WHITE PAPER

Secure Networking: Five Things to Consider

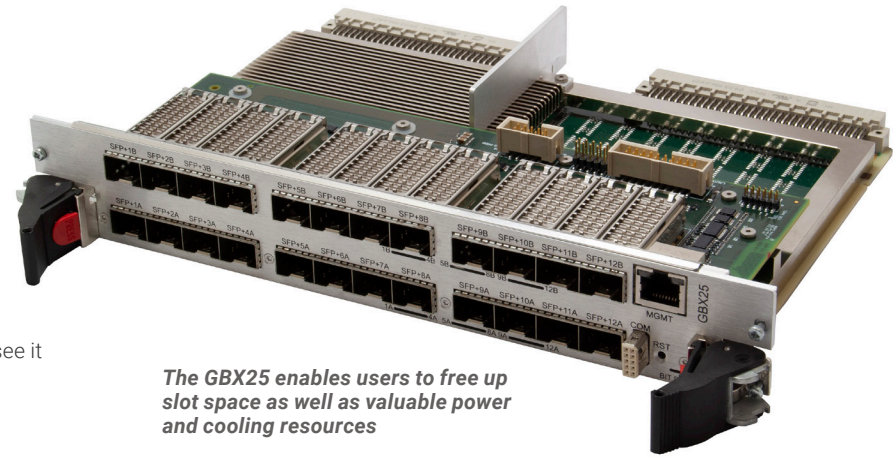
abaco SYSTEMS

Secure Networking: Five Things to Consider

Introduction

Few devices have a more critical role to play in safeguarding sensitive data than switches and routers. While every element within a modern embedded computing system should make appropriate provision for securing mission critical data, it is the switch/router that provides the interface between that system and the outside world – from which any attempt to acquire or corrupt that data is most likely to be initiated.

This white paper describes the key considerations in implementing secure networking using advanced switch management software such as Abaco's OpenWare™.



The GBX25 enables users to free up slot space as well as valuable power and cooling resources

1. Understanding Security

Security is the process of maintaining the following aspects of a system:

Confidentiality
Ensure only the people you want to see information can see it

Integrity
Ensure the data is what it is supposed to be

Availability
Ensure the system or data is available for use

It's important to build and deploy products with these concepts in mind and encourage users to take appropriate care in securing their networking products and solutions.

1.1 Isn't the firewall I have sufficient?

Firewalls and other network security products, including data diodes and intrusion prevention devices, can be an important component of any security strategy. However, a strategy based solely on any single security mechanism will not be as resilient as one that includes multiple, independent layers of security. Abaco therefore recommends taking a Defense in Depth approach to security.

1.2 What is Defense in Depth?

Defense in Depth is the concept of using multiple, independent layers of security to raise the cost and complexity of a successful attack. To carry out a successful attack on a system, an attacker would need to find not just a single exploitable vulnerability, but would need to exploit vulnerabilities in each layer of defense that protects an asset.

For example, if a system is protected by being on a network protected by a firewall, the attacker only needs to circumvent the firewall to gain unauthorized access. However, if there is an additional layer of defense, such as a username/password authentication requirement, the attacker now needs to find a way to circumvent both the firewall and the username/password authentication.

1.3 General recommendations

When using networking products and solutions, consider adopting the following security best practices:

- Deploy and configure firewalls to limit the exposure of control system networks to other networks, including internal business networks and the Internet. If a control system requires external connectivity, take care to control, limit and monitor all access, using, for example, virtual private networks (VPNs) or Demilitarized Zone (DMZ) architectures.
- Harden system configurations by enabling/using the available security features, and by disabling unnecessary ports, services and functionality.

Secure Networking: Five Things to Consider

1.4 Checklist

The following is a sample checklist to help guide the process of securely deploying products that support advanced network management software:

1. Create or locate a network diagram.
2. Identify and record the required communication paths between nodes.
3. Identify and record the protocols required along each path, including the role of each node (see section 2).
4. Revise the network as needed to ensure appropriate partitioning, adding firewalls or other network security devices as appropriate. Update the network diagram (see section 5).
5. Configure firewalls and other network security devices (see section 6).
6. Enable and/or configure the appropriate security features on each switch/router (see section 3).
7. 7. On each switch/router, change every supported password to something other than its default value (see section 3.4).
8. Harden the configuration of each switch/router, disabling unneeded features, protocols and ports (see section 4).
9. Test and qualify the system.
10. Create an update/maintenance plan.

NOTE: Secure deployment is only one part of a robust security program. This white paper, including the checklist above, is limited to providing secure deployment guidance only.

For more information about security programs in general, see section 6.

2. Communications Requirements

Communication between different parts of a networked system is, and must be, supported. However, the security of a system can be enhanced by limiting the protocols allowed, and the paths across which they are allowed, only to what is needed. This can be accomplished by disabling every communication protocol that is not needed on a particular device (see section 3), and by using appropriately configured and deployed network security devices (for example, firewalls and routers) to block every protocol (whether disabled or not) that does not need to pass from one network/segment to another.

Recommendations include limiting the protocols allowed by the network infrastructure to the minimum set required for the intended application. To do this successfully requires knowing which protocol is needed for each system-level interaction.

The following areas of knowledge are required to achieve these aims on a switch/router device:

- The communications through the switch/router
- The communication with the switch management interface

2.1 Through-switch protocols

There is a long list of Ethernet protocols that may be transferred through the switch/router device - see the product documentation for a full list.

Most of the protocols are transparently transferred through the switch at wire-speed and without the intervention of advanced network management software such as Abaco's OpenWare. However, some protocols are handled entirely by the management software, and others have some level of intervention to configure the hardware. For example, IGMP snooping may require control packets to be passed to the switch management environment for complete control, and routing may require the header of a stream's first packet to be passed for the completion of the hardware configuration.

This transfer between the switch fabric and the management processor is through a conduit that is hardware-protected against Denial of Service and enforces rate limiting - both important security considerations.

2.2 Switch management protocols

While the switch may be controlled both in-band (via the switching ports) and out-of-band (via a dedicated interface) the management interface is essentially identical.

The following protocols are an example of supported communication with switch management interfaces.

PORT	CLASS	PROTOCOL
161	UDP	SNMPv1
		SNMPv2
		SNMPv3
23	TCP	TELNET
80	TCP	HTTP
443	TCP	HTTPS
22	TCP	SSH
N/A	N/A	Serial port

Table 3-1 Protocols Supported for Switch Management

Secure Networking: Five Things to Consider

3. Security Capabilities

There are many layers of security (outlined below). Together, they provide a comprehensive Defense in Depth capability.

3.1 Access control and authorization

Advanced network management software may have a number of different access levels. As an example, Abaco's OpenWare has three levels of access:

- A read-only user (with limited access to commands)
- An optional read-write user that may modify a limited subset of the configuration
- A read-write user that may modify the configuration

PROTOCOL	DEFAULT USERS
Serial port	Read-only: status Read-write: admin
Telnet	
SSH	
HTTP	Read-only: (none by default) Read-write: admin
HTTPS	
SNMP v1 & v2	Read-only: public Read-write: private
SNMP v3	

Table 4-1 Common Default Users per Protocol

For each of the protocol groups, additional users may be configured, existing ones removed and passwords modified. Login timeouts should be configured on a per user basis.

NOTE: Do not deploy products with default passwords still active.Always change default passwords before deployment.

3.2 Authentication

Secure versions of the management application protocols are available

(see section 3.4). Authentication for the HTTP and serial/Telnet interfaces to the management application are not encrypted and should be disabled if possible.

User credentials may be used with Port Access control lists to define the authentication to be used for that user, for instance IEEE 802.1x and RADIUS.

MAC filtering can be used to limit the physical devices that may connect to a port.

3.3 Password and certificate management

In some cases, certificates can be loaded onto the switch/router to allow secure protocols to be used. Management protocols that use security certificates or keys are: SSH for remote command line access and SSL/TLS for web access.

Passwords may be stored securely on the switch/router in a manner that prevents them being read even by administrators.

A strong password policy is recommended. Some of the possible controls that can be implemented for effective passwords are:

- A minimum length of 8 characters
- At least one upper-case letter
- At least one numeric character
- At least one special character, such as @, #, $ etc.
- The user ID and password should not be the same

3.4 Confidentiality and integrity

Some communications protocols provide features that help protect data while it is actively moving through a network.

The following table shows the common insecure switch management access protocols, together with their secure alternatives provided by the switch:

INSECURE SERVICE	SECURE SERVICE
Serial port	None
Telnet	SSH
HTTP web server	HTTPS secure web server
SNMP v1 & v2	SNMP v3

Table 4-2 Insecure Protocols and their Secure Alternatives

NOTES: Abaco recommends the use of the secure services in all deployed systems. SSH version 1 is not completely cryptographically safe. Use version 2 in preference. Use TLSv1 in preference to SSLv3 for HTTPS communication.

Secure Networking: Five Things to Consider

3.5 Built-In Test
Switch/router products may contain a Built-In Test (BIT) which runs at power-on and checks the correct operation of the switch, before passing control to the management software. (Some industry sectors refer to this as PBIT.)

Logs of BIT failures can be viewed using the switch management interfaces. If the switch is in the write-protected mode, only the failures from the current power cycle can be viewed – otherwise, it can contain the errors from many power cycles. Each failure is stamped with the power-on cycle counter for historical identification.

3.6 BCS and backup software images
Switch/router products may support a Background Condition Screening (BCS) feature which runs alongside the switch management application and checks the correct operation of the switch during its normal operation. (Some of the industry sectors we supply refer to this as CBIT.) Monitoring of this BCS information can provide excellent, real-time system health information to a remote system controller.

3.7 Update signatures
Some switch/router products allow in-field upgrading of the management software where downloaded firmware and configuration files are authenticated using a standard library encryption.

3.8 Logging and auditing
Logs of BIT failures can be viewed using the switch management interfaces (see section 3.5 for more details).

BCS logs any unusual activity for viewing, using the switch management interfaces.

Failed logins are recorded (with IP address if applicable).

These logs can be accessed by correctly authenticated users on the serial/Telnet/SSH management interfaces and are persistent over switch reboots.

3.9 Controlled management interface
On Abaco switches/routers, all command line configurations are performed with exact match checking of the input.

Only valid options are presented on web and SNMP interfaces (with their return values checked against the presented options before use).

3.10 Sanitization
Switch/routers may support a sanitization feature. Running this feature results in all user configuration data being securely removed from the switch. This returns the switch to the same condition as when it originally left the factory. (The only exceptions are the power-cycle counter and the elapsed time counter.)

3.11 Hardware Denial of Service protection
Wire-speed switching functionality is performed in a dedicated hardware device. The hardware interface to the CPU running the network management software would be protected with Denial of Service and rate limiting devices within the hardware.

3.12 Hardware write protection
Some switches have the ability to operate in a read-only manner. This adds an extra layer of security in that no configuration information or software may be modified. Regardless of what has happened on the switch, a power cycle will always restore it to a known state.

4. Configuration hardening
This section is intended to assist in reducing the potential attack surface by providing information that can be used to harden the configuration of the switch/router products that are present in a particular installation.

Configuration hardening should be considered in addition to enabling and using security features such as authentication, access control and authorization.

Consider closing unrequired services as per the following tables.

4.1 Switch management interface
It is important to disable any management interfaces that you do not need in your application to reduce the number of attack vectors that may be used against the switch. For those interfaces that remain, it is important to use secure protocols wherever possible.

INTERFACE
Serial port
Telnet
HTTP web server
SNMP v1 & v2
SNTP client
SSH
HTTPS secure web server
SNMP v3

Table 5-1 Interfaces Often Available for Switch Management

TIP: Abaco recommends disabling all interfaces that are not required for the intended application.

NOTES: Disable SSH version 1, as it is not completely cryptographically safe.

Given the recent exploits of SSLv3, it is probably best to disable this and use TLSv1 only for HTTPS communications.

Secure Networking: Five Things to Consider

4.2 Switch management server facilities

It is recommended to disable standard management server facilities where they are not to be used. Disabling the protocols closes ports that listen to network traffic, thereby reducing the number of ports that can be used as attack vectors by an assailant.

SERVER FACILITY
DHCP server (IPv4)
DHCP server (IPv6)
DHCP boot relay
SNTP server
SNMP trap
Syslog
Port access control

Table 5-2 Disabling Switch Management Server Facilities

TIP: Abaco recommends disabling all server facilities that are not required for the intended application.

4.3 Standard protocols

There are several protocols whose function is to allow the remote changing of network configurations. These should be disabled to stop an attacker modifying the traffic flows within your system, either to gain access to your data, or to stop you accessing it (a Denial of Service or DoS attack).

PROTOCOL	PRECAUTIONS
STP	The switch should not be configured to use 802.1d (STP) due to published vulnerabilities in the protocol
LLDP	Link Layer Discovery Protocol should be disabled Advertising of capabilities is a security risk
LACP	Given the methods of automated reconfiguration of a link or links using this protocol, it should be disabled unless its use is specifically required
GMRP	Given the methods of automated reconfiguration of a link or links using this protocol, it should be disabled unless its use is specifically required
GVRP	Given the methods of automated reconfiguration of a link or links using this protocol, it should be disabled unless its use is specifically required

Table 5 3 Taking Precautions with Standard Protocols

TIP: Abaco recommends disabling all protocols that are not required for the intended application.

5. Secure Deployment

This section provides security recommendations for deploying switches/routers in the context of a larger network.

1. **Initial design:**

   a. Connections to other untrusted networks should be via firewalls or secure routers to minimize the protocols and ports used to communicate between the networks.

   b. Limit external access to specified IP addresses and user credentials.

   c. Design-in redundant network links for resilience.

   d. Only use the secure versions of access methods to the switch management interface.

   e. Consider only enabling the out-of-band management interface.

   f. Can the switch be used in a write-protected mode?

   g. Disable unrequired protocols, services and ports.

   h. Ensure all passwords are changed to complex values.

   i. Consider synchronizing switch time to a central SNTP server so that system-wide logging is synchronized.

2. **Monitoring:**

   a. Check the BIT and BCS logs of the switches on a regular basis.

   b. Consider actively monitoring the BCS port throughput logs for unusual traffic patterns (understand what the normal traffic patterns are).

   c. Consider monitoring the running configuration of the switch for modification.

3. **Control:**

   a. Keep a list of all software and hardware assets with serial numbers and firmware version numbers.

   b. Keep configuration settings in text format within a version control system.

Secure Networking: Five Things to Consider

6. Other Considerations

6.1 Patch management

The security plan should include a strategy for applying security fixes, including software updates and configuration changes. Although the software or configuration may be downloaded while the switch is in use, a reboot will be required to activate the new settings. This may be at a policy-related point in time. The security policy should note the length of time taken for a reboot to complete in the given application.

6.2 Additional guidance

6.2.1 Government agencies and standards organizations

Government agencies and international standards organizations may provide guidance on creating and maintaining a robust security program, including how to securely deploy and use Control Systems.

The US Department of Homeland Security has published guidance on Secure Architecture Design and on Recommended Practices for cybersecurity with Control Systems.

LINK:
https://ics-cert.us-cert.gov/Standards-and-References

Such documentation, when appropriate, should be considered in addition to this document. Similarly, the International Society of Automation publishes the ISA-99 specifications to provide guidance on establishing and operating a cyber-security program, including recommended technologies for industrial automation and control systems.

LINK:
https://www.isa.org/standards-publications

The UK Centre for the Protection of National Infrastructure has published guidance on cyber security consideration.

LINK:
https://www.cpni.gov.uk/cyber-security

6.2.2 Company guidelines

Any recommendations made here are subservient to your company's guidelines.

Abaco routers and switches

Abaco's rugged routers and switches are specifically designed to be deployed in security-sensitive mission critical applications that will be deployed in the harshest, most challenging settings.

OpenWare is Abaco's switch management environment. It is GNU/Linux-based firmware, bringing together the best of open source and proprietary switch control, routing and protocol implementations, and provides the user with a switch that can be easily configured for any network requirement – from the trivially simple through to the very complex.

Highly flexible, OpenWare environment allows for customization for specific customer requirements and provides integrated switch management services, including configuration, monitoring, switching control, addressing, routing and all supported protocols.

Abaco's Networking Innovation Center provides our customers with in-depth support in designing and deploying complex, secure networks.