

---

---

*Department of Veterans Affairs*  
*Medical Device Isolation Architecture Guide*

---

---



Published by  
Center for Engineering & Occupational Safety and Health (CEOSH), St. Louis, MO  
In conjunction with the  
Department of Veterans Affairs and Veterans Health Administration, Washington, DC

April 30, 2004

---

---

*Department of Veterans Affairs*  
*Medical Device Isolation Architecture Guide*

---

---



Published by  
Center for Engineering & Occupational Safety and Health (CEOSH), St. Louis, MO  
In conjunction with the  
Department of Veterans Affairs and Veterans Health Administration, Washington, DC

April 30, 2004

---

---

# Table of Contents

---

---

Executive Summary..... iii

Acknowledgements ..... v

**Introduction** ..... 1

    A. Purpose..... 1

    B. Medical Device Isolation Architecture Working Group ..... 1

**Step 1: Data Gathering** ..... 3

**Step 2: Grouping By Systems**..... 5

    A. System Name ..... 5

    B. System Function..... 5

    C. System Manufacturer ..... 5

    D. Vendor System Contact..... 5

    E. VA System Contact..... 5

    F. Device Name..... 5

    G. Device Description..... 5

    H. Device IP Address..... 5

    I. Device Subnet Mask ..... 5

    J. Device Network Gateway ..... 5

**Step 3: Categorize By Communication Requirements**..... 7

    A. Information Gathering..... 7

        1. Does the system communicate with any other device or system outside of its home system?..... 7

        2. What is the name and IP address of the device(s) the system communicates with? ..... 7

        3. What protocol does the system use to communicate with outside devices?..... 7

        4. What port number does the system use for this outside communication?..... 8

        5. Who initiates the connection? ..... 8

    B. Categories..... 8

        1. Standalone..... 8

        2. Non-Domain Restricted..... 8

        3. Domain Restricted..... 8

        4. Non-Domain Limited ..... 8

5. Domain Limited .....	8
6. Internet Only .....	8
7. Internet Restricted .....	8
<b>Step 4: Device Migration .....</b>	<b>11</b>
A. Standalone Migration .....	11
B. All Other Migrations .....	11
C. Migration Options .....	12
<b>Step 5: Protecting the VLANs .....</b>	<b>13</b>
A. Non-Domain Restricted .....	14
1. Sample Data for Non-Domain Restricted (Category 2) .....	14
2. Example of Non-Domain Restricted ACL (Out).....	14
3. Example of Non-Domain Restricted ACL (In) .....	15
B. Non-Domain Limited .....	16
1. Sample Data for Non-Domain Limited (Category 4).....	16
2. Example of Non-Domain Limited ACL (Out) .....	17
3. Example of Non-Domain Limited ACL (In).....	18
C. Domain Limited .....	19
1. Sample Data for Domain Limited (Category 5) .....	19
2. Example of Domain Limited ACL (Out) .....	20
3. Example of Domain Limited ACL (In).....	21
D. Internet Only .....	22
1. Sample Data for Internet Only (Category 6) .....	22
2. Example of Internet Only (Out) .....	23
E. Internet Restricted .....	24
1. Sample Data for Internet Restricted (Category 7).....	24
2. Example of Internet Restricted (Out) .....	25
3. Example of Internet Restricted (In).....	26
<b>Glossary .....</b>	<b>29</b>

---

## *Executive Summary*

---

As networked technology continues to expand to meet the needs of modern medicine, it also exposes critical hospital equipment and records to risk of attack by a software worm, virus or other breach of security. These attacks have the potential to destabilize an entire network, shut down key hospital operations, corrupt data and jeopardize patient safety. While the impact on medical devices is presently low, attacks on computer software have been on the rise, making the susceptibility of medical devices to this kind of attack real for VA and, indeed, for all healthcare providers. It should also be recognized as a genuine threat to homeland security, as the healthcare community is among the first responders to terrorist action.

Securing our information networks and protecting devices connected to those networks remains a high priority in VA. Because medical devices have a very special purpose with specific design considerations and constraints, routine patching of commercial operating systems employed by some medical devices or application of anti-virus software to medical devices is not available in most cases. Such actions can potentially change the operating function of the medical device with the possibility for negative impact on patient safety and, therefore, cannot be readily undertaken without the expressed support and consent of the original equipment manufacturer. The isolation architecture described here in this Department of Veterans Affairs Medical Device Isolation Architecture Guide addresses risks associated with medical devices connected to facility information networks without impacting the operational characteristics of the devices. It describes a five-step approach for moving networked medical devices from the more common, open or flat Local Area Network to a more protected Virtual Local Area Network or VLAN structure.

The Guide references IT hardware and medical devices by brand name. This is for illustrative purposes only; it does not constitute an endorsement of these products nor does it imply that only these products are necessary to successfully implement this strategy. The protected VLAN is a generic concept that may be applied to a variety of configurations and indeed may be used with products other than medical devices that benefit from networked technology. It will not completely eliminate risk; rather it elevates the security posture by establishing a well-defined structure with a level of isolation from the main facility information network, giving technical staff with responsibility for managing the networks an enhanced level of control.



---

---

## *Acknowledgements*

---

---

The material in this guide was developed by IT staff working for the Veterans Health Administration (VHA) in the Department of Veterans Affairs. In addition to managing their daily activities, including technical and management responsibility for VHA information networks, they dedicated their time and expertise to make this publication available:

***Hal Haislip*** - VISN 16 WAN Manager, North Little Rock, AR

***Troy Tepp*** - VISN 12 WAN Manager, Chicago, IL

***John Deltognoarmanasco*** - VISN 18 WAN Manager, Mesa, AZ

The vision to find a solution and conceptualize this guide was provided by:

***Steven Wexler*** - VHA Chief Biomedical Engineer, Washington, DC

We also want to recognize the many reviewers and other contributors to this guide including both VA and VHA technical staff:

***Ken Hartmann*** - VA Health Information Security Division, Martinsburg, WV

***Ron Hensel*** - VA Health Information Security Division, Martinsburg, WV

***John Baron*** - VA Health Information Security Division, Martinsburg, WV

***Stan Smith*** - VHA WAN Manager, North Little Rock, AR

***Richard Mason*** - VHA WAN Manager, North Little Rock, AR

***Rob Turner*** - VHA WAN Manager, North Little Rock, AR

***Charles Armato*** - VHA Biomedical Engineer, Little Rock, AR

***Charles Ward*** - VHA Biomedical Engineering Technician, Little Rock, AR

***Roland Hutchins*** - VHA Biomedical Engineering Technician, Little Rock, AR

A special thanks goes to the staff and management of the Center for Engineering & Occupational Safety and Health (CEOSH) whose devoted attention led to the publication of this Guide.



---

# *Introduction*

---

## ***A. Purpose***

---

This document has a target audience of VA Local Area Network (LAN) managers, Information Technology (IT) staff assigned to network support and Biomedical Engineers. The purpose of this document is to provide a step-by-step process for moving networked medical devices from open or flat LANs to a more protected Virtual LAN (VLAN) structure. Moving medical devices to a separate VLAN is just the first step of the process; it is, however, the most difficult and time consuming. More than likely, there will be more than one medical VLAN. The reason for this is that different systems may have dissimilar communication requirements.

Every IT person in the VA is painfully aware of computer viruses and network worms. Moving our medical devices to a separate VLAN and then protecting access to and from that VLAN is the only reliable way to protect our medical devices and still have them on our network. The primary methods of protecting access to a medical VLAN are using a firewall or a router-based access control list (ACL). Regardless of what mechanism is chosen, the steps in this document will still apply. There are five steps in moving medical devices to protected VLANS:

1. Gather a list of all networked medical devices.
2. Group the individual devices into systems.
3. Categorize those systems by communication requirements.
4. Migrate the systems into VLANS.
5. Protect the VLANS with an ACL or Firewall configuration.

## ***B. Medical Device Isolation Architecture Working Group***

---

A Medical Device Isolation Architecture Working Group has been established within the VA to provide guidance and assistance in securing medical devices. The following e-mail address has been setup for the group: [vamedicaldeviceisolationarchitecture@mail.va.gov](mailto:vamedicaldeviceisolationarchitecture@mail.va.gov).

The workgroup consist of the following individuals:

Ken Hartmann, Program Manager, Health Information Security Division  
Ron Hensel, IT Specialist, Health Information Security Division  
John Baron, IT Specialist, Health Information Security Division  
Steven Wexler, VHA Chief Biomedical Engineer (VACO)  
Hal Haislip, VISN 16 WAN Manager  
John Deltognoamanasco, VISN 18 WAN Manager  
Troy Tepp, VISN 12 WAN Manager  
Randy Ledsome, VISN 4 ISO



## ***Step 1: Data Gathering***

---

---

Facility IT and Biomedical Engineering staff need to create a list of all networked medical or medically related devices. This list should not be limited to only Food and Drug Administration (FDA) approved devices. Many facilities have devices that fall into a “gray area” in that they are not FDA approved but must run non-VA standard applications and operating systems in order to perform a medically related function. An example would be a computer that must run only Windows NT and only Service Pack 3 in order to operate medication-dispensing devices. While these are not strictly medical devices, they are vulnerable to attack and need to be protected from viruses and worms. Conversely, the rest of the network needs to be protected from them. Include them in your list of medical devices for this reason. A partial list should already be available. VACO requested a list of all networked medical devices in January of 2004, and provided an Excel spreadsheet as a template. It is recommended that this spreadsheet be used as a starting point. This list should include the name, location, IP address, switch IP address, switch port number and any other site-specific information that might be helpful in later moving the device.



---

## *Step 2: Grouping by Systems*

---

The facility IT and Biomedical Engineering staff now have to take the list from Step 1 (Data Gathering) and group the devices by system. When defining a system, the facility should ask the following questions:

1. What does the system do?
2. Who is the manufacturer of the system?
3. Who provides maintenance for the system?
4. Does all the equipment belong to the same manufacturer?

This information is already available in the Vista equipment management system, AEMS/MERS (Automated Engineering Management System/Medical Equipment Reporting System).

Facilities should also be aware that some systems will contain both FDA and non-FDA regulated components (devices). A spreadsheet will be the easiest way to do this and keep track of the data collected. The spreadsheet should contain the following data at a minimum:

- a. *System Name*. This is simply a label for easy identification. For consistency with other equipment maintenance and equipment planning activities, it is recommended that the identifiers from AEMS/MERS be used.
- b. *System Function*. This could be as simple as a single word, just to clarify the system for those not familiar with Biomedical Engineering terms. For example, “EKG” could be used for the GE Marquette Muse system.
- c. *System Manufacturer*. See AEMS/MERS.
- d. *Vendor System Contact*. This is the telephone number the facility would call for support on this system. It could be a local tech number or the number of the vendor’s help desk.
- e. *VA System Contact*. This is the number of the VA person responsible for this system (Biomedical Engineering or IRM contact).
- f. *Device Name*. There will probably be multiple entries for this column and the next three. In this column enter in the name of the device.
- g. *Device Description*. This is a short description of the function of the device so that IT, Biomedical Engineering, end user staff and the vendor all have a common frame of reference regarding this device. (See AEMS/MERS.)
- h. *Device IP Address*. This is the IP address of the device. All medical devices should use static IP addresses and not DHCP assigned addresses. In order for an ACL to function, the IP address of the device referenced in that ACL must be static.
- i. *Device Subnet Mask*. This is the subnet mask of the device.
- j. *Device Network Gateway*. This is the network gateway address for this device.



## ***Step 3: Categorize by Communication Requirements***

---

---

Facility IT and Biomedical Engineering staff will now identify how these systems communicate with each other and what protocols are used. Facility IT and Biomedical Engineering staff will use the spreadsheet they developed in the previous section (Step 2) to facilitate this process. This is a two-step process. First, certain information about each medical device has to be gathered. Then using the data gathered, each system must be categorized. For each device listed in each system, utilize the following process:

*Note: The sections below are written from the perspective of the medical system/devices communicating to an outside entity (i.e. VA devices, VA Intranet devices or Internet device); however, Facility IT and Biomedical Engineering staff need to answer the questions from both directions.*

### ***A. Information Gathering***

---

For categorization the following questions must be answered:

1. Does the system communicate with any other device or system outside of its home system?

If the answer is No, then this system automatically falls into the Standalone category. If the answer is Yes, then go ahead and finish questions 2 through 5.

2. What is the name and IP address of the device(s) the system communicates with?

This may be as few as one address and as many as a thousand. If this system communicates with a great many users, simply list the network number(s) of those locations. The Facility Network Manager will be able to find this piece of data. This question defines the system's borders, and this is the first step in the ACL and/or firewall process. If this system has Microsoft components and they use the Windows Domain Service for authentication, make sure to list those systems. If only one or two devices in the system communicate to other outside devices, then make sure to note this fact. If a single device in a system communicates with multiple outside devices or systems, note this as well. Connections between devices within the same system will not be passing through an ACL or a firewall, so they may be ignored. It is very important, however, that **all external** (incoming and outgoing) connections be identified.

3. What protocol does the system use to communicate with outside devices?

Does the system use an IP protocol, LAT or DDP? If the system uses an IP protocol, please identify them (TCP, UDP or ICMP). If the system uses LAT or DDP, it must be located on the same VLAN as Vista. The reason for this is that LAT and DDP are not routable protocols and cannot be passed securely from one VLAN to another. If the system uses both an IP

protocol and LAT, then protecting the system becomes very difficult. If both are used, then facility and Biomedical Engineering staff need to indicate if both protocols are on the same network card (NIC) or on two separate NICs.

4. What port number does the system use for this outside communication?

This may be the most difficult piece of data to acquire. If this information cannot be found or there are not any defined ports for this system, then we will have to block by the information found in questions 3 and 5. It will not, however, be as secure.

5. Who initiates the connection?

Does the outside device, such as Vista, open the connection to the medical device, or does the medical device open the connection to the outside device? Think of this like a telephone call: One end or the other must open the connection; once the connection is open, the traffic will flow in both directions.

## ***B. Categories***

---

Based on the information collected above, the systems will be put into one of these seven categories:

1. *Standalone*. This category of system only communicates within its own devices. It does not communicate with any other device or system. These systems simply need a non-routed VLAN, and do not use any network services such as WINS or DNS.
2. *Non-Domain Restricted*. This category does not communicate with the VA Microsoft Domain (i.e. use the NetBIOS protocols), and it only communicates with a few well-defined devices on the facility LAN. In most cases the devices communicated with will be Vista and/or VistaRad. This category does not use WINS, DNS or have access to the Internet. An example of this category would be a GE Imaging System.
3. *Domain Restricted*. This category does communicate with the VA Microsoft Domain, and it only communicates with one or two well-defined devices on the facility LAN. In most cases those devices communicated with will be Vista and VistaRad. This category does not have access to the Internet. This category requires access to DNS and/or WINS, and Local Domain Controllers.
4. *Non-Domain Limited*. This category does not communicate with the VA Microsoft Domain, but it does communicate with several devices on the facility, VISN or VA network. This category does not communicate with the Internet, but it does require access to DNS and/or WINS. In some cases WINS and DNS access may be avoided by having the device(s) use local HOST and/or LMHOST files. An example of this category would be the Marquette Muse System.
5. *Domain Limited*. This category does communicate with the VA Microsoft Domain, and it communicates with several devices on the facility, VISN or VA network. This category does not have access to the Internet, but it does require access to DNS, WINS and Local Domain Controllers. An example of this category would be the Audiology NOAH System.
6. *Internet Only*. This category communicates with the Internet but not with the VA Microsoft Domain or with any internal devices. If possible these devices should be configured to use Internet DNS servers instead of VA DNS servers. An example of this category would be the Walsh QSS System.
7. *Internet Restricted*. This category communicates with the Internet and with specific internal devices, but not with the VA Microsoft Domain. If possible these devices should be configured

to use Internet DNS servers instead of VA DNS servers. WINS and DNS access should, if possible, be avoided by having the device(s) use local HOST and/or LMHOST files. An example of this category would be the Data Innovations LAB Interface System.



---

## ***Step 4: Device Migration***

---

This step will take a great deal of planning and some business hours or after-hour downtime depending upon Vendor availability. Facility IT and Biomedical Engineering staff need to take a look at the systems in each category and rate them in terms of complexity. In many instances, systems in the same category will need to communicate with the same external devices (internal to the VA, external to the VLAN). If doing so does not violate any maintenance/warranty issues or create other technical or legal problems, then these systems should be placed on the same VLAN; the goal is to create as few VLANs as possible but as many as necessary. Medical device VLANs, just like other facility VLANs, should conform to VISN VLAN standards including:

1. Common VLAN numbering scheme.
2. Common ACL numbering scheme.
3. Common naming convention.

Once the VLAN design has been completed, the Network Manager will be responsible for creating and activating the new VLANs. The Network Manager will communicate the network number, subnet mask, default gateway and available IP addresses to the IT and/or Biomedical Engineering staff involved in the migration process. When developing a migration plan or strategy, facility IT and Biomedical Engineering staff should use the following guidelines to make the migration process as simple as possible:

1. Move smaller or simpler systems first.
2. The actual address, subnet mask, gateway and protocol changes should be made by the Vendors or Contractors of these systems.
3. Do not activate any ACLs or install a firewall during this step. The trouble-shooting process will be much simpler if it only has to contend with one change at a time.

### ***A. Standalone Migration***

---

This is a simple and straightforward process. Simply create a Layer 2 (MAC Layer) VLAN, but do not create the Layer 3 (TCP/IP) router component for it. Identify all of the switch ports, and move them (as simultaneously as possible) to the new Layer 2 VLAN. They are now trapped on this new VLAN without any way out. It is recommended that the IP addresses of the standalone system be changed to the 192.168.x.x network. Should someone accidentally move the switch ports to a different VLAN, this will prevent them from communicating to anything on the VA network.

### ***B. All Other Migrations***

---

The migration process for all other categories of systems will follow the same pattern. The first step in this process is to identify the device or devices that will need to be able to communicate outside of the new VLAN(s). These devices should have been identified in Step 3. Since this is often a server of

some type, we will call this device a server. Create a new VLAN with both Layers 2 and 3 active. Move the server to the new Medical VLAN, and change its IP address, subnet mask and default gateway to match that of the new VLAN. Before moving any further in the process, make sure the server and its outside communication partners can PING each other. Once this is accomplished move the other devices of that system to the new VLAN, change their network parameters; and make sure they can PING their server. Once all devices are moved, verify that the whole system works. If any of these devices are found in DNS, make sure to update those records. If any device initiates contact with this moved system using IP addresses (as opposed to DNS), make sure to update their configurations to reflect the new addresses.

### ***C. Migration Options***

---

Below are a few variations that might be considered (included are pros and cons for each option):

1. If a complete medical system is within an area served by a single signal closet, the Network Manager might consider putting the medical system on its own switch. On the positive side, in case of an extreme emergency the switch would be disconnected from the rest of the LAN, and the medical system could temporarily run as a standalone system. The drawback is the cost of the extra switch and the extra management overhead.
2. A system manager could leave the default gateways off of all the medical devices that do not need to communicate outside of the VLAN. The upside is that this would prevent **any** communication from outside the VLAN. The downside is that unless a Network Sniffer is actually attached to the infected VLAN, the Network Manager will have a very difficult time detecting an infection should one occur.

---

## Step 5: Protecting the VLANs

---

Once the medical systems are functioning properly on the new VLANs, facility IT and Biomedical Engineering staff will schedule time with the Vendor and end-users to implement the security rules developed in Step 3. The goal is to remove as much outside access into the VA network and as much internal access to the medical VLAN as possible, while still allowing the medical systems to operate normally. As the rules are implemented, the end-user can verify that the systems are still operating correctly and the vendor can aid IT and Biomedical Engineering staff in resolving any issues that develop as the rules are implemented.

Until now this document has been Vendor neutral. However, since well over 90% of the facilities in the Department of Veterans Affairs use Cisco networking hardware, the sample ACLs in this document are written for Cisco IOS based routers (with little modification they will also work in Cisco PIX Firewalls). Cisco ACLs test each packet against each line in an access list one by one from the top to bottom. The first match determines whether to accept or reject the packets. As soon as the first match to the ACL is made, the testing stops. Because of this, the ordering of the statements is critical. For example, if a deny statement matches before a permit statement, the packet is discarded before arriving at the permit statement. Because the access list is read from top to bottom, it is more efficient to put the most heavily used match statements at the top of an ACL and the least common matches at the bottom. The access-list “remark” statements are allowed on any IOS-based system with version 12.0 and higher. These are simply comment statements, and do not effect data flow.

Cisco Access Control Lists are applied per interface and per direction. They can be applied to filter all packets entering an interface, leaving an interface or both. Due to the format of the access-list statements, an ACL written to filter outgoing packets will often not work if applied as an incoming filter.

Since these are Virtual LANs, there can be a great deal of confusion as to what “in” and “out” actually mean. The “**in**” direction filters packets from the protected medical VLAN **into the virtual router interface**. The “**out**” direction filters packets from other virtual interfaces and **out the virtual interface of the medical VLAN** going to the protected medical devices. Only one inbound and one outbound ACL can be applied to an interface.

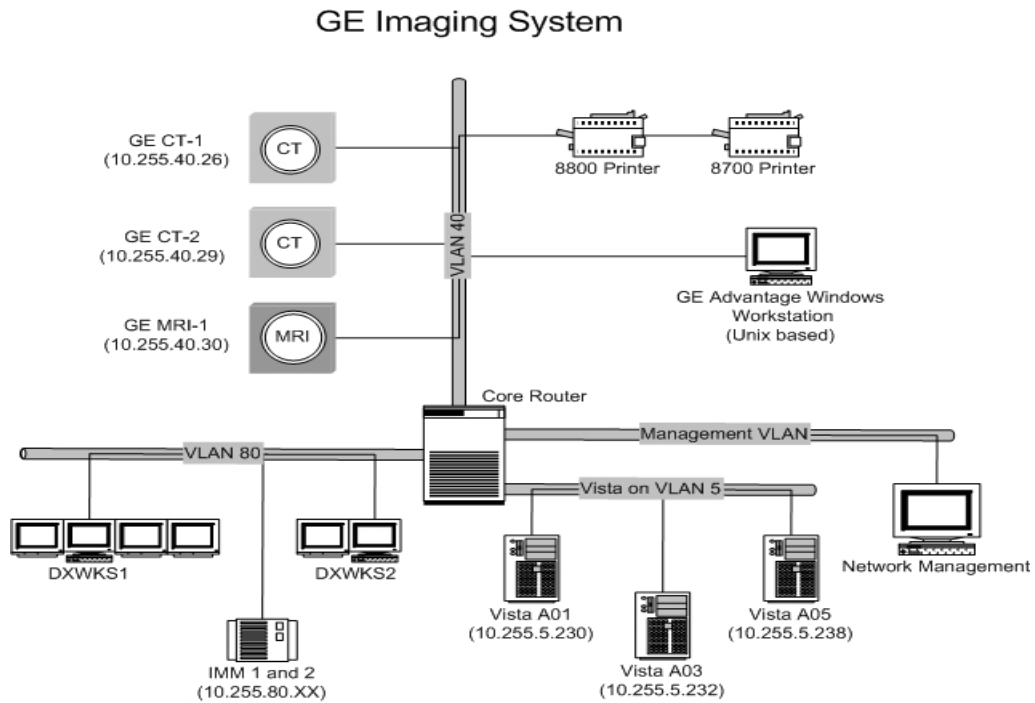
There are several different types of ACLs. For the purpose of this document we will only work what is called an extended access-list. The valid numbers for Cisco extended ACLs are from 100 to 199 and from 2000 to 2699. For more information on Cisco ACLs, go to the Cisco Web site ([www.cisco.com](http://www.cisco.com)) or contact your Cisco Field Engineer. There are also several good books on the topic. As a convention, the ACLs in this document match closely to the VLAN they are assigned to (just add 100 to the VLAN number if it is below 100). For filtering both directions, just add 101 to the number. The VLAN number also matches the third octet of the IP address range for the VLAN. While this is not a requirement, it is a recommended practice.

Allowing access to and from the Facility network management VLAN may or may not be desirable contingent upon a variety of factors. Facility IT and Biomedical Engineering staff need to make this decision when writing the access control lists.

Examples of Non-Domain Restricted, Non-Domain Limited, Domain Limited, Internet Only and Internet Restricted are provided within this document.

**A. Non-Domain Restricted**

1. Sample Data for Non-Domain Restricted (Category 2):
  - a. GE Imaging System.
  - b. CT and MRI scanners.
  - c. Yes.
  - d. CT-1 10.255.40.26  
 CT-2 10.255.40.29  
 MRI-1 10.255.40.30 communicates with:  
     Vista, 10.255.5.231 - 238 via TCP various  
     VistaRad, various devices via TCP  
     10.255.1.0/24 for Net Management
  - e. Sessions with Vista and VistaRad are initiated in both directions.  
     Net Management initiates sessions with GE Imaging Systems



2. Example of Non-Domain Restricted ACL (Out): The following Cisco ACL protects the GE Imaging System from unwanted network traffic while allowing them to function normally.

*Note 1: The line numbers are not part of the ACL; instead, they are being used as a reference for the line-by-line description below the ACL.*

*Note 2: Some versions of Cisco IOS do list line numbers when the command “show access-list” is entered.)*

a. ACL 140 is applied as an “out” filter

- 1) Access-list 140 remark \*\*\* GE Imaging System ACL out \*\*\* rev 1-21-04 hh
- 2) Access-list 140 permit tcp 10.255.5.224 0.0.0.15 host 10.255.40.26
- 3) Access-list 140 permit tcp 10.255.5.224 0.0.0.15 host 10.255.40.29
- 4) Access-list 140 permit tcp 10.255.5.224 0.0.0.15 host 10.255.40.30
- 5) Access-list 140 permit tcp 10.255.80.0 0.0.0.255 host 10.255.40.26
- 6) Access-list 140 permit tcp 10.255.80.0 0.0.0.255 host 10.255.40.29
- 7) Access-list 140 permit tcp 10.255.80.0 0.0.0.255 host 10.255.40.30
- 8) Access-list 140 permit icmp 10.255.5.224 0.0.0.15 10.255.40.0 0.0.0.255
- 9) Access-list 140 permit icmp 10.255.80.0 0.0.0.255 10.255.40.0 0.0.0.255
- 10) Access-list 140 permit ip 10.255.1.0 0.0.0.255 10.255.40.0 0.0.0.255
- 11) Access-list 140 deny ip any log-input
- 12) Interface vlan40
- 13) IP access-group 140 out

b. ACL 140 Descriptions

- 1) Remark statement to show purpose, date installed and author.
- 2) Allow TCP access from Vista systems (this ACL statement allows 10.255.5.224 thru 239) to CT-1.
- 3) Allow TCP access from Vista systems to CT-2.
- 4) Allow TCP access from Vista systems to MRI-1.
- 5) Allow TCP access from Vista Imaging VLAN to CT-1.
- 6) Allow TCP access from Vista Imaging VLAN to CT-2.
- 7) Allow TCP access from Vista Imaging VLAN to MRI-1.
- 8) Allow ICMP (ping and tracert for diagnostic purposes) from the Vista systems to VLAN 40.
- 9) Allow ICMP (ping and tracert for diagnostic purposes) from Vista Imaging VLAN 80 to VLAN 40.
- 10) Allow IP access from Management Network devices.
- 11) Deny all other IP based traffic and log the denied packets.
- 12) Get “into” the router interface for VLAN 40. All subsequent commands apply only to VLAN 40.
- 13) Use ACL 140 to filter packets as they go out to VLAN 40.

3. Example of Non-Domain Restricted ACL (In):

a. ACL 141 is applied as an “in” filter

- 1) Access-list 141 remark \*\*\* GE Imaging System ACL in \*\*\* rev 1-21-04 hh
- 2) Access-list 141 permit tcp host 10.255.40.26 10.255.5.224 0.0.0.15
- 3) Access-list 141 permit tcp host 10.255.40.29 10.255.5.224 0.0.0.15
- 4) Access-list 141 permit tcp host 10.255.40.30 10.255.5.224 0.0.0.15
- 5) Access-list 141 permit tcp host 10.255.40.26 10.255.80.0 0.0.0.255
- 6) Access-list 141 permit tcp host 10.255.40.29 10.255.80.0 0.0.0.255

- 7) Access-list 141 permit tcp host 10.255.40.30 10.255.80.0 0.0.0.255
- 8) Access-list 141 permit icmp 10.255.40.0 0.0.0.255 10.255.5.224 0.0.0.15
- 9) Access-list 141 permit icmp 10.255.40.0 0.0.0.255 10.255.80.0 0.0.0.255
- 10) Access-list 141 permit ip 10.255.40.0 0.0.0.255 10.255.1.0 0.0.0.255
- 11) Access-list 141 deny ip any log-input
- 12) Interface vlan41
- 13) IP access-group 141 in

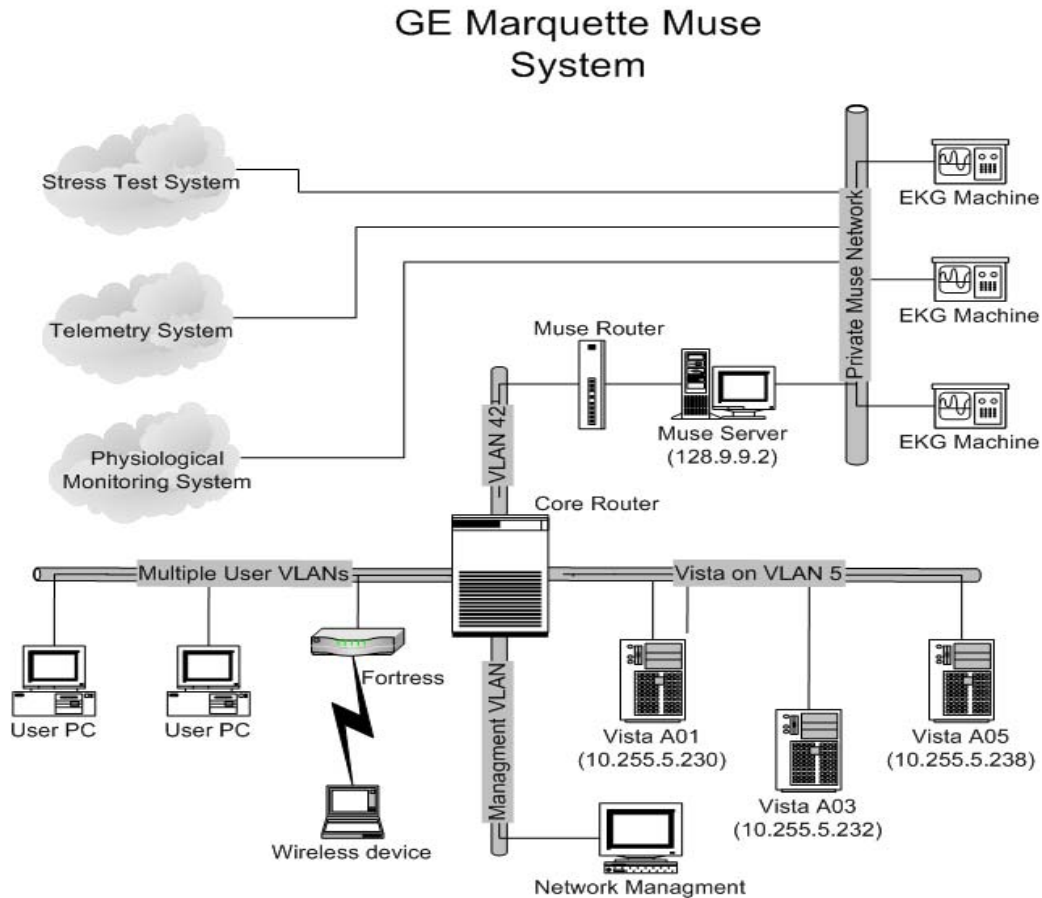
b. ACL 141 Descriptions

- 1) Remark statement to show purpose, date installed and author.
- 2) Allow TCP access from CT-1 (this ACL statement allows 10.255.5.224 thru 239) to the Vista systems.
- 3) Allow TCP access from CT-2 to the Vista systems.
- 4) Allow TCP access from MRI-1 systems to the Vista systems.
- 5) Allow TCP access from CT-1 to the Vista Imaging VLAN.
- 6) Allow TCP access from CT-2 to the Vista Imaging VLAN.
- 7) Allow TCP access from MRI-1 to the Vista Imaging VLAN.
- 8) Allow ICMP from VLAN 40 access to Vista Systems.
- 9) Allow ICMP access to Vista Imaging VLAN 80.
- 10) Allow IP access to the Management Network devices.
- 11) Deny all other IP based traffic and log the denied packets.
- 12) Get “into” the router interface for VLAN 40. All subsequent commands apply only to VLAN 40.
- 13) Use ACL 141 to filter packets as they leave VLAN 40.

## ***B. Non-Domain Limited***

---

1. Sample Data for Non-Domain Limited: (Category 4)
  - a. Marquette Muse.
  - b. EKG system.
  - c. Yes.
  - d. Muse server 10.255.42.33 communicates with:  
Vista, 10.255.5.231/232/233 via TCP various  
BCMA Users 10.255.0.0/17 via TCP 139, 445, 3351  
BCMA Users 10.255.0.0/17 via ICMP (ping and trace)  
Muse network switch 10.255.42.33 to 10.255.1.0/24 for Net Management.
  - e. BCMA users initiate connections with Muse.  
Sessions are initiated in both directions between Vista and Muse.  
Net Management initiates connections with the Muse server for scanning and diagnostics.



2. Example of Non-Domain Limited ACL (Out): There are other systems behind the Muse server, and they all communicate to BCMA through the Muse. Although the Muse is not on the VA Microsoft domain, it is Microsoft based and must use some of the “well known” Microsoft ports in order to communicate with other Microsoft devices (PCs). Also note that the Muse is using a non-standard IP addressing scheme. These are Vendor standard IP addresses that predate Vista Imaging and the need to connect to the VA network. The Facility IT and Biomedical Engineering staff determined it would be more cost effective and secure to simply add a router between the Muse VLAN and the Muse server. The router uses only static routes and does not advertise the private 128.9.9.0 network. The facility adds a static route to 128.9.9.2, but does not redistribute it. Using this technique the local facility has access to the Muse system, but nothing outside the facility does. The following Cisco ACL protects GE Marquette Muse system from unwanted network traffic. This ACL may reside in the Core router or the Muse router.
  - a. ACL 142 is applied as an “out” filter
    - 1) Access-list 142 remark \*\*\* Muse ACL out \*\*\* rev 3-03-04 \*\*\* hh
    - 2) Access-list 142 permit tcp 10.255.0.0 0.0.127.255 host 128.9.9.2 eq 3351
    - 3) Access-list 142 permit tcp 10.255.0.0 0.0.127.255 host 128.9.9.2 eq 445

- 4) Access-list 142 permit tcp 10.255.0.0 0.0.127.255 host 128.9.9.2 eq 139
- 5) Access-list 142 permit udp 10.255.0.0 0.0.127.255 host 128.9.9.2 eq 137
- 6) Access-list 142 permit icmp 10.255.0.0 0.0.127.255 host 128.9.9.2
- 7) Access-list 142 permit ip 10.255.1.0 0.0.0.255 host 128.9.9.2
- 8) Access-list 142 deny ip any log-input
- 9) Interface vlan42
- 10) IP access-group 142 out

b. ACL 142 Descriptions

- 1) Remark statement to show purpose, date installed and author.
- 2) Allow TCP port 3351 access from any local device to the Muse Server (3351 is for data transfer).
- 3) Allow TCP port 445 access from any local device.
- 4) Allow TCP port 139 access from any local device.
- 5) Allow UDP port 139 access from any local device.
- 6) Allow ICMP access from any local device.
- 7) Allow access from Management Network devices.
- 8) Deny all other IP based traffic and log the denied packets.
- 9) Get “into” the router interface for VLAN 42. All subsequent commands apply only to VLAN 42.
- 10) Use ACL 142 to filter packets as they go out to VLAN 42.

Because only the incoming ports (in from the network but going out interface VLAN 42 to the medical devices) are well known, it is very difficult to tightly filter packets coming in from VLAN 42 and out to the rest of the network. An “in” ACL could only filter by source IP and the facility network range. Remember there are many other devices on the Muse private LAN. ACL 143 permits only the packets from the Muse server to access the facility LAN.

3. Example of Non-Domain Limited ACL (in):

a. ACL 143 is applied as an “in” filter.

- 1) Access-list 143 remark \*\*\* Muse ACL in \*\*\* rev 3-03-04 \*\*\* hh
- 2) Access-list 143 permit tcp host 128.9.9.2 10.255.0.0 0.0.127.255
- 3) Access-list 143 permit udp host 128.9.9.2 10.255.0.0 0.0.127.255 eq 137
- 4) Access-list 143 permit icmp host 128.9.9.2 10.255.0.0 0.0.127.255
- 5) Access-list 143 permit ip host 128.9.9.2 10.255.1.0 0.0.0.255
- 6) Access-list 143 deny ip any log-input
- 7) Interface vlan42
- 8) IP access-group 143 in

b. ACL 143 Descriptions

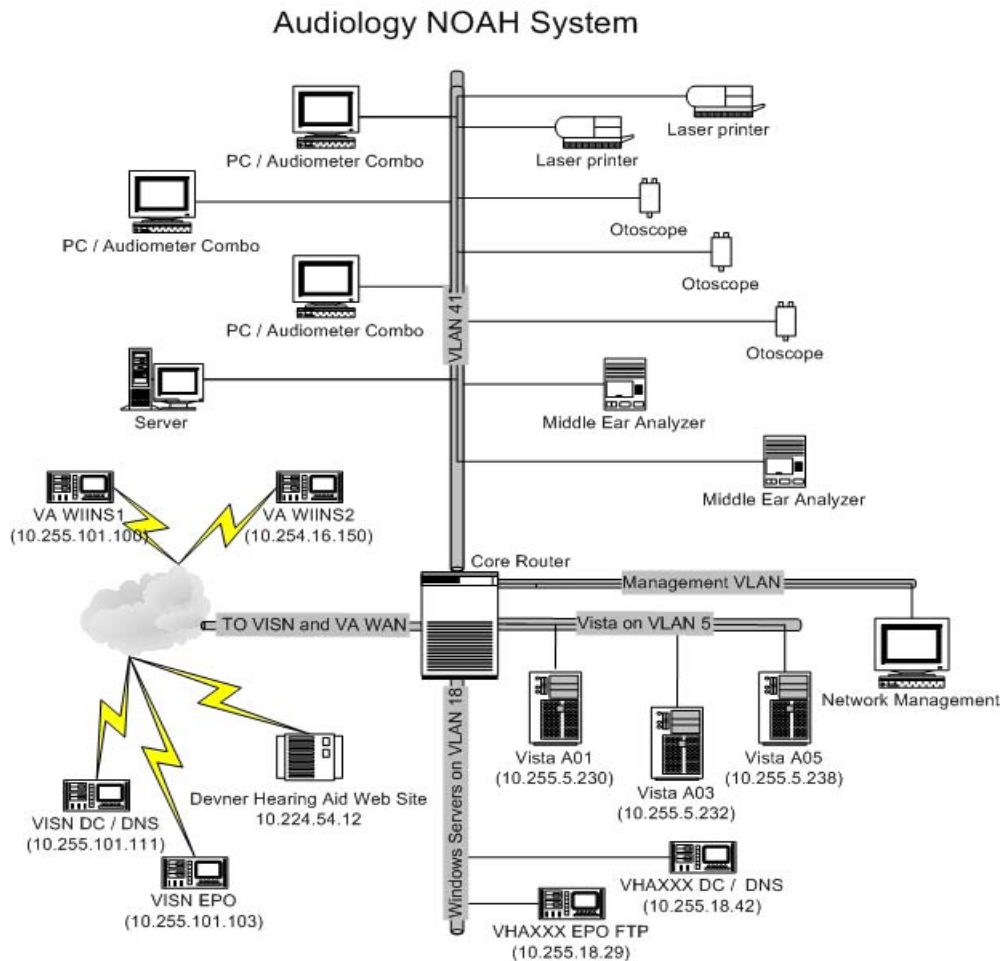
- 1) Remark statement to show purpose, date installed and author.
- 2) Allow TCP access from the Muse Server to any local device.
- 3) Allow UDP access from the Muse Server to any local device using port 137.
- 4) Allow ICMP access from the Muse Server to any local device.
- 5) Allow access to and from Management Network devices.
- 6) Deny all other IP based traffic and log the denied packets.
- 7) Get “into” the router interface for VLAN 42. All subsequent commands apply only to VLAN 42.

- 8) Use ACL 142 to filter packets as they enter interface VLAN42 on their way to the rest of the LAN.

### ***C. Domain Limited***

---

1. Sample Data for Domain Limited (Category 5):
  - a. Audiology NOAH System.
  - b. Hearing tests.
  - c. Yes.
  - d. Audiometer PCs communicate with:
    - Vista, 10.255.5.231 - 238 via TCP port 23 and 9200
    - Denver Web site 10.224.54.12 via TCP port 80
    - DNS servers 10.255.18.42 and 10.255.101.111 via UDP port 53
    - Domain Controllers 10.255.18.42 and 10.255.101.111 via TCP and UDP various
    - National WINS 10.255.101.100 and 10.254.150.16 via UDP 137
    - Microsoft Auto-Update Web sites via TCP 80
    - EPO console 10.255.101.103 initiates TCP traffic to agents via 30081 (ports are selected during install)
    - EPO agents initiate connections to EPO Server via TCP 8081 (ports are selected during install)
    - EPO agents initiate downloads from EPO FTP server 10.255.18.29 via TCP 20 and 21
  - e. PCs initiate connections to Vista, Denver Web site, and Auto-update.
    - Sessions are initiated in both directions between DNS, Domain Controllers, WINS, and EPO.
    - Net Management initiates sessions with Audiology systems for scanning and diagnostics.



2. Example of Domain Limited ACL (Out): The following Cisco ACL protects an Audiology NOAH system from unwanted network traffic while allowing it to function normally. In this case the Vendor and the local Biomedical Engineering shop are testing the feasibility of running auto-updates and allowing EPO to run on the PCs connected to the Audiometers. Both the Audiometers and the software on the PCs that drive them are FDA approved. The PCs are used to gather and report data from the Audiometers to a local Audiology server. They are also used to upload Audiograms into CPRS, answering consults and entering progress notes. Below is the ACL used to protect the Audiology VLAN. Again, the line numbers are not part of the ACL; instead, they are being used as a reference for the line-by-line description below the ACL.

a. ACL 144 is applied as an “out” filter

- 1) Access-list 144 remark \*\*\* AUDIOLOGY ACL, Domain Access out \*\*\* rev 1-13-04  
\*\*\* hh
- 2) Access-list 144 permit tcp 10.255.5.224 0.0.0.15 10.255.44.0 0.0.0.255
- 3) Access-list 144 permit ip host 10.255.18.42 10.255.44.0 0.0.0.255
- 4) Access-list 144 permit ip host 10.255.101.111 10.255.44.0 0.0.0.255
- 5) Access-list 144 permit ip host 10.255.18.31 10.255.44.0 0.0.0.255
- 6) Access-list 144 permit ip host 10.255.18.35 10.255.44.0 0.0.0.255
- 7) Access-list 144 permit tcp host 10.224.54.12 10.255.44.0 0.0.0.255

- 8) Access-list 144 permit ip 10.255.28.0 0.0.0.255 10.255.44.0 0.0.0.255
- 9) Access-list 144 permit udp host 10.255.101.100 10.255.44.0 0.0.0.255
- 10) Access-list 144 permit udp host 10.254.16.150 10.255.44.0 0.0.0.255
- 11) Access-list 144 permit ip host 10.255.101.103 10.255.44.0 0.0.0.255
- 12) Access-list 144 permit ip host 10.255.18.29 10.255.44.0 0.0.0.255
- 13) Access-list 144 permit tcp 207.46.0.0 0.0.255.255 10.255.44.0 0.0.0.255
- 14) Access-list 144 permit tcp 207.68.0.0 0.0.255.255 10.255.44.0 0.0.0.255
- 15) Access-list 144 permit tcp 209.245.0.0 0.0.255.255 10.255.44.0 0.0.0.255
- 16) Access-list 144 permit ip 10.255.0.0 0.0.1.255 10.255.44.0 0.0.0.255
- 17) Access-list 144 deny ip any log-input
- 18) Interface vlan44
- 19) IP access-group 144 out

#### b. ACL 144 Descriptions

- 1) Remark statement to show purpose, date installed and author.
- 2) Allow TCP access from Vista to VLAN 44.
- 3) Allow IP access from primary Domain Controller and DNS.
- 4) Allow IP access from secondary Domain Controller and DNS.
- 5) Allow IP access from Logon Script server #1 (generic server, could be Hercules).
- 6) Allow IP access from Logon Script server #2 (generic server, could be SMS or Stat Scanner).
- 7) Allow TCP access from vaww.ddc.oamm.va.gov, Audiology web site in Denver.
- 8) Allow IP access from network printers.
- 9) Allow UDP access from primary WINS.
- 10) Allow UDP access from secondary WINS.
- 11) Allow IP access from EPO Console.
- 12) Allow IP access from EPO FTP Server.
- 13) Allow TCP access from Microsoft Auto-Update network #1.
- 14) Allow TCP access from Microsoft Auto-Update network #2.
- 15) Allow TCP access from Microsoft Auto-Update network #3.
- 16) Allow IP access from Management Network devices.
- 17) Deny all other IP based traffic and log the denied packets.
- 18) Get "into" the router interface for VLAN 44. All subsequent commands apply only to VLAN 44.
- 19) Use ACL 144 to filter packets as they leave interface VLAN44 on their way to the Audiology devices.

### 3. Example of Domain Limited ACL (In)

#### a. ACL 145 is applied as an "in" filter

- 1) Access-list 145 remark \*\*\* AUDIOLOGY ACL, Domain Access in \*\*\* rev 1-13-04 \*\*\*  
hh
- 2) Access-list 145 permit tcp 10.255.44.0 0.0.0.255 10.255.5.224 0.0.0.15
- 3) Access-list 145 permit 10.255.44.0 0.0.0.255 ip host 10.255.18.42
- 4) Access-list 145 permit 10.255.44.0 0.0.0.255 ip host 10.255.101.111
- 5) Access-list 145 permit 10.255.44.0 0.0.0.255 ip host 10.255.18.31
- 6) Access-list 145 permit 10.255.44.0 0.0.0.255 ip host 10.255.18.35
- 7) Access-list 145 permit 10.255.44.0 0.0.0.255 tcp host 10.224.54.12
- 8) Access-list 145 permit ip 10.255.44.0 0.0.0.255 10.255.28.0 0.0.0.255
- 9) Access-list 145 permit udp 10.255.44.0 0.0.0.255 host 10.255.101.100

- 10) Access-list 145 permit udp 10.255.44.0 0.0.0.255 host 10.254.16.150
- 11) Access-list 145 permit ip 10.255.44.0 0.0.0.255 host 10.255.101.103
- 12) Access-list 145 permit ip 10.255.44.0 0.0.0.255 host 10.255.18.29
- 13) Access-list 145 permit tcp 10.255.44.0 0.0.0.255 207.46.0.0 0.0.255.255
- 14) Access-list 145 permit tcp 10.255.44.0 0.0.0.255 207.68.0.0 0.0.255.255
- 15) Access-list 145 permit tcp 10.255.44.0 0.0.0.255 209.245.0.0 0.0.255.255
- 16) Access-list 145 permit ip 10.255.44.0 0.0.0.255 10.255.0.0 0.0.1.255
- 17) Access-list 145 deny ip any log-input
- 18) Interface vlan44
- 19) IP access-group 145 in

b. ACL 145 Descriptions

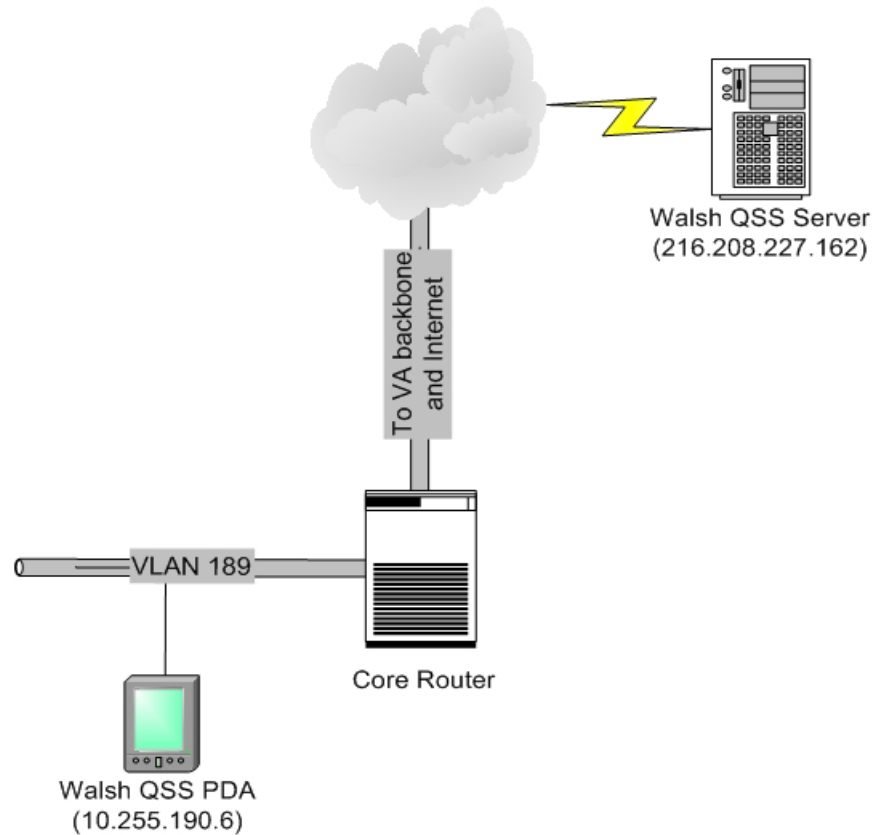
- 1) Remark statement to show purpose, date installed and author.
- 2) Allow TCP access from VLAN 44 to Vista.
- 3) Allow IP access to primary Domain Controller and DNS.
- 4) Allow IP access to secondary Domain Controller and DNS.
- 5) Allow IP access to Logon Script server #1 (generic server, could be Hercules).
- 6) Allow IP access to Logon Script server #2 (generic server, could be SMS or Stat Scanner).
- 7) Allow TCP access to vaww.ddc.oamm.va.gov, Audiology web site in Denver.
- 8) Allow IP access to network printers.
- 9) Allow UDP access to primary WINS.
- 10) Allow UDP access to secondary WINS.
- 11) Allow IP access to EPO Console.
- 12) Allow IP access to EPO FTP Server.
- 13) Allow TCP access to Microsoft Auto-Update network #1.
- 14) Allow TCP access to Microsoft Auto-Update network #2.
- 15) Allow TCP access to Microsoft Auto-Update network #3.
- 16) Allow IP access to Management Network devices.
- 17) Deny all other IP based traffic and log the denied packets.
- 18) Get “into” the router interface for VLAN 44. All subsequent commands apply only to VLAN 44.
- 19) Use ACL 145 to filter packets as they enter interface VLAN44 on their way to the rest of the LAN.

## ***D. Internet Only***

---

1. Sample Data for Internet Only (Category 6):
  - a. Walsh QSS System
  - b. Environmental Management QA System
  - c. IP
  - d. HTTP (80), HTTPS (443), FTP (20, 21)
  - e. The Walsh QSS PDA initiates an HTTP/HTTPS connection to the Walsh QSS web page. It also downloads software updates from this site via FTP.

## Walsh QSS System



2. Example of Internet Only (Out): The following ACL protects the VA network by allowing the Walsh QSS system to communicate only with one host IP address on the Internet.
  - a. ACL 190 is applied as an “out” filter
    - 1) Access-list 190 remark \*\*\* Walsh QSS System ACL \*\*\* rev 1-21-04 jrtda
    - 2) Access-list 190 permit tcp host 10.255.190.6 host 216.206.227.162
    - 3) Access-list 190 deny ip any log-input
    - 4) Interface vlan190
    - 5) IP access-group 190 out
  - b. ACL 190 Descriptions
    - 1) Remark statement to show purpose, date installed and author.
    - 2) Allow TCP access from the Walsh QSS PDA to their Web Server.
    - 3) Deny all other IP based traffic and log the denied packets.
    - 4) Get “into” the router interface for VLAN 190. All subsequent commands apply only to VLAN 190.
    - 5) Use ACL 190 to filter packets as they go out to VLAN 190 from the backbone of the core router.

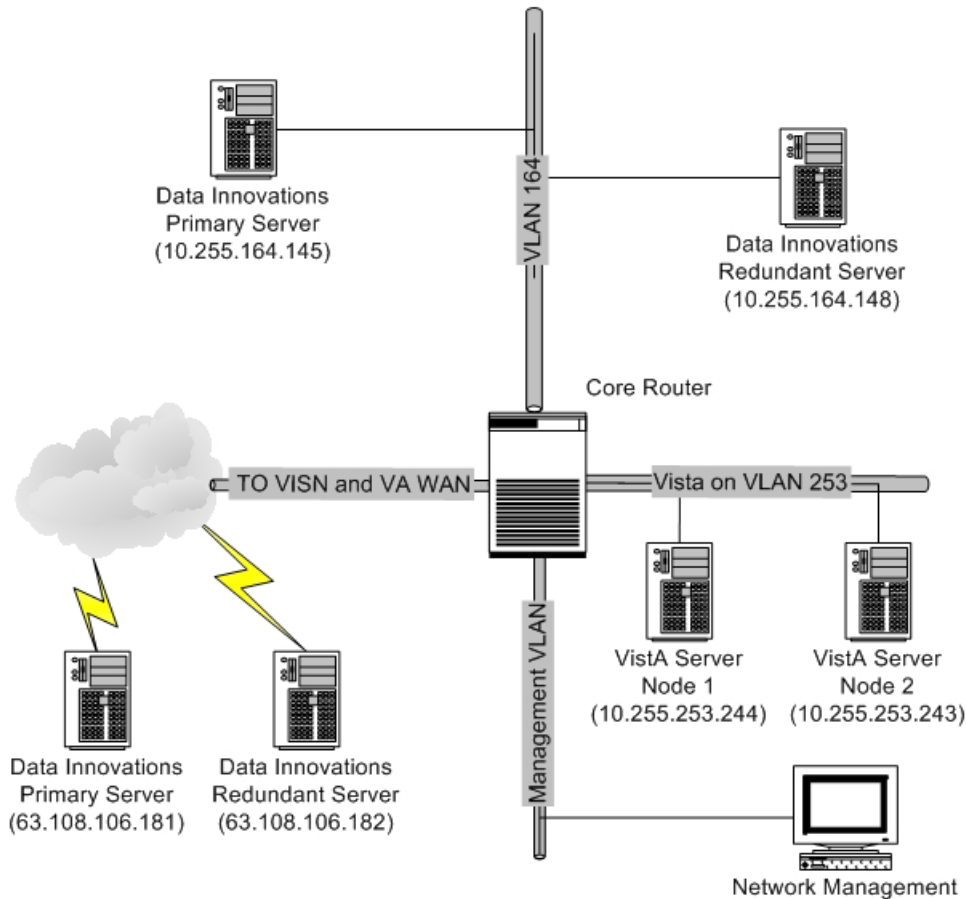
- c. ACL 191 is applied as an “in” filter. Note the source and destination IP addresses have changed places.
  - 1) Access-list 191 remark \*\*\* Walsh QSS System ACL \*\*\* rev 1-21-04 jrdta
  - 2) Access-list 191 permit tcp host 216.206.227.162 host 10.255.190.6
  - 3) Access-list 191 deny ip any log-input
  - 4) Interface vlan191
  - 5) IP access-group 191 in
  
- d. ACL 191 Descriptions
  - 1) Remark statement to show purpose, date installed and author.
  - 2) Allow TCP access from the Walsh Web Server to the QSS PDA.
  - 3) Deny all other IP based traffic and log the denied packets.
  - 4) Get “into” the router interface for VLAN 190. All subsequent commands apply only to VLAN 190.
  - 5) Use ACL 191 to filter packets as they enter interface VLAN 190 on their way to the rest of the network.

### ***E. Internet Restricted***

---

- 1. Sample Data for Internet Restricted (Category 7):
  - a. Data Innovations LAB Interface System
  - b. LAB Interface System
  - c. IP
  - d. Private TCP ports: 20073, 20074, 21073, 21074, 10010, 10011 and 10012
  - e. The Data Innovations System 10.255.164.145 and 148 initiates connections to the Quest contract LAB using LEDI-II (ports TCP 20073, 21073) and receives connects from the Quest contract lab using LEDI-II (ports TCP 20074, 21074). It also communicates with Vista 10.255.253.243 and 244 on HL7 port 10012 and receives connections from Vista on HL7 ports 10010 and 10011.

## Data Innovations System



2. Example of Internet Restricted (out): The following example has two different ACLs, one for incoming connections and one for outgoing connections. Having a tightly restricted ACL for each direction is only possible if the exact TCP/IP port numbers for each connection is known.
  - a. ACL 164 is applied for packets leaving interface VLAN164 and is applied as an “out” filter
    - 1) Access-list 164 remark \*\*\* Data Innovations System ACL out \*\*\* rev 1-21-04 jrtda
    - 2) Access-list 164 permit tcp host 10.255.164.145 host 63.108.106.181 eq 20073
    - 3) Access-list 164 permit tcp host 10.255.164.148 host 63.108.106.181 eq 21073
    - 4) Access-list 164 permit tcp host 10.255.164.145 host 63.108.106.182 eq 20073
    - 5) Access-list 164 permit tcp host 10.255.164.148 host 63.108.106.182 eq 21073
    - 6) Access-list 164 permit tcp host 10.255.164.145 host 10.255.253.244 eq 10012
    - 7) Access-list 164 permit tcp host 10.255.164.148 host 10.255.253.244 eq 10012
    - 8) Access-list 164 deny ip any log-input
    - 9) Interface vlan1164
    - 10) IP access-group 164 out
  - b. ACL 164 Descriptions
    - 1) Remark statement to show purpose, date installed and author.

- 2) Allow TCP access from the Primary Data Inn. LAB LSI to the Quest Primary server on port 20073.
- 3) Allow TCP access from the Redundant Data Inn. LAB LSI to the Quest Primary server on port 21073.
- 4) Allow TCP access from the Primary Data Inn. LAB LSI to the Quest Test server on port 20073.
- 5) Allow TCP access from the Redundant Data Inn. LAB LSI to the Quest Test server on port 21073.
- 6) Allow TCP access from the Primary Data Inn. LAB LSI to Vista node 1 on port 10012.
- 7) Allow TCP access from the Redundant Data Inn. LAB LSI to Vista node 2 on port 10012.
- 8) Deny all other IP based traffic and log the denied packets.
- 9) Get “into” the router interface for VLAN 164. All subsequent commands apply only to VLAN 164.
- 10) Use ACL 164 to filter packets as they go out to VLAN 164.

### 3. Example of Internet Restricted: (in)

- a. ACL 165 is applied to filter packets entering Interface VLAN164 and is applied as an “in” filter

- 1) Access-list 165 remark \*\*\* Data Innovations System ACL in \*\*\* rev 1-21-04 jrda.
- 2) Access-list 165 permit tcp host 63.108.106.181 host 10.255.164.145 eq 20074.
- 3) Access-list 165 permit tcp host 63.108.161.181 host 10.255.164.148 eq 20074.
- 4) Access-list 165 permit tcp host 63.108.106.182 host 10.255.164.145 eq 21074.
- 5) Access-list 165 permit tcp host 63.108.106.182 host 10.255.164.148 eq 21074.
- 6) Access-list 165 permit tcp host 10.255.253.244 host 10.255.164.145 range 10010 10011.
- 7) Access-list 165 permit tcp host 10.255.253.243 host 10.255.164.145 range 10010 10011.
- 8) Access-list 165 permit tcp host 10.255.253.244 host 10.255.164.148 range 10010 10011.
- 9) Access-list 165 permit tcp host 10.255.253.243 host 10.255.164.148 range 10010 10011.
- 10) Access-list 165 deny ip any log-input.
- 11) Interface vlan1164.
- 12) IP access-group 165 in.

- b. ACL 165 Descriptions

- 1) Remark statement to show purpose, date installed and author.
- 2) Allow TCP access from the Quest P server to the Data Inn. server on port 20074.
- 3) Allow TCP access from the Test Quest server to the Redundant Data Inn. server on port 20074.
- 4) Allow TCP access from the Quest P server to the Data Inn. server on port 21074.
- 5) Allow TCP access from the Quest T server to the Redundant Data Inn. server on port 21074.
- 6) Allow TCP access from Vista node 1 to the Primary Data Inn. server on ports 10010 and 10011.
- 7) Allow TCP access from Vista node 1 to the Redundant Data Inn. server on ports 10010 and 10011.
- 8) Allow TCP access from Vista node 2 to the Primary Data Inn. server on ports 10010 and 10011.
- 9) Allow TCP access from Vista node 2 to the Redundant Data Inn. server on ports 10010 and 10011.
- 10) Deny all other IP based traffic and log the denied packets.

- 11) Get “into” the router interface for VLAN 164. All subsequent commands apply only to VLAN 164.
- 12) Use ACL 165 to filter packets as they enter interface VLAN 164 and go to the rest of the LAN.



---

## *Glossary*

---

<b>ACL</b>	Access Control List. This is a filtering mechanism used to allow or disallow network packets. Packets can be filtered by protocol, source, destination or port number.
<b>DDP</b>	Distributed Data Protocol. A proprietary communications protocol developed by Digital Equipment Corporation (DEC) for host-to-host communications.
<b>DNS</b>	Domain Naming System. The DNS is a distributed database system for translating computer names and vice-versa. DNS allows you to use the internet without having to remember long lists of numbers. On TCP/IP networks, the DNS provides IP address translation for a given computer's domain name or Uniform Resource Locator (URL).
<b>Firewall</b>	A system or systems that enforce a boundary between two or more networks. Most firewalls limit the data allowed between networks by protocol, type, source, destination, port number or a combination of two or more of these decision factors.
<b>HOST File</b>	The name of a text file found on Unix-based systems that contains the name and IP address of other computers on the network. This is like a built-in local DNS.
<b>ICMP</b>	Internet Control Message Protocol. A Layer 3 protocol that provides error reporting and diagnostic functions. This is what PING and TRACE(RT) use.
<b>IOS</b>	Internetwork Operating System. The primary operating system on Cisco routers and switches.
<b>IP</b>	Internet Protocol. This protocol is made up of three primary components: TCP, UDP and ICMP. Like it says, the Internet (and the VA network) is based on IP.
<b>LAT</b>	Local Area Transport. A proprietary communications protocol developed by Digital Equipment Corporation (DEC) for terminal-to-host communications.
<b>Layer 2</b>	The second layer in the OSI networking model. It is officially called the Data Link Layer. The MAC address of a device is its Layer 2 address. Layer 2 moves data from one device to another.
<b>Layer 3</b>	The third layer in the OSI network model. It is officially called the Network Layer. The IP number is a device's Layer 3 address. Layer 3 moves data from one network to another.
<b>LMHost File</b>	The name of a text file found on Microsoft-based systems that contains the Windows Network name and IP address of other computers on the network. This is like a built-in local DNS.

<b>MAC</b>	Media Access Control. The MAC is layer two of the seven layer Open System Interconnection (OSI) network model.
<b>NIC</b>	Network Interface Card. The hardware that connects a device to a network.
<b>PING</b>	Packet InterNet Groper. A very common program used to test whether or not a system is accessible. PING is useful for network diagnostics.
<b>PIX</b>	Private Internet eXchange. The generic term for the Cisco family of firewalls.
<b>Port</b>	Logical points of connection in the TCP/IP protocol suite. Commonly used ports are called “well-known.” Examples of well-known ports are port 80 for HTTP (www) and port 25 for SMTP (mail).
<b>System</b>	A collection of devices working together to accomplish a certain task.
<b>TCP</b>	Transmission Control Protocol. This is a connection-oriented, end-to-end protocol that provides reliable, sequenced and unduplicated data delivery across a network. TCP operates at Layers 4 and 5 of the OSI model. Telnet and FTP are examples of TCP connections.
<b>UDP</b>	User Datagram Protocol. This is a connectionless protocol that is less reliable than TCP. UDP operates at Layer 4 of the OSI model. TFTP and SNMP are examples of UDP protocols.
<b>VLAN</b>	Virtual Local Area Network. A method of separating network devices into different logical segments without regard to their physical location.
<b>WINS</b>	Windows Internet Name Service. A name resolution service that resolves Windows network computer names to IP addresses in a routed environment. A WINS server, which is a Windows NT Server computer, handles name registrations, queries and releases.