

Securing the Data Link Layer (L2) on the Welsh Ambulance Network Infrastructure.

Introduction

L2, also known as the Data Link Layer, provides network access to users.

Switches interconnect and communicate using management protocols to make autonomous decisions. in relation to network traffic. flows.

Many of the protocols are easy to configure, however if a vulnerability of a protocol is compromised, there is a risk that administrators could be faced with a severe network outage that is complex to troubleshoot due to the impact caused.

Welsh Ambulance have these protocols running on their L2 infrastructure, however best practice in relation to the security of the L2 network running these protocols has been overlooked.

Welsh Ambulance are a Cisco house as far as L2 is concerned.

This report will highlight the vulnerabilities and propose mitigations in line with Cisco recommendations.

However, the research conducted, is not limited to Cisco.

Aims and Objectives

Aim

The aim of this report is to evaluate if the current Layer 2(L2) / Data Link implementation at Welsh Ambulance Service Team (WAST) is secure enough or if further measures can or need to be implemented to ensure WAST are in the optimal posture and are adequately protected against threats and vulnerabilities.

Objectives

- Research L2 protocols that are used across the WAST health board and identify best practices for securing them,
- Conduct an extensive analysis of L2 protocols on existing WAST network
- Replicate the existing infrastructure in a home laboratory environment
- Identify the vulnerabilities and implement the recommended mitigations safely
- In a testing environment, apply configuration to enable the mitigations and interrogate them by attacking the specific protocols
- Evaluate the results of the mitigations and decide if there is a business case to implement themProvide the IT Ops board with a clear plan to implement the new measures on the production network.

The Protocols

Dynamic Host Configuration protocol (DHCP)

Vlan Trunking Protocol (VTP)

Rapid Spanning Tree Protocol (RSTP)

Cisco Discovery Protocol (CDP)

Address Resolution Protocol (ARP)

Dynamic Trunking Protocol (DTP)

Hot Standby Routing Protocol (HSRP)

The Laboratory Topology

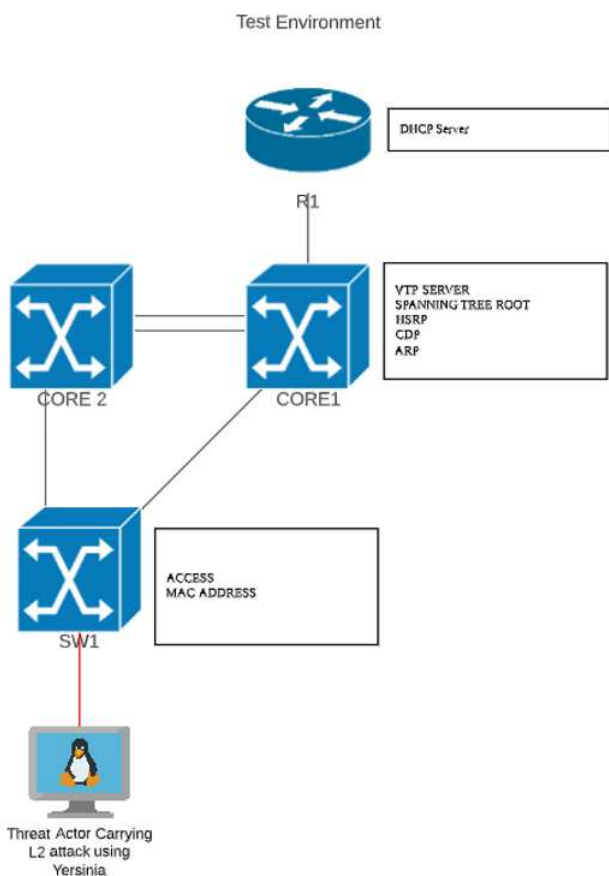


Figure 1

Conclusions

All of the attacks have suitable mitigations that are recognised by industry experts.

The current L2 protocol configurations are not adequate and need updating to make them more secure.

The mitigations suggested, mitigations were tested in a laboratory environment.

The results of the testing did not suggest that the mitigations would have an impact on the production network.

To implement the mitigations on the network would need a discussion with the Information Technology Operations Board.

If approved, the change control process will be followed in WAST to ensure minimal impact.

To ensure compliance, the control measures and mitigations will be reviewed to ensure that WAST is adequately protected in the future.

Attack Example

This attack using Yersinia demonstrates a simple DTP attack to form a trunk port on an unprotected interface.

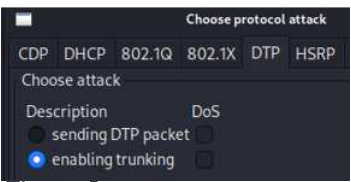


Figure 2

CDP	DHCP	802.1Q	802.1X	DTP	HSRP	ISL	MPLS	STP	VTP	Yersinia log
Neighbor-ID	Status	Domain	Interface	Count	Last seen					
001BD5366F14	04 ACCESS/AUTO	WAST	eth0	1	14 Jun 09:00:22					
0C7CE846D595	03 ACCESS/DESIRABLE		eth0	3	14 Jun 09:00:43					
001BD5366F14	84 TRUNK/AUTO	WAST	eth0	3	14 Jun 09:00:43					

Figure 3

```
WAST-SW2(config)#
05:25:19: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0/17, changed state to down
05:25:20: %LINK-3-UPDOWN: Interface FastEthernet1/0/17, changed state to down
05:25:23: %LINK-3-UPDOWN: Interface FastEthernet1/0/18, changed state to up
05:25:24: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0/18, changed state to up
WAST-SW2(config)#
05:26:11: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0/18, changed state to down
05:26:14: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0/18, changed state to up
```

Figure 4

Testing

Extensive testing was conducted.

Attacks using Yersinia were conducted on the configuration prior to mitigations.

Attacks using Yersinia were conducted post mitigation .

Results were compared to see whether the mitigations averted the risk.

References

Figure 1 - Created by the author. Laboratory topology
Figure 2 - A DTP Attack on the Yersinia Platform
Figure 3 - DTP Packets being sent over the network
Figure 4 - The WAST switch debug in relation to DTP messages