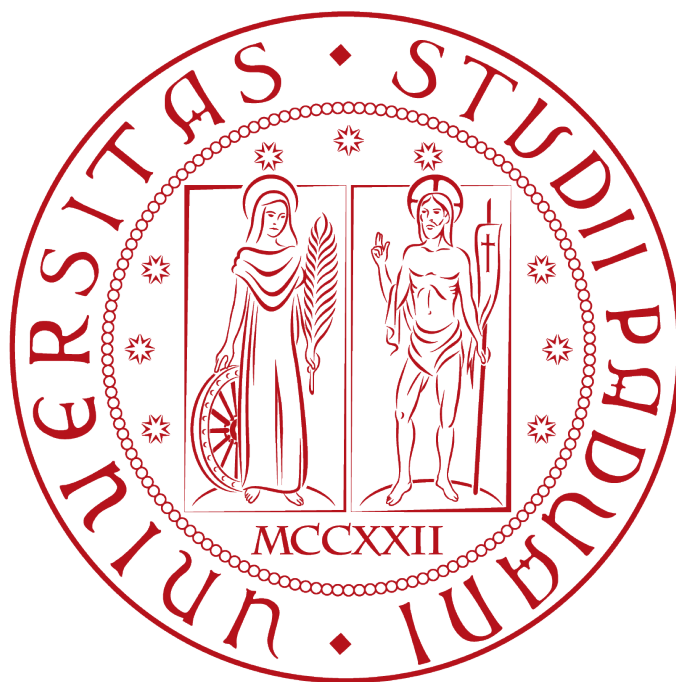


UNIVERSITÀ DEGLI STUDI DI PADOVA
DIPARTIMENTO DI MATEMATICA

Corso di Laurea in INFORMATICA



Monitoraggio e sicurezza fisica di reti
LAN Campus

Tirocinante:	Mirco Cailotto, mat. 1123521
Relatore:	Dott. Paolo Baldan
Azienda Ospitante:	Wintech Spa
Tutor aziendale:	Roberto Pezzile

Anno Accademico 2017/2018

TODO DEDICA

Indice

1	Contesto aziendale	2
1.1	Dominio applicativo	2
1.1.1	Com'è cambiata la Cybersecurity negli ultimi anni?	2
1.1.2	La proposta di Wintech	3
1.2	Tipologia di clientela aziendale	3
1.3	Processi aziendali	3
2	Progetto di stage	4
2.1	Pianificazione	4
2.1.1	Fase 1: Analisi	4
2.1.2	Fase 2: Progettazione	5
2.1.3	Fase 3: Implementazione	5
2.1.4	Fase 4: Test in produzione	6
2.1.5	Fase 5: Tuning	6
2.2	Riepilogo ore	6
2.3	Obiettivi	7
2.3.1	Obiettivo aziendale	7
2.3.2	Obiettivo formativo	7
3	Tecnologie	8
3.0.1	802.1X	8
3.0.2	PRTG Network Monitor	8
3.0.3	Observium	9
3.0.4	RConfig	9
4	Realizzazione	11
4.1	Analisi	11
4.1.1	Lista apparati	11
4.1.2	Analisi sistemi di sicurezza fisica	11
4.1.3	Analisi sistemi di monitoraggio	12
4.1.4	Schema di rete	13

4.2	Progettazione	14
4.2.1	Progettazione Observium	14
4.2.2	Progettazione RConfig	14
4.2.3	Definizione name-convention	14
4.2.4	Inserimento nomi DNS sulla lista apparati	15
4.3	Implementazione	16
4.4	Test in produzione	17
4.5	Tuning	18
5	Valutazione retrospettiva	19
5.1	Risultati ottenuti	19
5.2	Vincoli del progetto	19
	Appendici	19
	Appendice A: Schemi di rete	20
	Appendice B: Script di popolamento rConfig	24
	Glossario	27
	Bibliografia	29

Elenco delle figure

1.1	Logo di Wintech	2
3.1	Logo di PRTG	9
3.2	Logo di Observium	9
3.3	Logo di RConfig	10
4.1	Armadietto di rete da esterni	12
4.2	Schermata di PRTG Network Monitor	13
5.1	Schema Visio della rete datato 2015	21
5.2	Schema Visio della rete a fine stage, prima parte	22
5.3	Schema Visio della rete a fine stage, seconda parte	23

ABSTRACT

Capitolo 1

Contesto aziendale

Nata nel 1987, Wintech Comumunication Factory SPA è ad oggi uno dei pochi *System Integrator*_G capace di vantare una lunga tradizione e un patrimonio di conoscenze nei diversi ambiti di competenza del settore ICT.

Tra le partnership si possono citare IBM, Symantec, Hewlett Packard, Microsoft, Oracle, VMWare e Sophos.



Figura 1.1: Logo di Wintech

1.1 Dominio applicativo

Wintech opera in un dominio molto vasto, che spazia dal Cloud alla *Digital Transformation*_G, per tale motivo in questa sezione verrà analizzato unicamente il dominio relativo allo stage conseguito, cioè quello del monitoraggio e della sicurezza fisica delle reti.

1.1.1 Com'è cambiata la Cybersecurity negli ultimi anni?

Il panorama attuale per tipologia di attacchi e motivazioni, è profondamente mutato rispetto anche solo a qualche anno fa. Tutti gli osservatori sulla tematica Cybersecurity lo confermano con i dati. Non è fare terrorismo psicologico, ma essere realisti, quando si afferma che tutti si è potenzialmente vulnerabili e bersagli del cybercrime e quindi "is not a matter of if, but a matter of when". Bisogna

sfatare l'immaginario collettivo in cui siano solo le grandi società americane, grandi brand, ad essere attaccate per attivismo. Le motivazioni sono notevolmente mutate e hanno come target qualsiasi azienda, anche le realtà della piccole e medie imprese che costituiscono il tessuto delle aziende italiane sono pesantemente bersagliate.

1.1.2 La proposta di Wintech

La proposta per consentire di mantenere un elevato livello di sicurezza all'interno delle proprie reti proposto da Wintech si compone di svariate tecnologie, che vanno ad incastrarsi per permettere una protezione completa su tutti i possibili fronti di attacco.

Le tecnologie proposte saranno riguardanti il monitoraggio della rete, il controllo della configurazione degli apparati ed il port-based Network Access Control.

1.2 Tipologia di clientela aziendale

TODO mettere o no?

1.3 Processi aziendali

TODO chiedere a Lisa

Capitolo 2

Progetto di stage

Lo scopo dell'attività di stage è l'analisi, la progettazione e l'implementazione di un sistema di monitoraggio della sicurezza fisica di una LAN Campus.

Le conoscenze apprese durante lo svolgimento dell'attività consistono nella capacità di progettare ed implementare una soluzione per raggiungere gli obiettivi prefissati, oltre che ad effettuare attività di tuning per perfezionarla.

2.1 Pianificazione

Le attività sono state suddivise in cinque fasi principali, le quali andranno a coprire tutta la durata del percorso formativo stabilito.

2.1.1 Fase 1: Analisi

- **Periodo previsto:** dal 04/06/2018 al 08/06/2018;
- **Numero di ore previste:** 40h;
- **Periodo effettivo:** ;
- **Numero di ore effettive:** .

L'obiettivo di questa prima fase del percorso è familiarizzare con l'infrastruttura amministrata da Wintech e con i supporti hardware e software da utilizzare per la realizzazione del progetto.

Nello specifico è stato analizzato lo schema di rete dell'infrastruttura, la lista degli apparati e delle loro caratteristiche, il sistema di sicurezza fisica attivi e il sistema di monitoraggio presenti.

2.1.2 Fase 2: Progettazione

- **Periodo previsto:** dal 11/06/2018 al 22/06/2018;
- **Numero di ore previste:** 40h;
- **Periodo effettivo:** ;
- **Numero di ore effettive:** .

Nella seconda fase si procederà alla configurazione del software di monitoraggio Observium e del software di gestione della versione RConfig.

Per facilitare le attività verrà definita la nomenclatura da dare ai dispositivi.

Ulteriormente si procederà alla definizione delle logiche di sicurezza che verranno implementate basate sul protocollo 802.11X.

Durante questa fase verrà anche prodotta la prima bozza della documentazione progettuale.

2.1.3 Fase 3: Implementazione

- **Periodo previsto:** dal 25/06/2018 al 06/07/2018;
- **Numero di ore previste:** 80h;
- **Periodo effettivo:** ;
- **Numero di ore effettive:** .

In questa fase è stata implementata la nuova infrastruttura e si sono resi operativi i software precedentemente configurati.

È stato creato un laboratorio con uno nuovo switch sul quale sono state testate le politiche precedentemente scelte per valutarne l'efficacia.

Una volta completata questa fase si procederà alla creazione delle nuove configurazioni per tutti gli switch comprendenti la nuova politica di sicurezza e la loro installazione.

Oltre a questo i dispositivi verranno inseriti all'interno del DNS e verranno resi operativi i software Observium e RConfig.

Durante questo periodo la documentazione progettuale è stata aggiornata di conseguenza alle attività svolte.

2.1.4 Fase 4: Test in produzione

- **Periodo previsto:** dal 09/06/2018 al 13/07/2018;
- **Numero di ore previste:** 80h;
- **Periodo effettivo:** ;
- **Numero di ore effettive:** .

La fase di test in produzione è la più importante perché verrà messo alla prova l'intero sistema con il picco dell'utenza.

L'attività che è stata svolta è il monitoraggio di eventuali anomalie, per poi censirle, cercare la fonte del problema, identificare una soluzione ed implementarla.

Durante questo periodo la documentazione progettuale è stata aggiornata di conseguenza alle attività svolte.

2.1.5 Fase 5: Tuning

- **Periodo previsto:** dal 16/07/2018 al 27/07/2018;
- **Numero di ore previste:** 80h;
- **Periodo effettivo:** ;
- **Numero di ore effettive:** .

Nella fase finale del progetto sono stati eseguiti tuning su tutta la rete, ove possibili, sia sugli apparati che nelle configurazioni dei software.

Questa attività sarà supportata dal software Observium, che nel frattempo avrà raccolto una mole di dati tale da permettere uno studio dei miglioramenti effettuabili.

Un'altra attività derivante dallo studio dei dati raccolti sarà la configurazione delle soglie di allarmi automatici, che verranno comunicati tramite messaggio e-mail e Telegram.

In questa ultima fase si procederà anche a completare la documentazione.

2.2 Riepilogo ore

Durata in ore	Durata effettiva	Descrizione dell'attività
---------------	------------------	---------------------------

40		Analisi
80		Progettazione
80		Implementazione
40		Test in produzione
80		Tuning

Numero di ore previste: 320h

2.3 Obiettivi

2.3.1 Obiettivo aziendale

L'obiettivo a fine stage è aumentare la sicurezza fisica di una LAN Campus dove accedono migliaia di persone, impedendo l'uso illecito e non controllato dei servizi di rete, sabotaggi e furto di dati.

Questo comprende l'implementazione di software di monitoring e lo sfruttamento dei servizi avanzati che offrono per ottenere le migliori performance ed il miglior controllo possibile.

2.3.2 Obiettivo formativo

L'obiettivo per il tirocinante è acquisire competenze in ambito networking e security in un contesto reale quale una LAN Campus estesa, variegata e con un numero di utenti elevato.

Questo al fine di permettergli di mettere in pratica le conoscenze acquisiti durante lo svolgimento dei corsi universitari e fornirgli un forte stimolo ad approfondire ancora di più queste tematiche.

Capitolo 3

Tecnologie

Questa sezione illustra le principali tecnologie utilizzate da Wintech S.P.A per il controllo ed il monitoraggio delle reti di loro competenza.

Essendo la sicurezza informatica un settore nel quale gli standard, le leggi e le tipologie di attacco evolvono molto in fretta, le tecnologie utilizzate devono adeguarsi di conseguenza. Questo porta i tool ed i programmi utilizzati a diventare obsoleti oppure variare con il passare del tempo.

3.0.1 802.1X

Il 802.1X è uno standard IEEE per il controllo di accesso alla rete port-based, parte della famiglia di protocolli IEEE 802.1. Fornisce un meccanismo di autenticazione mediante una combinazione username/password oppure un certificato digitale. Questa protezione va ad ampliare la *sicurezza fisica_G* delle risorse connesse alla rete, pur essendo di per sè una *sicurezza logica_G*, impedendone il raggiungimento ai dispositivi non autorizzati.

Lo standard viene implementato all'interno del firmware o del sistema operativo degli apparati di rete e dei dispositivi degli utenti.

Funziona sia su connessioni wired che wireless, anche se viene raramente utilizzato nelle connessioni cablate in quanto, ove possibile, viene favorita una protezione fisica perimetrale, apparentemente migliore.

3.0.2 PRTG Network Monitor

PRTG è un sistema di monitoraggio della rete, era utilizzato nella rete analizzata durante lo stage prima di Observium per rilevare eventuali anomalie, ma a causa delle limitazioni della versione gratuita e del suo elevato costo si è scelto di sostituirlo.

Il software consiste in un servizio al quale ci si collega mediante il client fornito

oppure attraverso una interfaccia web e permette di tenere sotto controllo anche siti web e servizi di varia natura.

Alla fine dell'attività di stage il software non è stato disabilitato, ma gran parte dei suoi compiti sono ora assolti da Observium, in quanto possiede alcune funzionalità che il suo concorrente non offre.



Figura 3.1: Logo di PRTG

3.0.3 Observium

Observium è un sistema di monitoraggio della rete compatibile con i dispositivi delle principali aziende produttrici di apparati di rete.

Tra i dispositivi supportati si possono citare Cisco, Dell, HP, Huawei, Lenovo, MikroTik, Netgear e ZTE.

Il software dispone anche di una ricerca automatica dei dispositivi presente all'interno della rete, utile per reti di piccola-media dimensione.

Le funzionalità che fornisce sono il monitoraggio del *Quality Of Service*_G, il raggruppamento dei dispositivi mediante regole definite dall'utente e l'alert automatico nel caso vengano superate determinate soglie.



Figura 3.2: Logo di Observium

3.0.4 RConfig

Il tool RConfig è un configuration management mirato ai dispositivi di rete che permette in modo veloce ed automatizzato di effettuare una copia delle configurazioni degli apparati di rete.

È completamente open source, protetto da licenza GNU v3.0, ed è scritto in linguaggio PHP, questo gli consente di essere installato facilmente su molti sistemi.



Figura 3.3: Logo di RConfig

Capitolo 4

Realizzazione

4.1 Analisi

Una delle prime attività svolte è stata la raccolta della documentazione e la sua analisi.

Sono subito emerse enormi incongruenze tra i vari documenti in quanto alcuni erano datati, quindi si è dovuto aggiornarli.

4.1.1 Lista apparati

Come base di questa attività si sono utilizzati alcuni documenti Excel con riportate informazioni sparpagliate sui dispositivi, sono stati integrati tra di loro e da questa attività è emerso che c'erano informazioni assenti per alcuni devices, che sono state completate.

Successivamente si è andato ad aggiungere la posizione GPS di ogni dispositivo, utilizzando i dati presenti nel software di monitoraggio presente.

I dispositivi sono stati nominati secondo la loro locazione in data precedente rispetto l'inizio dello stage.

4.1.2 Analisi sistemi di sicurezza fisica

La sicurezza fisica era perseguita prevalentemente controllando l'accesso fisico ai dispositivi di rete. Gli switch sono chiusi a chiave negli appositi armadietti e, ove possibile, mantenuti all'interno delle strutture dove l'accesso è consentito solo al personale.

Esiste una struttura di VLAN attua a impedire l'accesso alle risorse a coloro che

non ne possiedono i permessi, ma da sola non era sufficiente a garantire la sicurezza.

Un possibile attacco che si poteva praticare era forzare un armadietto di rete, costruiti in plastica, ed utilizzare una porta Ethernet untagged per poter connettersi ai dispositivi di quella VLAN.

In questo contesto si è andati ad operare sul controllo d'accesso, impedendo ad un dispositivo non riconosciuto di entrare in una VLAN semplicemente connettendosi ad una porta corretta, ma richiedendogli informazioni aggiuntive mediante lo standard 802.1X.



Figura 4.1: Armadietto di rete da esterni

4.1.3 Analisi sistemi di monitoraggio

La rete analizzata presentava già un software per il monitoraggio, denominato PRTG Network Monitor.

Il suo compito era quello di controllare che tutti i sensori in esso inserito appartenenti ai devices funzionassero correttamente, avvisando qualora ci fossero dei problemi.

Una delle problematiche fondamentali di questo software era la difficoltà nel tracciare grafici relativi alla connessione, impedendo di identificare eventuali colli di bottiglia, pacchetti persi o errori di trasmissione.

Questo software veniva utilizzato in versione gratuita e quindi presentava alcune limitazioni, la più critica era la quantità di sensori che può monitorare, limitata a 1000, che non consentiva di controllare in modo soddisfacente tutti gli apparati di rete presenti.

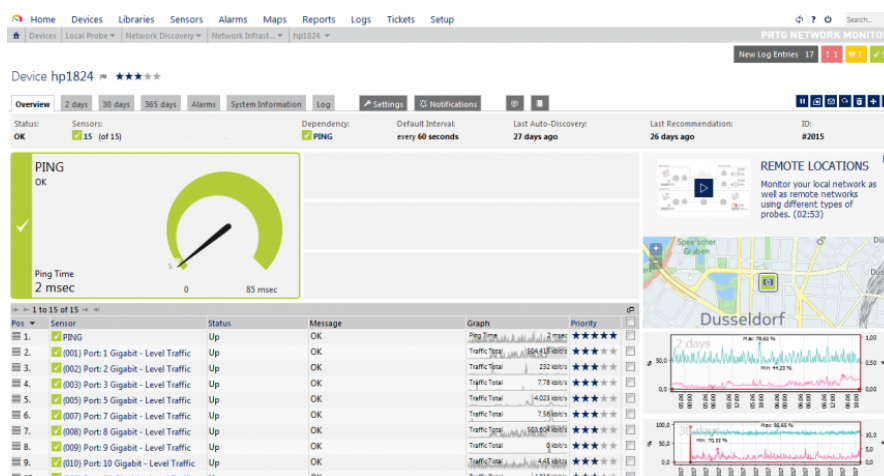


Figura 4.2: Schermata di PRTG Network Monitor

4.1.4 Schema di rete

Per facilitare tutte le attività successive di configurazione e monitoraggio si è proceduto alla redazione di uno schema di rete.

Essendo già disponibile uno schema datato 2015 della rete realizzato dal cliente in Microsoft Visio si è scelto di procedere con lo stesso software.

A supporto di questo lavoro si sono utilizzate svariate mappe prodotte in tempi e per fini diversi tra di loro, la cui integrazione ha evidenziato degli errori che sono stati segnalati.

Lo schema di rete di partenza e quello realizzato, presentanti il nome, il modello di dispositivo e l'indirizzo ip, sono presenti in Appendice A.

Si può notare come nella prima versione c'erano molte incongruenze nella forma nella quale sono stati riportati i dati, in quanto è stata prevalentemente scritta ed utilizzata da una singola persona e quindi non c'è stata attenzione verso alla chiarezza espositiva.

La posizione degli apparati è stata modificata in modo da seguire più fedelmente la loro collocazione reale, favorendone una identificazione più veloce.

Alcune informazioni riportate sugli schemi sono state redatte o omesse per motivi di sicurezza e di privacy.

4.2 Progettazione

Schema di rete? Aggiornamenti configurazioni di rete; Nuove politiche di sicurezza fisica Nuove politiche di sicurezza logica basata su 802.1X

4.2.1 Progettazione Observium

4.2.2 Progettazione RConfig

4.2.3 Definizione name-convention

La name-convention scelta per la denominazione degli apparati è la seguente:

DEVICE-ZONA[-LOCAZIONE] [-NUMERO_INC]

Nella quale i campi presenti indicano:

- **DEVICE**: Il modello del dispositivo installato, ad esempio "HP-2520-8-PoE";
- **ZONA**: La zona di appartenenza del dispositivo, ad esempio "ZONA-A", "EDIFICIO" o "AMMINISTRAZIONE";
- **LOCAZIONE**: La locazione geografica utilizzata per identificare il dispositivo, opzionale nel caso basti la zona per l'identificazione univoca dell'armadio;
- **NUMERO_INC**: Numero incrementale, da incrementare nel caso di più apparati nello stesso armadio di rete.

Questa convenzione è stata scelta in accordo con il cliente per permettere una identificazione veloce dell'apparato di rete anche ai manutentori, in linea con le denominazione utilizzata internamente.

La presenza del modello di dispositivo è contrario alla best-practice da seguire, in quanto la sostituzione di un apparato con un modello successivo richiede la sostituzione della voce all'interno del DNS e di conseguenza la riconfigurazione dei software di monitoraggio. Ciò è stato richiesto in quanto si favorisce l'immediatezza dell'identificazione del dispositivo a discapito della manutenibilità, tenendo in considerazione che gli upgrade non sono frequenti.

4.2.4 Inserimento nomi DNS sulla lista apparati

TODO:

Nuovo sistema di monitoraggio di rete complementare basato su software Observius;

Nuovo sistema di backup configurazioni apparati di rete basato su software RCon-
fig;
Definizione name-convention per gli apparati;
Lista dei test e risultati previsti;
Produzione della prima bozza della documentazione progettuale.

4.3 Implementazione

4.4 Test in produzione

4.5 Tuning

Capitolo 5

Valutazione retrospettiva

5.1 Risultati ottenuti

5.2 Vincoli del progetto

Vincoli tecnologici

Vincoli metodologici e di lavoro

Vincoli temporali

Appendici

Appendice A: Schemi di rete

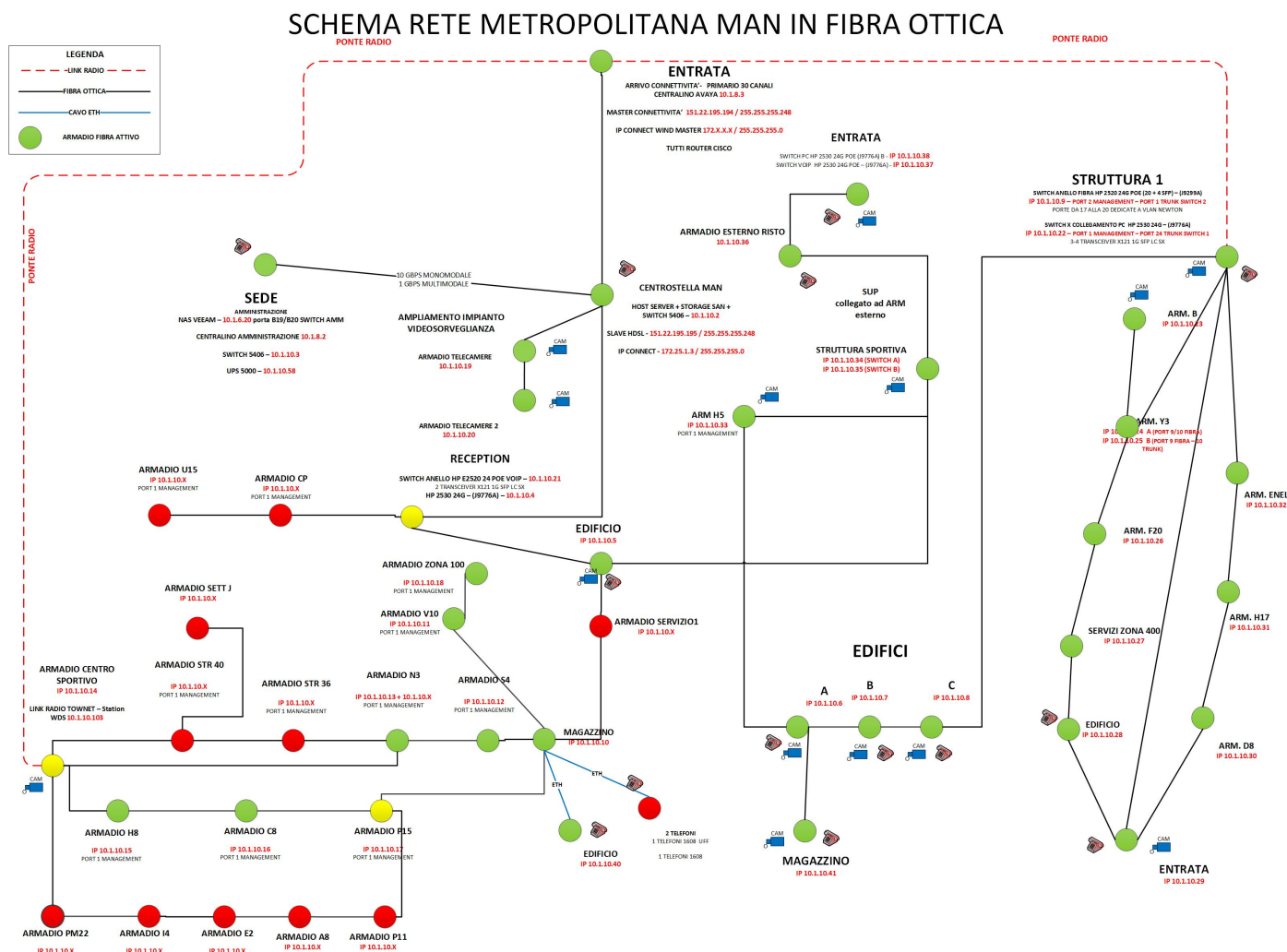


Figura 5.1: Schema Visio della rete datato 2015

LITANA MAN IN FIBRA OTTICA

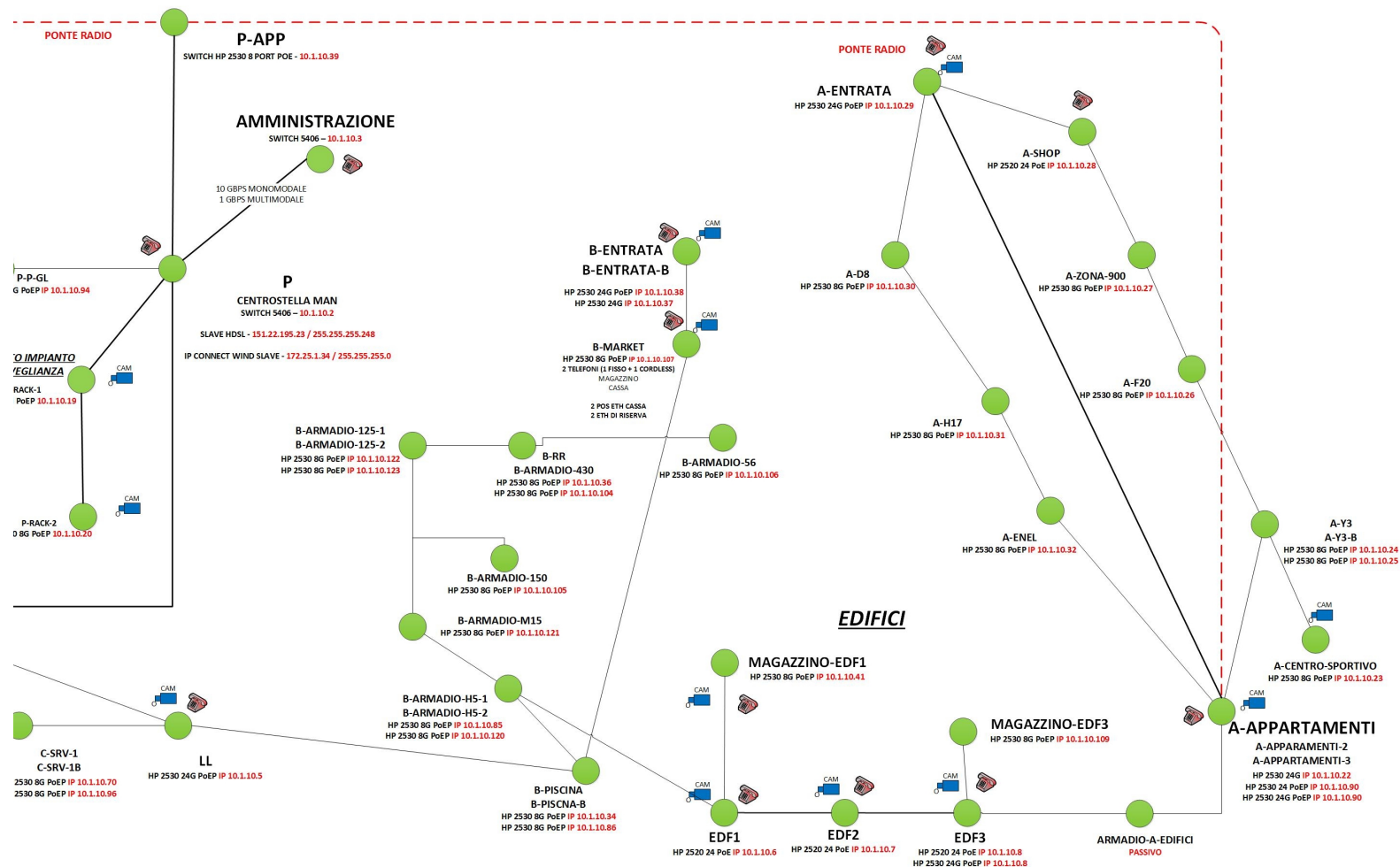


Figura 5.3: Schema Visio della rete a fine stage, seconda parte

Appendice B: Script di popolamento rConfig

Il codice sotto riportato è uno script in linguaggio JavaScript per il popolamento automatico, una volta inseriti i dati, di rConfig.

Lo script può essere utilizzato mediante il plug-in GreaseMonkey versione 4.0 o successive, in quanto richiede l'archiviazione di un valore nella memoria dell'estensione per funzionare.

```

1  // ==UserScript==
2  // @name      auto-insert-devices-rConfig
3  // @namespace  MircoCailottoWintech
4  // @include    https://INDIRIZZO_RCONFIG/devices.php
5  // @version    1
6  // @grant      GM.setValue
7  // @grant      GM.getValue
8  // ==/UserScript==
9
10 // DATA
11
12 const data = [
13 ["INDIRIZZO-DISPOSITIVO-IN-DNS", "", "ENABLE-PROMPT#", "MARCA", "
14  MODELLO", "GRUPPO", "LOCAZIONE", "TEMPLATE_DI_RECUPERO_DATI"],
15 ["HP3850-24G-POE-C-ARMADIO-S123", "", "ARMADIO-S123#", "HP", "
16  HP3850-24G-POE", "SwitchesHP", "ClienteA", "HP Procurve SSH no
17  enable - HP-Procurve-SSH-no-enable.yml"],
18 ["HP3850-24G-POE-C-ARMADIO-C23", "", "C-ARMADIO-C23#", "HP", "
19  HP3850-24G-POE", "SwitchesHP", "ClienteA", "HP Procurve SSH no
20  enable - HP-Procurve-SSH-no-enable.yml"],
21 ];
22
23 function insertData(index) {
24     document.getElementById('deviceName').value = data[index][0];
25     document.getElementById('deviceEnablePrompt').value = data[index
26     ][1];
27     document.getElementById('devicePrompt').value = data[index][2];
28
29     var select = document.getElementById('vendorId');
30     for (var i = 0; i < select.options.length; i++) {
31         if (select.options[i].text === data[index][3]) {
32             select.selectedIndex = i;
33             break;
34         }
35     }
36
37     document.getElementById('deviceModel').value = data[index][4];
38 }

```

```

34 select = document.getElementById('catId');
35 for (var i = 0; i < select.options.length; i++) {
36     if (select.options[i].text === data[index][5]) {
37         select.selectedIndex = i;
38         break;
39     }
40 }
41
42 document.getElementById('custom_Location').value = data[index
    ][6];
43
44 select = document.getElementById('templateId');
45 for (var i = 0; i < select.options.length; i++) {
46     if (select.options[i].text === data[index][7]) {
47         select.selectedIndex = i;
48         break;
49     }
50 }
51
52 //LOGIN
53 document.getElementById('defaultCreds').checked = true;
54 // document.getElementById('deviceUsername').value = "username";
55 // document.getElementById('devicePassword').value = "password";
56 // document.getElementById('deviceEnablePassword').value = "
    passwordroot";
57 };
58
59 function clickOkButton() {
60     setTimeout(function(){
61         unsafeWindow.resolveDevice(document.getElementById('deviceName
            ').value);
62         setTimeout(function(){
63             document.getElementById("submit").click();
64         }, 500);
65     }, 500);
66 };
67
68 window.addEventListener('load', function() {
69     // once loaded
70     (async () => {
71         console.log("Async call");
72
73         // ----- RESET THE SCRIPT -----
74         var reset = false;
75
76         if(reset) {
77             GM.setValue('count', 0);
78         } else {
79             var index = await GM.getValue('count', 0);

```



```

80
81     if(index < data.length) {
82         //insert
83         console.log("Adding item number:");
84         console.log(index);
85         insertData(index);
86         GM.setValue('count', index + 1);
87         clickOkButton();
88     } else {
89         //done, do nothing
90         console.log("Already done");
91     }
92 }
93 }();
94 }, false);

```

Listing 5.1: My Javascript Example

Le linee 13, 14 e 15 sono 3 apparati che saranno inseriti alla esecuzione dello script, i campi sono:

1. Indirizzo DNS del dispositivo
2. Prompt del dispositivo in modalità non privilegiata, opzionale
3. Prompt del dispositivo in modalità privilegiata
4. Marca del dispositivo
5. Modello del dispositivo
6. Gruppo rConfig di appartenenza del dispositivo, utilizzabile per il filtraggio
7. Locazione del dispositivo, utilizzabile per il filtraggio
8. Template rConfig relativo alla configurazione da utilizzare per il recupero dei dati

Le linee 54, 55 e 56 presentano la possibilità di specificare i parametri per effettuare il login ai dispositivi, attualmente non utilizzati in quanto si utilizza le credenziali impostate come di default.

La linea 74 presenta un variabile "reset" che se impostata a true, invece che eseguire lo script, va ad azzerare i valori utilizzati dal plugin, permettendone una seconda esecuzione.

Glossario

Digital Transformation

La Digital Transformation, o trasformazione digitale, è quell'insieme di cambiamenti nei comportamenti aziendali e di business collegato e veicolato dalla tecnologia digitale, tramite il quale è possibile trapiantare una maggiore competitività di mercato.

Quality Of Service

La qualità del servizio, documentata mediante *Request For Comments*_G, è la descrizione o la misurazione delle performance di un servizio di rete, secondo la visione da parte dell'utente a seconda della possibile attività che sta svolgendo.

Request For Comments

Una "richiesta di commenti", usualmente indicata utilizzando unicamente la sigla RFC, è un documento pubblicato dalla Internet Engineering Task Force, che riporta informazioni riguardanti nuove ricerche, innovazioni e metodologie dell'ambito informatico.

Sicurezza fisica

Per sicurezza fisica si intendono il complesso di soluzioni tecnico-pratiche il cui obiettivo è quello di impedire che utenti non autorizzati possano accedere a risorse, sistemi, impianti, dispositivi, apparati, informazioni e dati di natura riservata.

Sicurezza logica

Per sicurezza logica si intendono il complesso di soluzioni che impediscono ad utenti non autorizzati di compiere azioni che richiedono dei privilegi più elevati rispetto a quelli in loro possesso.

System Integrator

Con il termine System Integrator viene indicata una azienda che si occupa di far dialogare impianti diversi tra di loro allo scopo di creare una nuova struttura funzionale che possa utilizzare le potenzialità di impianti d'origine e creare quindi funzionalità originariamente non presenti.

Bibliografia

asd