WHITE PAPER: IRONSHIELD BEST PRACTICES MANAGEMENT VLANS

Written By: Philip Kwan

April 2003

April 2003
Version 1.0.0

Summary

The IronShield Best Practices: Management VLANs document is designed to help network and security administrators understand how to implement Foundry Management VLANs. The document gives the reasons why the Management VLANs are required to fully secure the network infrastructure devices and how to best implement them to compliment existing security strategies. This paper complements the *Foundry IronShield Best Practices: Hardening Foundry Routers and Switches* document.

IronShield Security is not meant to replace Data Security infrastructures. With careful planning and implementation, IronShield Security features can help improve Network Security and enhance Data Security where it's needed.

Contents

Introduction

Foundry's IronShield Security "Best Practices" papers serves as a guide to assist network and security designers in architecting and applying Foundry security features in their networks. Modern enterprise security is applied in layers – Defense in Depth. Consideration must be given to all the various layers with a full understanding of what threats are possible at each layer before implementing a defense strategy. By applying security in multiple layers, the defense is strengthened and vulnerabilities in one layer will not likely lead to successful attacks of corporate resources. The goal is to make it harder to attack your network by layering security chokepoints.

These practices should accompany your Security and Computer Usage Policies, not replace them. Applying the steps outlined in this "Best Practices" guide does not guarantee that attacks will not be successful against your security defenses and network resources. The best security design is dynamic. It must be coupled with a strong security policy, proactive network monitoring, diligent network and security staff that are working to stay on top of security alerts and system software upgrades and patches. Enterprise data security is always changing and growing with the advent of new security threats. Thorough, rigorous, and continuous inspection of all security components and processes will help you keep on top of the enterprise network.

IronShield Security documents are specifically written to work with Foundry products and work in conjunction with related Foundry documentation. Reference to other Foundry documentation is made with regards to command syntax and general feature information.

This Best Practices White Paper is designed to help network and security administrators understand how to implement Foundry Management VLANs. It identifies the strengths of management VLANs and how they can be part of your enterprise's strategy for hardening your network infrastructure devices. This paper complements the *Foundry IronShield Best Practices: Hardening Foundry Routers and Switches* document.

Audience

IronShield Security "Best Practices" papers are designed to help the personnel responsible for designing and configuring the network and security components of an enterprise network. The topics discussed are at an intermediate to advanced level and assumes a good understanding of TCP/IP and related technologies.

Nomenclature

This guide uses the following typographical conventions to show information:

Italic highlights the title of another publication and occasionally emphasizes a word or phrase.

Bold highlights a CLI command.

Bold Italic highlights a term that is being defined.

Underline highlights a link on the Web management interface.

Capitals highlights field names and buttons that appear in the Web management interface.

NOTE: A note emphasizes an important fact or calls your attention to a dependency.

Related Publications

The following Foundry Networks documents supplement the information in this guide.

Foundry Security Guide - provides procedures for securing management access to Foundry devices and for protecting against Denial of Service (DoS) attacks.

Foundry Switch and Router Command Line Interface Reference - provides a list and syntax information for all the Layer 2 Switch and Layer 3 Switch CLI commands.

Foundry Diagnostic Guide - provides descriptions of diagnostic commands that can help you diagnose and solve issues on Layer 2 Switches and Layer 3 Switches.

IronShield Best Practices: Hardening Foundry Routers and Switches – provides a detailed explanation of how Foundry devices can be protected from authorized access and other security related issues.

IronShield Best Practices: Enhancing Internal Network Security – provides a detailed explanation of how to implement Foundry IronShield Security features to harden internal network infrastructures.

Device Management

Foundry switches can be managed locally with a direct serial connection through the console port or through remote methods such as telnet, SSH, HTTP Web, TFTP, and SNMP. Direct access through a console port is the most secure, but is the least convenient as physical access to the device is required. With remote management, convenience is greatly enhanced but security is often sacrificed. Foundry Management VLANs can help secure remote management of Foundry switches and routers by removing the management IP address from the regular data VLANs or subnets and placing them into secure "out-of-band" VLANs to which only authorized personnel have access.

By default, all ports on a Foundry switch belong to the default VLAN and when a management IP address is assigned to the Foundry switch, it is accessible by all ports belonging to the default VLAN. The advantage of having the switch's management IP address in the default VLAN is accessibility. Remote administration of the switch is possible from many users on an enterprise-wide perspective. The disadvantage of having the switch's management IP address in the default VLAN is the possibility of unauthorized access, Denial of Service attacks, and malicious intent against the network device.

Remote Administration Concerns

Any method of remotely connecting to Foundry devices automatically exposes the device to some level of risk. Common remote access methods used to manage Foundry devices include Telnet, SSH, and Web management. Each of these methods has its strengths and weaknesses. Many remote administration-hardening techniques are discussed in the *IronShield Best Practices: Hardening Foundry Routers and Switches* document.

Some of the most common concerns associated with remote access include:

Management Station IP Address Spoofing	The management station's IP address can be spoofed with Spoofing crafted packets that fake the source IP address of the management station. The intruder hopes to fool any address restriction rules on the device to gain access.
Password Attacks	Hackers attempting to gain access to network devices can use brute-force type of applications to try to break simple password controls. By default, many routers and switches do not limit the number of unsuccessful logon attempts and do not log the unsuccessful entries.
Password Sniffing	There are many "sniffer" applications that are freely available on the Internet, which may be used to capture packets traveling across the network. A simple feature of these applications is to capture packets based on signatures within the packet – such as the words login or password. This poses significant risks when using unencrypted remote control methods to access network devices.
Session Hijacking	Session hijacking occurs when a hacker uses tools to take over your TCP connection to the device to which you are authenticated. The hacker sends jamming packets to your management workstation and configures their management host to assume your IP address.
Authentication Server Compromise	Authentication methods which use third-party authentication servers such as TACACS, TACACS+, and RADIUS are at risk if the authentication server can be

	compromised by an attacker and the authentication database manipulated. Passwords can be changed and unauthorized accounts can be added to gain access.
Dial-In Access	For security purposes, Foundry does not recommend the direct connection of an analog modem to the device's console port. It is better to dial into a secure Remote Access Server that uses strong authentication and then access the device using a secure management protocol such as SSH. Analog modems do not support strong authentication or encryption.

Defending Foundry Devices

The strongest defense strategy that can be used to secure Foundry devices from unauthorized access, hacking attempts, and malicious intent is through a combination of hardening techniques. Depending on the level of security required, a layering approach can be used to achieve maximum hardening of the management topology and the Foundry devices. Examples of hardening techniques include:

- Physically securing the network devices to prevent unauthorized access. Switches and routers should be in locked network rooms with the proper access restrictions and environmental conditions.
- Placing switches and routers in Management VLANs to isolate network devices' management IP addresses.
- Restricting management access through:
  - Access Control Lists (ACLs)
  - Management station IP addresses
  - VLAN ID
- Governing management access through:
  - User accounts and privilege levels
  - AAA servers such as TACACS+ and RADIUS
- Disabling unused management services such as Web, Telnet, SNMP, etc.
- Using external Syslog servers to capture and coordinate events and logs for auditing.
- Synchronizing time on network devices for central log coordination.

NOTE: For more information on device hardening techniques for Foundry devices, please refer to the *IronShield Best Practices: Hardening Foundry Routers and Switches* document or the *Foundry Security Guide*.

Port-Based VLANs

A Layer 2 port-based VLAN is a subset of ports on a Foundry device that has its own broadcast domain. By default, all ports on a Foundry switch belong to the default VLAN (VLAN 1) and share a single Layer 2 broadcast domain. As new port-based VLANs are created, the ports are removed from the default VLAN and moved into the new port-based VLAN. Port-based VLANs are logically separated from each other and is considered the most secure of all VLAN types.

A port can belong to only one port-based VLAN, unless 802.1q tagging is applied to the port. 802.1q tagging uses a four-byte tag field on each packet transmitted from the port to identify the VLAN ID and allows the VLAN to span multiple devices. Each Layer 2 VLAN runs its own separate instance of the Spanning Tree Protocol (STP) and all Layer 2 traffic is bridged within the port-based VLAN supporting a single broadcast domain.

Management VLANs

A Management VLAN is a port-based VLAN that is used to isolate the management IP address of the Foundry switch – creating an "out-of-band" network for management purposes. By isolating the Foundry switch's management IP address from the normal data traffic, access by unauthorized users and malicious attacks from the general user population can be eliminated. The management stations are placed in the management VLAN to allow them access to the Foundry switches and to protect the management stations from external threats and attacks.

There are several ways to create management VLANs:

- Using untagged port-based VLANs
- Using tagged port-based VLANs
- Using Virtual Ethernet interfaces on Foundry Routers to span management VLANs

The most isolated form of management VLAN is the untagged port-based VLAN. This type of management VLAN does not use VLAN tagging and has dedicated uplink connections between the management VLANs defined on each switch. This model works well for installations that have their switches concentrated in one secure area, where physical cable plants are available to connect the management VLANs together and distance limitations are not an issue.

Many installations have switches distributed throughout the enterprise, in multiple network wiring closets, buildings and campuses. With this model, setting up separate management planes with dedicated untagged port-based VLANs may not be possible and tagged port-based VLANs must be used. For large enterprises with multiple management VLANs, routers can be used to route or bridge management traffic between management VLANs and control access.

The Default-VLAN-ID Command

Foundry devices use VLAN ID 1 as the default VLAN and all ports are originally part of this VLAN until they are removed and placed in another VLAN. For installations that require the Management VLAN or some pre-existing VLAN to be VLAN 1, Foundry devices can change their default VLAN ID from 1 to any other ***unused VLAN ID*** between 2 and 4095. This can be quickly accomplished with the **default-vlan-id** command.

Syntax: default-vlan-id <new vlan-id>

The Management-VLAN Command

The **management-vlan** command is used to configure the Foundry switch to use a particular port-based VLAN as the management VLAN. When a port-based VLAN is configured with the **management-vlan** command, the device's management IP address is associated only with the ports in the designated VLAN. All management stations must be connected to one of the ports belonging to the management VLAN in order to establish a remote session with the switch.

Syntax: [no] management-vlan

Untagged Management VLAN Example

The following illustration in Figure 1 shows how untagged port-based VLANs can be used to create a simple management VLAN topology. In this example, the three switches are installed within 100 meters of each other and there is an existing cable plant with the sufficient cable runs between the three switches. A dedicated management VLAN (VLAN 10) is created on each switch and ports 8/21 to 8/24 are untagged members of VLAN 10. By taking these ports out of the Default VLAN and placing them into port-based VLAN 10, they are completely isolated from all the other ports and data traffic.

Dedicated CAT 5e cables are used to connect the three separate VLAN 10's together to form an insolated broadcast domain that will serve as the Management VLAN. The switches are given management IP addresses that belong to the management VLAN and the management stations are made members of the management VLAN by connecting them to the ports belonging to VLAN 10. They are assigned IP addresses that are part of the management VLAN's subnet range (192.168.1.0/24).

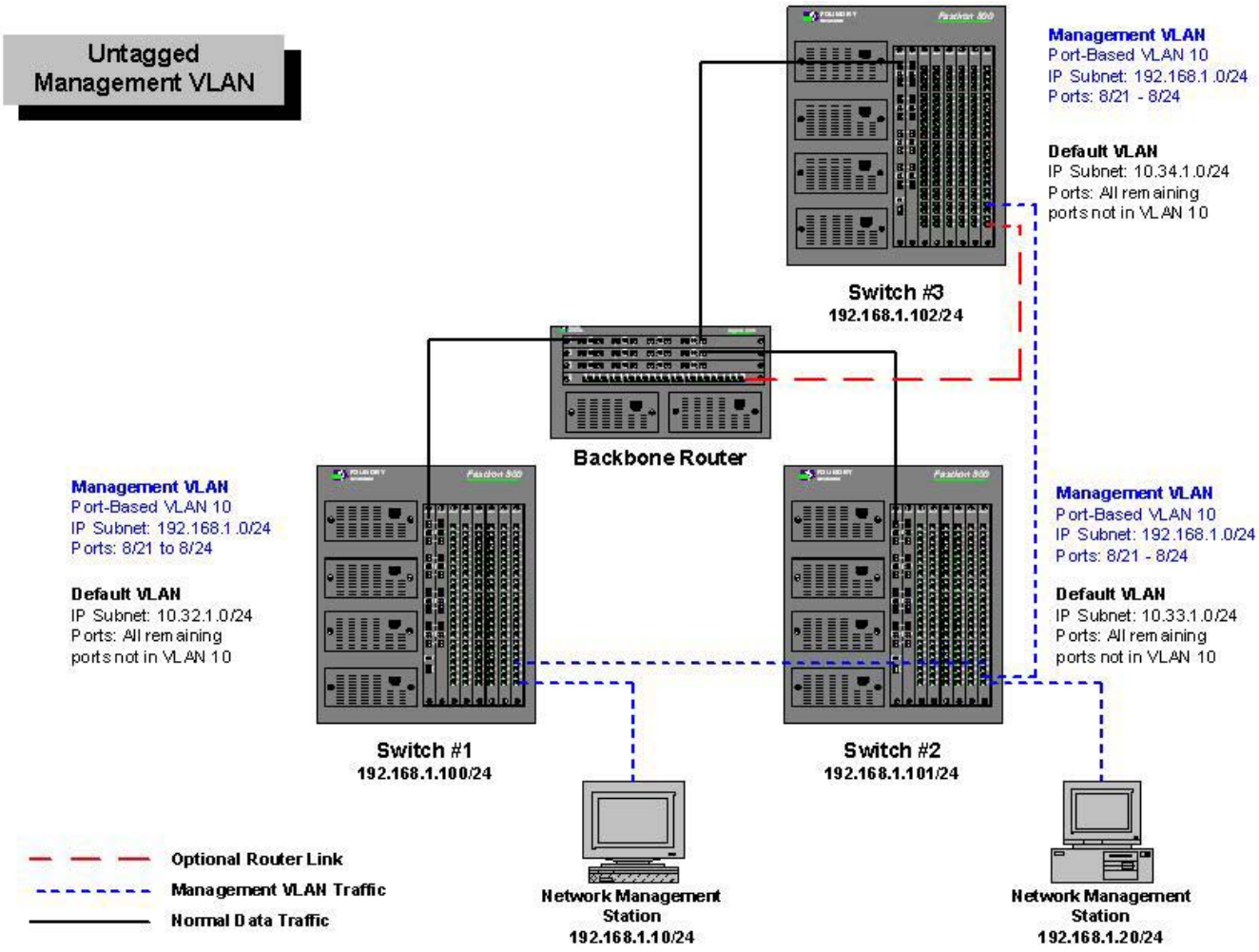

Figure 1. Untagged Management VLAN Example

The advantages of using an Untagged Management VLAN include:

- Extremely secure, all ports are dedicated to management VLAN.
- Simple topology, easy to build and trouble shoot.

The disadvantages of using an Untagged Management VLAN include:

- Scalability - limited to centralized network wiring closets.
- Requires additional uplink ports and cable plant.
- May limit location of management stations.

Setup Procedure

To create a simple Untagged Management VLAN, each switch will require the following configuration steps:

Step 1: Assign a management IP address to each switch.

```
Dept_Switch-1(config)# ip address 192.168.1.100/24
Dept_Switch-1(config)# write memory
```

Step 2: Create a port-based VLAN on each switch, add the necessary untagged ports, and designate the VLAN as the management VLAN.

To create the port-based VLAN: **Syntax:** vlan <vlan-id> by port

To add ports: **Syntax:** untagged ethernet | pos <portnum> [to <portnum> | ethernet <portnum>]

To turn on Spanning Tree Protocol: **Syntax:** [no] spanning-tree

To designate the management VLAN: **Syntax:** [no] management-vlan

EXAMPLE
To create the port-based VLAN used in Switch #1, enter the following:

```
Dept_Switch-1(config)# vlan 10 by port
Dept_Switch-1(config-vlan-10)# untagged eth 8/21 to 8/24
Dept_Switch-1(config-vlan-10)# spanning-tree
Dept_Switch-1(config-vlan-10)# management-vlan
Dept_Switch-1(config-vlan-10)# exit
Dept_Switch-1(config)# write memory
```

The ports specified in the **untagged** command will be removed from the default VLAN and placed in VLAN 10. All remaining ports are left in the default VLAN. The **management-vlan** command will designate this port-based VLAN as the management VLAN and will associate the switch's management IP address with the VLAN. Although this example reserved 4 ports for its management VLAN, your installation's requirements may vary and you can add as many ports as needed to support your management stations. Remember to disable any unused ports to prevent unauthorized access.

Step 3: Connect the management VLAN defined on each switch to each other with the necessary cables.

Step 4: Connect the management stations to the management VLAN ports and assign them the necessary IP address, subnet mask, and default gateway information.

Step 5 (optional): If external access is required for the management stations, setup a router port to support the management VLAN. ACLs should be used to deny access into the management VLAN from all other corporate subnets and only permit "established" TCP connections back into the management VLAN to prevent sessions originating from outside the management VLAN.

Depending on each installation's security needs, these ACLs can vary significantly. Another way to secure the management VLAN is to use a firewall in between the management VLAN and the regular data subnets.

Router Port ACL Example:
The following allows "established" TCP traffic from the Internet or the 10.0.0.0/8 networks to return only to the two management stations and denies all other traffic. With careful planning of the management VLAN's subnet range(s), the complexity of the ACLs can be very simple. In this example, the regular data subnets used for all non-management traffic were on 10.0.0.0/8 subnet ranges and all management traffic was isolated to the 192.168.1.0/24 subnet. These ACLs should not replace firewall rules that can also be used to protect the management VLAN.

On Switch #3, define the inbound ACL by entering:

```
Dept_Switch-3(config)# access-list 115 permit tcp any host 192.168.1.10 established
Dept_Switch-3(config)# access-list 115 permit tcp any host 192.168.1.20 established
Dept_Switch-3(config)# access-list 115 deny ip any any
```

Apply the inbound ACL to the port that connects to the router.

```
Dept_Switch-3(config)# interface E8/24
Dept_Switch-3(config-if-8/24)# ip access-group 115 in
Dept_Switch-3(config-if-8/24)# write memory
```

Step 6: Layer additional switch hardening features to restrict access to the authorized management stations and create the necessary user accounts and policies to govern access. This will prevent unauthorized access by illegal management stations if they were able to gain physical access to the management VLAN.

Examples of additional defenses include:

- Restricting management access through:
  - Access Control Lists (ACLs)
  - Management station IP addresses
  - VLAN ID
- Governing management access through:
  - User accounts and privilege levels
  - AAA servers such as TACACS+ and RADIUS
- Disabling unused management services such as Web, Telnet, SNMP, etc.
- Using external Syslog servers to capture and coordinate events and logs for auditing

NOTE: The **telnet-client**, **web-client**, and **snmp-client** commands should also be considered as additional hardening techniques for Foundry devices. For more information on device hardening techniques, please refer to the *IronShield Best Practices: Hardening Foundry Routers and Switches* document or the *Foundry Security Guide*.

Tagged Management VLAN Example

The following illustration in Figure 2 shows how 802.1q tagged VLANs can be used to create a management VLAN to isolate management traffic from regular data traffic. In this example, there are three switches connected together with trunked 2 GB uplinks to form the 10.96.0.0/16 subnet and there is no extra fiber runs between the switches to allow for a dedicated untagged management VLAN to be created.

Four ports (E8/21 to E8/24) were removed from the default VLAN on each switch to form the management VLAN. These four ports were added to the VLAN as untagged ports. To link the VLANs together from each switch, the uplink ports on each switch were added to the management VLAN as tagged ports. The switches are given management IP addresses that belong to the management VLAN and the management stations are made members of the management VLAN by connecting them to the ports belonging to VLAN 10. All management stations are assigned IP addresses that are part of the management VLAN subnet range (192.168.1.0/24).

The remaining ports were removed from the default VLAN and placed into a newly created port-based VLAN to allow the uplink port to be used as a tagged interface in the management VLAN.

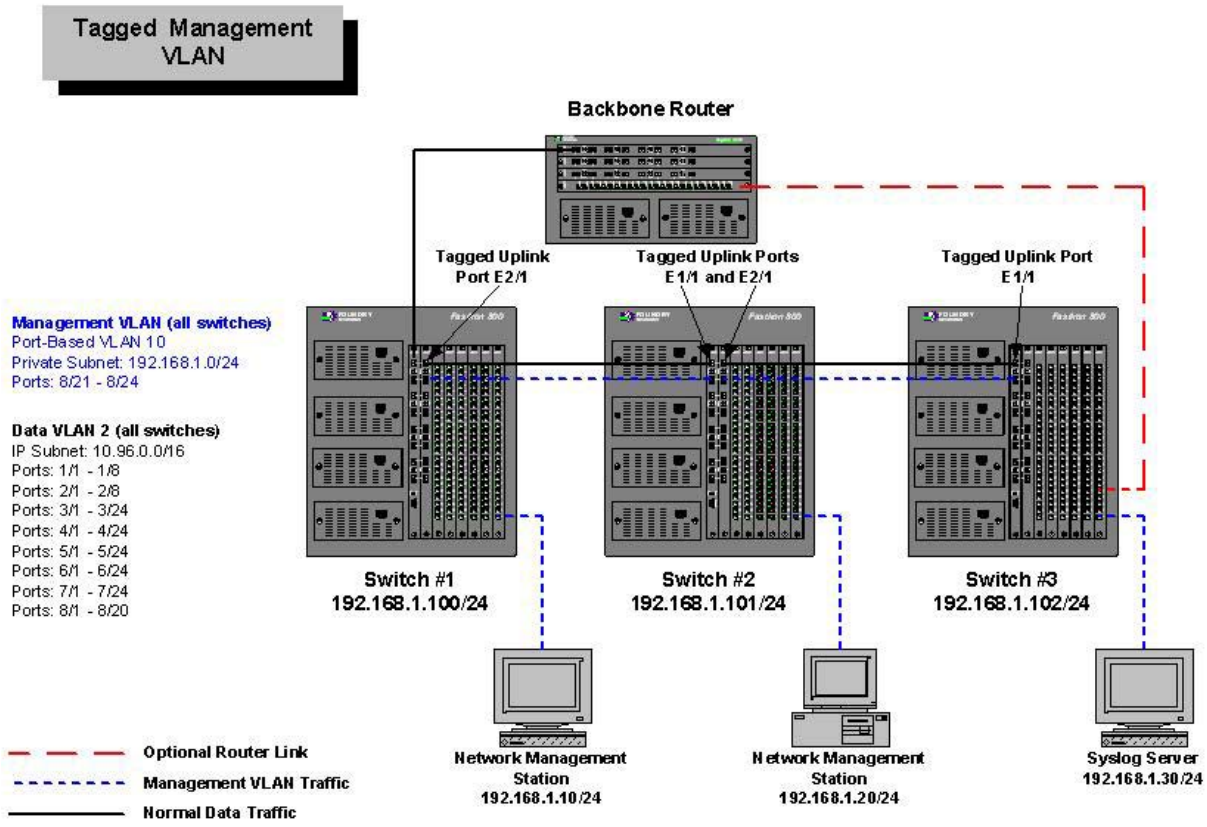

Figure 2. Tagged Management VLAN Example

The advantages of using a Tagged Management VLAN include:

- Traffic is physically secure as all ports are dedicated to management VLAN and tagged between switches.
- No additional cables or uplink ports are required to connect to each management VLAN.
- Provides scalability and allows switches in distributed network wiring closets to be managed through a single management VLAN.

The disadvantages of using a Tagged Management VLAN include:

- Management traffic is shared with regular data traffic as it traverses the uplink ports. Management traffic may not be guaranteed under extreme peak traffic loads.
- Possibility of management traffic being intercepted by an unauthorized user (if monitoring or sniffing the uplink is possible).

Setup Procedure

To create a Tagged Management VLAN, each switch will require the following configuration steps:

Step 1: Assign a management IP address to each switch.

```
Dept_Switch-1(config)# ip address 192.168.1.100/24
Dept_Switch-1(config)# write memory
```

Step 2: Create a port-based VLAN on each switch, add the necessary untagged and tagged ports, and designate it as the management VLAN. The untagged ports will be the ports dedicated to the management stations and the tagged port(s) will be the uplink port.

To create the port-based VLAN: **Syntax:** vlan <vlan-id> by port

To add ports: **Syntax:** untagged ethernet | pos <portnum> [to <portnum> | ethernet <portnum>]
Syntax: tagged ethernet | pos <portnum> [to <portnum> | ethernet <portnum>]

To turn on Spanning Tree Protocol: **Syntax:** [no] spanning-tree

To designate the management VLAN: **Syntax:** [no] management-vlan

EXAMPLE
To create the port-based VLAN used in Switch #1, enter the following:

```
Dept_Switch-1(config)# vlan 10 name Mgmt-VLAN by port
Dept_Switch-1(config-vlan-10)# untagged eth 8/21 to 8/24
Dept_Switch-1(config-vlan-10)# tagged eth 2/1
Dept_Switch-1(config-vlan-10)# spanning-tree
Dept_Switch-1(config-vlan-10)# management-vlan
Dept_Switch-1(config-vlan-10)# exit
Dept_Switch-1(config)# write memory
```

To create the port-based VLAN used in Switch #2, enter the following:

```
Dept_Switch-2(config)# vlan 10 by port
Dept_Switch-2(config-vlan-10)# untagged eth 8/21 to 8/24
Dept_Switch-2(config-vlan-10)# tagged eth 1/1 eth 2/1
Dept_Switch-2(config-vlan-10)# spanning-tree
Dept_Switch-2(config-vlan-10)# management-vlan
Dept_Switch-2(config-vlan-10)# exit
Dept_Switch-2(config)# write memory
```

To create the port-based VLAN used in Switch #3, enter the following:

```
Dept_Switch-3(config)# vlan 10 by port
Dept_Switch-3(config-vlan-10)# untagged eth 8/21 to 8/24
Dept_Switch-3(config-vlan-10)# tagged eth 1/1
Dept_Switch-3(config-vlan-10)# spanning-tree
Dept_Switch-3(config-vlan-10)# management-vlan
Dept_Switch-3(config-vlan-10)# exit
Dept_Switch-3(config)# write memory
```

The ports specified in the **untagged** command will be removed from the default VLAN and placed in VLAN 10. All remaining ports are left in the default VLAN. The uplink ports specified in the **tagged** command will allow the traffic from the management VLAN to traverse the switches. The **management-vlan** command will designate this port-based VLAN as the management VLAN and will associate the switch's management IP address with the VLAN.

Step 3: Foundry FastIron, BigIron, and NetIron devices will not permit a tagged port to belong to the Default VLAN for security reasons. The remaining ports in the Default VLAN must be transferred to a new port-based VLAN to allow the shared uplink port(s) to be tagged on multiple port-based VLANs.

EXAMPLE
To create a new port-based VLAN on Switch #1 and transfer the remaining Default VLAN ports:

```
Dept_Switch-1(config)# vlan 2 name Normal-Data-VLAN by port
Dept_Switch-1(config-vlan-2)# untagged eth 1/1 to 8/20
Dept_Switch-1(config-vlan-2)# tagged eth 2/1
Dept_Switch-1(config-vlan-2)# spanning-tree
Dept_Switch-1(config-vlan-2)# exit
Dept_Switch-1(config)# write memory
```

To create a new port-based VLAN on Switch #2 and transfer the remaining Default VLAN ports:

```
Dept_Switch-2(config)# vlan 2 name Normal-Data-VLAN by port
Dept_Switch-2(config-vlan-2)# untagged eth 1/1 to 8/20
Dept_Switch-2(config-vlan-2)# tagged eth 1/1 eth 2/1
Dept_Switch-2(config-vlan-2)# spanning-tree
Dept_Switch-2(config-vlan-2)# exit
Dept_Switch-2(config)# write memory
```

To create a new port-based VLAN on Switch #3 and transfer the remaining Default VLAN ports:

```
Dept_Switch-3(config)# vlan 2 name Normal-Data-VLAN by port
Dept_Switch-3(config-vlan-2)# untagged eth 1/1 to 8/20
Dept_Switch-3(config-vlan-2)# tagged eth 1/1
Dept_Switch-3(config-vlan-2)# spanning-tree
Dept_Switch-3(config-vlan-2)# exit
Dept_Switch-3(config)# write memory
```

Step 4: Connect the management stations to the management VLAN ports and assign them the necessary IP address, subnet mask, and gateway address (if necessary).

Step 5 (optional): If external access is required for the management stations, setup a router port to support the management VLAN. ACLs should be used to deny access into the management VLAN from all other corporate subnets and only permit "established" TCP connections back into the management VLAN to prevent sessions originating from outside the management VLAN. For additional security, a firewall can be used to regulate traffic between the management VLAN and the other subnets.

See the previous example for an example of a router ACL that can be used to restrict access into the management VLAN.

Step 6: Layer additional switch hardening features to restrict access to the authorized management stations and create the necessary user accounts and policies to govern access. This will prevent unauthorized access by illegal management stations if they were able to gain physical access to the management VLAN.

Examples of additional defenses include:

- Restricting management access through:
  - Access Control Lists (ACLs)
  - Management station IP addresses
  - VLAN ID
- Governing management access through:
  - User accounts and privilege levels
  - AAA servers such as TACACS+ and RADIUS
- Disabling unused management services such as Web, Telnet, SNMP, etc.
- Using external Syslog servers to capture and coordinate events and logs for auditing

---

NOTE: The **telnet-client**, **web-client**, and **snmp-client** commands should also be considered as additional hardening techniques for Foundry devices. For more information on device hardening techniques, please refer to the *IronShield Best Practices: Hardening Foundry Routers and Switches* document or the *Foundry Security Guide*.

Management VLANs Through Routed Backbones

In medium to large installations, there may be a need to create multiple management VLANs for each building, campus, or regional office. Distributed management VLANs can be connected together by either switching or routing traffic through the corporate backbone. The method selected depends on the security, growth, and access criteria of each company. Each method has its advantages and disadvantages.

Layer 2 Connected Management VLANs

Figure 3 shows how multiple management VLANs in different physical locations can be connected through the enterprise backbone using a Layer 2 Tagged Port-Based VLAN. All management VLANs belong to the ***same broadcast domain*** and are part of the same IP subnet. The routers connecting the corporate subnets and management VLANs must support Layer 2 Port-Based VLANs.

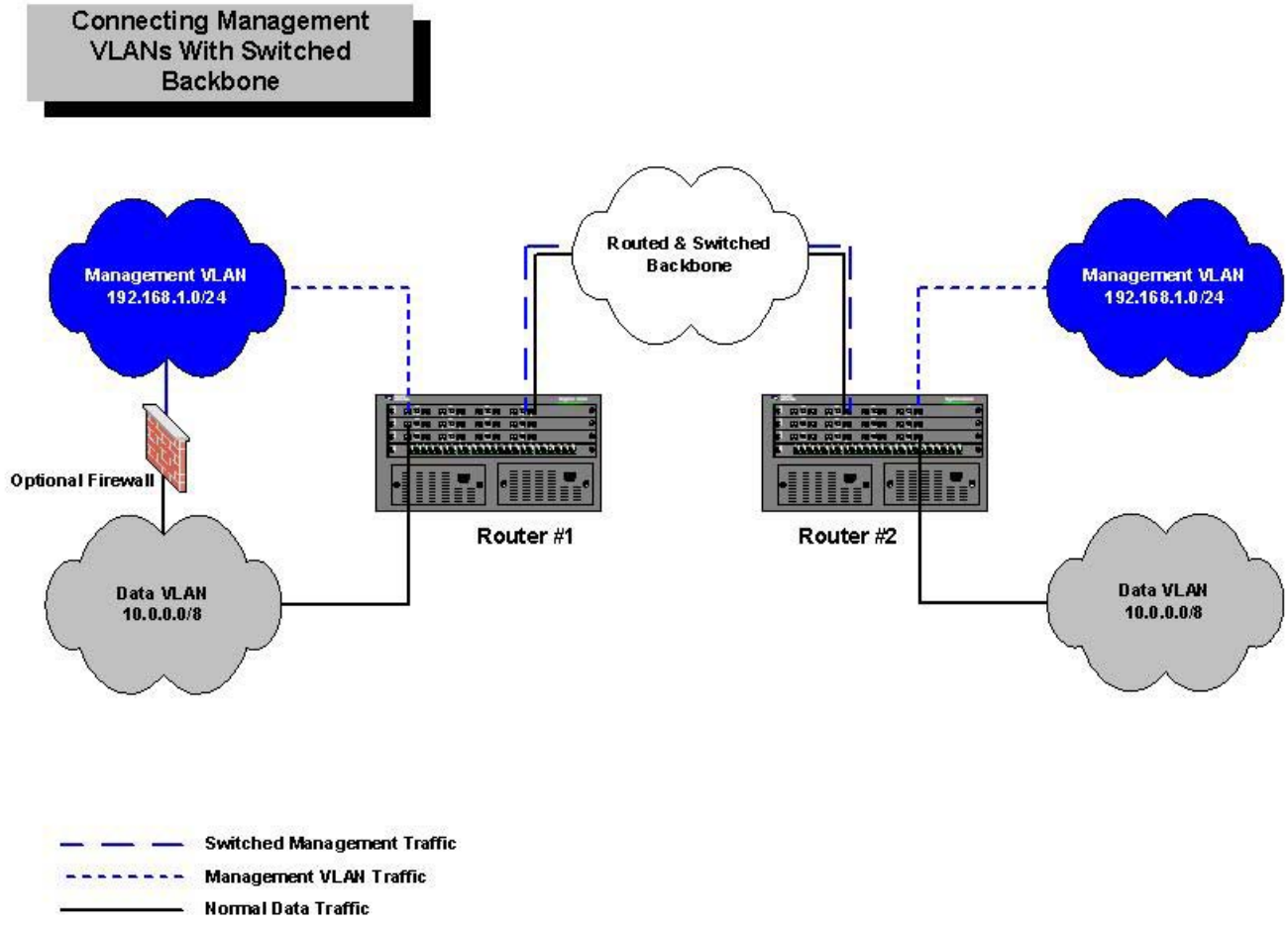

Figure 3. Connecting Management VLANs Through Layer 2 Port-Based VLANs

The advantages of connecting all the management VLANs together with a Layer 2 Switched VLAN include:

- Strong security through "out-of-band" management subnet – totally separated from other Layer 3 networks.
- One continuous management VLAN supporting all network devices – simplifies addressing scheme for devices.
- Ability to add additional security devices such as firewalls to control access between the management VLAN and other Layer 3 networks.

The disadvantages of a single management VLAN throughout the entire enterprise includes:

- Single broadcast domain may not be a good choice through slow WAN links.
- Scaling the management VLAN may become an issue as the number of network devices increase.
- All personnel requiring access to the network devices will need access to the single management VLAN.

Setup Procedure

To create a Layer 2 VLAN across a Layer 3 backbone, each Layer 3 switch/router will require the following configuration steps to create the necessary Layer 2 VLANs. The VLANs created on the Layer 3 switch/routers will need to support the management VLAN traffic in bridge mode and also route non-management traffic in Layer 3 mode.

Step 1: Create the Layer 2 port-based VLAN on each router that will be used to connect to the management VLANs. In the example shown in Figure 3, dedicated router ports were used to connect the management VLANs to the router. Router #1 used interface E1/1 and Router #2 used interface E1/8 and these were added as untagged ports. The router ports connecting to the core were added as tagged ports in the Layer 2 Port-Based VLAN.

To create the port-based VLAN: **Syntax:** vlan <vlan-id> by port

To add ports: **Syntax:** untagged ethernet | pos <portnum> [to <portnum> | ethernet <portnum>]
Syntax: tagged ethernet | pos <portnum> [to <portnum> | ethernet <portnum>]

To turn on Spanning Tree Protocol: **Syntax:** [no] spanning-tree

EXAMPLE
To create the port-based VLAN used by Router #1, enter the following:

```
Router-1(config)# vlan 110 name Mgmt-VLAN by port
Router-1(config-vlan-110)# untagged eth 1/1
Router-1(config-vlan-110)# tagged eth 1/8
Router-1(config-vlan-110)# spanning-tree
Router-1(config-vlan-110)# exit
Router-1(config)# write memory
```

To create the port-based VLAN used by Router #2, enter the following:

```
Router-2(config)# vlan 110 name Mgmt-VLAN by port
Router-2(config-vlan-110)# untagged eth 1/8
Router-2(config-vlan-110)# tagged eth 1/4
Router-2(config-vlan-110)# spanning-tree
Router-2(config-vlan-110)# exit
Router-2(config)# write memory
```

Step 2: Create the Layer 3 Tagged Port-Based VLAN on each backbone router to support the routing of regular data traffic. Remember that tagged ports are taken out of the Default VLAN and must be defined explicitly in a separate port-based VLAN to allow the tagged port to be used by more than one VLAN.

EXAMPLE
To create the Layer 3 Port-Based VLAN on Router #1 for routing regular data traffic, enter the following:

```
Router-1(config)# vlan 111 name Data-VLAN by port
Router-1(config-vlan-111)# tagged eth 1/8
Router-1(config-vlan-111)# router-interface ve 111
Router-1(config-vlan-111)# exit
Router-1(config)# write memory
```

To create the Layer 3 Port-Based VLAN on Router #2 for routing regular data traffic, enter the following:

```
Router-2(config)# vlan 111 name Data-VLAN by port
Router-2(config-vlan-111)# tagged eth 1/4
Router-2(config-vlan-111)# router-interface ve 111
Router-2(config-vlan-111)# exit
Router-2(config)# write memory
```

Step 3: Program the newly created virtual routing interface (VE) with the router configuration information to facilitate routing of regular data traffic across the backbone.

EXAMPLE
For Router #1, the backbone connection was set to 10.100.100.254/24 and OSPF was used as the routing protocol.

```
Router-1(config)# int ve 111
Router-1(config-vif-111)# ip address 10.100.100.254/24
Router-1(config-vif-111)# ip ospf area 0.0.0.0
Router-1(config-vif-111)# ip ospf dead 16
Router-1(config-vif-111)# ip ospf hello 2
Router-1(config-vif-111)# exit
Router-1(config)# write memory
```

For Router #2, the backbone connection was set to 10.100.100.1/24 and OSPF was used as the routing protocol.

```
Router-2(config)# int ve 111
Router-2(config-vif-111)# ip address 10.100.100.1/24
Router-2(config-vif-111)# ip ospf area 0.0.0.0
Router-2(config-vif-111)# ip ospf dead 16
Router-2(config-vif-111)# ip ospf hello 2
Router-2(config-vif-111)# exit
Router-2(config)# write memory
```

Layer 3 Connected Management VLANs

The illustration in Figure 4 shows how multiple management VLANs in different physical locations can be connected through the enterprise backbone using Layer 3 routers. All management VLANs are in ***separate broadcast domains*** for each location and act as traditional Layer 3 subnets. The routers connecting the corporate subnets and management VLANs are used to route the management traffic between management stations. Layer 3 and Layer 4 ACLs can be used to restrict access to and from the management VLANs.

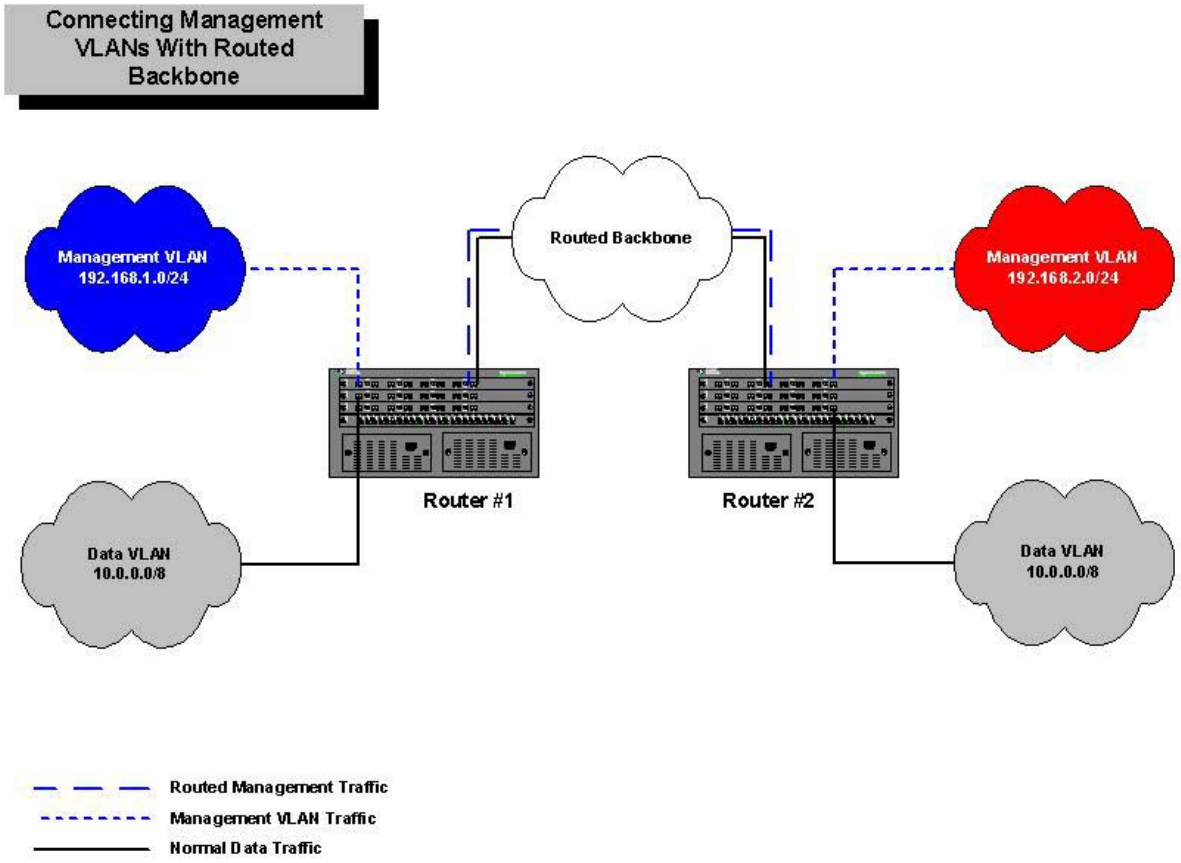

Figure 4. Connecting Management VLANs Through Layer 3 Routers

The advantages of connecting all the management VLANs together with Layer 3 routers include:

- Keeps management VLANs from each location separated.
- Keeps broadcasts from the management VLANs from traversing slow WAN links.
- Scales easily as more devices and management VLANs are required.
- Allows ACLs to be used to control granular access. Multiple groups of administrators can be allowed to have different access rights to the management VLAN.

The disadvantages of multiple routed management VLANs throughout the entire enterprise include:

- Access security is governed by packet filtering ACLs
- Addition of security devices such as firewalls to control access between the management VLAN and other networks supporting regular data traffic is more difficult with additional routed management VLANs

Setup Procedure

To route the distributed management VLANs across a Layer 3 backbone, a router interface will need to be defined on each router supporting the separate management VLANs. The management VLANs will be routed like traditional subnets across the Layer 3 backbone. Precautions should be taken to limit access into the management VLANs through the use of packet filtering ACLs or firewalls.

Step 1: Create the port-based VLAN and VE for the router interface that will be used to support the management VLAN. This VLAN will be used in the next section, **Guarding Access to Routers**, to restrict remote management access to the management VLAN.

EXAMPLE
For Router #1, create the following port-based VLAN:

```
Router-1(config)# vlan 100 name Data-VLAN by port
Router-1(config-vlan-100)# untagged eth 1/1
Router-1(config-vlan-100)# router-interface ve 100
Router-1(config-vlan-100)# exit
Router-1(config)# write memory
```

For Router #2, create the following port-based VLAN:

```
Router-2(config)# vlan 110 name Data-VLAN by port
Router-2(config-vlan-110)# untagged eth 1/8
Router-2(config-vlan-110)# router-interface ve 110
Router-2(config-vlan-110)# exit
Router-2(config)# write memory
```

Step 2: On each router, program the VE router interface to support the management VLAN that is connected to it. Program the required IP address and routing protocol information on the router port.

EXAMPLE
For this example, Router #1 will use the gateway address of 192.168.1.254/24 along with the OSFP routing protocol. To create the Layer 3 router interface to support the management VLAN used on Router #1, enter the following:

```
Router-1(config)# int ve 100
Router-1(config-vif-100)# ip address 192.168.1.254/24
Router-1(config-vif-100)# ip ospf area 0.0.0.10
Router-1(config-vif-100)# ip ospf dead 16
Router-1(config-vif-100)# ip ospf hello 4
Router-1(config-vif-100)# exit
Router-1(config)# write memory
```

For this example, Router #2 will use the gateway address of 192.168.2.254/24 along with the OSPF routing protocol. To create the Layer 3 router interface to support the management VLAN used on Router #2, enter the following:

```
Router-2(config)# int ve 110
Router-2(config-vif-110)# ip address 192.168.2.254/24
Router-2(config-vif-110)# ip ospf area 0.0.0.10
Router-2(config-vif-110)# ip ospf dead 16
Router-2(config-vif-110)# ip ospf hello 4
```

```
Router-2(config-vif-110)# exit
Router-2(config)# write memory
```

Step 3: Add the necessary packet filtering ACLs to limit access to and from each management VLAN. This example permits traffic generated from the management VLAN on Router #1 to enter the management stations on the management VLAN on Router #2. The management stations have the IP addresses 192.168.2.1 and 192.168.2.2.

This step should be repeated for each management VLAN subnet to create the necessary rules to govern access. For stricter security, create specific ACLs to govern each management protocol: SSH, Telnet, HTTP Web, SNMP, TFTP, etc.

EXAMPLE

```
Router-1(config)# access-list 101 permit ip 192.168.1.0/24 host 192.168.2.1
Router-1(config)# access-list 101 permit ip 192.168.1.0/24 host 192.168.2.2
Router-1(config)# access-list 101 deny any any

Router-1(config)# int ve 100
Router-1(config-vif-100)# ip access-group 101 in
Router-1(config-vif-100)# exit
Router-1(config)# write memory
```


Guarding Access to Routers

To complete the protection against unauthorized device access, the Layer 3 switch/routing devices will need to be configured with additional security measures. This will allow you to restrict remote management for all network devices, ensuring that only authorized management stations are permitted. IronShield Security features that can help control Telnet, SSH, Web management, SNMP, and TFTP access include:

- Access Control Lists (ACLs)
- Built-in CLI Commands
- VLAN ID (management VLAN)

Restricting remote management access with ACLs and Built-in CLI commands can be implemented as standalone features without the use of Management VLANs. For more information on these two security features, please refer to the *IronShield Best Practices: Hardening Foundry Routers and Switches* document or the *Foundry Security Guide*. This white paper concentrates on Management VLAN concepts and will assume that all Layer 2 switches and Layer 3 routers are to be accessed by the management stations located within the management VLAN.

Limiting Remote Access With VLAN IDs

Foundry Layer 3 switches/routers allow management protocols to be restricted to a specific VLAN ID. This VLAN ID must be a VLAN that is defined on the Layer 3 device and it must be the VLAN that is associated with the management VLAN.

By limiting remote management protocols to the management VLAN, the Layer 3 switch/router will only accept management protocols from hosts belonging to the management VLAN. The following management protocols can be restricted to port-based VLANs defined on Foundry devices:

- Telnet access
- Web management access
- SNMP access
- TFTP access

SSH access is limited by ACLs.

Syntax: [no] telnet server enable vlan <vlan-id>

Syntax: [no] web-management enable vlan <vlan-id>

Syntax: [no] snmp-server enable vlan <vlan-id>

Syntax: [no] tftp client enable vlan <vlan-id>

EXAMPLE:
Using the ***Layer 2 Connected Management VLANs*** example starting on page 15, the Layer 2 port-based VLAN that was created on each router to support the management VLAN was VLAN 110 (see Step 1 on page 16). Using this VLAN ID, the following remote management protocols are limited to management stations belonging to VLAN 110.

```
Router-1(config)# telnet server enable vlan 110
Router-1(config)# web-management enable vlan 110
Router-1(config)# snmp-server enable vlan 110
Router-1(config)# tftp client enable vlan 110
```

Using the configuration listed in this example, Telnet clients belonging to management VLAN 110 will be granted access. All other Telnet clients from ports outside of VLAN 110 will receive an error message similar to the following:

```
You are not authorized to telnet to this box!  Bye.
Connection to host lost.
C:\>
```

Summary

By using Management VLANs, access to network switches and routers can be restricted to authorized personnel. Management VLANs allow an "out-of-band" network to be created which greatly enhances security from other traditional hardening techniques, such as restricting access by Source IP Address filtering. By allowing the network device's management IP address to be placed into a private management subnet, the ability to remotely access the device from the regular data subnets and VLANs is greatly reduced.

With careful network planning and security design, management VLANs can add to your company's network defenses and help prevent unauthorized access to your network devices.

Foundry Networks, Inc.
Headquarters
2100 Gold Street
P.O. Box 649100
San Jose, CA 95164-9100

U.S. and Canada Toll-free: (888) TURBOLAN
Direct telephone: +1 408.586.1700
Fax: 1-408-586-1900
Email: info@foundrynet.com
Web: http://www.foundrynet.com