	ESTABLISHED
TCP	192.168.1.20:1026	192.168.1.20:48023	ESTABLISHED
TCP	192.168.1.20:1093	192.168.1.20:389	CLOSE_WAIT
TCP	192.168.1.20:1108	192.168.1.20:1026	ESTABLISHED
TCP	192.168.1.20:1111	192.168.1.20:389	CLOSE_WAIT



TCP	192.168.1.20:1112	192.168.1.20:691	ESTABLISHED
TCP	192.168.1.20:1130	192.168.1.20:389	CLOSE_WAIT
TCP	192.168.1.20:1159	192.168.1.20:389	CLOSE_WAIT
TCP	192.168.1.20:1169	192.168.1.20:691	ESTABLISHED
TCP	192.168.1.20:1175	192.168.1.20:135	ESTABLISHED
TCP	192.168.1.20:1206	192.168.1.20:1026	ESTABLISHED
TCP	192.168.1.20:1356	192.168.1.20:1026	ESTABLISHED
TCP	192.168.1.20:1914	192.168.1.20:389	CLOSE_WAIT
TCP	192.168.1.20:1917	192.168.1.20:3268	CLOSE_WAIT
TCP	192.168.1.20:3268	192.168.1.20:46113	ESTABLISHED
TCP	192.168.1.20:3268	192.168.1.20:46117	ESTABLISHED
TCP	192.168.1.20:3268	192.168.1.20:46120	ESTABLISHED
TCP	192.168.1.20:3268	192.168.1.20:46122	ESTABLISHED
TCP	192.168.1.20:36869	192.168.1.20:1026	ESTABLISHED
TCP	192.168.1.20:41522	192.168.1.20:389	CLOSE_WAIT
TCP	192.168.1.20:41523	192.168.1.20:3268	CLOSE_WAIT
TCP	192.168.1.20:43565	192.168.1.20:691	ESTABLISHED
TCP	192.168.1.20:46106	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:46108	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:46109	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:46110	192.168.1.20:389	CLOSE_WAIT
TCP	192.168.1.20:46111	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:46112	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:46113	192.168.1.20:3268	ESTABLISHED
TCP	192.168.1.20:46114	192.168.1.20:389	ESTABLISHED



TCP	192.168.1.20:46115	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:46117	192.168.1.20:3268	ESTABLISHED
TCP	192.168.1.20:46119	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:46120	192.168.1.20:3268	ESTABLISHED
TCP	192.168.1.20:46122	192.168.1.20:3268	ESTABLISHED
TCP	192.168.1.20:46123	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:46124	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:46125	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:46126	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:46127	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:46128	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:46155	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:46156	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:46157	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:47131	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:47888	192.168.1.20:389	CLOSE_WAIT
TCP	192.168.1.20:47924	192.168.1.20:389	ESTABLISHED
TCP	192.168.1.20:48019	192.168.1.20:34571	TIME_WAIT
TCP	192.168.1.20:48020	192.168.1.20:135	ESTABLISHED
TCP	192.168.1.20:48021	192.168.1.20:135	TIME_WAIT
TCP	192.168.1.20:48022	192.168.1.20:135	ESTABLISHED
TCP	192.168.1.20:48023	192.168.1.20:1026	ESTABLISHED
UDP	0.0.0.0:42	*.*	
UDP	0.0.0.0:135	*.*	
UDP	0.0.0.0:445	*.*	



UDP	0.0.0.0:500	*.*
UDP	0.0.0.0:1035	*.*
UDP	0.0.0.0:1065	*.*
UDP	0.0.0.0:1072	*.*
UDP	0.0.0.0:1082	*.*
UDP	0.0.0.0:1101	*.*
UDP	0.0.0.0:1132	*.*
UDP	0.0.0.0:1172	*.*
UDP	0.0.0.0:1207	*.*
UDP	0.0.0.0:1434	*.*
UDP	0.0.0.0:2160	*.*
UDP	0.0.0.0:2161	*.*
UDP	0.0.0.0:3456	*.*
UDP	0.0.0.0:3457	*.*
UDP	0.0.0.0:4500	*.*
UDP	0.0.0.0:7846	*.*
UDP	0.0.0.0:38293	*.*
UDP	127.0.0.1:53	*.*
UDP	127.0.0.1:123	*.*
UDP	127.0.0.1:1064	*.*
UDP	127.0.0.1:1066	*.*
UDP	127.0.0.1:1083	*.*
UDP	127.0.0.1:1092	*.*
UDP	127.0.0.1:1102	*.*
UDP	127.0.0.1:1105	*.*



UDP 127.0.0.1:1141 *.*
UDP 127.0.0.1:1156 *.*
UDP 127.0.0.1:1163 *.*
UDP 127.0.0.1:1176 *.*
UDP 127.0.0.1:1185 *.*
UDP 127.0.0.1:1191 *.*
UDP 127.0.0.1:1200 *.*
UDP 127.0.0.1:1358 *.*
UDP 127.0.0.1:3456 *.*
UDP 127.0.0.1:3457 *.*
UDP 127.0.0.1:3979 *.*
UDP 127.0.0.1:14786 *.*
UDP 192.168.1.20:53 *.*
UDP 192.168.1.20:67 *.*
UDP 192.168.1.20:68 *.*
UDP 192.168.1.20:88 *.*
UDP 192.168.1.20:123 *.*
UDP 192.168.1.20:137 *.*
UDP 192.168.1.20:138 *.*
UDP 192.168.1.20:389 *.*
UDP 192.168.1.20:464 *.*
UDP 192.168.1.20:2535 *.*

C:\Documents and Settings\Administrator>systeminfo



Host Name: BOE

OS Name: Microsoft(R) Windows(R) Server 2003 for Small Business Server

OS Version: 5.2.3790 Service Pack 1 Build 3790

OS Manufacturer: Microsoft Corporation

OS Configuration: Primary Domain Controller

OS Build Type: Multiprocessor Free

Registered Owner: Allegheny County, PA

Registered Organization: Board of Elections

Product ID: 74995-OEM-4211904-03020

Original Install Date: 5/8/2006, 1:24:53 PM

System Up Time: 171 Days, 1 Hours, 30 Minutes, 40 Seconds

System Manufacturer: Dell Inc.

System Model: PowerEdge SC1420

System Type: X86-based PC

Processor(s): 2 Processor(s) Installed.

[01]: x86 Family 15 Model 4 Stepping 3 GenuineIntel ~
3192 Mhz

[02]: x86 Family 15 Model 4 Stepping 3 GenuineIntel ~
3192 Mhz

BIOS Version: DELL - 7

Windows Directory: C:\WINDOWS

System Directory: C:\WINDOWS\system32

Boot Device: \Device\HarddiskVolume2

System Locale: en-us;English (United States)



Input Locale: en-us;English (United States)
Time Zone: (GMT-05:00) Eastern Time (US & Canada)
Total Physical Memory: 2,046 MB
Available Physical Memory: 650 MB
Page File: Max Size: 3,435 MB
Page File: Available: 2,048 MB
Page File: In Use: 1,387 MB
Page File Location(s): C:\pagefile.sys
Domain: elections.local
Logon Server: \\BOE
Hotfix(s): 19 Hotfix(s) Installed.

- [01]: File 1
- [02]: File 1
- [03]: File 1
- [04]: File 1
- [05]: File 1
- [06]: File 1
- [07]: File 1
- [08]: File 1
- [09]: File 1
- [10]: Q147222
- [11]: KB896358 - Update
- [12]: KB896422 - Update
- [13]: KB896424 - Update
- [14]: KB896688 - Update



[15]: KB901214 - Update

[16]: KB902400 - Update

[17]: KB904706 - Update

[18]: KB908519 - Update

[19]: KB912919 - Update

Network Card(s): 1 NIC(s) Installed.

[01]: Intel(R) PRO/1000 MT Network Connection

Connection Name: Server LAN NIC

DHCP Enabled: No

IP address(es)

[01]: 192.168.1.20

C:\Documents and Settings\Administrator>

Post-Election Review:

The same output was capture from the system at the CLI and a file diff was performed. Below are the differences.

C:\Documents and Settings\Administrator>arp -a				C:\Documents and Settings\Administrator>arp -a			
Interface	Internet Address	Physical Address	Type	Interface	Internet Address	Physical Address	Type
192.168.1.20	---	0x10003		192.168.1.20	---	0x10003	
192.168.1.11		18-03-73-14-1c-2c	dynamic	192.168.1.11		18-03-73-14-1c-2c	dynamic
192.168.1.12		18-03-73-15-97-68	dynamic				
192.168.1.40		18-03-73-1b-cf-e2	dynamic	192.168.1.40		18-03-73-1b-cf-e2	dynamic
192.168.1.41		d4-be-d9-a4-d1-c5	dynamic	192.168.1.41		d4-be-d9-a4-d1-c5	dynamic
192.168.1.101		00-19-b9-1f-f2-17	dynamic	192.168.1.101		00-19-b9-1f-f2-17	dynamic



Netstat -an

C:\Users\Frank\OneDrive - solutions4networks Inc\COA\Air Gap Analysis\airgap_13Mar2018\BOE-Pre-AG.txt				C:\Users\Frank\OneDrive - solutions4networks Inc\COA\Air Gap Analysis\airgap_13Mar2018\BOE-Post-AG.txt			
TCP	127.0.0.1:389	127.0.0.1:46118	ESTABLISHE	TCP	127.0.0.1:389	127.0.0.1:11571	ESTABLISHE
TCP	127.0.0.1:1090	127.0.0.1:389	CLOSE_WAIT	TCP	127.0.0.1:389	127.0.0.1:14375	TIME_WAIT
TCP	127.0.0.1:1109	127.0.0.1:389	CLOSE_WAIT	TCP	127.0.0.1:1090	127.0.0.1:389	CLOSE_WAIT
TCP	127.0.0.1:1158	127.0.0.1:389	CLOSE_WAIT	TCP	127.0.0.1:1109	127.0.0.1:389	CLOSE_WAIT
TCP	127.0.0.1:43563	127.0.0.1:389	CLOSE_WAIT	TCP	127.0.0.1:1158	127.0.0.1:389	CLOSE_WAIT
TCP	127.0.0.1:46118	127.0.0.1:389	ESTABLISHE	TCP	127.0.0.1:11571	127.0.0.1:389	ESTABLISHE
TCP	192.168.1.20:135	192.168.1.20:1175	ESTABLISHE	TCP	127.0.0.1:14375	127.0.0.1:389	TIME_WAIT
TCP	192.168.1.20:135	192.168.1.20:48020	ESTABLISHE	TCP	127.0.0.1:43563	127.0.0.1:389	CLOSE_WAIT
TCP	192.168.1.20:135	192.168.1.20:48022	ESTABLISHE	TCP	192.168.1.20:135	192.168.1.11:1087	ESTABLISHE
TCP	192.168.1.20:139	0.0.0.0:0	LISTENING	TCP	192.168.1.20:135	192.168.1.20:1175	ESTABLISHE
TCP	192.168.1.20:389	192.168.1.20:46106	ESTABLISHE	TCP	192.168.1.20:135	192.168.1.20:14369	ESTABLISHE
TCP	192.168.1.20:389	192.168.1.20:46108	ESTABLISHE	TCP	192.168.1.20:135	192.168.1.20:14371	ESTABLISHE
TCP	192.168.1.20:389	192.168.1.20:46109	ESTABLISHE	TCP	192.168.1.20:135	192.168.1.20:14376	ESTABLISHE
TCP	192.168.1.20:389	192.168.1.20:46111	ESTABLISHE	TCP	192.168.1.20:139	0.0.0.0:0	LISTENING
TCP	192.168.1.20:389	192.168.1.20:46112	ESTABLISHE	TCP	192.168.1.20:139	192.168.1.41:1081	ESTABLISHE
TCP	192.168.1.20:389	192.168.1.20:46114	ESTABLISHE	TCP	192.168.1.20:139	192.168.1.20:11545	ESTABLISHE
TCP	192.168.1.20:389	192.168.1.20:46115	ESTABLISHE	TCP	192.168.1.20:389	192.168.1.20:11546	ESTABLISHE
TCP	192.168.1.20:389	192.168.1.20:46119	ESTABLISHE	TCP	192.168.1.20:389	192.168.1.20:11547	ESTABLISHE
TCP	192.168.1.20:389	192.168.1.20:46123	ESTABLISHE	TCP	192.168.1.20:389	192.168.1.20:11548	ESTABLISHE
TCP	192.168.1.20:389	192.168.1.20:46124	ESTABLISHE	TCP	192.168.1.20:389	192.168.1.20:11550	ESTABLISHE
TCP	192.168.1.20:389	192.168.1.20:46125	ESTABLISHE	TCP	192.168.1.20:389	192.168.1.20:11551	ESTABLISHE
TCP	192.168.1.20:389	192.168.1.20:46126	ESTABLISHE	TCP	192.168.1.20:389	192.168.1.20:11552	ESTABLISHE
TCP	192.168.1.20:389	192.168.1.20:46127	ESTABLISHE	TCP	192.168.1.20:389	192.168.1.20:11554	ESTABLISHE
TCP	192.168.1.20:389	192.168.1.20:46128	ESTABLISHE	TCP	192.168.1.20:389	192.168.1.20:11558	ESTABLISHE
TCP	192.168.1.20:389	192.168.1.20:46155	ESTABLISHE	TCP	192.168.1.20:389	192.168.1.20:11564	ESTABLISHE
TCP	192.168.1.20:389	192.168.1.20:46156	ESTABLISHE	TCP	192.168.1.20:389	192.168.1.20:11565	ESTABLISHE
TCP	192.168.1.20:389	192.168.1.20:46157	ESTABLISHE	TCP	192.168.1.20:389	192.168.1.20:11566	ESTABLISHE
TCP	192.168.1.20:389	192.168.1.20:47131	ESTABLISHE	TCP	192.168.1.20:389	192.168.1.20:11567	ESTABLISHE
TCP	192.168.1.20:389	192.168.1.20:47924	ESTABLISHE	TCP	192.168.1.20:389	192.168.1.20:11568	ESTABLISHE
TCP	192.168.1.20:445	192.168.1.11:1202	ESTABLISHE	TCP	192.168.1.20:389	192.168.1.20:11569	ESTABLISHE
TCP	192.168.1.20:445	192.168.1.12:1166	ESTABLISHE	TCP	192.168.1.20:389	192.168.1.20:11593	ESTABLISHE
TCP	192.168.1.20:691	192.168.1.20:1112	ESTABLISHE	TCP	192.168.1.20:389	192.168.1.20:11594	ESTABLISHE
TCP	192.168.1.20:691	192.168.1.20:1169	ESTABLISHE	TCP	192.168.1.20:389	192.168.1.20:11595	ESTABLISHE
TCP	192.168.1.20:691	192.168.1.20:43565	ESTABLISHE	TCP	192.168.1.20:389	192.168.1.20:14293	FIN_WAIT_2
TCP	192.168.1.20:1026	192.168.1.20:1108	ESTABLISHE	TCP	192.168.1.20:389	192.168.1.20:14314	ESTABLISHE
TCP	192.168.1.20:1026	192.168.1.20:1206	ESTABLISHE	TCP	192.168.1.20:389	192.168.1.20:14382	TIME_WAIT
TCP	192.168.1.20:1026	192.168.1.20:1356	ESTABLISHE	TCP	192.168.1.20:445	192.168.1.20:14380	ESTABLISHE
TCP	192.168.1.20:1026	192.168.1.20:36869	ESTABLISHE	TCP	192.168.1.20:445	192.168.1.40:1092	ESTABLISHE
TCP	192.168.1.20:1026	192.168.1.20:48023	ESTABLISHE	TCP	192.168.1.20:445	192.168.1.20:1112	ESTABLISHE
TCP	192.168.1.20:1093	192.168.1.20:389	CLOSE_WAIT	TCP	192.168.1.20:691	192.168.1.20:1169	ESTABLISHE
TCP	192.168.1.20:1108	192.168.1.20:1026	ESTABLISHE	TCP	192.168.1.20:691	192.168.1.20:43565	ESTABLISHE
TCP	192.168.1.20:1111	192.168.1.20:389	CLOSE_WAIT	TCP	192.168.1.20:1026	192.168.1.20:1108	ESTABLISHE
TCP	192.168.1.20:1112	192.168.1.20:691	ESTABLISHE	TCP	192.168.1.20:1026	192.168.1.20:1206	ESTABLISHE
TCP	192.168.1.20:1130	192.168.1.20:389	CLOSE_WAIT	TCP	192.168.1.20:1026	192.168.1.20:1356	ESTABLISHE
TCP	192.168.1.20:1159	192.168.1.20:389	CLOSE_WAIT	TCP	192.168.1.20:1026	192.168.1.20:12454	ESTABLISHE
TCP	192.168.1.20:1169	192.168.1.20:691	ESTABLISHE	TCP	192.168.1.20:1026	192.168.1.20:14372	ESTABLISHE
TCP	192.168.1.20:1175	192.168.1.20:135	ESTABLISHE	TCP	192.168.1.20:1026	192.168.1.20:14377	ESTABLISHE
TCP	192.168.1.20:1206	192.168.1.20:1026	ESTABLISHE	TCP	192.168.1.20:1093	192.168.1.20:389	CLOSE_WAIT
TCP	192.168.1.20:1356	192.168.1.20:1026	ESTABLISHE	TCP	192.168.1.20:1108	192.168.1.20:1026	ESTABLISHE
TCP	192.168.1.20:1914	192.168.1.20:389	CLOSE_WAIT	TCP	192.168.1.20:1111	192.168.1.20:389	CLOSE_WAIT
TCP	192.168.1.20:1917	192.168.1.20:3268	CLOSE_WAIT	TCP	192.168.1.20:1112	192.168.1.20:691	ESTABLISHE
TCP	192.168.1.20:3268	192.168.1.20:46113	ESTABLISHE	TCP	192.168.1.20:1130	192.168.1.20:389	CLOSE_WAIT
TCP	192.168.1.20:3268	192.168.1.20:46117	ESTABLISHE	TCP	192.168.1.20:1159	192.168.1.20:389	CLOSE_WAIT
TCP	192.168.1.20:3268	192.168.1.20:46120	ESTABLISHE	TCP	192.168.1.20:1169	192.168.1.20:691	ESTABLISHE
TCP	192.168.1.20:3268	192.168.1.20:46122	ESTABLISHE	TCP	192.168.1.20:1175	192.168.1.20:135	ESTABLISHE
TCP	192.168.1.20:36869	192.168.1.20:1026	ESTABLISHE	TCP	192.168.1.20:1206	192.168.1.20:1026	ESTABLISHE
TCP				TCP	192.168.1.20:1356	192.168.1.20:1026	ESTABLISHE
				TCP	192.168.1.20:1914	192.168.1.20:389	CLOSE_WAIT
				TCP	192.168.1.20:1917	192.168.1.20:3268	CLOSE_WAIT
				TCP	192.168.1.20:3268	192.168.1.20:11544	ESTABLISHE
				TCP	192.168.1.20:3268	192.168.1.20:11553	ESTABLISHE
				TCP	192.168.1.20:3268	192.168.1.20:11555	ESTABLISHE
				TCP	192.168.1.20:3268	192.168.1.20:11557	ESTABLISHE
				TCP	192.168.1.20:11544	192.168.1.20:3268	ESTABLISHE
				TCP	192.168.1.20:11545	192.168.1.20:389	ESTABLISHE
				TCP	192.168.1.20:11546	192.168.1.20:389	ESTABLISHE
				TCP	192.168.1.20:11547	192.168.1.20:389	ESTABLISHE

			TCP	192.168.1.20:11548	192.168.1.20:389	ESTABLISHE
			TCP	192.168.1.20:11550	192.168.1.20:389	ESTABLISHE
			TCP	192.168.1.20:11551	192.168.1.20:389	ESTABLISHE
			TCP	192.168.1.20:11552	192.168.1.20:389	ESTABLISHE
			TCP	192.168.1.20:11553	192.168.1.20:3268	ESTABLISHE
			TCP	192.168.1.20:11554	192.168.1.20:389	ESTABLISHE
			TCP	192.168.1.20:11555	192.168.1.20:3268	ESTABLISHE
			TCP	192.168.1.20:11557	192.168.1.20:3268	ESTABLISHE
			TCP	192.168.1.20:11558	192.168.1.20:389	ESTABLISHE
			TCP	192.168.1.20:11559	192.168.1.20:389	CLOSE_WAIT
			TCP	192.168.1.20:11564	192.168.1.20:389	ESTABLISHE
			TCP	192.168.1.20:11565	192.168.1.20:389	ESTABLISHE
			TCP	192.168.1.20:11566	192.168.1.20:389	ESTABLISHE
			TCP	192.168.1.20:11567	192.168.1.20:389	ESTABLISHE
			TCP	192.168.1.20:11568	192.168.1.20:389	ESTABLISHE
			TCP	192.168.1.20:11569	192.168.1.20:389	ESTABLISHE
			TCP	192.168.1.20:11593	192.168.1.20:389	ESTABLISHE
			TCP	192.168.1.20:11594	192.168.1.20:389	ESTABLISHE
			TCP	192.168.1.20:11595	192.168.1.20:389	ESTABLISHE
			TCP	192.168.1.20:12454	192.168.1.20:1026	ESTABLISHE
			TCP	192.168.1.20:14293	192.168.1.20:389	CLOSE_WAIT
			TCP	192.168.1.20:14314	192.168.1.20:389	ESTABLISHE
			TCP	192.168.1.20:14333	192.168.1.20:389	ESTABLISHE
			TCP	192.168.1.20:14340	192.168.1.20:1026	TIME_WAIT
			TCP	192.168.1.20:14369	192.168.1.20:135	ESTABLISHE
			TCP	192.168.1.20:14371	192.168.1.20:135	ESTABLISHE
			TCP	192.168.1.20:14372	192.168.1.20:1026	ESTABLISHE
			TCP	192.168.1.20:14373	192.168.1.20:34571	TIME_WAIT
			TCP	192.168.1.20:14376	192.168.1.20:135	ESTABLISHE
			TCP	192.168.1.20:14377	192.168.1.20:1026	ESTABLISHE
			TCP	192.168.1.20:14380	192.168.1.20:445	ESTABLISHE
			TCP	192.168.1.20:46106	192.168.1.20:389	ESTABLISHE
			TCP	192.168.1.20:46108	192.168.1.20:389	ESTABLISHE
			TCP	192.168.1.20:46109	192.168.1.20:389	ESTABLISHE
			TCP	192.168.1.20:46110	192.168.1.20:389	CLOSE_WAIT
			TCP	192.168.1.20:46111	192.168.1.20:389	ESTABLISHE
			TCP	192.168.1.20:46112	192.168.1.20:389	ESTABLISHE
			TCP	192.168.1.20:46113	192.168.1.20:3268	ESTABLISHE
			TCP	192.168.1.20:46114	192.168.1.20:389	ESTABLISHE
			TCP	192.168.1.20:46115	192.168.1.20:389	ESTABLISHE
			TCP	192.168.1.20:46117	192.168.1.20:3268	ESTABLISHE
			TCP	192.168.1.20:46119	192.168.1.20:389	ESTABLISHE
			TCP	192.168.1.20:46120	192.168.1.20:3268	ESTABLISHE
			TCP	192.168.1.20:46122	192.168.1.20:3268	ESTABLISHE
			TCP	192.168.1.20:46123	192.168.1.20:389	ESTABLISHE
			TCP	192.168.1.20:46124	192.168.1.20:389	ESTABLISHE
			TCP	192.168.1.20:46125	192.168.1.20:389	ESTABLISHE
			TCP	192.168.1.20:46126	192.168.1.20:389	ESTABLISHE
			TCP	192.168.1.20:46127	192.168.1.20:389	ESTABLISHE
			TCP	192.168.1.20:46128	192.168.1.20:389	ESTABLISHE
			TCP	192.168.1.20:46155	192.168.1.20:389	ESTABLISHE
			TCP	192.168.1.20:46156	192.168.1.20:389	ESTABLISHE
			TCP	192.168.1.20:46157	192.168.1.20:389	ESTABLISHE
			TCP	192.168.1.20:47131	192.168.1.20:389	ESTABLISHE
			TCP	192.168.1.20:47888	192.168.1.20:389	CLOSE_WAIT
			TCP	192.168.1.20:47924	192.168.1.20:389	ESTABLISHE
			TCP	192.168.1.20:48019	192.168.1.20:34571	TIME_WAIT
			TCP	192.168.1.20:48020	192.168.1.20:135	ESTABLISHE
			TCP	192.168.1.20:48021	192.168.1.20:135	TIME_WAIT
			TCP	192.168.1.20:48022	192.168.1.20:135	ESTABLISHE
			TCP	192.168.1.20:48023	192.168.1.20:1026	ESTABLISHE

Systeminfo:

System Up Time:	171 Days, 1 Hours, 30 Minutes, 40 Seco	System Up Time:	174 Days, 1 Hours, 26 Minutes, 22 Seco
System Manufacturer:	Dell Inc.	System Manufacturer:	Dell Inc.
System Model:	PowerEdge SC1420	System Model:	PowerEdge SC1420
System Type:	X86-based PC	System Type:	X86-based PC
Processor(s):	2 Processor(s) Installed. [01]: x86 Family 15 Model 4 Stepping 3	Processor(s):	2 Processor(s) Installed. [01]: x86 Family 15 Model 4 Stepping 3
3192 Mhz		3192 Mhz	
	[02]: x86 Family 15 Model 4 Stepping 3		[02]: x86 Family 15 Model 4 Stepping 3
3192 Mhz		3192 Mhz	
BIOS Version:	DELL - 7	BIOS Version:	DELL - 7
Windows Directory:	C:\WINDOWS	Windows Directory:	C:\WINDOWS
System Directory:	C:\WINDOWS\system32	System Directory:	C:\WINDOWS\system32
Boot Device:	\Device\HarddiskVolume2	Boot Device:	\Device\HarddiskVolume2
System Locale:	en-us;English (United States)	System Locale:	en-us;English (United States)
Input Locale:	en-us;English (United States)	Input Locale:	en-us;English (United States)
Time Zone:	(GMT-05:00) Eastern Time (US & Canada)	Time Zone:	(GMT-05:00) Eastern Time (US & Canada)
Total Physical Memory:	2,046 MB	Total Physical Memory:	2,046 MB
Available Physical Memory:	650 MB	Available Physical Memory:	640 MB
Page File: Max Size:	3,435 MB	Page File: Max Size:	3,435 MB
Page File: Available:	2,048 MB	Page File: Available:	2,042 MB
Page File: In Use:	1,387 MB	Page File: In Use:	1,393 MB

TAB5.elections.local

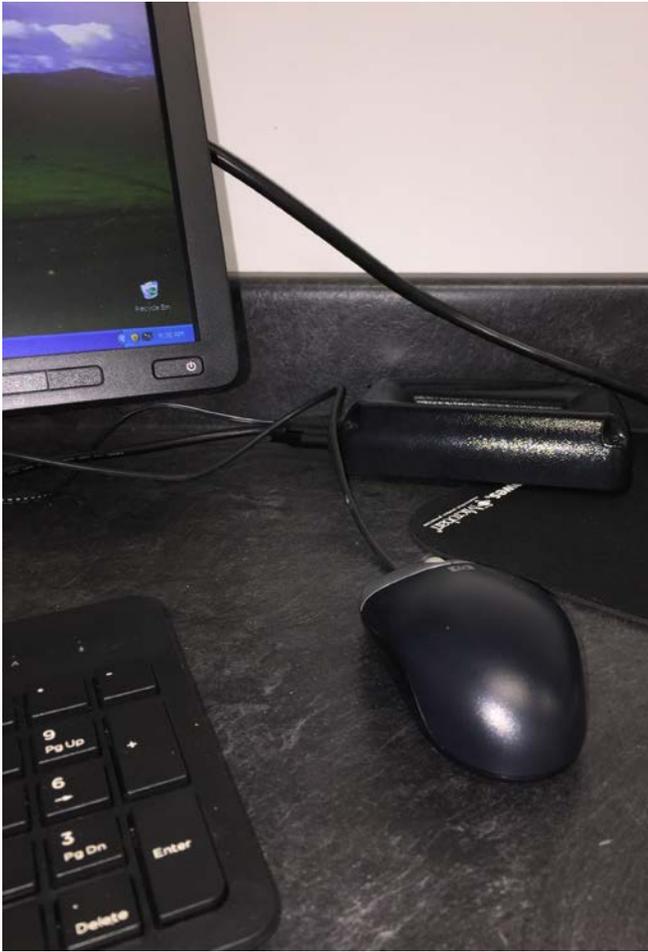
TAB5 Front



TAB5 Rear



TAB5 Desktop



Additional Information Collected from TAB5 CLI:

Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.

```
C:\Documents and Settings\administrator.ELECTIONS>hostname
```

TAB5

```
C:\Documents and Settings\administrator.ELECTIONS>whoami
```

'whoami' is not recognized as an internal or external command,
operable program or batch file.



DNS Servers : 192.168.1.20
 Primary WINS Server : 192.168.1.20
 Lease Obtained. : Monday, March 12, 2018 8:44:57 AM
 Lease Expires : Tuesday, March 20, 2018 8:44:57 AM

C:\Documents and Settings\administrator.ELECTIONS>arp -a

Interface: 192.168.1.11 --- 0x2

Internet Address	Physical Address	Type
192.168.1.20	00-14-22-60-3f-94	dynamic

C:\Documents and Settings\administrator.ELECTIONS>Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\administrator.ELECTIONS>netstat -rn

Route Table

=====

Interface List

0x1 MS TCP Loopback interface
 0x2 ...18 03 73 14 1c 2c Intel(R) 82579LM Gigabit Network Connection - Pa
 cket Scheduler Miniport

=====

=====

Active Routes:



Network	Destination	Netmask	Gateway	Interface	Metric
	0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.11	10
	127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
	192.168.1.0	255.255.255.0	192.168.1.11	192.168.1.11	10
	192.168.1.11	255.255.255.255	127.0.0.1	127.0.0.1	10
	192.168.1.255	255.255.255.255	192.168.1.11	192.168.1.11	10
	224.0.0.0	240.0.0.0	192.168.1.11	192.168.1.11	10
	255.255.255.255	255.255.255.255	192.168.1.11	192.168.1.11	1

Default Gateway: 192.168.1.1

=====

Persistent Routes:

None

C:\Documents and Settings\administrator.ELECTIONS>netstat -an

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3306	0.0.0.0:0	LISTENING
TCP	127.0.0.1:1036	127.0.0.1:1037	ESTABLISHED
TCP	127.0.0.1:1037	127.0.0.1:1036	ESTABLISHED
TCP	127.0.0.1:1043	0.0.0.0:0	LISTENING
TCP	127.0.0.1:1044	0.0.0.0:0	LISTENING



```
TCP 192.168.1.11:139 0.0.0.0:0 LISTENING
TCP 192.168.1.11:1202 192.168.1.20:445 ESTABLISHED
UDP 0.0.0.0:445 *.*
UDP 0.0.0.0:500 *.*
UDP 0.0.0.0:4500 *.*
UDP 127.0.0.1:123 *.*
UDP 127.0.0.1:1025 *.*
UDP 127.0.0.1:1048 *.*
UDP 127.0.0.1:1900 *.*
UDP 192.168.1.11:123 *.*
UDP 192.168.1.11:137 *.*
UDP 192.168.1.11:138 *.*
UDP 192.168.1.11:1900 *.*
```

C:\Documents and Settings\administrator.ELECTIONS>Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\administrator.ELECTIONS>systeminfo

```
Host Name:          TAB5
OS Name:            Microsoft Windows XP Professional
OS Version:        5.1.2600 Service Pack 3 Build 2600
OS Manufacturer:   Microsoft Corporation
OS Configuration:  Member Workstation
OS Build Type:      Multiprocessor Free
```



Registered Owner: admin

Registered Organization:

Product ID: 76487-OEM-0060807-79698

Original Install Date: 8/2/2016, 6:04:17 PM

System Up Time: 0 Days, 0 Hours, 21 Minutes, 31 Seconds

System Manufacturer: Dell Inc.

System Model: OptiPlex 790

System type: X86-based PC

Processor(s): 1 Processor(s) Installed.

[01]: x86 Family 6 Model 42 Stepping 7 GenuineIntel ~

3093 Mhz

BIOS Version: DELL - 6222004

Windows Directory: C:\WINDOWS

System Directory: C:\WINDOWS\system32

Boot Device: \Device\HarddiskVolume1

System Locale: en-us;English (United States)

Input Locale: en-us;English (United States)

Time Zone: (GMT-05:00) Eastern Time (US & Canada)

Total Physical Memory: 3,241 MB

Available Physical Memory: 2,798 MB

Virtual Memory: Max Size: 2,048 MB

Virtual Memory: Available: 2,008 MB

Virtual Memory: In Use: 40 MB

Page File Location(s): C:\pagefile.sys

Domain: elections.local



Logon Server: \\BOE

Hotfix(s): 250 Hotfix(s) Installed.

[01]: File 1

[02]: File 1

[03]: File 1

[04]: File 1

[05]: File 1

[06]: File 1

[07]: File 1

[08]: File 1

[09]: File 1

[10]: File 1

[11]: File 1

[12]: File 1

[13]: File 1

[14]: File 1

[15]: File 1

[16]: File 1

[17]: File 1

[18]: File 1

[19]: File 1

[20]: File 1

[21]: File 1

[22]: File 1

[23]: File 1



[24]: File 1

[25]: File 1

[26]: File 1

[27]: File 1

[28]: File 1

[29]: File 1

[30]: File 1

[31]: File 1

[32]: File 1

[33]: File 1

[34]: File 1

[35]: File 1

[36]: File 1

[37]: File 1

[38]: File 1

[39]: File 1

[40]: File 1

[41]: File 1

[42]: File 1

[43]: File 1

[44]: File 1

[45]: File 1

[46]: File 1

[47]: File 1

[48]: File 1



[49]: File 1

[50]: File 1

[51]: File 1

[52]: File 1

[53]: File 1

[54]: File 1

[55]: File 1

[56]: File 1

[57]: File 1

[58]: File 1

[59]: File 1

[60]: File 1

[61]: File 1

[62]: File 1

[63]: File 1

[64]: File 1

[65]: File 1

[66]: File 1

[67]: File 1

[68]: File 1

[69]: File 1

[70]: File 1

[71]: File 1

[72]: File 1

[73]: File 1



[74]: File 1

[75]: File 1

[76]: File 1

[77]: File 1

[78]: File 1

[79]: File 1

[80]: File 1

[81]: File 1

[82]: File 1

[83]: File 1

[84]: File 1

[85]: File 1

[86]: File 1

[87]: File 1

[88]: File 1

[89]: File 1

[90]: File 1

[91]: File 1

[92]: File 1

[93]: File 1

[94]: File 1

[95]: File 1

[96]: File 1

[97]: File 1

[98]: File 1



- [99]: File 1
- [100]: File 1
- [101]: File 1
- [102]: File 1
- [103]: File 1
- [104]: File 1
- [105]: File 1
- [106]: File 1
- [107]: File 1
- [108]: File 1
- [109]: File 1
- [110]: File 1
- [111]: File 1
- [112]: File 1
- [113]: File 1
- [114]: File 1
- [115]: File 1
- [116]: File 1
- [117]: File 1
- [118]: File 1
- [119]: File 1
- [120]: File 1
- [121]: File 1
- [122]: Q147222
- [123]: KB2378111_WM9



- [124]: KB2803821-v2_WM9
- [125]: KB952069_WM9
- [126]: KB954155_WM9
- [127]: KB973540_WM9
- [128]: KB975558_WM8
- [129]: KB978695_WM9
- [130]: KB2564958 - Update
- [131]: KB936929 - Service Pack
- [132]: KB2115168 - Update
- [133]: KB2229593 - Update
- [134]: KB2296011 - Update
- [135]: KB2347290 - Update
- [136]: KB2387149 - Update
- [137]: KB2393802 - Update
- [138]: KB2419632 - Update
- [139]: KB2423089 - Update
- [140]: KB2443105 - Update
- [141]: KB2478960 - Update
- [142]: KB2478971 - Update
- [143]: KB2479943 - Update
- [144]: KB2481109 - Update
- [145]: KB2483185 - Update
- [146]: KB2485663 - Update
- [147]: KB2506212 - Update
- [148]: KB2507938 - Update



- [149]: KB2508429 - Update
- [150]: KB2509553 - Update
- [151]: KB2510581 - Update
- [152]: KB2535512 - Update
- [153]: KB2536276-v2 - Update
- [154]: KB2544893-v2 - Update
- [155]: KB2566454 - Update
- [156]: KB2570947 - Update
- [157]: KB2584146 - Update
- [158]: KB2585542 - Update
- [159]: KB2592799 - Update
- [160]: KB2598479 - Update
- [161]: KB2603381 - Update
- [162]: KB2619339 - Update
- [163]: KB2620712 - Update
- [164]: KB2631813 - Update
- [165]: KB2653956 - Update
- [166]: KB2655992 - Update
- [167]: KB2659262 - Update
- [168]: KB2661637 - Update
- [169]: KB2676562 - Update
- [170]: KB2686509 - Update
- [171]: KB2691442 - Update
- [172]: KB2698365 - Update
- [173]: KB2705219-v2 - Update



- [174]: KB2712808 - Update
- [175]: KB2719985 - Update
- [176]: KB2723135-v2 - Update
- [177]: KB2727528 - Update
- [178]: KB2757638 - Update
- [179]: KB2770660 - Update
- [180]: KB2780091 - Update
- [181]: KB2802968 - Update
- [182]: KB2807986 - Update
- [183]: KB2813345 - Update
- [184]: KB2820917 - Update
- [185]: KB2834886 - Update
- [186]: KB2847311 - Update
- [187]: KB2850869 - Update
- [188]: KB2859537 - Update
- [189]: KB2862152 - Update
- [190]: KB2862330 - Update
- [191]: KB2862335 - Update
- [192]: KB2864063 - Update
- [193]: KB2868038 - Update
- [194]: KB2868626 - Update
- [195]: KB2876217 - Update
- [196]: KB2876331 - Update
- [197]: KB2884256 - Update
- [198]: KB2892075 - Update



- [199]: KB2893294 - Update
- [200]: KB2898715 - Update
- [201]: KB2900986 - Update
- [202]: KB2904266 - Update
- [203]: KB2909212 - Update
- [204]: KB2914368 - Update
- [205]: KB2916036 - Update
- [206]: KB2922229 - Update
- [207]: KB2929961 - Update
- [208]: KB2930275 - Update
- [209]: KB2936068 - Update
- [210]: KB2964358 - Update
- [211]: KB923561 - Update
- [212]: KB942288-v3 - Update
- [213]: KB946648 - Update
- [214]: KB950762 - Update
- [215]: KB950974 - Update
- [216]: KB951376-v2 - Update
- [217]: KB952004 - Update
- [218]: KB95

NetWork Card(s): 1 NIC(s) Installed.

[01]: Intel(R) 82579LM Gigabit Network Connection

Connection Name: Local Area Connection

DHCP Enabled: Yes



DHCP Server: 192.168.1.20

IP address(es)

[01]: 192.168.1.11

C:\Documents and Settings\administrator.ELECTIONS>

Post-Election Review:

The same output was capture from the system at the CLI and a file diff was performed. Below are the differences.

C:\Users\Frank\OneDrive - solutions4networks Inc\COA\Air Gap Analysis\airgap_13Mar2018,TAB5-Pre-AG.txt	C:\Users\Frank\OneDrive - solutions4networks Inc\COA\Air Gap Analysis\airgap_13Mar2018,TAB5-Post-AG.txt
DHCP Server : 192.168.1.20	DHCP Server : 192.168.1.20
DNS Servers : 192.168.1.20	DNS Servers : 192.168.1.20
Primary WINS Server : 192.168.1.20	Primary WINS Server : 192.168.1.20
Lease Obtained. : Monday, March 12, 2018 8:44:	Lease Obtained. : Thursday, March 15, 2018 8:47:
Lease Expires : Tuesday, March 20, 2018 8:44:	Lease Expires : Friday, March 23, 2018 8:47:
ments and Settings\administrator.ELECTIONS>arp -a	ments and Settings\administrator.ELECTIONS>arp -a
ce: 192.168.1.11 --- 0x2	ce: 192.168.1.11 --- 0x2
net Address Physical Address Type	net Address Physical Address Type
68.1.20 00-14-22-60-3f-94 dynamic	68.1.20 00-14-22-60-3f-94 dynamic
ments and Settings\administrator.ELECTIONS>Microsoft Windows XP [ft Windows XP [Version 5.1.2600]

Netstat -an

C:\Documents and Settings\administrator.ELECTIONS>netstat -an	C:\Documents and Settings\administrator.ELECTIONS>netstat -an
Active Connections	Active Connections
Proto Local Address Foreign Address State	Proto Local Address Foreign Address State
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING	TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING	TCP 0.0.0.0:445 0.0.0.0:0 LISTENING
TCP 0.0.0.0:3306 0.0.0.0:0 LISTENING	TCP 0.0.0.0:3306 0.0.0.0:0 LISTENING
TCP 127.0.0.1:1036 127.0.0.1:1037 ESTABLISHED	TCP 127.0.0.1:1036 127.0.0.1:1037 ESTABLISHED
TCP 127.0.0.1:1037 127.0.0.1:1036 ESTABLISHED	TCP 127.0.0.1:1037 127.0.0.1:1036 ESTABLISHED
TCP 127.0.0.1:1043 0.0.0.0:0 LISTENING	TCP 127.0.0.1:1043 0.0.0.0:0 LISTENING
TCP 127.0.0.1:1044 0.0.0.0:0 LISTENING	TCP 127.0.0.1:1044 0.0.0.0:0 LISTENING
TCP 192.168.1.11:139 0.0.0.0:0 LISTENING	TCP 192.168.1.11:139 0.0.0.0:0 LISTENING
TCP 192.168.1.11:1202 192.168.1.20:445 ESTABLISHED	TCP 192.168.1.11:1166 192.168.1.20:445 ESTABLISHED
	TCP 192.168.1.11:1168 192.168.1.20:135 TIME_WAIT
	TCP 192.168.1.11:1169 192.168.1.20:1026 TIME_WAIT
	TCP 192.168.1.11:1172 192.168.1.20:389 TIME_WAIT
	TCP 192.168.1.11:1175 192.168.1.20:389 TIME_WAIT
	TCP 192.168.1.11:1176 192.168.1.20:445 TIME_WAIT
	TCP 192.168.1.11:1180 192.168.1.20:389 TIME_WAIT
	TCP 192.168.1.11:1181 192.168.1.20:389 TIME_WAIT

Systeminfo

System Up Time: 0 Days, 0 Hours, 21 Minutes, 31 Second	System Up Time: 0 Days, 0 Hours, 6 Minutes, 47 Seconds
System Manufacturer: Dell Inc.	System Manufacturer: Dell Inc.
System Model: OptiPlex 790	System Model: OptiPlex 790
System type: X86-based PC	System type: X86-based PC
Processor(s): 1 Processor(s) Installed.	Processor(s): 1 Processor(s) Installed.
[01]: x86 Family 6 Model 42 Stepping 7	[01]: x86 Family 6 Model 42 Stepping 7
3093 Mhz	3092 Mhz
BIOS Version: DELL - 6222004	BIOS Version: DELL - 6222004
Windows Directory: C:\WINDOWS	Windows Directory: C:\WINDOWS
System Directory: C:\WINDOWS\system32	System Directory: C:\WINDOWS\system32
Boot Device: \Device\HarddiskVolumel	Boot Device: \Device\HarddiskVolumel
System Locale: en-us:English (United States)	System Locale: en-us:English (United States)
Input Locale: en-us:English (United States)	Input Locale: en-us:English (United States)
Time Zone: (GMT-05:00) Eastern Time (US & Canada)	Time Zone: (GMT-05:00) Eastern Time (US & Canada)
Total Physical Memory: 3,241 MB	Total Physical Memory: 3,241 MB
Available Physical Memory: 2,798 MB	Available Physical Memory: 2,797 MB
Virtual Memory: Max Size: 2.048 MB	Virtual Memory: Max Size: 2.048 MB

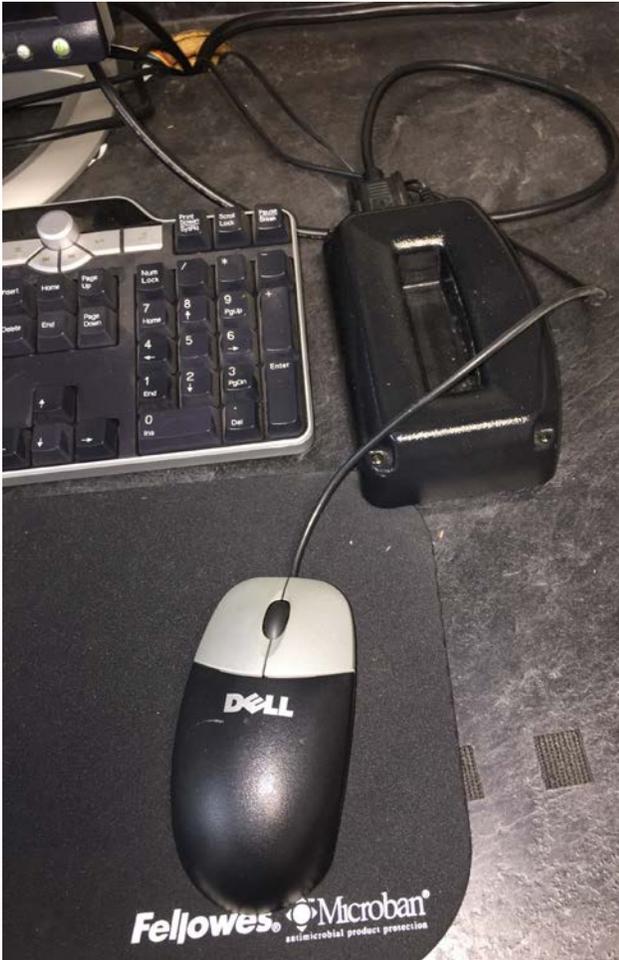
TAB9 Front



TAB9 Rear



TAB9 Desktop



Additional Information Collected from TAB9 CLI:

Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.

```
C:\Documents and Settings\Administrator.ELECTIONS>hostname
```

TAB9

```
C:\Documents and Settings\Administrator.ELECTIONS>whoami
```

'whoami' is not recognized as an internal or external command,



DHCP Server : 192.168.1.20
 DNS Servers : 192.168.1.20
 Primary WINS Server : 192.168.1.20
 Lease Obtained. : Monday, March 12, 2018 8:49:43 AM
 Lease Expires : Tuesday, March 20, 2018 8:49:43 AM

C:\Documents and Settings\Administrator.ELECTIONS>arp -a

Interface: 192.168.1.12 --- 0x2

Internet Address	Physical Address	Type
192.168.1.20	00-14-22-60-3f-94	dynamic

C:\Documents and Settings\Administrator.ELECTIONS>Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator.ELECTIONS>netstat -rn

Route Table

=====

Interface List

0x1 MS TCP Loopback interface
 0x2 ...18 03 73 15 97 68 Intel(R) 82579LM Gigabit Network Connection - Pa
 cket Scheduler Miniport

=====

=====



Active Routes:

Network	Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.12		10
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1		1
192.168.1.0	255.255.255.0	192.168.1.12	192.168.1.12		10
192.168.1.12	255.255.255.255	127.0.0.1	127.0.0.1		10
192.168.1.255	255.255.255.255	192.168.1.12	192.168.1.12		10
224.0.0.0	240.0.0.0	192.168.1.12	192.168.1.12		10
255.255.255.255	255.255.255.255	192.168.1.12	192.168.1.12		1

Default Gateway: 192.168.1.1

=====

Persistent Routes:

None

C:\Documents and Settings\Administrator\ELECTIONS>netstat -an

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3306	0.0.0.0:0	LISTENING
TCP	127.0.0.1:1037	127.0.0.1:1038	ESTABLISHED
TCP	127.0.0.1:1038	127.0.0.1:1037	ESTABLISHED
TCP	127.0.0.1:1043	0.0.0.0:0	LISTENING



TCP	127.0.0.1:1051	0.0.0.0:0	LISTENING
TCP	192.168.1.12:139	0.0.0.0:0	LISTENING
UDP	0.0.0.0:445	*.*	
UDP	0.0.0.0:500	*.*	
UDP	0.0.0.0:4500	*.*	
UDP	127.0.0.1:123	*.*	
UDP	127.0.0.1:1025	*.*	
UDP	127.0.0.1:1047	*.*	
UDP	127.0.0.1:1900	*.*	
UDP	192.168.1.12:123	*.*	
UDP	192.168.1.12:137	*.*	
UDP	192.168.1.12:138	*.*	
UDP	192.168.1.12:1900	*.*	

C:\Documents and Settings\Administrator.ELECTIONS>Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator.ELECTIONS>systeminfo

Host Name: TAB9
OS Name: Microsoft Windows XP Professional
OS Version: 5.1.2600 Service Pack 3 Build 2600
OS Manufacturer: Microsoft Corporation
OS Configuration: Member Workstation
OS Build Type: Multiprocessor Free



Registered Owner: admin

Registered Organization:

Product ID: 76487-OEM-0060807-79698

Original Install Date: 8/2/2016, 6:04:17 PM

System Up Time: 0 Days, 0 Hours, 21 Minutes, 20 Seconds

System Manufacturer: Dell Inc.

System Model: OptiPlex 790

System type: X86-based PC

Processor(s): 1 Processor(s) Installed.

[01]: x86 Family 6 Model 42 Stepping 7 GenuineIntel ~
3092 Mhz

BIOS Version: DELL - 6222004

Windows Directory: C:\WINDOWS

System Directory: C:\WINDOWS\system32

Boot Device: \Device\HarddiskVolume1

System Locale: en-us;English (United States)

Input Locale: en-us;English (United States)

Time Zone: (GMT-05:00) Eastern Time (US & Canada)

Total Physical Memory: 3,241 MB

Available Physical Memory: 2,752 MB

Virtual Memory: Max Size: 2,048 MB

Virtual Memory: Available: 2,008 MB

Virtual Memory: In Use: 40 MB

Page File Location(s): C:\pagefile.sys

Domain: elections.local



Logon Server: \\BOE

Hotfix(s): 250 Hotfix(s) Installed.

[01]: File 1

[02]: File 1

[03]: File 1

[04]: File 1

[05]: File 1

[06]: File 1

[07]: File 1

[08]: File 1

[09]: File 1

[10]: File 1

[11]: File 1

[12]: File 1

[13]: File 1

[14]: File 1

[15]: File 1

[16]: File 1

[17]: File 1

[18]: File 1

[19]: File 1

[20]: File 1

[21]: File 1

[22]: File 1

[23]: File 1



[24]: File 1

[25]: File 1

[26]: File 1

[27]: File 1

[28]: File 1

[29]: File 1

[30]: File 1

[31]: File 1

[32]: File 1

[33]: File 1

[34]: File 1

[35]: File 1

[36]: File 1

[37]: File 1

[38]: File 1

[39]: File 1

[40]: File 1

[41]: File 1

[42]: File 1

[43]: File 1

[44]: File 1

[45]: File 1

[46]: File 1

[47]: File 1

[48]: File 1



[49]: File 1

[50]: File 1

[51]: File 1

[52]: File 1

[53]: File 1

[54]: File 1

[55]: File 1

[56]: File 1

[57]: File 1

[58]: File 1

[59]: File 1

[60]: File 1

[61]: File 1

[62]: File 1

[63]: File 1

[64]: File 1

[65]: File 1

[66]: File 1

[67]: File 1

[68]: File 1

[69]: File 1

[70]: File 1

[71]: File 1

[72]: File 1

[73]: File 1



[74]: File 1

[75]: File 1

[76]: File 1

[77]: File 1

[78]: File 1

[79]: File 1

[80]: File 1

[81]: File 1

[82]: File 1

[83]: File 1

[84]: File 1

[85]: File 1

[86]: File 1

[87]: File 1

[88]: File 1

[89]: File 1

[90]: File 1

[91]: File 1

[92]: File 1

[93]: File 1

[94]: File 1

[95]: File 1

[96]: File 1

[97]: File 1

[98]: File 1



- [99]: File 1
- [100]: File 1
- [101]: File 1
- [102]: File 1
- [103]: File 1
- [104]: File 1
- [105]: File 1
- [106]: File 1
- [107]: File 1
- [108]: File 1
- [109]: File 1
- [110]: File 1
- [111]: File 1
- [112]: File 1
- [113]: File 1
- [114]: File 1
- [115]: File 1
- [116]: File 1
- [117]: File 1
- [118]: File 1
- [119]: File 1
- [120]: File 1
- [121]: File 1
- [122]: Q147222
- [123]: KB2378111_WM9



- [124]: KB2803821-v2_WM9
- [125]: KB952069_WM9
- [126]: KB954155_WM9
- [127]: KB973540_WM9
- [128]: KB975558_WM8
- [129]: KB978695_WM9
- [130]: KB2564958 - Update
- [131]: KB936929 - Service Pack
- [132]: KB2115168 - Update
- [133]: KB2229593 - Update
- [134]: KB2296011 - Update
- [135]: KB2347290 - Update
- [136]: KB2387149 - Update
- [137]: KB2393802 - Update
- [138]: KB2419632 - Update
- [139]: KB2423089 - Update
- [140]: KB2443105 - Update
- [141]: KB2478960 - Update
- [142]: KB2478971 - Update
- [143]: KB2479943 - Update
- [144]: KB2481109 - Update
- [145]: KB2483185 - Update
- [146]: KB2485663 - Update
- [147]: KB2506212 - Update
- [148]: KB2507938 - Update



- [149]: KB2508429 - Update
- [150]: KB2509553 - Update
- [151]: KB2510581 - Update
- [152]: KB2535512 - Update
- [153]: KB2536276-v2 - Update
- [154]: KB2544893-v2 - Update
- [155]: KB2566454 - Update
- [156]: KB2570947 - Update
- [157]: KB2584146 - Update
- [158]: KB2585542 - Update
- [159]: KB2592799 - Update
- [160]: KB2598479 - Update
- [161]: KB2603381 - Update
- [162]: KB2619339 - Update
- [163]: KB2620712 - Update
- [164]: KB2631813 - Update
- [165]: KB2653956 - Update
- [166]: KB2655992 - Update
- [167]: KB2659262 - Update
- [168]: KB2661637 - Update
- [169]: KB2676562 - Update
- [170]: KB2686509 - Update
- [171]: KB2691442 - Update
- [172]: KB2698365 - Update
- [173]: KB2705219-v2 - Update



- [174]: KB2712808 - Update
- [175]: KB2719985 - Update
- [176]: KB2723135-v2 - Update
- [177]: KB2727528 - Update
- [178]: KB2757638 - Update
- [179]: KB2770660 - Update
- [180]: KB2780091 - Update
- [181]: KB2802968 - Update
- [182]: KB2807986 - Update
- [183]: KB2813345 - Update
- [184]: KB2820917 - Update
- [185]: KB2834886 - Update
- [186]: KB2847311 - Update
- [187]: KB2850869 - Update
- [188]: KB2859537 - Update
- [189]: KB2862152 - Update
- [190]: KB2862330 - Update
- [191]: KB2862335 - Update
- [192]: KB2864063 - Update
- [193]: KB2868038 - Update
- [194]: KB2868626 - Update
- [195]: KB2876217 - Update
- [196]: KB2876331 - Update
- [197]: KB2884256 - Update
- [198]: KB2892075 - Update



- [199]: KB2893294 - Update
- [200]: KB2898715 - Update
- [201]: KB2900986 - Update
- [202]: KB2904266 - Update
- [203]: KB2909212 - Update
- [204]: KB2914368 - Update
- [205]: KB2916036 - Update
- [206]: KB2922229 - Update
- [207]: KB2929961 - Update
- [208]: KB2930275 - Update
- [209]: KB2936068 - Update
- [210]: KB2964358 - Update
- [211]: KB923561 - Update
- [212]: KB942288-v3 - Update
- [213]: KB946648 - Update
- [214]: KB950762 - Update
- [215]: KB950974 - Update
- [216]: KB951376-v2 - Update
- [217]: KB952004 - Update
- [218]: KB95

NetWork Card(s): 1 NIC(s) Installed.

[01]: Intel(R) 82579LM Gigabit Network Connection

Connection Name: Local Area Connection

DHCP Enabled: Yes



DHCP Server: 192.168.1.20

IP address(es)

[01]: 192.168.1.12

C:\Documents and Settings\Administrator.ELECTIONS>

Post-Election Review:

The same output was capture from the system at the CLI and a file diff was performed. Below are the differences.

<pre>C:\Users\Frank\OneDrive - solutions4networks Inc\COA\Air Gap Analysis\airgap_13Mar2018\TAB9-Pre-AG.txt Physical Address. : 18-03-73-15-97-68 Dhcp Enabled. : Yes Autoconfiguration Enabled : Yes IP Address. : 192.168.1.12 Subnet Mask : 255.255.255.0 Default Gateway : 192.168.1.1 DHCP Server : 192.168.1.20 DNS Servers : 192.168.1.20 Primary WINS Server : 192.168.1.20 Lease Obtained. : Monday, March 12, 2018 Lease Expires : Tuesday, March 20, 2018 C:\Documents and Settings\Administrator.ELECTIONS>arp -a Interface: 192.168.1.12 --- 0x2 Internet Address Physical Address Type 192.168.1.20 00-14-22-60-3f-94 dynamic C:\Documents and Settings\Administrator.ELECTIONS>Microsoft Windows [Version 5.1.2600.5512] (C) Copyright 1985-2001 Microsoft Corp.</pre>	<pre>C:\Users\Frank\OneDrive - solutions4networks Inc\COA\Air Gap Analysis\airgap_13Mar2018\TAB9-Post-AG.txt Physical Address. : 18-03-73-15-97-68 Dhcp Enabled. : Yes Autoconfiguration Enabled : Yes IP Address. : 192.168.1.12 Subnet Mask : 255.255.255.0 Default Gateway : 192.168.1.1 DHCP Server : 192.168.1.20 DNS Servers : 192.168.1.20 Primary WINS Server : 192.168.1.20 Lease Obtained. : Monday, March 12, 2018 Lease Expires : Tuesday, March 20, 2018 C:\Documents and Settings\Administrator.ELECTIONS>arp -a Interface: 192.168.1.12 --- 0x2 Internet Address Physical Address Type 192.168.1.20 00-14-22-60-3f-94 dynamic C:\Documents and Settings\Administrator.ELECTIONS>Microsoft Windows [Version 5.1.2600.5512] (C) Copyright 1985-2001 Microsoft Corp.</pre>
---	--

Netstat – an

<pre>C:\Documents and Settings\Administrator.ELECTIONS>netstat -an TCP 192.168.1.12:1126 0.0.0.0:0 LISTENING UDP 0.0.0.0:445 *:* UDP 0.0.0.0:500 *:* UDP 0.0.0.0:4500 *:* UDP 127.0.0.1:123 *:* UDP 127.0.0.1:1025 *:* UDP 127.0.0.1:1047 *:* UDP 127.0.0.1:1900 *:* UDP 192.168.1.12:123 *:* UDP 192.168.1.12:137 *:* UDP 192.168.1.12:138 *:* UDP 192.168.1.12:1900 *:* C:\Documents and Settings\Administrator.ELECTIONS>Microsoft Windows [Version 5.1.2600.5512] (C) Copyright 1985-2001 Microsoft Corp.</pre>	<pre>C:\Documents and Settings\Administrator.ELECTIONS>netstat -an TCP 192.168.1.12:1126 192.168.1.20:445 ESTABLISHED UDP 0.0.0.0:445 *:* UDP 0.0.0.0:500 *:* UDP 0.0.0.0:4500 *:* UDP 127.0.0.1:123 *:* Microsoft Windows [Version 5.1.2600.5512] (C) Copyright 1985-2001 Microsoft Corp.</pre>
---	--

Systeminfo

<pre>System Up Time: 0 Days, 0 Hours, 21 Minutes, 20 Seconds System Manufacturer: Dell Inc. System Model: OptiPlex 790 System type: X86-based PC Processor(s): 1 Processor(s) Installed. [01]: x86 Family 6 Model 42 Stepping 7 3092 Mhz BIOS Version: DELL - 6222004 Windows Directory: C:\WINDOWS System Directory: C:\WINDOWS\system32 Boot Device: \Device\HarddiskVolume1 System Locale: en-us;English (United States) Input Locale: en-us;English (United States) Time Zone: (GMT-05:00) Eastern Time (US & Canada) Total Physical Memory: 3,241 MB Available Physical Memory: 2,752 MB Virtual Memory: Max Size: 2,048 MB</pre>	<pre>System Up Time: 0 Days, 0 Hours, 6 Minutes, 57 Seconds System Manufacturer: Dell Inc. System Model: OptiPlex 790 System type: X86-based PC Processor(s): 1 Processor(s) Installed. [01]: x86 Family 6 Model 42 Stepping 7 3092 Mhz BIOS Version: DELL - 6222004 Windows Directory: C:\WINDOWS System Directory: C:\WINDOWS\system32 Boot Device: \Device\HarddiskVolume1 System Locale: en-us;English (United States) Input Locale: en-us;English (United States) Time Zone: (GMT-05:00) Eastern Time (US & Canada) Total Physical Memory: 3,241 MB Available Physical Memory: 2,775 MB Virtual Memory: Max Size: 2,048 MB</pre>
--	---

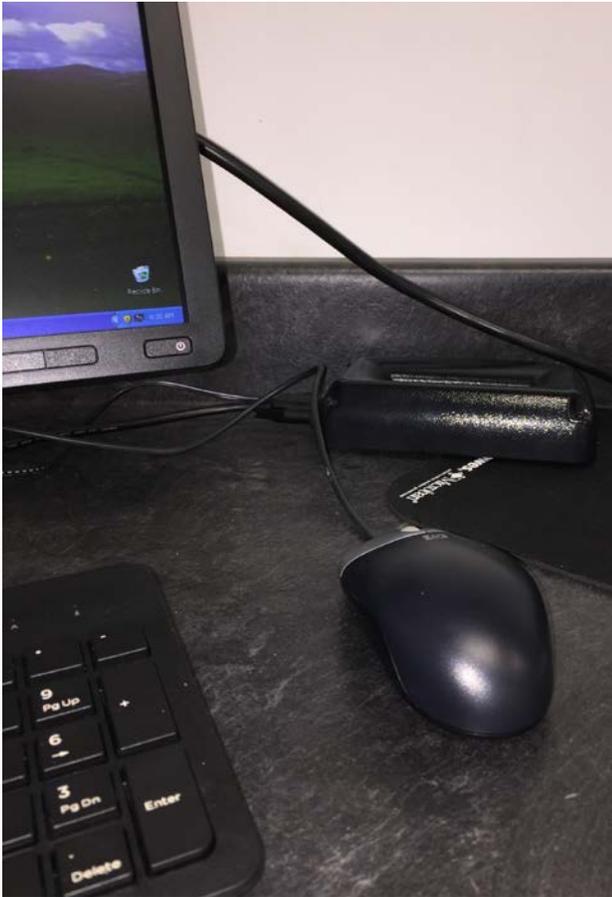
TAB7 Front



TAB7 Rear



TAB7 Desktop



Additional Information Collected from TAB7 CLI:

Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.

```
C:\Documents and Settings\Administrator.ELECTIONS>hostname
```

```
TAB7
```

```
C:\Documents and Settings\Administrator.ELECTIONS>whoami
```

'whoami' is not recognized as an internal or external command,
operable program or batch file.



DNS Servers : 192.168.1.20
 Primary WINS Server : 192.168.1.20
 Lease Obtained. : Monday, March 12, 2018 8:44:15 AM
 Lease Expires : Tuesday, March 20, 2018 8:44:15 AM

C:\Documents and Settings\Administrator.ELECTIONS>arp -a

Interface: 192.168.1.40 --- 0x2

Internet Address	Physical Address	Type
192.168.1.20	00-14-22-60-3f-94	dynamic

C:\Documents and Settings\Administrator.ELECTIONS>Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator.ELECTIONS>netstat -rn

Route Table

=====

Interface List

0x1 MS TCP Loopback interface
 0x2 ...18 03 73 1b cf e2 Intel(R) 82579LM Gigabit Network Connection - Pa
 cket Scheduler Miniport

=====

=====

Active Routes:



```
Network Destination    Netmask    Gateway    Interface    Metric
0.0.0.0                0.0.0.0    192.168.1.1 192.168.1.40 10
127.0.0.0              255.0.0.0    127.0.0.1   127.0.0.1   1
192.168.1.0            255.255.255.0 192.168.1.40 192.168.1.40 10
192.168.1.40           255.255.255.255 127.0.0.1   127.0.0.1   10
192.168.1.255         255.255.255.255 192.168.1.40 192.168.1.40 10
224.0.0.0              240.0.0.0    192.168.1.40 192.168.1.40 10
255.255.255.255       255.255.255.255 192.168.1.40 192.168.1.40 1
```

Default Gateway: 192.168.1.1

=====

Persistent Routes:

None

C:\Documents and Settings\Administrator\ELECTIONS>netstat -an

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3306	0.0.0.0:0	LISTENING
TCP	127.0.0.1:1047	0.0.0.0:0	LISTENING
TCP	127.0.0.1:1048	127.0.0.1:1049	ESTABLISHED
TCP	127.0.0.1:1049	127.0.0.1:1048	ESTABLISHED
TCP	127.0.0.1:1055	0.0.0.0:0	LISTENING



```
TCP 192.168.1.40:139 0.0.0.0:0 LISTENING
UDP 0.0.0.0:445 *.*
UDP 0.0.0.0:500 *.*
UDP 0.0.0.0:4500 *.*
UDP 127.0.0.1:123 *.*
UDP 127.0.0.1:1025 *.*
UDP 127.0.0.1:1041 *.*
UDP 127.0.0.1:1900 *.*
UDP 192.168.1.40:123 *.*
UDP 192.168.1.40:137 *.*
UDP 192.168.1.40:138 *.*
UDP 192.168.1.40:1900 *.*
```

C:\Documents and Settings\Administrator.ELECTIONS>Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator.ELECTIONS>systeminfo

```
Host Name: TAB7
OS Name: Microsoft Windows XP Professional
OS Version: 5.1.2600 Service Pack 3 Build 2600
OS Manufacturer: Microsoft Corporation
OS Configuration: Member Workstation
OS Build Type: Multiprocessor Free
Registered Owner: admin
```



Registered Organization:

Product ID: 76487-OEM-0060807-79698

Original Install Date: 8/2/2016, 6:04:17 PM

System Up Time: 0 Days, 0 Hours, 26 Minutes, 8 Seconds

System Manufacturer: Dell Inc.

System Model: OptiPlex 790

System type: X86-based PC

Processor(s): 1 Processor(s) Installed.

[01]: x86 Family 6 Model 42 Stepping 7 GenuineIntel ~

3092 Mhz

BIOS Version: DELL - 6222004

Windows Directory: C:\WINDOWS

System Directory: C:\WINDOWS\system32

Boot Device: \Device\HarddiskVolume1

System Locale: en-us;English (United States)

Input Locale: en-us;English (United States)

Time Zone: (GMT-05:00) Eastern Time (US & Canada)

Total Physical Memory: 3,241 MB

Available Physical Memory: 2,854 MB

Virtual Memory: Max Size: 2,048 MB

Virtual Memory: Available: 2,008 MB

Virtual Memory: In Use: 40 MB

Page File Location(s): C:\pagefile.sys

Domain: elections.local

Logon Server: \\BOE



Hotfix(s): 250 Hotfix(s) Installed.

[01]: File 1

[02]: File 1

[03]: File 1

[04]: File 1

[05]: File 1

[06]: File 1

[07]: File 1

[08]: File 1

[09]: File 1

[10]: File 1

[11]: File 1

[12]: File 1

[13]: File 1

[14]: File 1

[15]: File 1

[16]: File 1

[17]: File 1

[18]: File 1

[19]: File 1

[20]: File 1

[21]: File 1

[22]: File 1

[23]: File 1

[24]: File 1



[25]: File 1

[26]: File 1

[27]: File 1

[28]: File 1

[29]: File 1

[30]: File 1

[31]: File 1

[32]: File 1

[33]: File 1

[34]: File 1

[35]: File 1

[36]: File 1

[37]: File 1

[38]: File 1

[39]: File 1

[40]: File 1

[41]: File 1

[42]: File 1

[43]: File 1

[44]: File 1

[45]: File 1

[46]: File 1

[47]: File 1

[48]: File 1

[49]: File 1



[50]: File 1

[51]: File 1

[52]: File 1

[53]: File 1

[54]: File 1

[55]: File 1

[56]: File 1

[57]: File 1

[58]: File 1

[59]: File 1

[60]: File 1

[61]: File 1

[62]: File 1

[63]: File 1

[64]: File 1

[65]: File 1

[66]: File 1

[67]: File 1

[68]: File 1

[69]: File 1

[70]: File 1

[71]: File 1

[72]: File 1

[73]: File 1

[74]: File 1



[75]: File 1

[76]: File 1

[77]: File 1

[78]: File 1

[79]: File 1

[80]: File 1

[81]: File 1

[82]: File 1

[83]: File 1

[84]: File 1

[85]: File 1

[86]: File 1

[87]: File 1

[88]: File 1

[89]: File 1

[90]: File 1

[91]: File 1

[92]: File 1

[93]: File 1

[94]: File 1

[95]: File 1

[96]: File 1

[97]: File 1

[98]: File 1

[99]: File 1



- [100]: File 1
- [101]: File 1
- [102]: File 1
- [103]: File 1
- [104]: File 1
- [105]: File 1
- [106]: File 1
- [107]: File 1
- [108]: File 1
- [109]: File 1
- [110]: File 1
- [111]: File 1
- [112]: File 1
- [113]: File 1
- [114]: File 1
- [115]: File 1
- [116]: File 1
- [117]: File 1
- [118]: File 1
- [119]: File 1
- [120]: File 1
- [121]: File 1
- [122]: Q147222
- [123]: KB2378111_WM9
- [124]: KB2803821-v2_WM9



- [125]: KB952069_WM9
- [126]: KB954155_WM9
- [127]: KB973540_WM9
- [128]: KB975558_WM8
- [129]: KB978695_WM9
- [130]: KB2564958 - Update
- [131]: KB936929 - Service Pack
- [132]: KB2115168 - Update
- [133]: KB2229593 - Update
- [134]: KB2296011 - Update
- [135]: KB2347290 - Update
- [136]: KB2387149 - Update
- [137]: KB2393802 - Update
- [138]: KB2419632 - Update
- [139]: KB2423089 - Update
- [140]: KB2443105 - Update
- [141]: KB2478960 - Update
- [142]: KB2478971 - Update
- [143]: KB2479943 - Update
- [144]: KB2481109 - Update
- [145]: KB2483185 - Update
- [146]: KB2485663 - Update
- [147]: KB2506212 - Update
- [148]: KB2507938 - Update
- [149]: KB2508429 - Update



- [150]: KB2509553 - Update
- [151]: KB2510581 - Update
- [152]: KB2535512 - Update
- [153]: KB2536276-v2 - Update
- [154]: KB2544893-v2 - Update
- [155]: KB2566454 - Update
- [156]: KB2570947 - Update
- [157]: KB2584146 - Update
- [158]: KB2585542 - Update
- [159]: KB2592799 - Update
- [160]: KB2598479 - Update
- [161]: KB2603381 - Update
- [162]: KB2619339 - Update
- [163]: KB2620712 - Update
- [164]: KB2631813 - Update
- [165]: KB2653956 - Update
- [166]: KB2655992 - Update
- [167]: KB2659262 - Update
- [168]: KB2661637 - Update
- [169]: KB2676562 - Update
- [170]: KB2686509 - Update
- [171]: KB2691442 - Update
- [172]: KB2698365 - Update
- [173]: KB2705219-v2 - Update
- [174]: KB2712808 - Update



- [175]: KB2719985 - Update
- [176]: KB2723135-v2 - Update
- [177]: KB2727528 - Update
- [178]: KB2757638 - Update
- [179]: KB2770660 - Update
- [180]: KB2780091 - Update
- [181]: KB2802968 - Update
- [182]: KB2807986 - Update
- [183]: KB2813345 - Update
- [184]: KB2820917 - Update
- [185]: KB2834886 - Update
- [186]: KB2847311 - Update
- [187]: KB2850869 - Update
- [188]: KB2859537 - Update
- [189]: KB2862152 - Update
- [190]: KB2862330 - Update
- [191]: KB2862335 - Update
- [192]: KB2864063 - Update
- [193]: KB2868038 - Update
- [194]: KB2868626 - Update
- [195]: KB2876217 - Update
- [196]: KB2876331 - Update
- [197]: KB2884256 - Update
- [198]: KB2892075 - Update
- [199]: KB2893294 - Update



- [200]: KB2898715 - Update
- [201]: KB2900986 - Update
- [202]: KB2904266 - Update
- [203]: KB2909212 - Update
- [204]: KB2914368 - Update
- [205]: KB2916036 - Update
- [206]: KB2922229 - Update
- [207]: KB2929961 - Update
- [208]: KB2930275 - Update
- [209]: KB2936068 - Update
- [210]: KB2964358 - Update
- [211]: KB923561 - Update
- [212]: KB942288-v3 - Update
- [213]: KB946648 - Update
- [214]: KB950762 - Update
- [215]: KB950974 - Update
- [216]: KB951376-v2 - Update
- [217]: KB952004 - Update
- [218]: KB95

NetWork Card(s): 1 NIC(s) Installed.

[01]: Intel(R) 82579LM Gigabit Network Connection

Connection Name: Local Area Connection

DHCP Enabled: Yes

DHCP Server: 192.168.1.20



IP address(es)

[01]: 192.168.1.40

C:\Documents and Settings\Administrator.ELECTIONS>

Post-Election Review:

The same output was capture from the system at the CLI and a file diff was performed. Below are the differences.

C:\Users\Frank\OneDrive - solutions4networks Inc\COA\Air Gap Analysis\airgap_13Mar2018\TAB7-Pre-AG.txt	C:\Users\Frank\OneDrive - solutions4networks Inc\COA\Air Gap Analysis\airgap_13Mar2018\TAB7-Post-AG.txt
DHCP Server : 192.168.1.20	DHCP Server : 192.168.1.20
DNS Servers : 192.168.1.20	DNS Servers : 192.168.1.20
Primary WINS Server : 192.168.1.20	Primary WINS Server : 192.168.1.20
Lease Obtained. : Monday, March 12, 2018	Lease Obtained. : Thursday, March 15, 2018
Lease Expires : Tuesday, March 20, 2018	Lease Expires : Friday, March 23, 2018

C:\Users\Frank\OneDrive - solutions4networks Inc\COA\Air Gap Analysis\airgap_13Mar2018\TAB7-Pre-AG.txt	C:\Users\Frank\OneDrive - solutions4networks Inc\COA\Air Gap Analysis\airgap_13Mar2018\TAB7-Post-AG.txt
Persistent Routes: None	Persistent Routes: None
C:\Documents and Settings\Administrator.ELECTIONS>netstat -an	C:\Documents and Settings\Administrator.ELECTIONS>netstat -an
Active Connections	Active Connections
Proto Local Address Foreign Address State	Proto Local Address Foreign Address State
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING	TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING	TCP 0.0.0.0:445 0.0.0.0:0 LISTENING
TCP 0.0.0.0:3306 0.0.0.0:0 LISTENING	TCP 0.0.0.0:3306 0.0.0.0:0 LISTENING
TCP 127.0.0.1:1047 0.0.0.0:0 LISTENING	TCP 127.0.0.1:1038 127.0.0.1:1039 ESTABLISHED
TCP 127.0.0.1:1048 127.0.0.1:1049 ESTABLISHED	TCP 127.0.0.1:1039 127.0.0.1:1038 ESTABLISHED
TCP 127.0.0.1:1049 127.0.0.1:1048 ESTABLISHED	TCP 127.0.0.1:1053 0.0.0.0:0 LISTENING
TCP 127.0.0.1:1055 0.0.0.0:0 LISTENING	TCP 127.0.0.1:1055 0.0.0.0:0 LISTENING
TCP 192.168.1.40:139 0.0.0.0:0 LISTENING	TCP 192.168.1.40:139 0.0.0.0:0 LISTENING
TCP 192.168.1.40:1092 192.168.1.20:445 ESTABLISHED	TCP 192.168.1.40:1092 192.168.1.20:445 ESTABLISHED
UDP 0.0.0.0:445 *:*	UDP 0.0.0.0:445 *:*
UDP 0.0.0.0:500 *:*	UDP 0.0.0.0:500 *:*
UDP 0.0.0.0:4500 *:*	UDP 0.0.0.0:4500 *:*
UDP 127.0.0.1:123 *:*	UDP 127.0.0.1:123 *:*
UDP 127.0.0.1:1025 *:*	UDP 127.0.0.1:1025 *:*
UDP 127.0.0.1:1041 *:*	UDP 127.0.0.1:1047 *:*
UDP 127.0.0.1:1900 *:*	UDP 127.0.0.1:1900 *:*
UDP 192.168.1.40:123 *:*	UDP 192.168.1.40:123 *:*
UDP 192.168.1.40:137 *:*	UDP 192.168.1.40:137 *:*
UDP 192.168.1.40:138 *:*	UDP 192.168.1.40:138 *:*
UDP 192.168.1.40:1900 *:*	UDP 192.168.1.40:1900 *:*



C:\Users\Frank\OneDrive - solutions4networks Inc\COA\Air Gap Analysis\airgap_13Mar2018\TAB7-Pre-AG.txt	C:\Users\Frank\OneDrive - solutions4networks Inc\COA\Air Gap Analysis\airgap_13Mar2018\TAB7-Post-AG.txt
(C) Copyright 1985-2001 Microsoft Corp.	(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Administrator.ELECTIONS>systeminfo	C:\Documents and Settings\Administrator.ELECTIONS>systeminfo
Host Name: TAB7	Host Name: TAB7
OS Name: Microsoft Windows XP Professional	OS Name: Microsoft Windows XP Professional
OS Version: 5.1.2600 Service Pack 3 Build 2600	OS Version: 5.1.2600 Service Pack 3 Build 2600
OS Manufacturer: Microsoft Corporation	OS Manufacturer: Microsoft Corporation
OS Configuration: Member Workstation	OS Configuration: Member Workstation
OS Build Type: Multiprocessor Free	OS Build Type: Multiprocessor Free
Registered Owner: admin	Registered Owner: admin
Registered Organization:	Registered Organization:
Product ID: 76487-OEM-0060807-79698	Product ID: 76487-OEM-0060807-79698
Original Install Date: 8/2/2016, 6:04:17 PM	Original Install Date: 8/2/2016, 6:04:17 PM
System Up Time: 0 Days, 0 Hours, 26 Minutes, 8 Seconds	System Up Time: 0 Days, 0 Hours, 10 Minutes, 53 Seconds
System Manufacturer: Dell Inc.	System Manufacturer: Dell Inc.
System Model: OptiPlex 790	System Model: OptiPlex 790
System type: X86-based PC	System type: X86-based PC
Processor(s): 1 Processor(s) Installed.	Processor(s): 1 Processor(s) Installed.
[01]: x86 Family 6 Model 42 Stepping 7	[01]: x86 Family 6 Model 42 Stepping 7
3092 Mhz	3092 Mhz
BIOS Version: DELL - 6222004	BIOS Version: DELL - 6222004
Windows Directory: C:\WINDOWS	Windows Directory: C:\WINDOWS
System Directory: C:\WINDOWS\system32	System Directory: C:\WINDOWS\system32
Boot Device: \Device\HarddiskVolum1	Boot Device: \Device\HarddiskVolum1
System Locale: en-us;English (United States)	System Locale: en-us;English (United States)
Input Locale: en-us;English (United States)	Input Locale: en-us;English (United States)
Time Zone: (GMT-05:00) Eastern Time (US & Canada)	Time Zone: (GMT-05:00) Eastern Time (US & Canada)
Total Physical Memory: 3,241 MB	Total Physical Memory: 3,241 MB
Available Physical Memory: 2,854 MB	Available Physical Memory: 2,871 MB
Virtual Memory: Max Size: 2,048 MB	Virtual Memory: Max Size: 2,048 MB

DAM Front



DAM Rear





Additional Information Collected from DAM CLI:

Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.

```
C:\Documents and Settings\administrator.ELECTIONS>hostname
```

DAM

```
C:\Documents and Settings\administrator.ELECTIONS>whoami
```

'whoami' is not recognized as an internal or external command,
operable program or batch file.

```
C:\Documents and Settings\administrator.ELECTIONS>ipconfig /all
```

Windows IP Configuration

```
Host Name . . . . . : DAM
Primary Dns Suffix . . . . . : elections.local
Node Type . . . . . : Broadcast
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : elections.local
```

Ethernet adapter Local Area Connection:

```
Connection-specific DNS Suffix . :
```



Description : Broadcom NetXtreme 57xx Gigabit Cont
roller
Physical Address. : 00-19-B9-1F-F2-17
Dhcp Enabled. : No
IP Address. : 192.168.1.101
Subnet Mask : 255.255.255.0
Default Gateway :
DNS Servers : 192.168.1.20

C:\Documents and Settings\administrator.ELECTIONS>arp -a

Interface: 192.168.1.101 --- 0x2

Internet Address	Physical Address	Type
192.168.1.20	00-14-22-60-3f-94	dynamic

C:\Documents and Settings\administrator.ELECTIONS>Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\administrator.ELECTIONS>netstat -rn

Route Table

=====

Interface List

0x1 MS TCP Loopback interface

0x2 ...00 19 b9 1f f2 17 Broadcom NetXtreme 57xx Gigabit Controller - Pac



ket Scheduler Miniport

=====
=====

Active Routes:

Network	Destination	Netmask	Gateway	Interface	Metric
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1	
192.168.1.0	255.255.255.0	192.168.1.101	192.168.1.101	10	
192.168.1.101	255.255.255.255	127.0.0.1	127.0.0.1	10	
192.168.1.255	255.255.255.255	192.168.1.101	192.168.1.101	10	
224.0.0.0	240.0.0.0	192.168.1.101	192.168.1.101	10	
255.255.255.255	255.255.255.255	192.168.1.101	192.168.1.101	1	

=====

Persistent Routes:

None

C:\Documents and Settings\administrator.ELECTIONS>netstat -an

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3071	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49152	0.0.0.0:0	LISTENING
TCP	127.0.0.1:1039	0.0.0.0:0	LISTENING



```
TCP 192.168.1.101:139 0.0.0.0 LISTENING
UDP 0.0.0.0:445 *.*
UDP 0.0.0.0:500 *.*
UDP 0.0.0.0:1025 *.*
UDP 0.0.0.0:1026 *.*
UDP 0.0.0.0:4500 *.*
UDP 127.0.0.1:123 *.*
UDP 127.0.0.1:1027 *.*
UDP 127.0.0.1:1043 *.*
UDP 127.0.0.1:1900 *.*
UDP 192.168.1.101:123 *.*
UDP 192.168.1.101:137 *.*
UDP 192.168.1.101:138 *.*
UDP 192.168.1.101:1900 *.*
```

C:\Documents and Settings\administrator.ELECTIONS>Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\administrator.ELECTIONS>systeminfo

```
Host Name: DAM
OS Name: Microsoft Windows XP Professional
OS Version: 5.1.2600 Service Pack 2 Build 2600
OS Manufacturer: Microsoft Corporation
OS Configuration: Member Workstation
```



OS Build Type: Multiprocessor Free

Registered Owner: damsw

Registered Organization:

Product ID: 76487-OEM-0011903-00102

Original Install Date: 7/25/2007, 9:15:46 AM

System Up Time: 0 Days, 0 Hours, 29 Minutes, 27 Seconds

System Manufacturer: Dell Inc.

System Model: Precision WorkStation 690

System type: X86-based PC

Processor(s): 2 Processor(s) Installed.

[01]: x86 Family 6 Model 15 Stepping 6 GenuineIntel ~
1595 Mhz

[02]: x86 Family 6 Model 15 Stepping 6 GenuineIntel ~
1595 Mhz

BIOS Version: DELL - d

Windows Directory: C:\WINDOWS

System Directory: C:\WINDOWS\system32

Boot Device: \Device\HarddiskVolume2

System Locale: en-us;English (United States)

Input Locale: en-us;English (United States)

Time Zone: (GMT-05:00) Eastern Time (US & Canada)

Total Physical Memory: 2,046 MB

Available Physical Memory: 1,734 MB

Virtual Memory: Max Size: 2,048 MB

Virtual Memory: Available: 2,008 MB



Virtual Memory: In Use: 40 MB

Page File Location(s): C:\pagefile.sys

Domain: elections.local

Logon Server: \\BOE

Hotfix(s): 94 Hotfix(s) Installed.

[01]: File 1

[02]: File 1

[03]: File 1

[04]: File 1

[05]: File 1

[06]: File 1

[07]: File 1

[08]: File 1

[09]: File 1

[10]: File 1

[11]: File 1

[12]: File 1

[13]: File 1

[14]: File 1

[15]: File 1

[16]: File 1

[17]: File 1

[18]: File 1

[19]: File 1

[20]: File 1



[21]: File 1

[22]: File 1

[23]: File 1

[24]: File 1

[25]: File 1

[26]: File 1

[27]: File 1

[28]: File 1

[29]: File 1

[30]: File 1

[31]: File 1

[32]: File 1

[33]: File 1

[34]: File 1

[35]: File 1

[36]: File 1

[37]: File 1

[38]: File 1

[39]: File 1

[40]: File 1

[41]: File 1

[42]: File 1

[43]: File 1

[44]: File 1

[45]: File 1



- [46]: Q147222
- [47]: S867460 - Update
- [48]: KB925398_WMP64
- [49]: KB923689
- [50]: KB873339 - Update
- [51]: KB885250 - Update
- [52]: KB885835 - Update
- [53]: KB887472 - Update
- [54]: KB889673 - Update
- [55]: KB891781 - Update
- [56]: KB896256 - Update
- [57]: KB896358 - Update
- [58]: KB896423 - Update
- [59]: KB896424 - Update
- [60]: KB899588 - Update
- [61]: KB899591 - Update
- [62]: KB901214 - Update
- [63]: KB904706 - Update
- [64]: KB908519 - Update
- [65]: KB908531 - Update
- [66]: KB908673 - Update
- [67]: KB909095 - Update
- [68]: KB911562 - Update
- [69]: KB912919 - Update
- [70]: KB912945 - Update



- [71]: KB914388 - Update
- [72]: KB917344 - Update
- [73]: KB917422 - Update
- [74]: KB918439 - Update
- [75]: KB918899 - Update
- [76]: KB919007 - Update
- [77]: KB920213 - Update
- [78]: KB920670 - Update
- [79]: KB920683 - Update
- [80]: KB920685 - Update
- [81]: KB921398 - Update
- [82]: KB922616 - Update
- [83]: KB923191 - Update
- [84]: KB923414 - Update
- [85]: KB923694 - Update
- [86]: KB923980 - Update
- [87]: KB924191 - Update
- [88]: KB924270 - Update
- [89]: KB924496 - Update
- [90]: KB925454 - Update
- [91]: KB926255 - Update
- [92]: KB928388 - Update
- [93]: KB929969 - Update
- [94]: KB835221WXP - Update

NetWork Card(s): 2 NIC(s) Installed.



[01]: Broadcom NetXtreme 57xx Gigabit Controller

Connection Name: Local Area Connection

DHCP Enabled: No

IP address(es)

[01]: 192.168.1.101

[02]: 1394 Net Adapter

Connection Name: 1394 Connection

DHCP Enabled: Yes

DHCP Server: N/A

IP address(es)

C:\Documents and Settings\administrator.ELECTIONS>

Post-Election Review:

The same output was capture from the system at the CLI and a file diff was performed. Below are the differences.

C:\Users\Frank\OneDrive - solutions4networks Inc\COA\Air Gap Analysis\airgap_13Mar2018\DAM-Pre-AG.txt				C:\Users\Frank\OneDrive - solutions4networks Inc\COA\Air Gap Analysis\airgap_13Mar2018\DAM-Post-AG.txt			
C:\Documents and Settings\administrator.ELECTIONS>netstat -an				C:\Documents and Settings\administrator.ELECTIONS>netstat -an			
Active Connections				Active Connections			
Proto	Local Address	Foreign Address	State	Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3071	0.0.0.0:0	LISTENING	TCP	0.0.0.0:3071	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49152	0.0.0.0:0	LISTENING	TCP	0.0.0.0:49152	0.0.0.0:0	LISTENING
TCP	127.0.0.1:1039	0.0.0.0:0	LISTENING	TCP	127.0.0.1:1039	0.0.0.0:0	LISTENING
TCP	192.168.1.101:139	0.0.0.0:0	LISTENING	TCP	192.168.1.101:139	0.0.0.0:0	LISTENING
				TCP	192.168.1.101:1073	192.168.1.20:445	TIME_WAIT
				TCP	192.168.1.101:1093	192.168.1.20:139	ESTABLISHED



C:\Users\Frank\OneDrive - solutions4networks Inc\COA\Air Gap Analysis\airgap_13Mar2018\DAM-Pre-AG.txt	C:\Users\Frank\OneDrive - solutions4networks Inc\COA\Air Gap Analysis\airgap_13Mar2018\DAM-Post-AG.txt
<pre>C:\Documents and Settings\administrator.ELECTIONS>systeminfo Host Name: DAM OS Name: Microsoft Windows XP Professional OS Version: 5.1.2600 Service Pack 2 Build 2600 OS Manufacturer: Microsoft Corporation OS Configuration: Member Workstation OS Build Type: Multiprocessor Free Registered Owner: damsw Registered Organization: Product ID: 76487-OEM-0011903-00102 Original Install Date: 7/25/2007, 9:15:46 AM System Up Time: 0 Days, 0 Hours, 29 Minutes, 27 Seconds System Manufacturer: Dell Inc. System Model: Precision WorkStation 690 System type: X86-based PC Processor(s): 2 Processor(s) Installed. [01]: x86 Family 6 Model 15 Stepping 6 [02]: x86 Family 6 Model 15 Stepping 6 1595 Mhz 1595 Mhz BIOS Version: DELL - d Windows Directory: C:\WINDOWS System Directory: C:\WINDOWS\system32 Boot Device: \Device\HarddiskVolume2 System Locale: en-us;English (United States) Input Locale: en-us;English (United States) Time Zone: (GMT-05:00) Eastern Time (US & Canada) Total Physical Memory: 2,046 MB Available Physical Memory: 1,734 MB Virtual Memory: Max Size: 2,048 MB</pre>	<pre>C:\Documents and Settings\administrator.ELECTIONS>systeminfo Host Name: DAM OS Name: Microsoft Windows XP Professional OS Version: 5.1.2600 Service Pack 2 Build 2600 OS Manufacturer: Microsoft Corporation OS Configuration: Member Workstation OS Build Type: Multiprocessor Free Registered Owner: damsw Registered Organization: Product ID: 76487-OEM-0011903-00102 Original Install Date: 7/25/2007, 9:15:46 AM System Up Time: 0 Days, 0 Hours, 13 Minutes, 53 Seconds System Manufacturer: Dell Inc. System Model: Precision WorkStation 690 System type: X86-based PC Processor(s): 2 Processor(s) Installed. [01]: x86 Family 6 Model 15 Stepping 6 [02]: x86 Family 6 Model 15 Stepping 6 1595 Mhz 1595 Mhz BIOS Version: DELL - d Windows Directory: C:\WINDOWS System Directory: C:\WINDOWS\system32 Boot Device: \Device\HarddiskVolume2 System Locale: en-us;English (United States) Input Locale: en-us;English (United States) Time Zone: (GMT-05:00) Eastern Time (US & Canada) Total Physical Memory: 2,046 MB Available Physical Memory: 1,745 MB Virtual Memory: Max Size: 2,048 MB</pre>

DAM3.elections.local

DAM3 Front



DAM3 Rear



Additional Information Collected from DAM3 CLI:

Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.



```
C:\Documents and Settings\Administrator.ELECTIONS>hostname
```

DAM3

```
C:\Documents and Settings\Administrator.ELECTIONS>whoami
```

'whoami' is not recognized as an internal or external command,
operable program or batch file.

```
C:\Documents and Settings\Administrator.ELECTIONS>ipconfig /all
```

Windows IP Configuration

```
Host Name . . . . . : DAM3
Primary Dns Suffix . . . . . : elections.local
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : elections.local
                                elections.local
```

Ethernet adapter Local Area Connection 2:

```
Connection-specific DNS Suffix . : elections.local
Description . . . . . : Intel(R) 82579LM Gigabit Network Con
nection
Physical Address. . . . . : D4-BE-D9-A4-D1-C5
```



Dhcp Enabled : Yes
Autoconfiguration Enabled : Yes
IP Address : 192.168.1.41
Subnet Mask : 255.255.255.0
Default Gateway : 192.168.1.1
DHCP Server : 192.168.1.20
DNS Servers : 192.168.1.20
Primary WINS Server : 192.168.1.20
Lease Obtained : Monday, March 12, 2018 7:45:41 AM
Lease Expires : Tuesday, March 20, 2018 7:45:41 AM

C:\Documents and Settings\Administrator.ELECTIONS>arp -a

Interface: 192.168.1.41 --- 0x2

Internet Address	Physical Address	Type
192.168.1.20	00-14-22-60-3f-94	dynamic

C:\Documents and Settings\Administrator.ELECTIONS>Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator.ELECTIONS>netstat -rn

Route Table

=====

Interface List



0x1 MS TCP Loopback interface
 0x2 ...d4 be d9 a4 d1 c5 Intel(R) 82579LM Gigabit Network Connection - Pa
 cket Scheduler Miniport

=====
 =====

Active Routes:

Network	Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.41	10	
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1	
192.168.1.0	255.255.255.0	192.168.1.41	192.168.1.41	10	
192.168.1.41	255.255.255.255	127.0.0.1	127.0.0.1	10	
192.168.1.255	255.255.255.255	192.168.1.41	192.168.1.41	10	
224.0.0.0	240.0.0.0	192.168.1.41	192.168.1.41	10	
255.255.255.255	255.255.255.255	192.168.1.41	192.168.1.41	1	

Default Gateway: 192.168.1.1

=====

Persistent Routes:

None

C:\Documents and Settings\Administrator.ELECTIONS>netstat -an

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING



```
TCP 0.0.0.0:445      0.0.0.0:0      LISTENING
TCP 127.0.0.1:1040   127.0.0.1:1041 ESTABLISHED
TCP 127.0.0.1:1041   127.0.0.1:1040 ESTABLISHED
TCP 127.0.0.1:1055   0.0.0.0:0      LISTENING
TCP 127.0.0.1:1057   0.0.0.0:0      LISTENING
TCP 192.168.1.41:139 0.0.0.0:0      LISTENING
TCP 192.168.1.41:1103 192.168.1.20:445 TIME_WAIT
UDP 0.0.0.0:445      *.*
UDP 0.0.0.0:500      *.*
UDP 0.0.0.0:1025     *.*
UDP 0.0.0.0:1026     *.*
UDP 0.0.0.0:4500     *.*
UDP 127.0.0.1:123    *.*
UDP 127.0.0.1:1027   *.*
UDP 127.0.0.1:1047   *.*
UDP 127.0.0.1:1900   *.*
UDP 192.168.1.41:123 *.*
UDP 192.168.1.41:137 *.*
UDP 192.168.1.41:138 *.*
UDP 192.168.1.41:1900 *.*
```

C:\Documents and Settings\Administrator.ELECTIONS>Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator.ELECTIONS>systeminfo



Host Name: DAM3
OS Name: Microsoft Windows XP Professional
OS Version: 5.1.2600 Service Pack 3 Build 2600
OS Manufacturer: Microsoft Corporation
OS Configuration: Member Workstation
OS Build Type: Multiprocessor Free
Registered Owner: ess
Registered Organization:
Product ID: 76487-OEM-0060807-79692
Original Install Date: 3/30/2016, 10:52:49 AM
System Up Time: 0 Days, 0 Hours, 29 Minutes, 56 Seconds
System Manufacturer: Dell Inc.
System Model: OptiPlex 790
System type: X86-based PC
Processor(s): 1 Processor(s) Installed.
[01]: x86 Family 6 Model 42 Stepping 7 GenuineIntel ~
3092 Mhz
BIOS Version: DELL - 6222004
Windows Directory: C:\WINDOWS
System Directory: C:\WINDOWS\system32
Boot Device: \Device\HarddiskVolume1
System Locale: en-us;English (United States)
Input Locale: en-us;English (United States)
Time Zone: (GMT-05:00) Eastern Time (US & Canada)



Total Physical Memory: 3,241 MB

Available Physical Memory: 2,917 MB

Virtual Memory: Max Size: 2,048 MB

Virtual Memory: Available: 2,008 MB

Virtual Memory: In Use: 40 MB

Page File Location(s): C:\pagefile.sys

Domain: elections.local

Logon Server: \\BOE

Hotfix(s): 10 Hotfix(s) Installed.

[01]: File 1

[02]: File 1

[03]: File 1

[04]: File 1

[05]: Q147222

[06]: KB936929 - Service Pack

[07]: KB942288-v3 - Update

[08]: KB953356 - Update

[09]: KB954550-v5 - Update

[10]: KB835221WXP - Update

NetWork Card(s): 1 NIC(s) Installed.

[01]: Intel(R) 82579LM Gigabit Network Connection

Connection Name: Local Area Connection 2

DHCP Enabled: Yes

DHCP Server: 192.168.1.20

IP address(es)



[01]: 192.168.1.41

C:\Documents and Settings\Administrator.ELECTIONS>

Post-Election Review:

The same output was capture from the system at the CLI and a file diff was performed. Below are the differences.

C:\Users\Frank\OneDrive - solutions4networks Inc\COA\Air Gap Analysis\airgap_13Mar2018\DAM3-Pre-AG.txt	C:\Users\Frank\OneDrive - solutions4networks Inc\COA\Air Gap Analysis\airgap_13Mar2018\DAM3-Post-AG.txt
Ethernet adapter Local Area Connection 2:	Ethernet adapter Local Area Connection 2:
Connection-specific DNS Suffix . : elections.local	Connection-specific DNS Suffix . : elections.local
Description : Intel(R) 82579LM Gigabit Ethernet Controller	Description : Intel(R) 82579LM Gigabit Ethernet Controller
Physical Address. : D4-BE-D9-A4-D1-C5	Physical Address. : D4-BE-D9-A4-D1-C5
Dhcp Enabled. : Yes	Dhcp Enabled. : Yes
Autoconfiguration Enabled : Yes	Autoconfiguration Enabled : Yes
IP Address. : 192.168.1.41	IP Address. : 192.168.1.41
Subnet Mask : 255.255.255.0	Subnet Mask : 255.255.255.0
Default Gateway : 192.168.1.1	Default Gateway : 192.168.1.1
DHCP Server : 192.168.1.20	DHCP Server : 192.168.1.20
DNS Servers : 192.168.1.20	DNS Servers : 192.168.1.20
Primary WINS Server : 192.168.1.20	Primary WINS Server : 192.168.1.20
Lease Obtained. : Monday, March 12, 2018 10:00:00 AM	Lease Obtained. : Thursday, March 15, 2018 10:00:00 AM
Lease Expires : Tuesday, March 20, 2018 10:00:00 AM	Lease Expires : Friday, March 23, 2018 10:00:00 AM

C:\Users\Frank\OneDrive - solutions4networks Inc\COA\Air Gap Analysis\airgap_13Mar2018\DAM3-Pre-AG.txt	C:\Users\Frank\OneDrive - solutions4networks Inc\COA\Air Gap Analysis\airgap_13Mar2018\DAM3-Post-AG.txt
C:\Documents and Settings\Administrator.ELECTIONS>netstat -an	C:\Documents and Settings\Administrator.ELECTIONS>netstat -an
Active Connections	Active Connections
Proto Local Address Foreign Address State	Proto Local Address Foreign Address State
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING	TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING	TCP 0.0.0.0:445 0.0.0.0:0 LISTENING
TCP 127.0.0.1:1040 127.0.0.1:1041 ESTABLISHED	TCP 127.0.0.1:1040 127.0.0.1:1041 ESTABLISHED
TCP 127.0.0.1:1041 127.0.0.1:1040 ESTABLISHED	TCP 127.0.0.1:1041 127.0.0.1:1040 ESTABLISHED
TCP 127.0.0.1:1055 0.0.0.0:0 LISTENING	TCP 127.0.0.1:1055 0.0.0.0:0 LISTENING
TCP 127.0.0.1:1057 0.0.0.0:0 LISTENING	TCP 127.0.0.1:1057 0.0.0.0:0 LISTENING
TCP 192.168.1.41:139 0.0.0.0:0 LISTENING	TCP 192.168.1.41:139 0.0.0.0:0 LISTENING
TCP 192.168.1.41:1103 192.168.1.20:445 TIME_WAIT	TCP 192.168.1.41:1103 192.168.1.20:445 TIME_WAIT
UDP 0.0.0.0:445 **	UDP 0.0.0.0:445 **
UDP 0.0.0.0:500 **	UDP 0.0.0.0:500 **
UDP 0.0.0.0:1025 **	UDP 0.0.0.0:1025 **
UDP 0.0.0.0:1026 **	UDP 0.0.0.0:1026 **
UDP 0.0.0.0:4500 **	UDP 0.0.0.0:4500 **
UDP 127.0.0.1:123 **	UDP 127.0.0.1:123 **
UDP 127.0.0.1:1027 **	UDP 127.0.0.1:1027 **
UDP 127.0.0.1:1047 **	UDP 127.0.0.1:1046 **
UDP 127.0.0.1:1900 **	UDP 127.0.0.1:1900 **
UDP 192.168.1.41:123 **	UDP 192.168.1.41:123 **
UDP 192.168.1.41:137 **	UDP 192.168.1.41:137 **
UDP 192.168.1.41:138 **	UDP 192.168.1.41:138 **
UDP 192.168.1.41:1900 **	UDP 192.168.1.41:1900 **

C:\Users\Frank\OneDrive - solutions4networks Inc\COA\Air Gap Analysis\airgap_13Mar2018\DAM3-Pre-AG.txt	C:\Users\Frank\OneDrive - solutions4networks Inc\COA\Air Gap Analysis\airgap_13Mar2018\DAM3-Post-AG.txt
C:\Documents and Settings\Administrator.ELECTIONS>systeminfo	C:\Documents and Settings\Administrator.ELECTIONS>systeminfo
Host Name: DAM3	Host Name: DAM3
OS Name: Microsoft Windows XP Professional	OS Name: Microsoft Windows XP Professional
OS Version: 5.1.2600 Service Pack 3 Build 2600	OS Version: 5.1.2600 Service Pack 3 Build 2600
OS Manufacturer: Microsoft Corporation	OS Manufacturer: Microsoft Corporation
OS Configuration: Member Workstation	OS Configuration: Member Workstation
OS Build Type: Multiprocessor Free	OS Build Type: Multiprocessor Free
Registered Owner: ess	Registered Owner: ess
Registered Organization:	Registered Organization:
Product ID: 76487-OEM-0060807-79692	Product ID: 76487-OEM-0060807-79692
Original Install Date: 3/30/2016, 10:52:49 AM	Original Install Date: 3/30/2016, 10:52:49 AM
System Up Time: 0 Days, 0 Hours, 29 Minutes, 56 Seconds	System Up Time: 0 Days, 0 Hours, 16 Minutes, 12 Seconds
System Manufacturer: Dell Inc.	System Manufacturer: Dell Inc.
System Model: OptiPlex 790	System Model: OptiPlex 790
System type: X86-based PC	System type: X86-based PC
Processor(s): 1 Processor(s) Installed. [01]: x86 Family 6 Model 42 Stepping 7	Processor(s): 1 Processor(s) Installed. [01]: x86 Family 6 Model 42 Stepping 7
3092 Mhz	3092 Mhz
BIOS Version: DELL - 6222004	BIOS Version: DELL - 6222004
Windows Directory: C:\WINDOWS	Windows Directory: C:\WINDOWS
System Directory: C:\WINDOWS\system32	System Directory: C:\WINDOWS\system32
Boot Device: \Device\HarddiskVolume1	Boot Device: \Device\HarddiskVolume1
System Locale: en-us:English (United States)	System Locale: en-us:English (United States)
Input Locale: en-us:English (United States)	Input Locale: en-us:English (United States)
Time Zone: (GMT-05:00) Eastern Time (US & Canada)	Time Zone: (GMT-05:00) Eastern Time (US & Canada)
Total Physical Memory: 3,241 MB	Total Physical Memory: 3,241 MB
Available Physical Memory: 2,917 MB	Available Physical Memory: 2,907 MB
Virtual Memory: Max Size: 2,048 MB	Virtual Memory: Max Size: 2,048 MB
Virtual Memory: Available: 2,008 MB	Virtual Memory: Available: 2,008 MB

External Connections on Client Devices

The only outside (external) connections found on the network were the dial-up modems on the 2 DAM servers which are part of the application and are outbound only. No other external connections were found on the network. Each server/workstation was tested and none of them had Internet access. The 7 Ethernet connections on the Dell 2716 switch were traced to valid devices. No other cables were connected to the Dell Switch and no loose cables were observed near the switch. The solutions4networks engineer asked if there was a valid login for the Dell 2716 switch but was told that no one was aware of one.

Modem Bank



Dell PowerConnect 2716



OKI B6300 Printer



No Wireless Adapters or Bluetooth Capability Found on Client Devices

Each PC was physically inspected for the presence of a wireless adapter or Bluetooth adapter and none were found.

The Windows “Device Manager” of each device was also inspected for the presence of any wireless devices.

No Wireless Keyboards and Mice

The keyboards and mice all had physical wires connected to the computers.

Post-Election Review: All items indicated above remained the same.

Network Air Gap Analysis

No issues found.

Air Gap Network Intact - Recommendations for Improvement

solutions4networks did not find any problems with the Election Tabulation Network, but have these recommendations to improve security of the network:

Client Operating Systems – Update the Clients to a supported OS.

The client PC’s were found to be running Windows XP which is no longer supported by Microsoft. These may be more vulnerable to attack if the network was ever compromised. The clients also had their internal Firewall



disabled. They did have Symantec Anti-virus installed, but the definitions were out of date. If this remains a closed air gapped network this should be a viable OS.

Server Operating System – Update the Server Operating System.

The server operating system is running Windows Server 2003, which is end of life July 2015. Any OS that is end of life is more vulnerable to attack if the network is ever compromised as it is no longer updated with any security patches. If this remains a closed air gapped network this should be a viable OS.

Remote Assistance Enabled.

Remote Assistance is enabled on the 3 clients and 2 DAM servers. This serves no positive purpose in a closed network environment where each machine is physically accessible and should be disabled in the event the network is ever compromised.

Remote Desktop is Enabled.

Remoted Desktop is enabled on the BOE server. Once again, this does not serve any positive purpose in a closed local network and should be disabled in the event the network is ever compromised.

Windows Update Enabled/None Selected.

The two DAM servers are configured differently from the rest of the computers on the network. Consistency should be the norm. All other computers have Auto Updates turned off. DAM1 has nothing selected and DAM2 has Auto Updates enabled and set for 3:00AM. Since this is a closed network and the OSes that are running are end of life there isn't a need to have Windows Update enabled.

Lock Physical Access to the Dell PowerConnect 2716

The Dell switch is easily accessible on the countertop. A locked cabinet would make it more difficult to connect an external cable. It is also recommended to disable any unused ports on the Dell Switch or move the unused ports to a different VLAN from the production network, but since the login is unknown a locked cabinet would suffice. Since the password is currently unknown and this is a flat network for ease of networking on the Dell switch there is the ability to reset it to unmanaged mode which would put all ports in Vlan 1.

Remove the Default Gateway Option

The DHCP server is giving the clients a default gateway of 192.168.1.1 even though no device exists. Removing the default gateway completely would make it more difficult for the clients to communicate with external networks. There is some inconsistency on the network in that not all the clients are set up for DHCP. Either set them all up for DHCP or set them all up for Static. For a more secure environment it would be better to disable DHCP on the BOE server entirely and configure static IPs on all the clients that way if someone were to ever connect to the Dell switch they would never obtain a DHCP address but would have to know the network addressing to hard code their PC.

**County of Allegheny,
Commonwealth of Pennsylvania**

Parallel Test Report
Special Election

January 23, 2018



BAKER TILLY

Candor. Insight. Results.

County of Allegheny, Commonwealth of Pennsylvania

Table of Contents
January 23, 2018

	<u>Page</u>
Parallel Test Report	1
Reconciliation of Vote Totals in Script to Final Results Tape, Flash Cards and Master PEB	2
Exhibit A - Parallel Testing Work Performed	
Exhibit B - Zero Tape	
Exhibit C - Scripts	
Exhibit D - Final Results Tape	
Exhibit E - Flash Cards and Personalized Ballot Printouts	
Exhibit F - Precinct Listing	
Exhibit G - Random Sample Selection	
Attachment - 2 Video Tapes	

Mr. William McKain, County Manager
County of Allegheny, Commonwealth of Pennsylvania
Office of the County Manager
436 Grant Street
Room 119 Courthouse
Pittsburgh, PA 15219

To assist with your evaluation of County of Allegheny's electronic voting machines, we randomly selected an election day polling location, scripted votes for parallel testing, and tested the functionality of the Direct Recording Electronic equipment, ES&S iVotronic voting machines. The test was performed on January 23, 2018, the date of the special election. The scripting component included creating hypothetical ballots for parallel testing by mimicking voter behavior and voting patterns from data and statistics provided by County of Allegheny, Department of Elections, for Precinct 469, Munhall, District 8. Our engagement was performed in accordance with the consulting standards prescribed by the American Institute of Certified Public Accountants.

The results of the work performed indicate that the two voting machines tested, accurately recorded and counted the results of 43 ballots cast for the selected polling location. Our results are supported by visual evidence that the electronic voting machine recorded and maintained the vote counts properly. At the beginning of the process, we verified that the zero tape did in fact contain zero vote counts for each candidate in each race. Testing was done under video surveillance, capturing votes as they were entered into each voting machine from the scripted ballots. At the end of the election process, we compared the vote totals in the script, the Master Personalized Electronic Ballot (PEB), the Final Results Tape, and Flash Cards from the machines tested and found them to be in agreement. There were no discrepancies between the number of ballots cast, ballots cast for a particular party, votes for a particular candidate, the number of under-votes, the number of canceled votes, and the audio ballot cast for the visually impaired.

Because of its special purpose, this report is not suited for any purpose other than to assist you in your evaluation and, as such, is intended only for your internal use.

Baker Tilly Virchow Krause, LLP

Pittsburgh, Pennsylvania
January 23, 2018

COUNTY OF ALLEGHENY, COMMONWEALTH OF PENNSYLVANIA
RECONCILIATION OF VOTE TOTALS IN SCRIPT TO FINAL RESULTS TAPE, FLASH CARDS AND MASTER PEB
JANUARY 23, 2018

PRECINCT: MUNHALL DISTRICT 8

	Voter Terminal Data per Script			Final Results Tape	Flash Card Data (from Precinct Report)			Master PEB Data	Differences
	V5185156	V5176005	Total		V5185156	V5176005	Total		
Public Count	26	0	26	26	26	0	26	26	0
	0	17	17	17	0	17	17	17	0
	<u>26</u>	<u>17</u>	<u>43</u>	<u>43</u>	<u>26</u>	<u>17</u>	<u>43</u>	<u>43</u>	<u>0</u>
Straight Party Option									
Democratic	1	2	3	3	1	2	3	3	0
Republican	3	3	6	6	3	3	6	6	0
Total	<u>4</u>	<u>5</u>	<u>9</u>	<u>9</u>	<u>4</u>	<u>5</u>	<u>9</u>	<u>9</u>	<u>0</u>
Representative in the General Assembly									
Austin Davis	13	9	22	22	9	13	22	22	0
Fawn Walker-Montgomery	10	5	15	15	5	10	15	15	0
Write-in: A (Alpha)	2	2	4	4	2	2	4	4	0
Write-in: B (Bravo)	1	1	2	2	1	1	2	2	0
Total	<u>26</u>	<u>17</u>	<u>43</u>	<u>43</u>	<u>17</u>	<u>26</u>	<u>43</u>	<u>43</u>	<u>0</u>

Exhibit A

The parallel testing work performed was as follows:

Control and Security Procedures

1. We randomly selected a precinct.
2. We selected two ES&S iVotronic voting machines with "tamper-evident" seals from the County of Allegheny warehouse. We test-voted on each of the ES&S iVotronic voting machines.
3. We created a script for parallel testing to mimic voter behavior and voting patterns for the polling location randomly selected.
4. We obtained and secured the Master Personalized Electronic Ballot (PEB) and two Supervisor PEBs. The Master PEB is used to open voting machines and to print the zero tape (a "zero-vote" count tape from the ES&S iVotronic voting machines) before electronic balloting starts, and the Supervisor PEB is used to activate an ES&S iVotronic voting machine for each voter. Each PEB was secured in a locked file in our office prior to election day to prevent access and tampering.
5. We set up parallel test equipment where all actions could be visibly recorded by video surveillance. One video camera was set up to document the votes cast on each of the ES&S iVotronic voting machines selected.
6. We conducted the parallel test in a low traffic area to avoid interruptions.

Casting Votes

1. Ballots were scripted to ensure that "voter turnout" in the mock election closely approximated the projected voter turnout for the randomly selected polling location.
2. The video camera was focused on the ES&S iVotronic voting machine screen in a manner that votes could be seen as they were entered.
3. Actual voting was conducted as follows:
 - First team member: Called out each vote as marked on the ballot script.
 - Second team member: As each vote was called, entered the vote in the ES&S iVotronic voting machine.
 - Second team member: Called back the votes cast as they appeared on the summary screen(s) on the ES&S iVotronic voting machine.
 - First team member: As the second team member called back the votes, verified that the vote was cast as it was read, and made a notation on the script.

The terminals closed at 8:00 PM. The final results tape was printed and the flash card from each voting machine was removed. Video camera tapes were marked according to the applicable voting machine and the time votes were entered into the voting machine selected for testing.

Terminal S/N: V5176005->
PEB S/N PS226406-_ (FMW 1.07)
Software Version 9.1.4.1
Created 02/01/06 8:50
Copyright ES&S, Inc. 1993-2005
All Rights Reserved
Diagnostic check completed: OK
iVotronic I

35 Legislative
MUNHALL DIST 8
POLLING LOCATION ZERO TAPE

Public Count Statistics

Total Ballots Cast: 0
Total Ballots Counted: 0

Number of Terminals Opened: 2
Individual Voter Terminal Data

S/N V5185156
Public Count: 0
Protective Count: 4645
OPENED 07:04:28 01/23/2018
NOT CLOSED

S/N V5176005
Public Count: 0
Protective Count: 3914
OPENED 07:06:47 01/23/2018
NOT CLOSED

PRECINCT: MUNHALL DIST 8
Public Count: 0
Ballot Style Counts
Ballot Style #63 0

Straight Party Option

(Vote for 1) Total:

0

Dem-Democratic

0

Rep-Republican

0

UnderVotes For Above contest:

0

LEG0035 Representative in the General As

(Vote for 1) Total:

0

Dem-Austin Davis

0

Rep-Fawn Walker-Montgomery

0

>Write-ins in above contest:

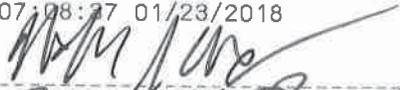
0

UnderVotes For Above contest:

0

Time/Date: 07:08:27 01/23/2018

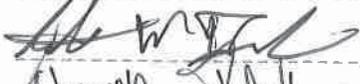
Signature:



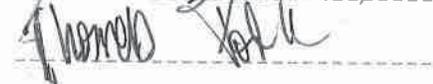
Signature:



Signature:



Signature:



**COUNTY OF ALLEGHENY, COMMONWEALTH OF PENNSYLVANIA
ELECTION, TUESDAY, JANUARY 23, 2018
SUMMARY OF SCRIPTS**

	Public Count #	Straight Party Option		Representative in the General Assembly				
		(vote for one)		(vote for one)				
		Democratic	Republican	Davis	Montgomery	(A) Alpha	(B) Bravo	Write-In
Machine 1 V5185156	26	1	3	13	10	2	1	0
Machine 2 V5176005	17	2	3	9	5	2	1	0
Total	43	3	6	22	15	4	2	0

Machine #
V5185156

COUNTY OF ALLEGHENY, COMMONWEALTH OF PENNSYLVANIA
ELECTION, TUESDAY, JANUARY 23, 2018
VOTER SIMULATION PROJECT SCRIPT

Public Count #	Straight Party Option (vote for one)		Representative in the General Assembly (vote for one)				
	Democratic	Republican	Davis	Montgomery	(A) Alpha	(B) Bravo	Write-In
1		1		1			
2	1		1				
3				1			
4		1		1			
5		1		1			
6			1				
7			1				
8			1				
9			1				
10				1			
11				1			
12				1			
13				1			
14			1				
15			1				
16			1				
17			1				
18			1				
19						1	
20				1			
21			1				
22				1			
23					1		
24			1				
25					1		
26			1				
Subtotal	1	3	13	10	2	1	0

Machine #
V5176005

COUNTY OF ALLEGHENY, COMMONWEALTH OF PENNSYLVANIA
ELECTION, TUESDAY, JANUARY 23, 2018
VOTER SIMULATION PROJECT SCRIPT

Public Count #	Straight Party Option (vote for one)		Representative in the General Assembly (vote for one)				
	Democratic	Republican	Davis	Montgomery	(A) Alpha	(B) Bravo	Write-In
1		1		1			
2	1		1				
3		1		1			
4	1		1				
5		1		1			
6			1				
7			1				
8			1				
9			1				
10				1			
11						1	
12					1		
13				1			
14					1		
15			1				
16			1				
17			1				
Subtotal	2	3	9	5	2	1	0

Terminal S/N: V5176005->
PEB S/N PS226406-_ (FMW 1.07)
Software Version 9.1.4.1
Created 02/01/06 8:50
Copyright ES&S, Inc. 1993-2005
All Rights Reserved
Diagnostic check completed: OK
iVotronic I

35 Legislative
MUNHALL DIST 8
POLLING LOCATION RESULTS

Public Count Statistics

Total Ballots Cast:	43
Total Ballots Counted:	43

Number of Terminals Opened: 2

Individual Voter Terminal Data

S/N V5185156

Public Count:	26
Protective Count:	4671
OPENED 07:04:28 01/23/2018	
CLOSED 20:01:43 01/23/2018	
Terminal Ballots Counted:	26

S/N V5176005

Public Count:	17
Protective Count:	3931
OPENED 07:06:47 01/23/2018	
CLOSED 20:04:41 01/23/2018	
Terminal Ballots Counted:	17

PRECINCT: MUNHALL DIST 8

Public Count:	43
Ballot Style Counts	
Ballot Style #63	43

Straight Ticket Counts

Democratic	3
Republican	6

Straight Party Option

(Vote for 1)	Total:	9
Dem-Democratic		3
Rep-Republican		6
UnderVotes For Above contest:		34

LEG0035 Representative in the General As

(Vote for 1)	Total:	43
Dem-Austin Davis		22
Rep-Fawn Walker-Montgomery		15

>A

>B

>A

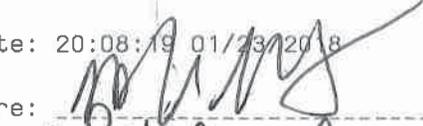
>A

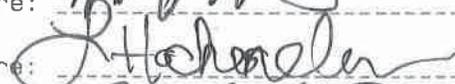
>A

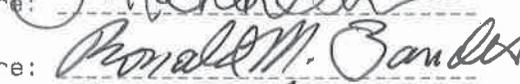
>B

>Write-ins in above contest:	6
UnderVotes For Above contest:	0

Time/Date: 20:08:19 01/23/2018

Signature: 

Signature: 

Signature: 

Signature: 

EL30

<HTML>
<PRE>
PRECINCT REPORT
RUN DATE: 02/13/18
RUN TIME: 11: 00 AM

0469 MUNHALL DIST 8

	VOTES	PERCENT
REGISTERED VOTERS - TOTAL	611	
BALLOTS CAST - TOTAL.	43	
VOTER TURNOUT - TOTAL		7.04

Straight Party Option
vote for 1

Democratic (Dem)	3	33.33
Republican (Rep)	6	66.67

Representative in the General Assembly 35TH DISTRICT
vote for 1

Austin Davis (Dem)	22	51.16
Fawn Walker-Montgomery (Rep)	15	34.88
WRITE-IN.	6	13.95

</HTML>
</PRE>

EL30A

<HTML>
<PRE>
PREC REPORT-GROUP DETAIL
RUN DATE: 02/13/18 11:03 AM

0469 MUNHALL DIST 8

	TOTAL VOTES	%	V5176005	V5185156
REGISTERED VOTERS - TOTAL	611			
BALLOTS CAST - TOTAL	43		17	26
VOTER TURNOUT - TOTAL		7.04		

Straight Party Option
vote for 1

Democratic (Dem)	3	33.33	2	1
Republican (Rep)	6	66.67	3	3

Representative in the General Assembly 35TH DISTRICT
vote for 1

Austin Davis (Dem)	22	51.16	9	13
Fawn Walker-Montgomery (Rep)	15	34.88	5	10
WRITE-IN	6	13.95	3	3

</HTML>
</PRE>

Registration Stats 35th Leg. District

Ballot #	<i>Municipality</i>	<i>Muni</i>	<i>Ward</i>	<i>District</i>	<i>Total Registered</i>
116	CLAIRTON	123	1	1	396
117	CLAIRTON	123	1	2	406
118	CLAIRTON	123	1	3	342
119	CLAIRTON	123	2	1	133
120	CLAIRTON	123	2	2	335
121	CLAIRTON	123	2	3	467
122	CLAIRTON	123	3	1	445
123	CLAIRTON	123	3	2	393
124	CLAIRTON	123	3	3	418
125	CLAIRTON	123	4	1	399
126	CLAIRTON	123	4	2	388
127	CLAIRTON	123	4	3	433
162	DUQUESNE	130	1	1	474
163	DUQUESNE	130	1	2	535
164	DUQUESNE	130	1	3	328
165	DUQUESNE	130	1	4	232
166	DUQUESNE	130	2	1	404
167	DUQUESNE	130	2	2	418
168	DUQUESNE	130	2	3	466
169	DUQUESNE	130	3	1	242
170	DUQUESNE	130	3	2	172
171	DUQUESNE	130	3	3	583
309	LINCOLN	164	0	1	684
338	MCKEESPORT	168	1	0	16
339	MCKEESPORT	168	2	0	258
340	MCKEESPORT	168	3	1	283
341	MCKEESPORT	168	3	2	124
342	MCKEESPORT	168	4	0	316
343	MCKEESPORT	168	5	0	525
344	MCKEESPORT	168	6	1	386
345	MCKEESPORT	168	6	2	317
346	MCKEESPORT	168	7	1	502
347	MCKEESPORT	168	7	2	288
348	MCKEESPORT	168	7	3	347
349	MCKEESPORT	168	7	4	471
350	MCKEESPORT	168	7	5	543
351	MCKEESPORT	168	7	6	472
352	MCKEESPORT	168	7	7	375
353	MCKEESPORT	168	8	1	314
354	MCKEESPORT	168	8	2	506
355	MCKEESPORT	168	8	3	558
356	MCKEESPORT	168	8	4	464
357	MCKEESPORT	168	8	5	542
358	MCKEESPORT	168	8	6	228
359	MCKEESPORT	168	9	1	456

Registration Stats 35th Leg. District

360	MCKEESPORT	168	9	2	592
361	MCKEESPORT	168	9	3	431
362	MCKEESPORT	168	10	1	332
363	MCKEESPORT	168	10	2	325
364	MCKEESPORT	168	11	1	458
365	MCKEESPORT	168	11	2	432
366	MCKEESPORT	168	11	3	266
367	MCKEESPORT	168	12	1	316
368	MCKEESPORT	168	12	2	363
369	MCKEESPORT	168	12	3	560
462	MUNHALL	175	0	1	497
463	MUNHALL	175	0	2	482
464	MUNHALL	175	0	3	517
465	MUNHALL	175	0	4	430
466	MUNHALL	175	0	5	740
467	MUNHALL	175	0	6	723
468	MUNHALL	175	0	7	1151
469	MUNHALL	175	0	8	613
470	MUNHALL	175	0	9	688
471	MUNHALL	175	0	10	507
472	MUNHALL	175	0	11	939
473	MUNHALL	175	0	12	570
1166	S VERSAILLES	206	0	1	214
1229	VERSAILLES	217	0	1	532
1230	VERSAILLES	217	0	2	472
1246	WEST MIFFLIN	222	0	3	475
1247	WEST MIFFLIN	222	0	4	447
1255	WEST MIFFLIN	222	0	12	995
1258	WEST MIFFLIN	222	0	15	589
1259	WEST MIFFLIN	222	0	16	1197
1272	WHITAKER	224	0	1	427
1273	WHITAKER	224	0	2	383
1290	WHITE OAK	226	0	1	739
1291	WHITE OAK	226	0	2	792
1292	WHITE OAK	226	0	3	864
1293	WHITE OAK	226	0	4	747
1294	WHITE OAK	226	0	5	795
1295	WHITE OAK	226	0	6	724
1296	WHITE OAK	226	0	7	1056
	Totals:				40,764

BALLOT	MUNICIPALITY	MUNI	WARD	DISTRICT	TOTAL_REGISTERED	SAM_RECNO
469	MUNHALL	175	0	8	613	63

**County of Allegheny,
Commonwealth of Pennsylvania**

Parallel Test Report
Special Election

March 6, 2018



BAKER TILLY

Candor. Insight. Results.

County of Allegheny, Commonwealth of Pennsylvania

Table of Contents

March 6, 2018

	<u>Page</u>
Parallel Test Report	1
Reconciliation of Vote Totals in Script to Final Results Tape, Flash Cards and Master PEB	2
Exhibit A - Parallel Testing Work Performed	
Exhibit B - Zero Tape	
Exhibit C - Scripts	
Exhibit D - Final Results Tape	
Exhibit E - Flash Cards and Personalized Ballot Printouts	
Exhibit F - Precinct Listing	
Exhibit G - Random Sample Selection	
Attachment - 2 Video Tapes	

Mr. William McKain, County Manager
County of Allegheny, Commonwealth of Pennsylvania
Office of the County Manager
436 Grant Street
Room 119 Courthouse
Pittsburgh, PA 15219

To assist with your evaluation of County of Allegheny's electronic voting machines, we randomly selected an election day polling location, scripted votes for parallel testing, and tested the functionality of the Direct Recording Electronic equipment, ES&S iVotronic voting machines. The test was performed on March 6, 2018, the date of the special election. The scripting component included creating hypothetical ballots for parallel testing by mimicking voter behavior and voting patterns from data and statistics provided by County of Allegheny, Department of Elections, for Precinct 638, Pittsburgh Ward 7 District 3. Our engagement was performed in accordance with the consulting standards prescribed by the American Institute of Certified Public Accountants.

The results of the work performed indicate that the two voting machines tested, accurately recorded and counted the results of 153 ballots cast for the selected polling location. Our results are supported by visual evidence that the electronic voting machine recorded and maintained the vote counts properly. At the beginning of the process, we verified that the zero tape did in fact contain zero vote counts for each candidate in each race. Testing was done under video surveillance, capturing votes as they were entered into each voting machine from the scripted ballots. At the end of the election process, we compared the vote totals in the script, the Master Personalized Electronic Ballot (PEB), the Final Results Tape, and Flash Cards from the machines tested and found them to be in agreement. There were no discrepancies between the number of ballots cast, ballots cast for a particular party, votes for a particular candidate, the number of under-votes, the number of canceled votes, and the audio ballot cast for the visually impaired.

Because of its special purpose, this report is not suited for any purpose other than to assist you in your evaluation and, as such, is intended only for your internal use.

Baker Tilly Virchow Krause, LLP

Pittsburgh, Pennsylvania
March 6, 2018

**COUNTY OF ALLEGHENY, COMMONWEALTH OF PENNSYLVANIA
RECONCILIATION OF VOTE TOTALS IN SCRIPT TO FINAL RESULTS TAPE, FLASH CARDS AND MASTER PEB
MARCH 6, 2018**

PRECINCT: PITTSBURGH WARD 7 DISTRICT 3

	Voter Terminal Data per Script			Final Results Tape	Flash Card Data (from Precinct Report)			Master PEB Data	Differences
	V5181874	V5173130	Total		V5181874	V5173130	Total		
Public Count	94	0	94	94	94	0	94	94	0
	0	59	59	59	0	59	59	59	0
	<u>94</u>	<u>59</u>	<u>153</u>	<u>153</u>	<u>94</u>	<u>59</u>	<u>153</u>	<u>153</u>	<u>0</u>
Straight Party Option									
Democratic	2	2	4	4	2	2	4	4	0
Republican	4	4	8	8	4	4	8	8	0
Inclusion	3	3	6	6	3	3	6	6	0
Vote Erika Strassburger	1	1	2	2	1	1	2	2	0
Total	<u>10</u>	<u>10</u>	<u>20</u>	<u>20</u>	<u>10</u>	<u>10</u>	<u>20</u>	<u>20</u>	<u>0</u>
Member of Council									
Sonja Finn	36	22	58	58	36	22	58	58	0
Rennick Remley	31	20	51	51	31	20	51	51	0
Marty Healey	11	8	19	19	11	8	19	19	0
Erika Strassburger	6	5	11	11	6	5	11	11	0
Write-in: Alpha	7	3	10	10	7	3	10	10	0
Write-in: Bravo	3	1	4	4	3	1	4	4	0
Total	<u>94</u>	<u>59</u>	<u>153</u>	<u>153</u>	<u>94</u>	<u>59</u>	<u>153</u>	<u>153</u>	<u>0</u>

Exhibit A

The parallel testing work performed was as follows:

Control and Security Procedures

1. We randomly selected a precinct.
2. We selected two ES&S iVotronic voting machines with "tamper-evident" seals from the County of Allegheny warehouse. We test-voted on each of the ES&S iVotronic voting machines.
3. We created a script for parallel testing to mimic voter behavior and voting patterns for the polling location randomly selected.
4. We obtained and secured the Master Personalized Electronic Ballot (PEB) and two Supervisor PEBs. The Master PEB is used to open voting machines and to print the zero tape (a "zero-vote" count tape from the ES&S iVotronic voting machines) before electronic balloting starts, and the Supervisor PEB is used to activate an ES&S iVotronic voting machine for each voter. Each PEB was secured in a locked file in our office prior to election day to prevent access and tampering.
5. We set up parallel test equipment where all actions could be visibly recorded by video surveillance. One video camera was set up to document the votes cast on each of the ES&S iVotronic voting machines selected.
6. We conducted the parallel test in a low traffic area to avoid interruptions.

Casting Votes

1. Ballots were scripted to ensure that "voter turnout" in the mock election closely approximated the projected voter turnout for the randomly selected polling location.
2. The video camera was focused on the ES&S iVotronic voting machine screen in a manner that votes could be seen as they were entered.
3. Actual voting was conducted as follows:
 - First team member: Called out each vote as marked on the ballot script.
 - Second team member: As each vote was called, entered the vote in the ES&S iVotronic voting machine.
 - Second team member: Called back the votes cast as they appeared on the summary screen(s) on the ES&S iVotronic voting machine.
 - First team member: As the second team member called back the votes, verified that the vote was cast as it was read, and made a notation on the script.

The terminals closed at 8:00 PM. The final results tape was printed and the flash card from each voting machine was removed. Video camera tapes were marked according to the applicable voting machine and the time votes were entered into the voting machine selected for testing.

Terminal S/N: V5173130->
PEB S/N PS226415- (FMW 1.07)
Software Version 9.1.4.1
Created 02/01/06 8:50
Copyright ES&S, Inc. 1993-2005
All Rights Reserved
Diagnostic check completed: OK
iVotronic I

8th Pittsburgh Council
PITTSBURGH WARD 7 DIST 3
POLLING LOCATION ZERO TAPE

Public Count Statistics
Total Ballots Cast: 0
Total Ballots Counted: 0

Number of Terminals Opened: 2

Individual Voter Terminal Data
S/N V5181874
Public Count: 0
Protective Count: 4257
OPENED 06:55:56 03/06/2018
NOT CLOSED

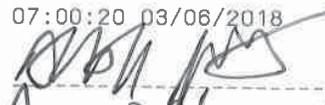
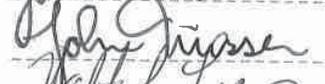
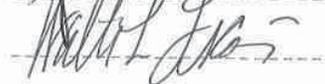
S/N V5173130
Public Count: 0
Protective Count: 3851
OPENED 06:58:31 03/06/2018
NOT CLOSED

PRECINCT: PITTSBURGH WARD 7 DIST 3
Public Count: 0
Ballot Style Counts
Ballot Style #9 0

Straight Party Option
(Vote for 1) Total: 0
Dem-Democratic 0
Rep-Republican 0
Inc-Inclusion 0
Ves-Vote Erika Strassburger 0
UnderVotes For Above contest: 0

CTYCL08 MEMBER OF PITTSBURGH COUNCIL 2
(Vote for 1) Total: 0
Dem-Sonja Finn 0
Rep-Rennick Remley 0
Inc-Marty Healey 0
Ves-Erika Strassburger 0

>Write-ins in above contest: 0
UnderVotes For Above contest: 0

Time/Date: 07:00:20 03/06/2018
Signature: 
Signature: 
Signature: 
Signature: 

COUNTY OF ALLEGHENY, COMMONWEALTH OF PENNSYLVANIA
 ELECTION, TUESDAY, MARCH 6, 2018
 SUMMARY OF SCRIPTS

Public Count #	Straight Party Option (vote for one)				Member of Council (vote for one)							
	Democratic	Republican	Inclusion	Vote Erika Strassburger	Finn	Remley	Healey	Strassburger	Alpha	Bravo	Write-In	
Machine 1 V5181874	94	2	4	3	1	36	31	11	6	7	3	0
Machine 2 V5173130	59	2	4	3	1	22	20	8	5	3	1	0
Total	153	4	8	6	2	58	51	19	11	10	4	0

Machine #
V5181874

COUNTY OF ALLEGHENY, COMMONWEALTH OF PENNSYLVANIA
ELECTION, TUESDAY, MARCH 6, 2018
VOTER SIMULATION PROJECT SCRIPT

Public Count #	Straight Party Option (vote for one)				Member of Council (vote for one)						
	Democratic	Republican	Inclusion	Vote Erika Strassburger	Finn	Remley	Healey	Stassburger	Alpha	Bravo	Write-In
	1				1				1		
2	1							1			
3			1					1			
4		1						1			
5								1			
6						1					
7								1			
8								1			
9						1					
10							1				
11									1		
12							1				
13							1				
14						1					
15						1					
16								1			
17	1					1					
18		1					1				
19			1					1			
20							1				
21						1					
22							1				
23									1		
24						1					
25									1		
26						1					
27							1				
28									1		
29							1				
30						1					
31						1					
32						1					
33		1					1				
34			1					1			
35		1					1				
36							1				
37							1				
38						1					
39						1					
40									1		
41						1					
42						1					
43										1	
44							1				
45						1					
46							1				
47									1		
48						1					
49									1		
50							1				
51							1				
52						1					
53								1			
54						1					
55						1					
56							1				
57								1			
58							1				
59							1				
60						1					
61						1					
62						1					
63									1		
64						1					
65										1	
66							1				
67						1					
68							1				
69									1		
70						1					
71									1		
72						1					
73							1				
74							1				
75							1				
76						1					
77								1			
78						1					
79						1					
80							1				
81									1		
82							1				
83							1				
84						1					
85								1			
86								1			
87						1					
88						1					
89										1	
90							1				
91						1					
92							1				
93									1		
94						1					
Subtotal	2	4	3	1	36	31	11	6	7	3	0

Machine #
V5173130

COUNTY OF ALLEGHENY, COMMONWEALTH OF PENNSYLVANIA
ELECTION, TUESDAY, MARCH 6, 2018
VOTER SIMULATION PROJECT SCRIPT

Public Count #	Straight Party Option (vote for one)				Member of Council (vote for one)						
	Democratic	Republican	Inclusion	Vote Erika Strassburger	Finn	Remley	Healey	Stassburger	Alpha	Bravo	Write-In
1				1				1			
2	1				1						
3			1				1				
4		1				1					
5						1					
6					1						
7							1				
8							1				
9					1						
10						1					
11								1			
12						1					
13						1					
14					1						
15					1						
16							1				
17	1				1						
18		1				1					
19			1				1				
20						1					
21					1						
22						1					
23									1		
24					1						
25								1			
26					1						
27						1					
28								1			
29						1					
30					1						
31					1						
32					1						
33		1				1					
34			1				1				
35		1				1					
36						1					
37						1					
38					1						
39					1						
40								1			
41					1						
42					1						
43										1	
44						1					
45					1						
46						1					
47									1		
48					1						
49								1			
50						1					
51						1					
52					1						
53							1				
54					1						
55					1						
56						1					
57							1				
58						1					
59					1						
Subtotal	2	4	3	1	22	20	8	5	3	1	0

Terminal S/N: V5173130->
PEB S/N PS226415- (FMW 1.07)
Software Version 9.1.4.1
Created 02/01/06 8:50
Copyright ES&S, Inc. 1993-2005
All Rights Reserved
Diagnostic check completed: OK
iVotronic I

8th Pittsburgh Council
PITTSBURGH WARD 7 DIST 3
POLLING LOCATION RESULTS

Public Count Statistics

Total Ballots Cast: 153
Total Ballots Counted: 153

Number of Terminals Opened: 2

Individual Voter Terminal Data

S/N V5181874

Public Count: 94
Protective Count: 4351
OPENED 06:55:56 03/06/2018
CLOSED 20:04:18 03/06/2018
Terminal Ballots Counted: 94

S/N V5173130

Public Count: 59
Protective Count: 3910
OPENED 06:58:31 03/06/2018
CLOSED 20:07:29 03/06/2018
Terminal Ballots Counted: 59

PRECINCT: PITTSBURGH WARD 7 DIST 3

Public Count: 153

Ballot Style Counts

Ballot Style #9 153

Straight Ticket Counts

Democratic 4
Republican 8
Inclusion 6
Vote Erika Strassburger 2

Straight Party Option

(Vote for 1) Total: 20
Dem-Democratic 4
Rep-Republican 8
Inc-Inclusion 6
Ves-Vote Erika Strassburger 2
UnderVotes For Above contest: 133

CTYCL08 MEMBER OF PITTSBURGH COUNCIL 2

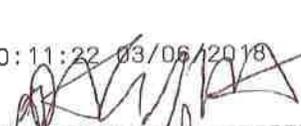
(Vote for 1) Total: 153
Dem-Sonja Finn 58
Rep-Rennick Remley 51
Inc-Marty Healey 19
Ves-Erika Strassburger 11

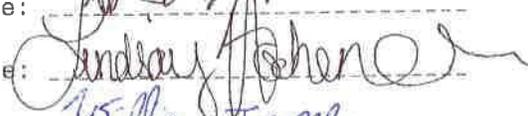
>ALPHA
>ALPHA
>ALPHA
>ALPHA
>BRAVO
>ALPHA
>BRAVO
>ALPHA
>ALPHA
>BRAVO
>ALPHA
>BRAVO
>ALPHA
>ALPHA

>Write-ins in above contest:
UnderVotes For Above contest:

14
0

Time/Date: 20:11:22 03/06/2018

Signature: 

Signature: 

Signature: 

Signature: 

EL30

<HTML>
<PRE>
PRECINCT REPORT
RUN DATE: 04/11/18
RUN TIME: 02: 22 PM

0638 PITTSBURGH WARD 7 DIST 3

	VOTES	PERCENT
REGISTERED VOTERS - TOTAL	0	
BALLOTS CAST - TOTAL.	153	

Straight Party Option

Vote for 1		
Democratic (Dem)	4	20.00
Republican (Rep)	8	40.00
Inclusion (Inc)	6	30.00
Vote Erika Strassbur (Ves).	2	10.00

Member of Council DISTRICT 8

Vote for 1		
Sonja Finn (Dem)	58	37.91
Rennick Reimley (Rep).	51	33.33
Marty Healey (Inc)	19	12.42
Erika Strassburger (Ves)	11	7.19
WRITE-IN.	14	9.15

</HTML>
</PRE>

EL30A

<HTML>
<PRE>
PREC REPORT-GROUP DETAIL
RUN DATE: 04/11/18 02:13 PM

0638 PITTSBURGH WARD 7 DIST 3

	TOTAL VOTES	%	V5173130	V5181874
REGISTERED VOTERS - TOTAL	0			
BALLOTS CAST - TOTAL.	153		59	94

Straight Party Option

Vote for 1				
Democratic (Dem)	4	20.00	2	2
Republican (Rep)	8	40.00	4	4
Inclusion (Inc)	6	30.00	3	3
Vote Erika Strassbur (Ves).	2	10.00	1	1

Member of Council DISTRICT 8

Vote for 1				
Sonja Finn (Dem)	58	37.91	22	36
Rennick Remley (Rep).	51	33.33	20	31
Marty Healey (Inc)	19	12.42	8	11
Erika Strassburger (Ves)	11	7.19	5	6
WRITE-IN.	14	9.15	4	10

</HTML>
</PRE>

Registration Stats 8th Pgh City Council District

<u>Ballot #</u>	<u>Municipality</u>	<u>Muni</u>	<u>Ward</u>	<u>District</u>	<u>Total Registered</u>
600	PITTSBURGH	188	4	7	3125
602	PITTSBURGH	188	4	9	686
603	PITTSBURGH	188	4	10	599
604	PITTSBURGH	188	4	11	569
605	PITTSBURGH	188	4	12	663
606	PITTSBURGH	188	4	13	893
636	PITTSBURGH	188	7	1	677
637	PITTSBURGH	188	7	2	1054
638	PITTSBURGH	188	7	3	761
639	PITTSBURGH	188	7	4	1103
640	PITTSBURGH	188	7	5	732
641	PITTSBURGH	188	7	6	671
642	PITTSBURGH	188	7	7	746
643	PITTSBURGH	188	7	8	744
644	PITTSBURGH	188	7	9	795
645	PITTSBURGH	188	7	10	1039
646	PITTSBURGH	188	7	11	1129
647	PITTSBURGH	188	7	12	979
648	PITTSBURGH	188	7	13	548
649	PITTSBURGH	188	7	14	462
744	PITTSBURGH	188	14	1	713
745	PITTSBURGH	188	14	2	1488
746	PITTSBURGH	188	14	3	882
747	PITTSBURGH	188	14	4	763
748	PITTSBURGH	188	14	5	805
749	PITTSBURGH	188	14	6	726
750	PITTSBURGH	188	14	7	3709
751	PITTSBURGH	188	14	8	774
752	PITTSBURGH	188	14	9	796
753	PITTSBURGH	188	14	10	699
754	PITTSBURGH	188	14	11	814
759	PITTSBURGH	188	14	16	511
764	PITTSBURGH	188	14	21	594
765	PITTSBURGH	188	14	22	729

BALLOT	MUNICIPALITY	MUNI	WARD	DISTRICT	TOTAL REGISTERED	SAM_RECNO
638	PITTSBURGH	188	7	3	761	9

**County of Allegheny,
Commonwealth of Pennsylvania**

Parallel Test Report
Special Election

March 13, 2018



BAKER TILLY

Candor. Insight. Results.

County of Allegheny, Commonwealth of Pennsylvania

Table of Contents

March 13, 2018

	<u>Page</u>
Parallel Test Report	1
Reconciliation of Vote Totals in Script to Final Results Tape, Flash Cards and Master PEB	2
Exhibit A - Parallel Testing Work Performed	
Exhibit B - Zero Tape	
Exhibit C - Scripts	
Exhibit D - Final Results Tape	
Exhibit E - Flash Cards and Personalized Ballot Printouts	
Exhibit F - Precinct Listing	
Exhibit G - Random Sample Selection	
Attachment - 2 Video Tapes	

Mr. William McKain, County Manager
County of Allegheny, Commonwealth of Pennsylvania
Office of the County Manager
436 Grant Street
Room 119 Courthouse
Pittsburgh, PA 15219

To assist with your evaluation of County of Allegheny's electronic voting machines, we randomly selected an election day polling location, scripted votes for parallel testing, and tested the functionality of the Direct Recording Electronic equipment, ES&S iVotronic voting machines. The test was performed on March 13, 2018, the date of the special election. The scripting component included creating hypothetical ballots for parallel testing by mimicking voter behavior and voting patterns from data and statistics provided by County of Allegheny, Department of Elections, for Precinct 218, Forward District 4. Our engagement was performed in accordance with the consulting standards prescribed by the American Institute of Certified Public Accountants.

The results of the work performed indicate that the two voting machines tested, accurately recorded and counted the results of 89 ballots cast for the selected polling location. Our results are supported by visual evidence that the electronic voting machine recorded and maintained the vote counts properly. At the beginning of the process, we verified that the zero tape did in fact contain zero vote counts for each candidate in each race. Testing was done under video surveillance, capturing votes as they were entered into each voting machine from the scripted ballots. At the end of the election process, we compared the vote totals in the script, the Master Personalized Electronic Ballot (PEB), the Final Results Tape, and Flash Cards from the machines tested and found them to be in agreement. There were no discrepancies between the number of ballots cast, ballots cast for a particular party, votes for a particular candidate, the number of under-votes, the number of canceled votes, and the audio ballot cast for the visually impaired.

Because of its special purpose, this report is not suited for any purpose other than to assist you in your evaluation and, as such, is intended only for your internal use.

Baker Tilly Virchow Krause, LLP

Pittsburgh, Pennsylvania
March 13, 2018

**COUNTY OF ALLEGHENY, COMMONWEALTH OF PENNSYLVANIA
RECONCILIATION OF VOTE TOTALS IN SCRIPT TO FINAL RESULTS TAPE, FLASH CARDS AND MASTER PEB
MARCH 13, 2018**

PRECINCT: FORWARD DISTRICT 4

	Voter Terminal Data per Script			Final Results Tape	Flash Card Data (from Precinct Report)			Master PEB Data	Differences
	V5185569	V5172529	Total		V5185569	V5172529	Total		
Public Count	56	0	56	56	56	0	56	56	0
	0	33	33	33	0	33	33	33	0
	<u>56</u>	<u>33</u>	<u>89</u>	<u>89</u>	<u>56</u>	<u>33</u>	<u>89</u>	<u>89</u>	<u>0</u>
Straight Party Option									
Democratic	2	3	5	5	2	3	5	5	0
Republican	4	2	6	6	4	2	6	6	0
Libertarian	3	1	4	4	3	1	4	4	0
Total	<u>9</u>	<u>6</u>	<u>15</u>	<u>15</u>	<u>9</u>	<u>6</u>	<u>15</u>	<u>15</u>	<u>0</u>
Member of Council									
Conor Lamb	21	13	34	34	21	13	34	34	0
Rick Saccone	20	11	31	31	20	11	31	31	0
Drew Gray Miller	10	6	16	16	10	6	16	16	0
Write-in: Alpha	4	2	6	6	4	2	6	6	0
Write-in: Bravo	1	1	2	2	1	1	2	2	0
Total	<u>56</u>	<u>33</u>	<u>89</u>	<u>89</u>	<u>56</u>	<u>33</u>	<u>89</u>	<u>89</u>	<u>0</u>

Exhibit A

The parallel testing work performed was as follows:

Control and Security Procedures

1. We randomly selected a precinct.
2. We selected two ES&S iVotronic voting machines with "tamper-evident" seals from the County of Allegheny warehouse. We test-voted on each of the ES&S iVotronic voting machines.
3. We created a script for parallel testing to mimic voter behavior and voting patterns for the polling location randomly selected.
4. We obtained and secured the Master Personalized Electronic Ballot (PEB) and two Supervisor PEBs. The Master PEB is used to open voting machines and to print the zero tape (a "zero-vote" count tape from the ES&S iVotronic voting machines) before electronic balloting starts, and the Supervisor PEB is used to activate an ES&S iVotronic voting machine for each voter. Each PEB was secured in a locked file in our office prior to election day to prevent access and tampering.
5. We set up parallel test equipment where all actions could be visibly recorded by video surveillance. One video camera was set up to document the votes cast on each of the ES&S iVotronic voting machines selected.
6. We conducted the parallel test in a low traffic area to avoid interruptions.

Casting Votes

1. Ballots were scripted to ensure that "voter turnout" in the mock election closely approximated the projected voter turnout for the randomly selected polling location.
2. The video camera was focused on the ES&S iVotronic voting machine screen in a manner that votes could be seen as they were entered.
3. Actual voting was conducted as follows:
 - First team member: Called out each vote as marked on the ballot script.
 - Second team member: As each vote was called, entered the vote in the ES&S iVotronic voting machine.
 - Second team member: Called back the votes cast as they appeared on the summary screen(s) on the ES&S iVotronic voting machine.
 - First team member: As the second team member called back the votes, verified that the vote was cast as it was read, and made a notation on the script.

The terminals closed at 8:00 PM. The final results tape was printed and the flash card from each voting machine was removed. Video camera tapes were marked according to the applicable voting machine and the time votes were entered into the voting machine selected for testing.

Terminal S/N: V5172529->
PEB S/N PS223792-_ (FMW 1.07)
Software Version 9.1.4.1
Created 02/01/06 8:50
Copyright ES&S, Inc. 1993-2005
All Rights Reserved
Diagnostic check completed: OK
iVotronic I

18Th Congressional
FORWARD DIST 4
POLLING LOCATION ZERO TAPE

Public Count Statistics
Total Ballots Cast: 0
Total Ballots Counted: 0

Number of Terminals Opened: 2

Individual Voter Terminal Data
S/N V5185569
Public Count: 0
Protective Count: 4734
OPENED 08:41:34 03/13/2018
NOT CLOSED

S/N V5172529
Public Count: 0
Protective Count: 4001
OPENED 08:43:47 03/13/2018
NOT CLOSED

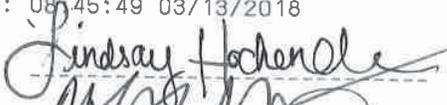
PRECINCT: FORWARD DIST 4
Public Count: 0
Ballot Style Counts
Ballot Style #77 0

Straight Party Option
(Vote for 1) Total: 0
Dem-Democratic 0
Rep-Republican 0
LIB-Libertarian 0
UnderVotes For Above contest: 0

CNG0018 Representative in Congress
(Vote for 1) Total: 0
Dem-Conor Lamb 0
Rep-Rick Saccone 0
LIB-Drew Gray Miller 0

>Write-ins in above contest: 0
UnderVotes For Above contest: 0

Time/Date: 08:45:49 03/13/2018

Signature: 

Signature: 

Signature: 

Signature: _____

COUNTY OF ALLEGHENY, COMMONWEALTH OF PENNSYLVANIA
 ELECTION, TUESDAY, MARCH 13, 2018
 SUMMARY OF SCRIPTS

Public Count #	Straight Party Option			Representative in Congress						
	(vote for one)			(vote for one)						
	Democratic	Republican	Libertarian	Lamb	Saccone	Miller	Alpha	Bravo	Write-In	
Machine 1 V5185569	56	2	4	3	21	20	10	4	1	0
Machine 2 V5172529	33	3	2	1	13	11	6	2	1	0
Total	89	5	6	4	34	31	16	6	2	0

Machine #
V5185569

COUNTY OF ALLEGHENY, COMMONWEALTH OF PENNSYLVANIA
ELECTION, TUESDAY, MARCH 13, 2018
VOTER SIMULATION PROJECT SCRIPT

Public Count #	Straight Party Option (vote for one)			Representative in Congress (vote for one)					
	Democratic	Republican	Libertarian	Lamb	Saccone	Miller	Alpha	Bravo	Write-In
1			1			1			
2	1			1					
3			1			1			
4		1			1				
5					1				
6				1					
7						1			
8						1			
9				1					
10					1				
11			1			1			
12		1			1				
13		1			1				
14				1					
15				1					
16						1			
17				1					
18					1				
19						1			
20					1				
21				1					
22					1				
23							1		
24				1					
25							1		
26				1					
27					1				
28						1			
29		1			1				
30	1			1					
31				1					
32				1					
33					1				
34					1				
35					1				
36					1				
37					1				
38				1					
39				1					
40						1			
41				1					
42				1					
43								1	
44					1				
45				1					
46					1				
47							1		
48				1					
49							1		
50					1				
51					1				
52				1					
53						1			
54				1					
55				1					
56					1				
Subtotal	2	4	3	21	20	10	4	1	0

Machine #
V5172529

COUNTY OF ALLEGHENY, COMMONWEALTH OF PENNSYLVANIA
ELECTION, TUESDAY, MARCH 13, 2018
VOTER SIMULATION PROJECT SCRIPT

Public Count #	Straight Party Option (vote for one)			Representative in Congress (vote for one)					
	Democratic	Republican	Libertarian	Lamb	Saccone	Miller	Alpha	Bravo	Write-In
1						1			
2					1				
3					1				
4				1					
5							1		
6							1		
7						1			
8				1					
9								1	
10					1				
11				1					
12					1				
13	1			1					
14		1			1				
15			1			1			
16				1					
17					1				
18					1				
19					1				
20				1					
21						1			
22				1					
23	1			1					
24		1			1				
25	1			1					
26					1				
27					1				
28				1					
29						1			
30						1			
31				1					
32				1					
33				1					
Subtotal	3	2	1	13	11	6	2	1	0

Terminal S/N: V5172529->
PEB S/N PS223792-_ (FMW 1.07)
Software Version 9.1.4.1
Created 02/01/06 8:50
Copyright ES&S, Inc. 1993-2005
All Rights Reserved
Diagnostic check completed: OK
iVotronic I

18Th Congressional
FORWARD DIST 4
POLLING LOCATION RESULTS

Public Count Statistics
Total Ballots Cast: 89
Total Ballots Counted: 89

Number of Terminals Opened: 2
Individual Voter Terminal Data
S/N V5185569
Public Count: 56
Protective Count: 4790
OPENED 08:41:34 03/13/2018
CLOSED 20:01:40 03/13/2018
Terminal Ballots Counted: 56

S/N V5172529
Public Count: 33
Protective Count: 4034
OPENED 08:43:47 03/13/2018
CLOSED 20:04:21 03/13/2018
Terminal Ballots Counted: 33

PRECINCT: FORWARD DIST 4
Public Count: 89
Ballot Style Counts
Ballot Style #77 89

Straight Ticket Counts
Democratic 5
Republican 6
Libertarian 4

Straight Party Option
(Vote for 1) Total: 15
Dem-Democratic 5
Rep-Republican 6
LIB-Libertarian 4
UnderVotes For Above contest: 74

CNG0018 Representative in Congress
(Vote for 1) Total: 89
Dem-Conor Lamb 34
Rep-Rick Saccone 31
LIB-Drew Gray Miller 16

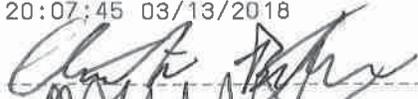
>ALPHA
>ALPHA
>BRAVO
>ALPHA
>ALPHA
>ALPHA
>BRAVO
>ALPHA

>Write-ins in above contest:
UnderVotes For Above contest:

8
0

Time/Date: 20:07:45 03/13/2018

Signature:

A handwritten signature in black ink, appearing to be "Chris Taylor", written over a dashed horizontal line.

Signature:

A handwritten signature in black ink, appearing to be "D. Taylor", written over a dashed horizontal line.

Signature:

A handwritten signature in black ink, appearing to be "D. Taylor", written over a dashed horizontal line.

Signature:

A dashed horizontal line for a signature, which is currently blank.

EL30

<HTML>
<PRE>
PRECINCT REPORT
RUN DATE: 04/11/18
RUN TIME: 02: 24 PM

0218 FORWARD DIST 4

	VOTES	PERCENT
REGISTERED VOTERS - TOTAL	0	
BALLOTS CAST - TOTAL.	89	

Straight Party Option

Vote for 1		
Democratic (Dem)	5	33.33
Republican (Rep)	6	40.00
Libertarian (LIB).	4	26.67

Representative in Congress 18TH DISTRICT

Vote for 1		
Conor Lamb (Dem)	34	38.20
Rick Saccone (Rep)	31	34.83
Drew Gray Miller (LIB)	16	17.98
WRITE-IN.	8	8.99

</HTML>
</PRE>

<HTML>
<PRE>
PREC REPORT-GROUP DETAIL
RUN DATE: 04/11/18 02:28 PM

0218 FORWARD DIST 4

	TOTAL VOTES	%	V5172529	V5185569
REGISTERED VOTERS - TOTAL	0			
BALLOTS CAST - TOTAL.	89		33	56

Straight Party Option
Vote for 1

Democratic (Dem)	5	33.33	3	2
Republican (Rep)	6	40.00	2	4
Libertarian (LIB).	4	26.67	1	3

Representative in Congress 18TH DISTRICT
Vote for 1

Conor Lamb (Dem)	34	38.20	13	21
Rick Saccone (Rep)	31	34.83	11	20
Drew Gray Miller (LIB)	16	17.98	6	10
WRITE-IN.	8	8.99	3	5

</HTML>
</PRE>

<u>Ballot #</u>	<u>Municipality</u>	<u>Muni</u>	<u>Ward</u>	<u>District</u>	<u>Total Registered</u>
41	BETHEL PARK	110	1	1	861
42	BETHEL PARK	110	1	2	822
43	BETHEL PARK	110	1	3	809
44	BETHEL PARK	110	2	1	726
45	BETHEL PARK	110	2	2	892
46	BETHEL PARK	110	2	3	1109
47	BETHEL PARK	110	3	1	791
48	BETHEL PARK	110	3	2	925
49	BETHEL PARK	110	3	3	1063
50	BETHEL PARK	110	4	1	1294
51	BETHEL PARK	110	4	2	786
52	BETHEL PARK	110	4	3	860
53	BETHEL PARK	110	5	1	597
54	BETHEL PARK	110	5	2	650
55	BETHEL PARK	110	5	3	1440
56	BETHEL PARK	110	6	1	1277
57	BETHEL PARK	110	6	2	963
58	BETHEL PARK	110	6	3	813
59	BETHEL PARK	110	7	1	1135
60	BETHEL PARK	110	7	2	1013
61	BETHEL PARK	110	7	3	758
62	BETHEL PARK	110	8	1	512
63	BETHEL PARK	110	8	2	543
64	BETHEL PARK	110	8	3	1225
65	BETHEL PARK	110	8	4	453
66	BETHEL PARK	110	9	1	568
67	BETHEL PARK	110	9	2	718
68	BETHEL PARK	110	9	3	1360
89	BRIDGEVILLE	117	0	1	799
90	BRIDGEVILLE	117	0	2	856
91	BRIDGEVILLE	117	0	3	853
92	BRIDGEVILLE	117	0	4	979
93	CARNEGIE	118	1	1	528
94	CARNEGIE	118	1	2	1205
95	CARNEGIE	118	1	3	822
96	CARNEGIE	118	1	4	381
97	CARNEGIE	118	2	1	649
98	CARNEGIE	118	2	2	509
99	CARNEGIE	118	2	3	478
100	CARNEGIE	118	2	4	948
101	CASTLE SHANNON	119	0	1	1063
102	CASTLE SHANNON	119	0	2	850
103	CASTLE SHANNON	119	0	3	805
104	CASTLE SHANNON	119	0	4	634
105	CASTLE SHANNON	119	0	5	619

106	CASTLE SHANNON	119	0	6	640
107	CASTLE SHANNON	119	0	7	755
108	CASTLE SHANNON	119	0	8	558
128	COLLIER	124	0	1	1167
129	COLLIER	124	0	2	1241
130	COLLIER	124	0	3	1210
131	COLLIER	124	0	4	765
132	COLLIER	124	0	5	960
133	COLLIER	124	0	6	1088
147	CRESCENT	127	1	0	1122
148	CRESCENT	127	2	0	671
183	EDGEWORTH	135	0	1	702
184	EDGEWORTH	135	0	2	754
185	ELIZABETH BORO	136	0	1	925
186	ELIZABETH TWP	137	1	1	565
187	ELIZABETH TWP	137	1	2	912
188	ELIZABETH TWP	137	2	0	1270
189	ELIZABETH TWP	137	3	0	1339
190	ELIZABETH TWP	137	4	1	902
191	ELIZABETH TWP	137	4	2	457
192	ELIZABETH TWP	137	5	1	455
193	ELIZABETH TWP	137	5	2	817
194	ELIZABETH TWP	137	6	1	602
195	ELIZABETH TWP	137	6	2	725
196	ELIZABETH TWP	137	7	0	1252
204	FINDLAY	141	0	1	1198
205	FINDLAY	141	0	2	1707
206	FINDLAY	141	0	3	1212
215	FORWARD	143	0	1	370
216	FORWARD	143	0	2	878
217	FORWARD	143	0	3	385
218	FORWARD	143	0	4	446
273	HEIDELBERG	154	0	1	861
288	JEFFERSON HILLS	158	0	1	1575
289	JEFFERSON HILLS	158	0	2	840
290	JEFFERSON HILLS	158	0	3	639
291	JEFFERSON HILLS	158	0	4	684
292	JEFFERSON HILLS	158	0	5	2052
293	JEFFERSON HILLS	158	0	6	943
294	JEFFERSON HILLS	158	0	7	365
295	JEFFERSON HILLS	158	0	8	1142
304	LEET	161	0	1	396
305	LEET	161	0	2	760
306	LEETSDALE	162	0	1	880
337	MCDONALD	167	0	5	206
386	MONROEVILLE	171	2	1	885
388	MONROEVILLE	171	2	3	1066

390	MONROEVILLE	171	3	2	649
393	MONROEVILLE	171	4	1	664
394	MONROEVILLE	171	4	2	1056
398	MONROEVILLE	171	5	3	923
407	MOON	172	0	1	1427
408	MOON	172	0	2	1800
409	MOON	172	0	3	1437
410	MOON	172	0	4	762
411	MOON	172	0	5	2426
412	MOON	172	0	6	2222
413	MOON	172	0	7	1514
414	MOON	172	0	8	965
415	MOON	172	0	9	1932
416	MOON	172	0	10	763
417	MOON	172	0	11	1321
418	MOON	172	0	12	996
419	MOON	172	0	13	705
420	MT LEBANON	173	1	1	845
421	MT LEBANON	173	1	2	681
422	MT LEBANON	173	1	3	649
423	MT LEBANON	173	1	4	789
424	MT LEBANON	173	1	5	619
425	MT LEBANON	173	1	6	1069
426	MT LEBANON	173	1	7	783
427	MT LEBANON	173	2	1	969
428	MT LEBANON	173	2	2	601
429	MT LEBANON	173	2	3	714
430	MT LEBANON	173	2	4	536
431	MT LEBANON	173	2	5	588
432	MT LEBANON	173	2	6	554
433	MT LEBANON	173	2	7	633
434	MT LEBANON	173	2	8	1008
435	MT LEBANON	173	3	1	662
436	MT LEBANON	173	3	2	862
437	MT LEBANON	173	3	3	684
438	MT LEBANON	173	3	4	747
439	MT LEBANON	173	3	5	700
440	MT LEBANON	173	3	6	455
441	MT LEBANON	173	3	7	817
442	MT LEBANON	173	3	8	324
443	MT LEBANON	173	4	1	800
444	MT LEBANON	173	4	2	899
445	MT LEBANON	173	4	3	725
446	MT LEBANON	173	4	4	674
447	MT LEBANON	173	4	5	613
448	MT LEBANON	173	4	6	671
449	MT LEBANON	173	4	7	801

450	MT LEBANON	173	5	1	621
451	MT LEBANON	173	5	2	461
452	MT LEBANON	173	5	3	598
453	MT LEBANON	173	5	4	580
454	MT LEBANON	173	5	5	621
455	MT LEBANON	173	5	6	467
456	MT LEBANON	173	5	7	784
457	MT LEBANON	173	5	8	1012
484	N FAYETTE	178	0	1	2018
485	N FAYETTE	178	0	2	2349
486	N FAYETTE	178	0	3	2421
487	N FAYETTE	178	0	4	1073
488	N FAYETTE	178	0	5	2434
502	OAKDALE	180	0	1	590
503	OAKDALE	180	0	2	441
987	PLEASANT HILLS	189	0	1	721
988	PLEASANT HILLS	189	0	2	534
989	PLEASANT HILLS	189	0	3	554
990	PLEASANT HILLS	189	0	4	533
991	PLEASANT HILLS	189	0	5	747
992	PLEASANT HILLS	189	0	6	914
993	PLEASANT HILLS	189	0	7	509
994	PLEASANT HILLS	189	0	8	513
995	PLEASANT HILLS	189	0	9	643
996	PLEASANT HILLS	189	0	10	515
1037	ROBINSON	195	0	1	1598
1038	ROBINSON	195	0	2	958
1040	ROBINSON	195	0	4	711
1042	ROBINSON	195	0	6	889
1043	ROBINSON	195	0	7	1383
1044	ROBINSON	195	0	8	1548
1045	ROBINSON	195	0	9	2417
1079	ROSSLYN FARMS	197	0	1	380
1080	SCOTT	198	1	1	564
1081	SCOTT	198	1	2	660
1082	SCOTT	198	2	1	488
1083	SCOTT	198	2	2	668
1084	SCOTT	198	3	1	506
1085	SCOTT	198	3	2	720
1086	SCOTT	198	4	1	761
1087	SCOTT	198	4	2	607
1088	SCOTT	198	5	1	594
1089	SCOTT	198	5	2	738
1090	SCOTT	198	6	1	703
1091	SCOTT	198	6	2	798
1092	SCOTT	198	7	1	898
1093	SCOTT	198	7	2	624

1094	SCOTT	198	8	1	513
1095	SCOTT	198	8	2	1010
1096	SCOTT	198	9	1	300
1097	SCOTT	198	9	2	330
1141	SOUTH FAYETTE	204	0	1	562
1142	SOUTH FAYETTE	204	0	2	1083
1143	SOUTH FAYETTE	204	0	3	1534
1144	SOUTH FAYETTE	204	0	4	857
1145	SOUTH FAYETTE	204	0	5	856
1146	SOUTH FAYETTE	204	0	6	1206
1147	SOUTH FAYETTE	204	0	7	630
1148	SOUTH FAYETTE	204	0	8	1466
1149	SOUTH FAYETTE	204	0	9	624
1150	SOUTH FAYETTE	204	0	10	772
1151	SOUTH FAYETTE	204	0	11	949
1152	SOUTH FAYETTE	204	0	12	468
1153	SOUTH PARK	205	0	1	725
1154	SOUTH PARK	205	0	2	750
1155	SOUTH PARK	205	0	3	617
1156	SOUTH PARK	205	0	4	460
1157	SOUTH PARK	205	0	5	751
1158	SOUTH PARK	205	0	6	835
1159	SOUTH PARK	205	0	7	1108
1160	SOUTH PARK	205	0	8	510
1161	SOUTH PARK	205	0	9	794
1162	SOUTH PARK	205	0	10	852
1163	SOUTH PARK	205	0	11	592
1164	SOUTH PARK	205	0	12	561
1165	SOUTH PARK	205	0	13	1047
1166	S VERSAILLES	206	0	1	214
1199	THORNBURG	212	0	1	429
1200	PENNSBURY VLG	212	0	2	564
1208	UPPER ST CLAIR	215	1	1	698
1209	UPPER ST CLAIR	215	1	2	830
1210	UPPER ST CLAIR	215	1	3	983
1211	UPPER ST CLAIR	215	1	4	814
1212	UPPER ST CLAIR	215	2	1	958
1213	UPPER ST CLAIR	215	2	2	698
1214	UPPER ST CLAIR	215	2	3	1018
1215	UPPER ST CLAIR	215	2	4	545
1216	UPPER ST CLAIR	215	3	1	1035
1217	UPPER ST CLAIR	215	3	2	872
1218	UPPER ST CLAIR	215	3	3	1169
1219	UPPER ST CLAIR	215	4	1	980
1220	UPPER ST CLAIR	215	4	2	769
1221	UPPER ST CLAIR	215	4	3	604
1222	UPPER ST CLAIR	215	4	4	1035

1223	UPPER ST CLAIR	215	5	1	1306
1224	UPPER ST CLAIR	215	5	2	812
1225	UPPER ST CLAIR	215	5	3	857
1240	WEST ELIZABETH	220	0	1	262
1274	WHITEHALL	225	0	1	520
1275	WHITEHALL	225	0	2	582
1276	WHITEHALL	225	0	3	656
1277	WHITEHALL	225	0	4	668
1278	WHITEHALL	225	0	5	685
1279	WHITEHALL	225	0	6	1016
1280	WHITEHALL	225	0	7	431
1281	WHITEHALL	225	0	8	802
1282	WHITEHALL	225	0	9	544
1283	WHITEHALL	225	0	10	613
1284	WHITEHALL	225	0	11	628
1285	WHITEHALL	225	0	12	545
1286	WHITEHALL	225	0	13	438
1287	WHITEHALL	225	0	14	586
1288	WHITEHALL	225	0	15	991
1289	WHITEHALL	225	0	16	604

BALLOT	MUNICIPALITY	MUNI	WARD	DISTRICT	TOTAL REGISTERED	SAM_RECNO
218	FORWARD	143	0	4	446	77