

CONSIDERATIONS WHEN DEPLOYING LAYER 2 ETHERNET SWITCHES

GOOD PRACTICE GUIDANCE

MAY 2009

Abstract:

There are a number of issues which should be considered at the design, procurement and installation stages of deploying Layer 2 Ethernet switches. This paper is aimed at the network owners and security professionals who have an input to these processes.

Disclaimer:

CPNI has taken every care in preparing this protective security advice, which is informed by intelligence on the threat. However, CPNI cannot accept any liability to any person or company for any financial loss or damage arising from the use of this advice or from any failure to give advice.

Introduction

During 2008 CPNI undertook a project to look into the current state of network security specifically as it relates to the data link layer, with Ethernet and Metro Ethernet protocols being the main focus of the project. As part of this work CPNI tested a range of commonly deployed switches from a number of vendors. New test suites were developed for this purpose by Codenomicon (<http://www.codenomicon.com/>).

A more complete report has already been made available by CPNI to all those who took part in the project.

This document is intended to provide a freely available summary of the best-practice guidance which was derived from the project. The advice below is aimed at anyone who owns, deploys or manages Ethernet devices: it is as relevant to small business as it is to large enterprise networks and carriers.

CPNI advice is:

When procuring new equipment, engage with your vendor and ask searching questions so that you understand the security available from your chosen device;

When installing and configuring new equipment, ensure that your network architects and designers take security into account.

CPNI advice

When procuring or specifying equipment:

- From a complexity standpoint, integrated data link layer switches / network layer routers present a much larger attack surface than simple data link layer devices. Consider procuring less complex devices over smarter ones if security is an overriding concern.
- Consider procuring modular devices. Enable your own team to choose the complexity level of the device. Require devices that are security-optimized by default.
- Require the option of turning off all unnecessary protocol interfaces by default. Allow your network architects to enable protocols only when they require them, thereby limiting the default attack surface of your devices.
- Require the full device configuration; often a protocol interface may be exposed to the network even though the device configuration file contains no reference to it.
- Require a secure deployment guide with the product. This guide could contain details on designing networks and topologies that are as resilient as possible towards both currently known and as yet unknown fundamental data link layer attacks.

Ask your suppliers about their design and testing regimes:

- Have they designed all code with security in mind?
- Is all input validated (its data type and format checked)? It may be appropriate to include a validation module as part of the design. The input validation should agree with the interface specification.
- Have they rigorously tested all code for security vulnerabilities, especially where development has been outsourced?
- Have they considered using the same testing practices for testing data link layer and Metro Ethernet interfaces as they would use for verifying protocol robustness at network layer and above?
- Have they considered a security flag in the configuration which auto-configures the device to its most secure state?
- Have they designed the architecture of the device so that unnecessary protocol logic can really be turned off? When the functionality of a protocol is turned off, no part of the system should analyze or attempt to make sense of protocol structures belonging to that particular protocol.

When installing and configuring equipment:

- Be aware of the existing configuration guidance which exists for your chosen products. The advice given here is supplementary to much of what is considered to be “business as usual” secure configuration guidance such as: using secure management protocols and creating a strong password. It is recommended that the latest secure configuration guides are obtained from your vendors.
- Document why you need each feature and how it should be configured in your environment. A switch will typically have a default configuration where the majority of features are enabled. This scenario will expose input paths to the protocols running on the switch from other devices and from people connected to the switch.
- Turn off or disable protocols on interfaces where they are not required. For example, the Spanning Tree Protocol (STP) can be disabled on specific logical or physical interfaces where it is not required.
- Permanently disable the process that provides a protocol where that protocol is not used at all.
- Once unused functionality and protocols are turned off, consider that all remaining protocols will be accessible from all (or specific) connected networks and devices. Enumerate and consider the vulnerabilities associated with each of the remaining protocols and make a risk management decision based on the presence of publicly known vulnerabilities and the availability of mitigation guidance.
- Consider rechecking device configurations after software upgrades, as new software may introduce new vulnerabilities. (Also remember that this guide is supplemental to standard switch, host and physical security practice.)
- Check vendors' default configurations for presence of unwanted protocols. (Remember that data link layer is fundamentally a broadcast domain). Be aware that in some switches a protocol may be turned on by default, even if it is not explicitly shown to be enabled in a

configuration file. The exact procedure for doing this varies, but the basic means for detecting the presence of unwanted data link layer services is to review the switch configuration, issue commands to check the status of a particular protocol service, and to look at the process table in the switch (if available) to see if separate protocol services can be observed as separate processes. Running protocol analysis tools on the network can assist in this check. For network layer and above protocols, this type of service discovery is more trivial, since it can also be done from the viewpoint of an outside attacker by way of port scans (e.g. nmap) in addition to investigations inside the network. For data link layer, discovering unwanted services can be very hard for an operator. Consider consulting your switch vendor(s) for more information.

- Only enable Operations Administration and Management (OAM) and any other optional protocols in those customer interfaces where they are absolutely required - every complex protocol increases your attack surface further.
- Avoid using protocols that have known design flaws and/or that can be abused easily to create load for switch processors, especially on interfaces through which external parties or customers may be able to generate data link layer traffic. This includes Link Layer Discovery Protocol (LLDP) and other discovery protocols; STP and other data link layer topology convergence protocols; and LACP/GARP VLAN Registration Protocol (GVRP) and other trunking/aggregation protocols. Some alternative proprietary or public protocols may also be considered to camouflage the standard attack surface. Examples are too numerous to list here, but it should be remembered that any given alternative may also come with its own problems, so should be rigorously tested before deployment.
- Avoid topologies and configurations that allow attackers to disrupt network operations with known protocol design flaws (for example: STP, LACP, Address Resolution Protocol (ARP)).

Existing advice

An important presentation specifically on Metro Ethernet / Carrier Ethernet protocol extensions and environments is "Security Best Practices for Carrier Ethernet Networks and Services" (Santitoro 2008). This presentation is available at:

http://metroethernetforum.org/PPT_Documents/CEWC2008/Carrier-Ethernet-Security-Santitoro-MEF-CEWC-2008.ppt

Cisco has also published a very good white paper on data link layer vulnerabilities as an addendum for their earlier SAFE Enterprise white paper called "SAFE Layer 2 Security In-Depth - Version 2" (Dubrawsky 2004). This white paper can be found at

http://www.cisco.com/warp/public/cc/so/cuso/epsq/sqfr/sfblu_wp.pdf.

Other valuable guides to Ethernet switch security include "Cisco IOS switch configuration" produced by the US National Security Agency, available at http://www.nsa.gov/snac/os/switch-guide-version1_01.pdf and "Enhancing Internal Network Security" from Foundry Networks, available at <http://www.foundrynet.com/pdf/wp-enhancing-lan-security.pdf>.

The state-of-the-art tool for data link layer testing has been the Yersinia framework (<http://www.yersinia.net/>). Yersinia brought data link layer attacks to the awareness of a widespread audience and pioneered the testing of both data link layer attacks that had been conjectured before as well as adding some innovative attacks based on its authors' own research. The authors (David Barroso and Alfredo Andres) presented the Yersinia framework at

Black Hat Europe 2005: The presentation, "Yersinia - Framework for layer 2 attacks", can be found at http://blackhat.com/presentations/bh-europe-05/BH_EU_05-Berrueta_Andres/BH_EU_05_Berrueta_Andres.pdf.

BlackHat Europe (April 2009) included a discussion paper on MPLS and Carrier Ethernet attacks. The paper can be found at http://www.ernw.de/content/e7/e181/index_eng.html.

Tools for testing at the Data Link Layer

Nmap	http://nmap.org/
Hping	http://www.hping.org/
Yersinia	http://www.yersinia.net/
Scapy	http://www.secdev.org/projects/scapy/
Wireshark	http://www.wireshark.org/
TCP Dump	http://www.tcpdump.org/
Ettercap	http://ettercap.sourceforge.net/
Mausezahn	http://www.perihel.at/sec/mz/index.html
Nemesis	http://nemesis.sourceforge.net/
packETH	http://packeth.sourceforge.net/

Data Link Layer Standards:

Bridging	802.1D	STP	802.1D
Ethernet	802.3	VPLS	RFC4761/2
VLAN	802.1Q	LLDP	802.1AB
LACP	803.ad	PPP/PPPoE	RFC1661/2516
PBT	802.1ay	L2TPv3	RFC3931

Acronyms:

ARP	Address Resolution Protocol
BFD	Bi-Direction Forwarding Detection
CFM	Connectivity Fault Management
E-LMI	Ethernet – Local Management Interface
GARP	Generic Attribute Registration Protocol
GVRP	GARP VLAN Registration Protocol
OAM	Operations Administration and Management
LACP	Link Aggregation Control Protocol
LFM	Link fault Management
LLDP	Link Layer Discovery Protocol
L2TP	Layer 2 Tunneling Protocol
MSTP	Multiple Spanning Tree Protocol
PBB	Provider Backbone Bridge
RSTP	Rapid Spanning Tree Protocol
PBT	Provider Backbone Trunking
PPP	Point to Point Protocol
STP	Spanning Tree Protocol
VLAN	Virtual Local Area Network