Defense in Depth + Sinema Remote Connect

Labs

Answers for industry.

Labs

Appendix

Labs

Initial Information

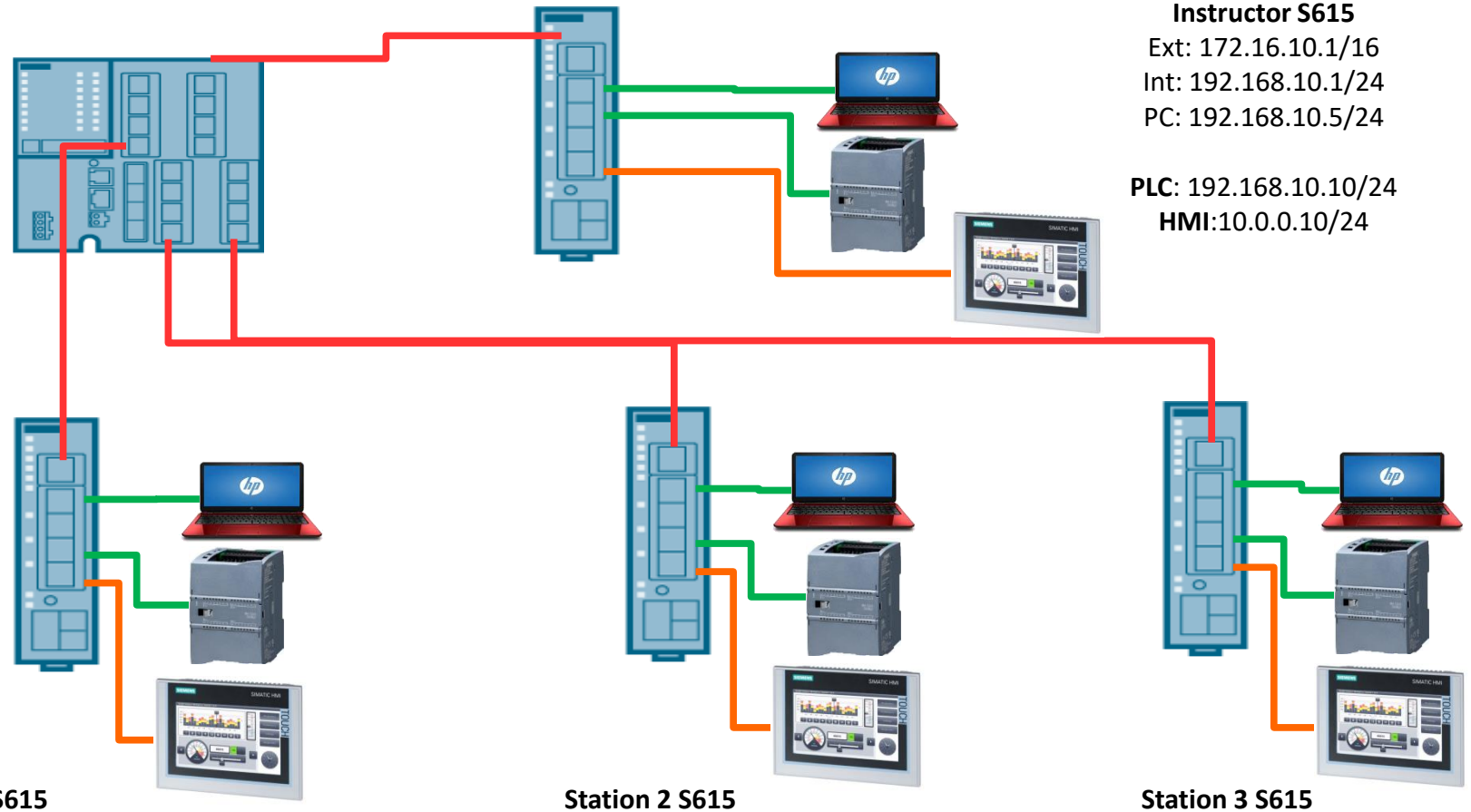
Routing / Masquerading – Additional Information
Lab

SIEMENS

Station	Instructor		1	2	3	4	5	6	7	8
S615										
Ext	172.16.10.1/16		172.16.1.1/16	172.16.2.1/16	172.16.3.1/16	172.16.4.1/16	172.16.5.1/16	172.16.6.1/16	172.16.7.1/16	172.16.8.1/16
Int	192.168.10.1/24		192.168.1.1/24	192.168.1.1/24	192.168.1.1/24	192.168.1.1/24	192.168.1.1/24	192.168.1.1/24	192.168.1.1/24	192.168.1.1/24
VLAN3	10.0.0.1/24		10.0.0.1/24	10.0.0.1/24	10.0.0.1/24	10.0.0.1/24	10.0.0.1/24	10.0.0.1/24	10.0.0.1/24	10.0.0.1/24
HMI	192.168.10.10/24		192.168.1.10/24	192.168.1.10/24	192.168.1.10/24	192.168.1.10/24	192.168.1.10/24	192.168.1.10/24	192.168.1.10/24	192.168.1.10/24
PLC	10.0.0.10/24		10.0.0.11/24	10.0.0.12/24	10.0.0.13/24	10.0.0.14/24	10.0.0.15/24	10.0.0.16/24	10.0.0.17/24	10.0.0.18/24

Routing / Masquerading – Network Layout

Lab



Instructor S615
Ext: 172.16.10.1/16
Int: 192.168.10.1/24
PC: 192.168.10.5/24

PLC: 192.168.10.10/24
HMI:10.0.0.10/24

Station 1 S615
Ext: 172.16.1.1/16 GW:172.16.10.1
Int: 192.168.1.1/24
PC: 192.168.1.5/24 GW 192.168.1.1

PLC:192.168.1.10/24
HMI: 10.0.0.11/24

Station 2 S615
Ext: 172.16.2.1/16 GW:172.16.10.1
Int: 192.168.1.1/24
PC: 192.168.1.5/24 GW:192.168.1.1

PLC:192.168.1.10/24
HMI: 10.0.0.12/24

Station 3 S615
Ext: 172.16.3.1/16 GW:172.16.10.1
Int: 192.168.1.1/24
PC: 192.168.1.5/24 GW:192.168.1.1

PLC:192.168.1.10/24
HMI: 10.0.0.13/24

Labs

Subnetting Lab Exercises

Subnetting Cheat Sheet

Quick Formulas:

- Number of subnets = 2^s (where s is the number of bits borrowed)
- Number of host addresses available per subnet = $2^h - 2$ (where h is the number of host bits remaining after bits are borrowed)

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	Power of 2
128	64	32	16	8	4	2	1	Network Increments (address multiples)
.128	.192	.224	.240	.248	.252	.254	.255	mask
2	4	8	16	32	64	128	256	# of subnetworks (2 to the power of # of borrowed bits)
/25	/26	/27	/28	/29	/30	/31	/32	CIDR C
/17	/18	/19	/20	/21	/22	/23	/24	CIDR B
/9	/10	/11	/12	/13	/14	/15	/16	CIDR A

Subnetting Lab Exercise #1

Task: Given the IP host address of 192.168.3.222/27, find the following:

- Subnet Mask
- Sub-network starting address
- 1st host address
- Last host address
- Broadcast address
- Starting address of the next network

IP host address	192.168.3.222/27
Mask	
Sub-network	
1st Host	
Last Host	
Broadcast	
Next Network	

Subnetting Lab Exercise #2

Task: Given the IP host address of 172.28.114.9/21, find the following:

- Subnet Mask
- Sub-network starting address
- 1st host address
- Last host address
- Broadcast address
- Starting address of the next network

IP host address	172.28.114.9/21
Mask	
Sub-network	
1st Host	
Last Host	
Broadcast	
Next Network	

Subnetting Lab Exercise #3

Task: Given the IP host address of 192.168.247.246/30, find the following:

- Subnet Mask
- Sub-network starting address
- 1st host address
- Last host address
- Broadcast address
- Starting address of the next network

IP host address	192.168.247.246/30
Mask	
Sub-network	
1st Host	
Last Host	
Broadcast	
Next Network	

Subnetting Bonus Question

On the network 131.1.123.0/27, what is the last IP address that can be assigned to a host?

A. 131.1.123.30

B. 131.1.123.31

C. 131.1.123.32

D. 131.1.123.33

Slide Intentionally Blank

Answer Key

Lab #1

IP host address	192.168.3.222/27
Mask	255.255.255.224
Sub-network	192.168.3.192
1st Host	192.168.3.193
Last Host	192.168.3.222
Broadcast	192.168.3.223
Next Network	192.168.3.224

Lab #2

IP host address	172.28.114.9/21
Mask	255.255.248.0
Sub-network	172.28.112.0
1st Host	172.28.112.1
Last Host	172.28.119.254
Broadcast	172.28.119.255
Next Network	172.28.120.0

Lab #3

IP host address	192.168.247.246/30
Mask	255.255.255.252
Sub-network	192.168.247.244
1st Host	192.168.247.245
Last Host	192.168.247.246
Broadcast	192.168.247.247
Next Network	192.168.247.248

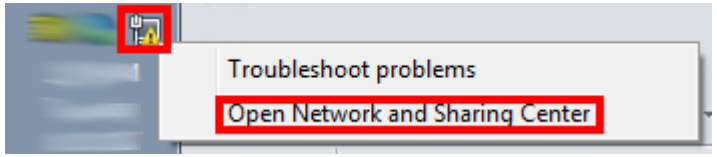
Bonus Question: A

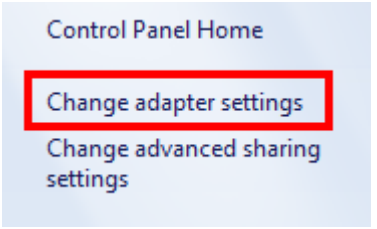
Labs

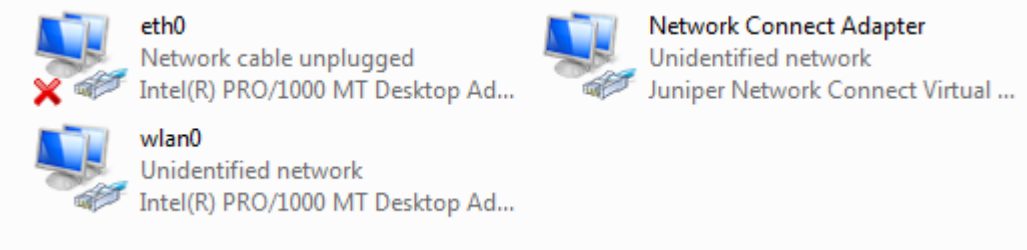
Initial Configuration Lab

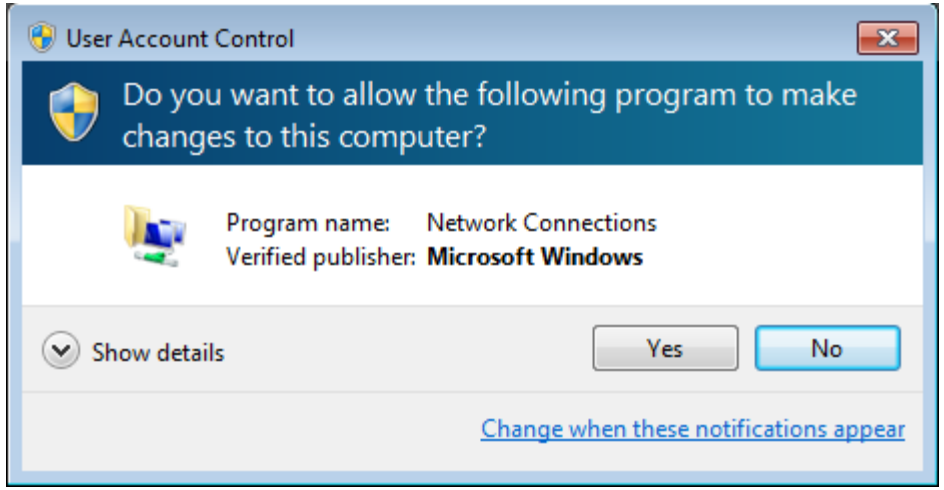
Initial Setup – Configure PC IP Address
Lab

1) Right Click on the Network Icon in the Notification Area
2) Click on Open Network and Sharing Center
3) Click Change adapter settings
4) Select the connected network and double click
5) Accept the Windows warning by clicking Yes





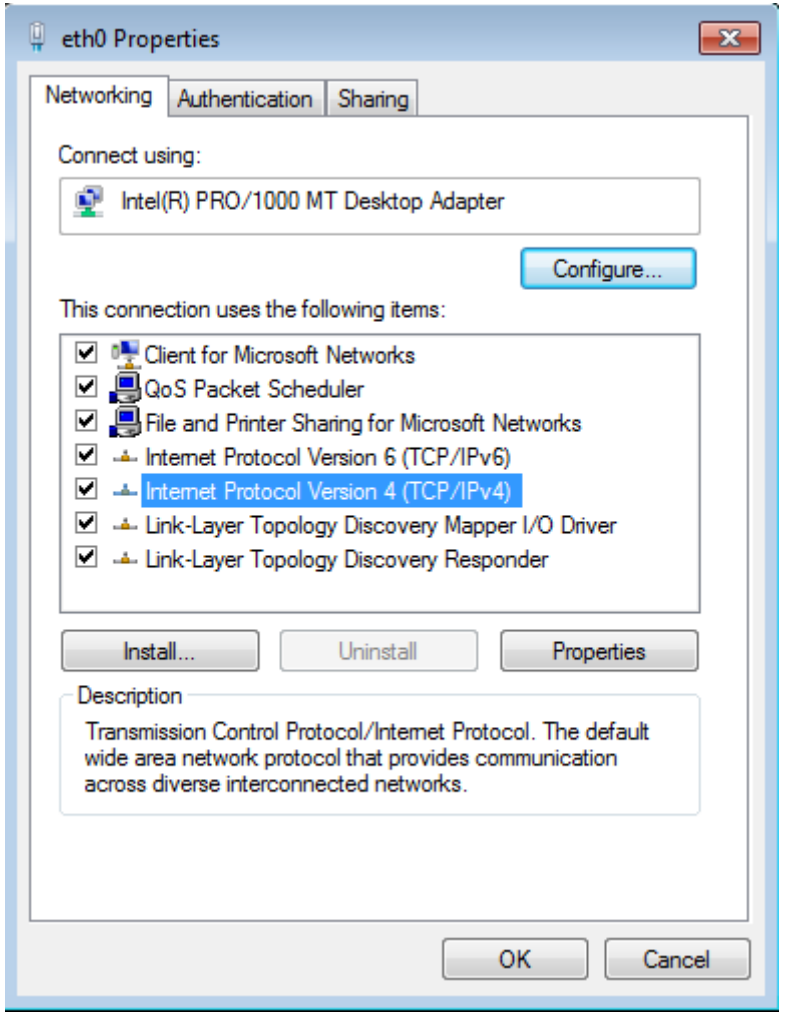


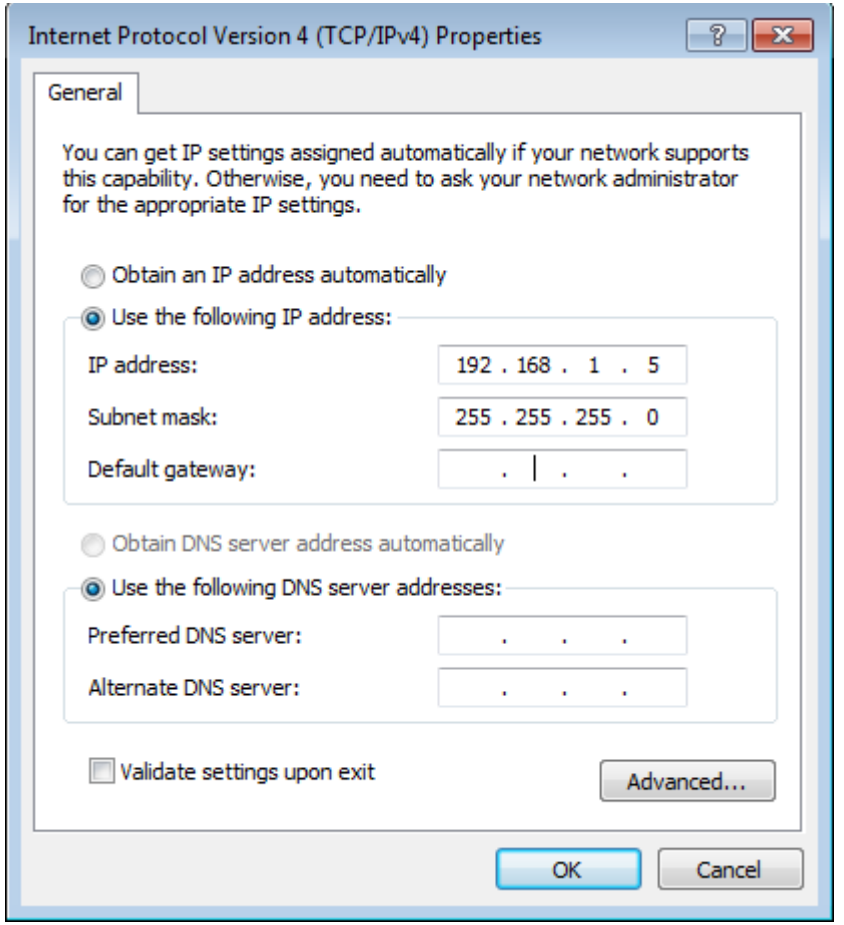


Initial Setup – Configure PC IP Address

Lab

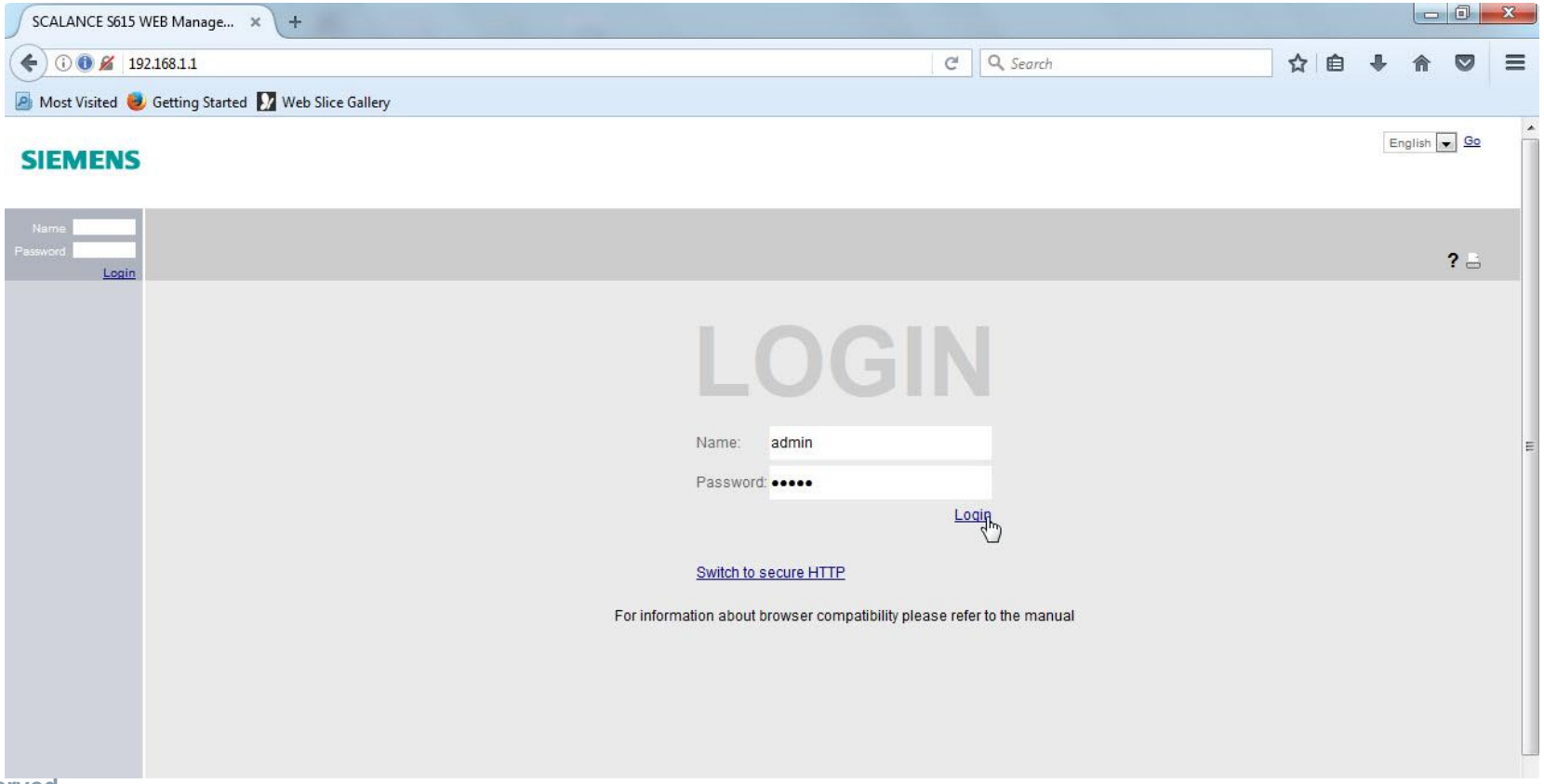
1) Click on Internet Protocol Version 4 (TCP/IPv4)
2) Click Properties
3) Select Use the following IP address:
4) Enter IP and Subnet Mask Only as shown
5) Click OK until all the way out of the network properties screens.
6) Close any remaining open screens.





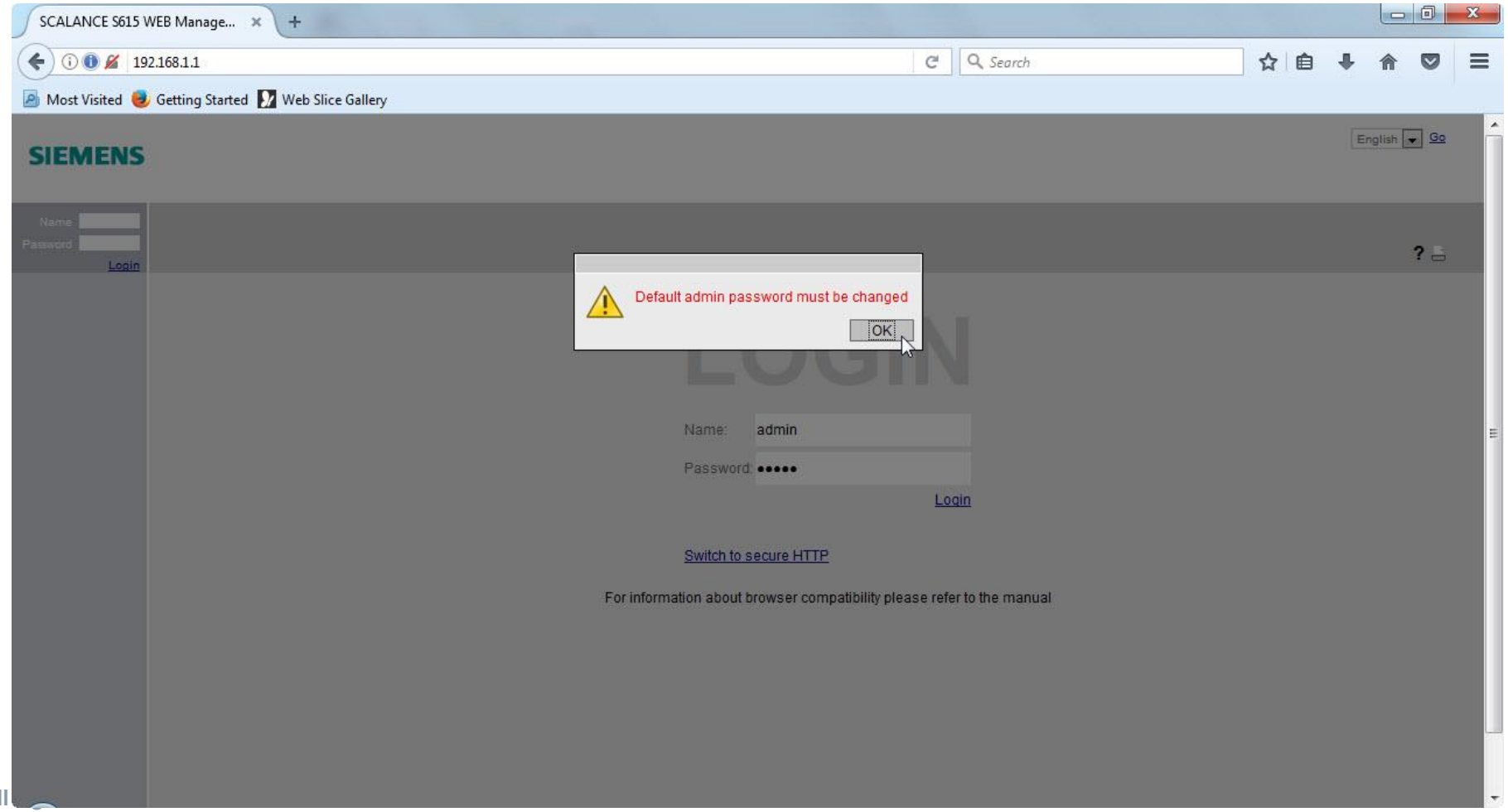
Initial Setup - Login
Lab

1) In web browser type http://192.168.1.1
2) Login with admin for the username and password
3) Click the Login button



Initial Setup - Login
Lab

1) Click OK to acknowledge that the password must be changed



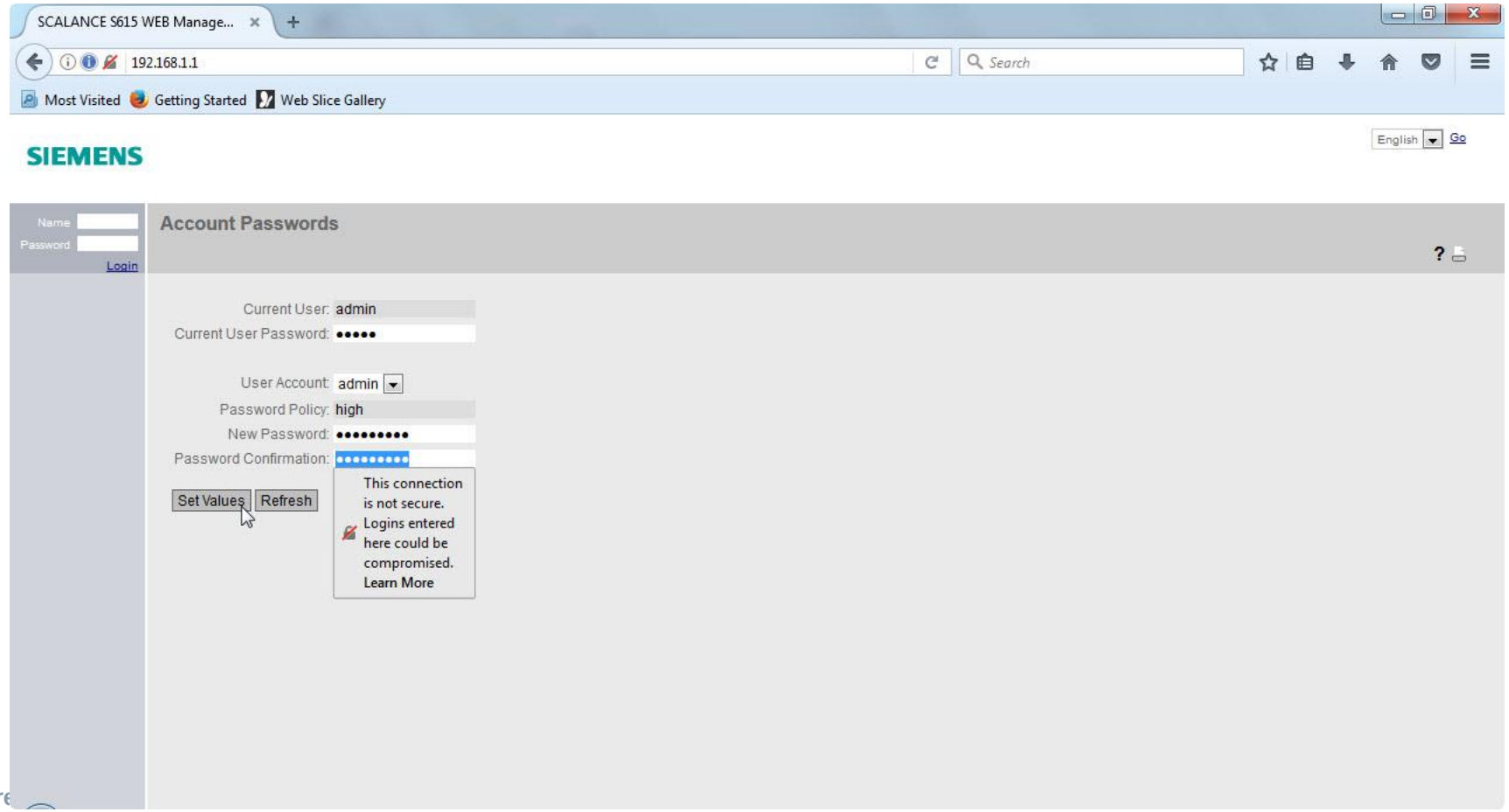
Initial Setup - Login
Lab

1) Enter the Current User Password for admin: admin

2) In New Password box type: Admin!123

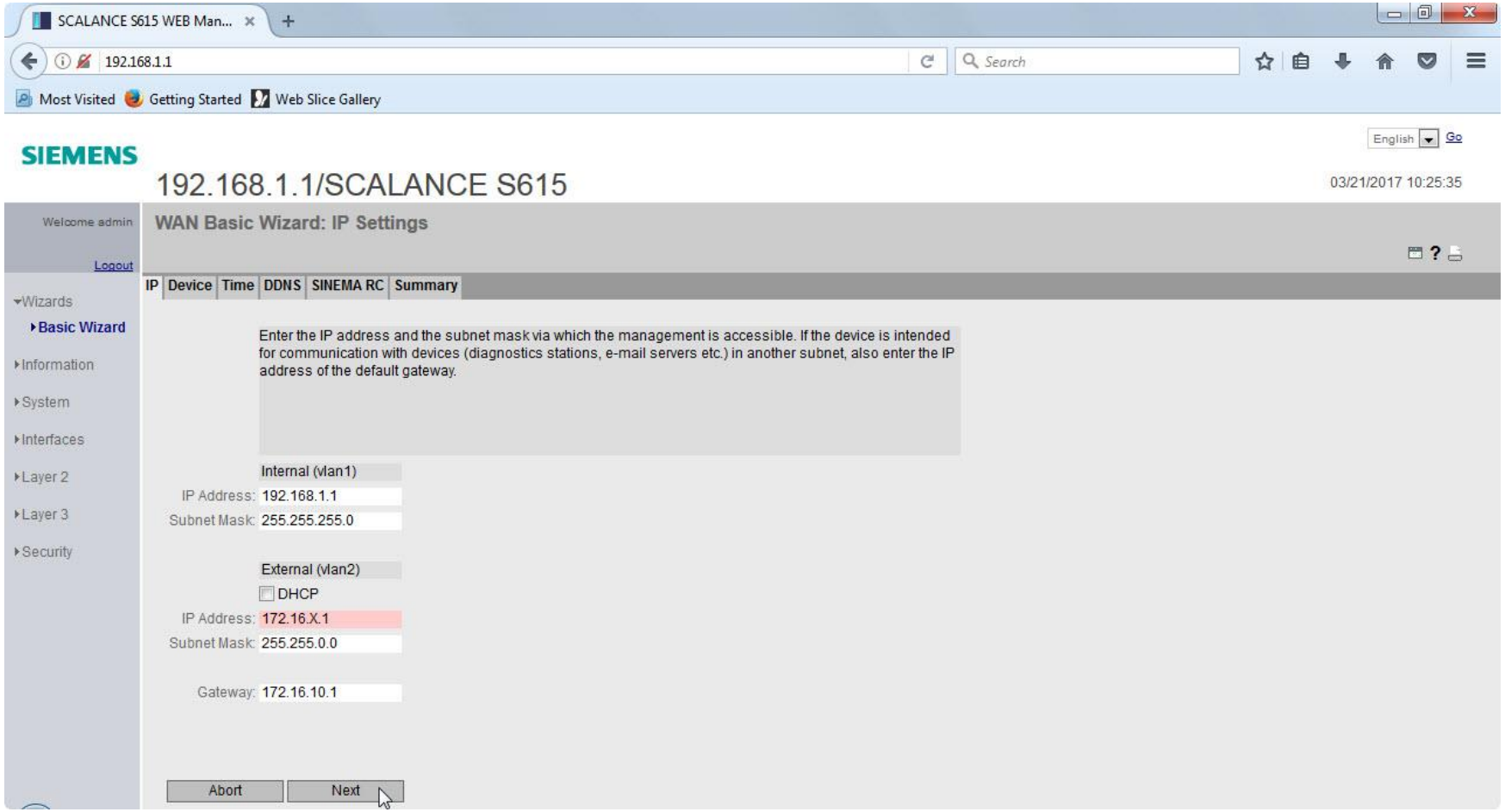
3) In Password Confirmation box type: Admin!123

4) Click Set Values



Initial Setup - Wizard
Lab

1) The Basic Wizard automatically launches
2) Find External (vlan2)
3) In the IP Address type in 172.16.X.1 where the X is replaced by the Station Number you were assigned
4) In the Subnet Mask box type in 255.255.0.0
5) In the Gateway box type 172.16.10.1
6) Click Next

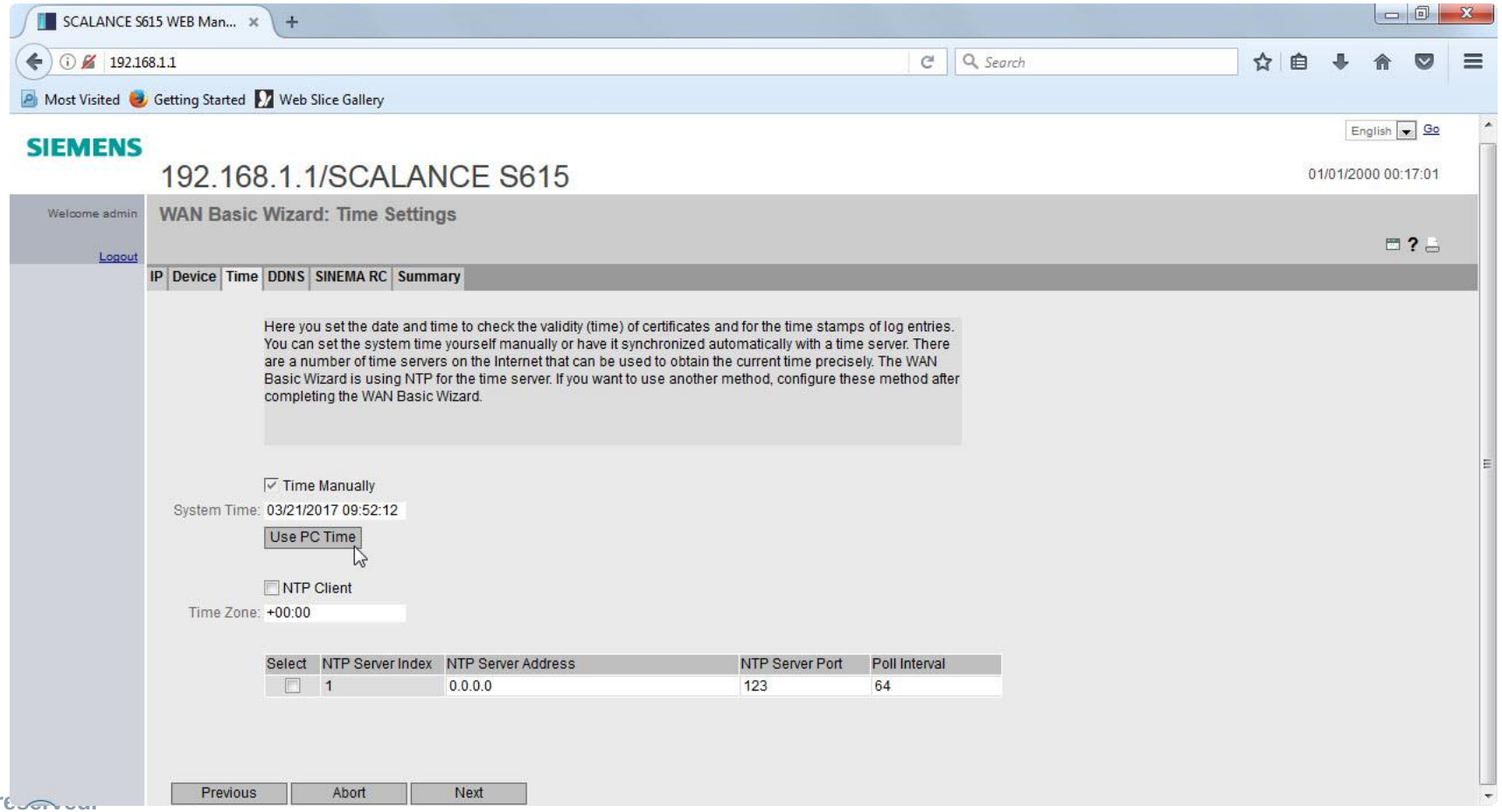


Initial Setup - Wizard
Lab

1) Click Next on the Device tab (we aren't naming the device)

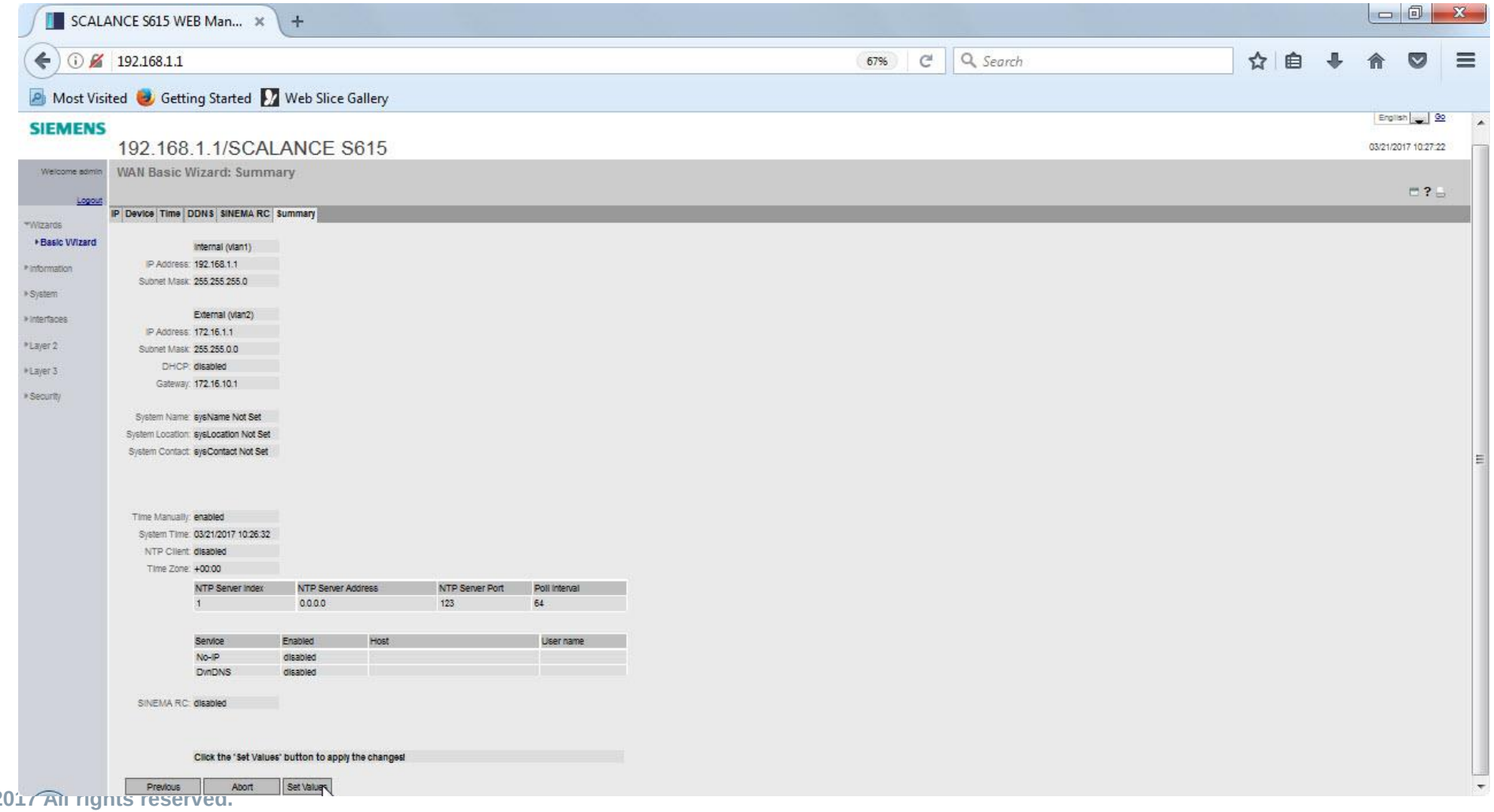
2) Click Use PC Time

3) Click Next



Initial Setup - Wizard
Lab

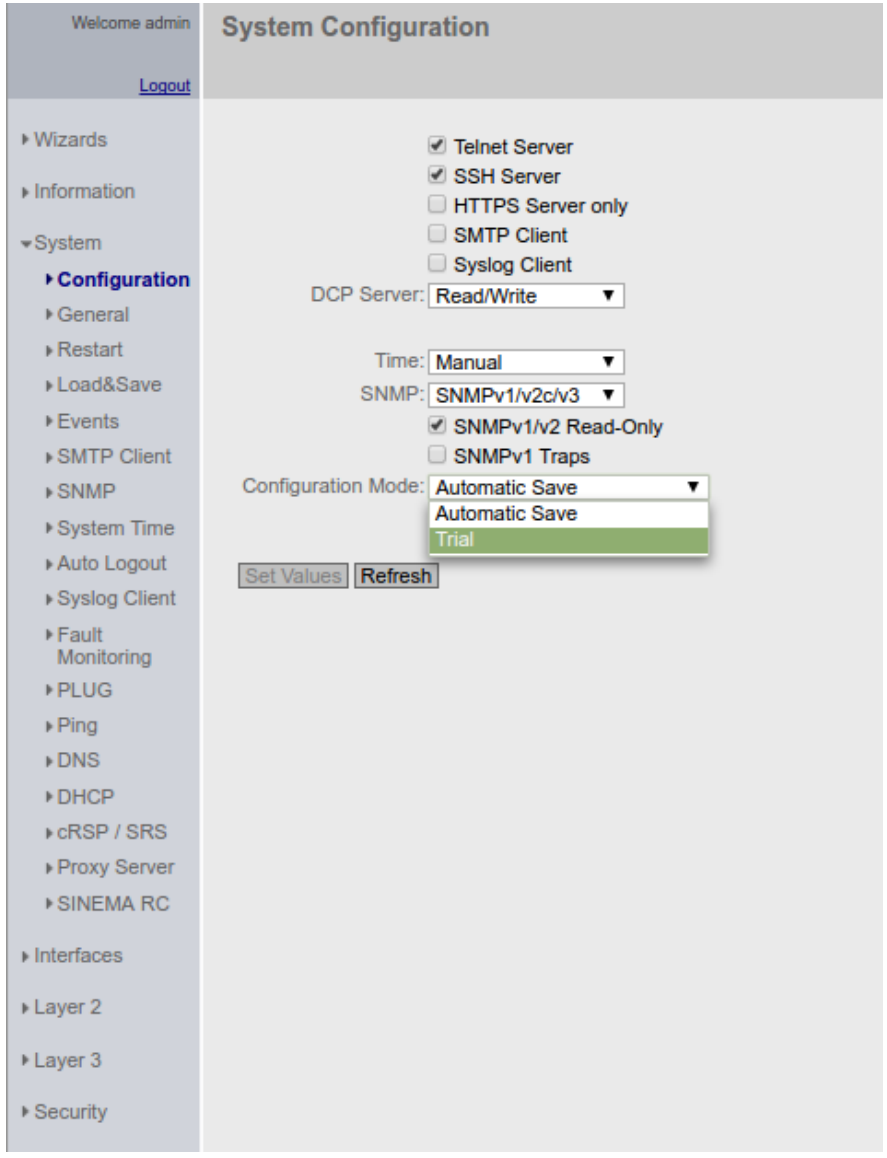
1) Click Next to bypass DDNS
2) Click Next to bypass Sinema RC
3) Verify Settings
4) Click Set Values



Initial Setup – Disable Automatic Save

Lab

1) Navigate to and click on System
2) Navigate to and click on Configuration
3) Change “Configuration Mode” from “Automatic Save” to “Trial”
4) Click Set Values



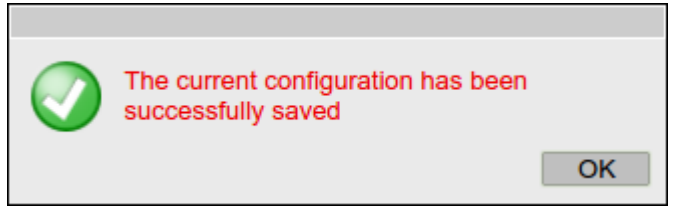
Initial Setup – Write Startup Config
Lab

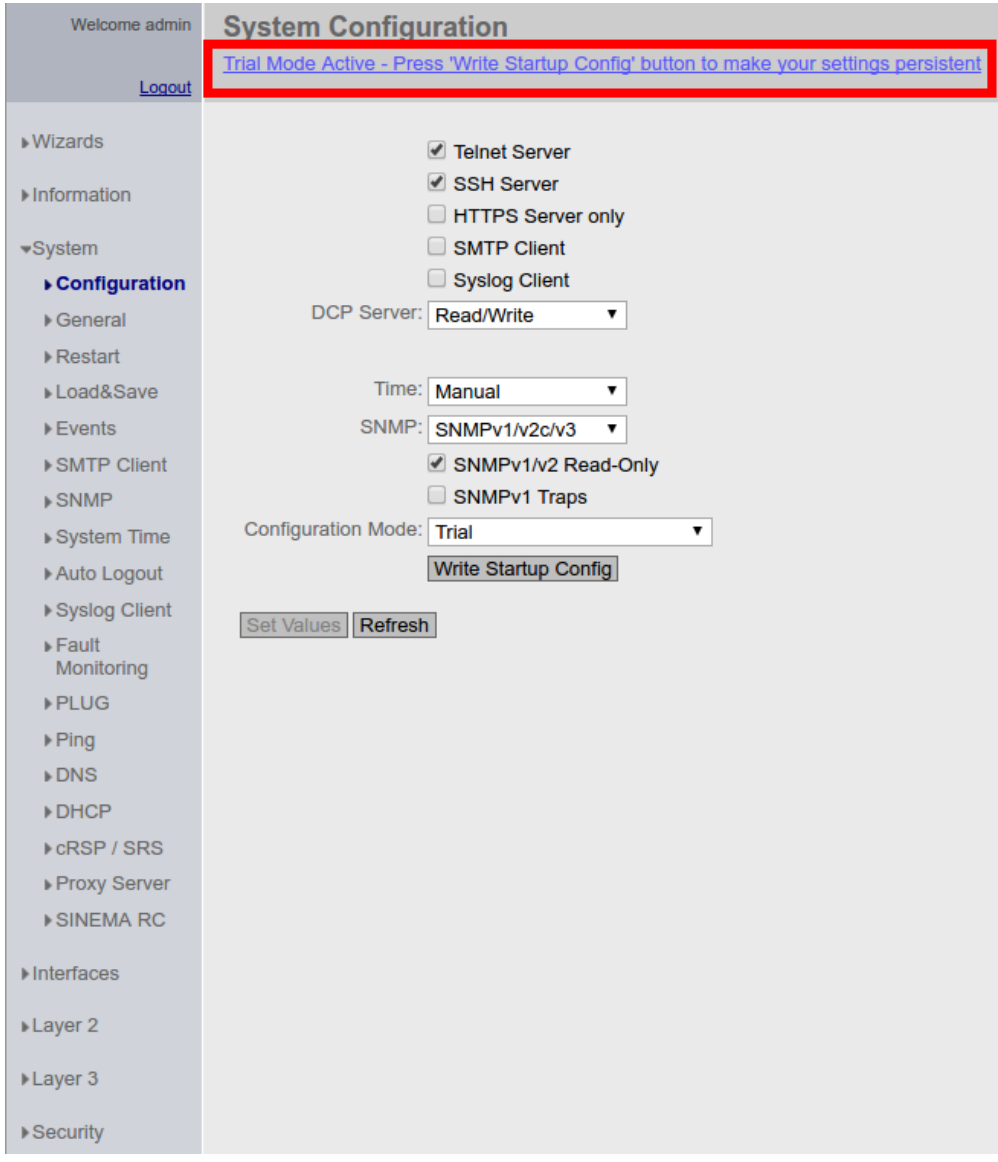
1) Navigate to and click on System

2) Navigate to and click on Configuration
   A. Alternatively, note the hot link at the top of the screen will go to the correct screen

3) Click Write Startup Config button

4) Acknowledge the Success Popup



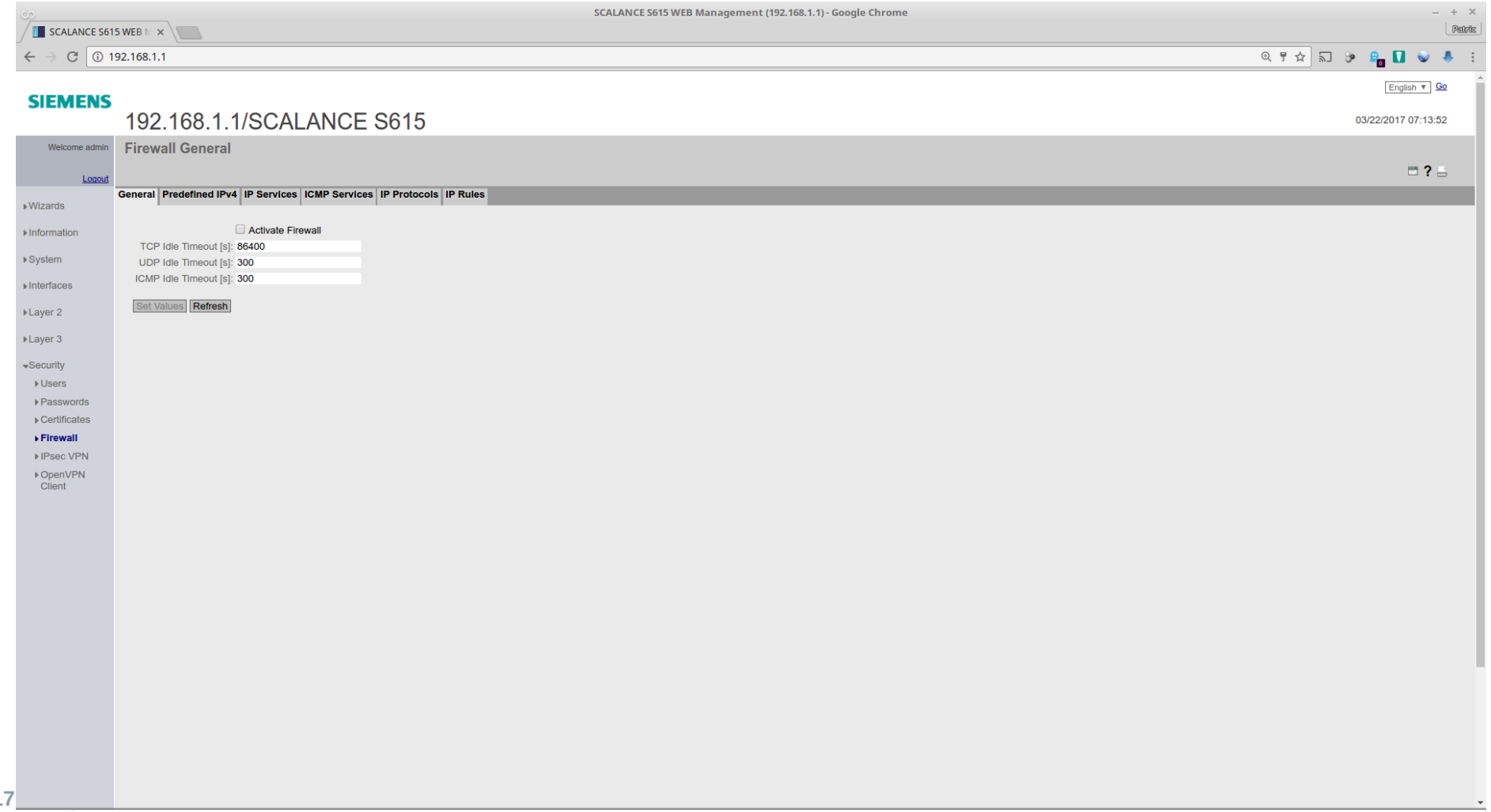


Labs

Routing / Masquerading Lab

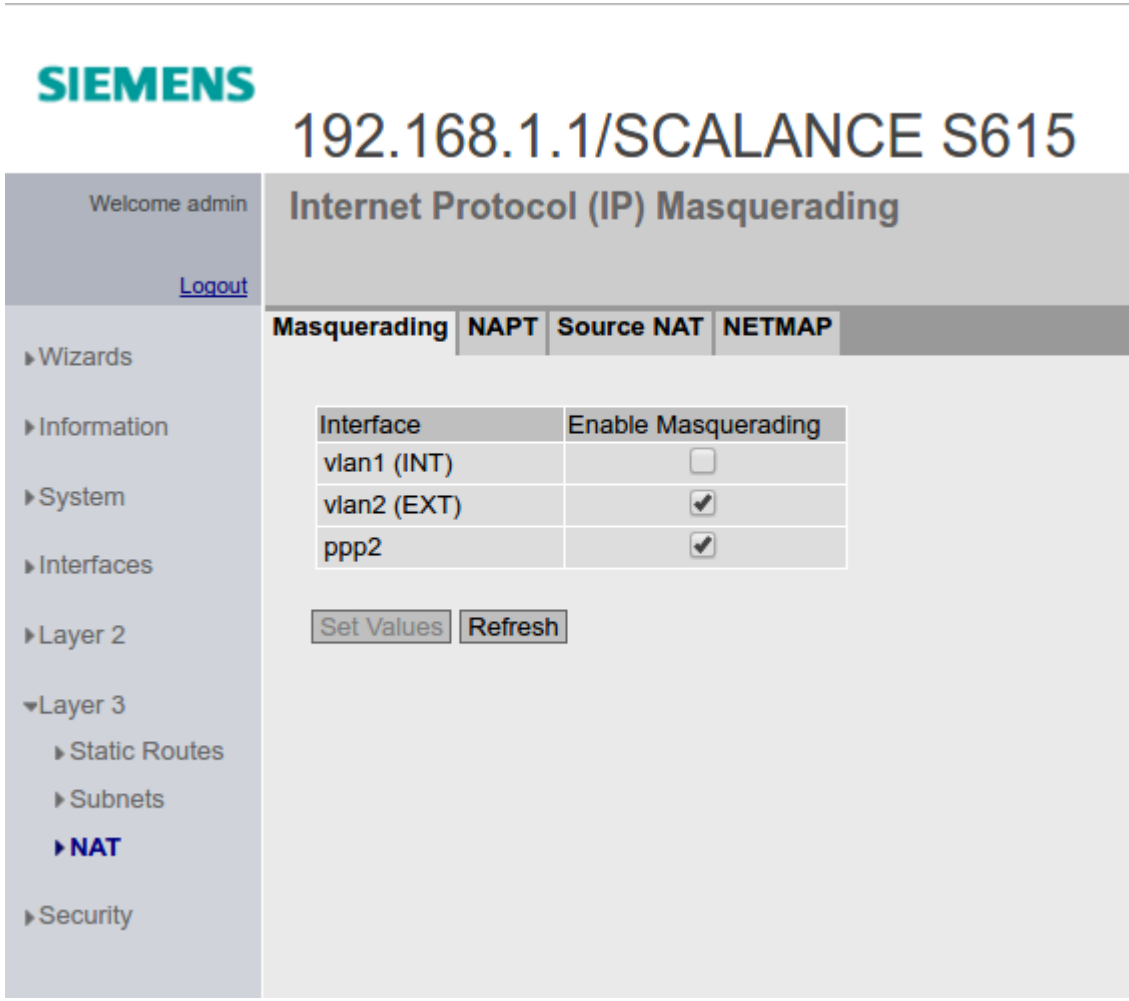
Routing / Masquerading – Disable Firewall
Lab

1) Navigate to and click on Security
2) Navigate to and click on Firewall
3) Uncheck the Activate Firewall box
4) Click Set Values



Routing / Masquerading – Enable Masquerading
Lab

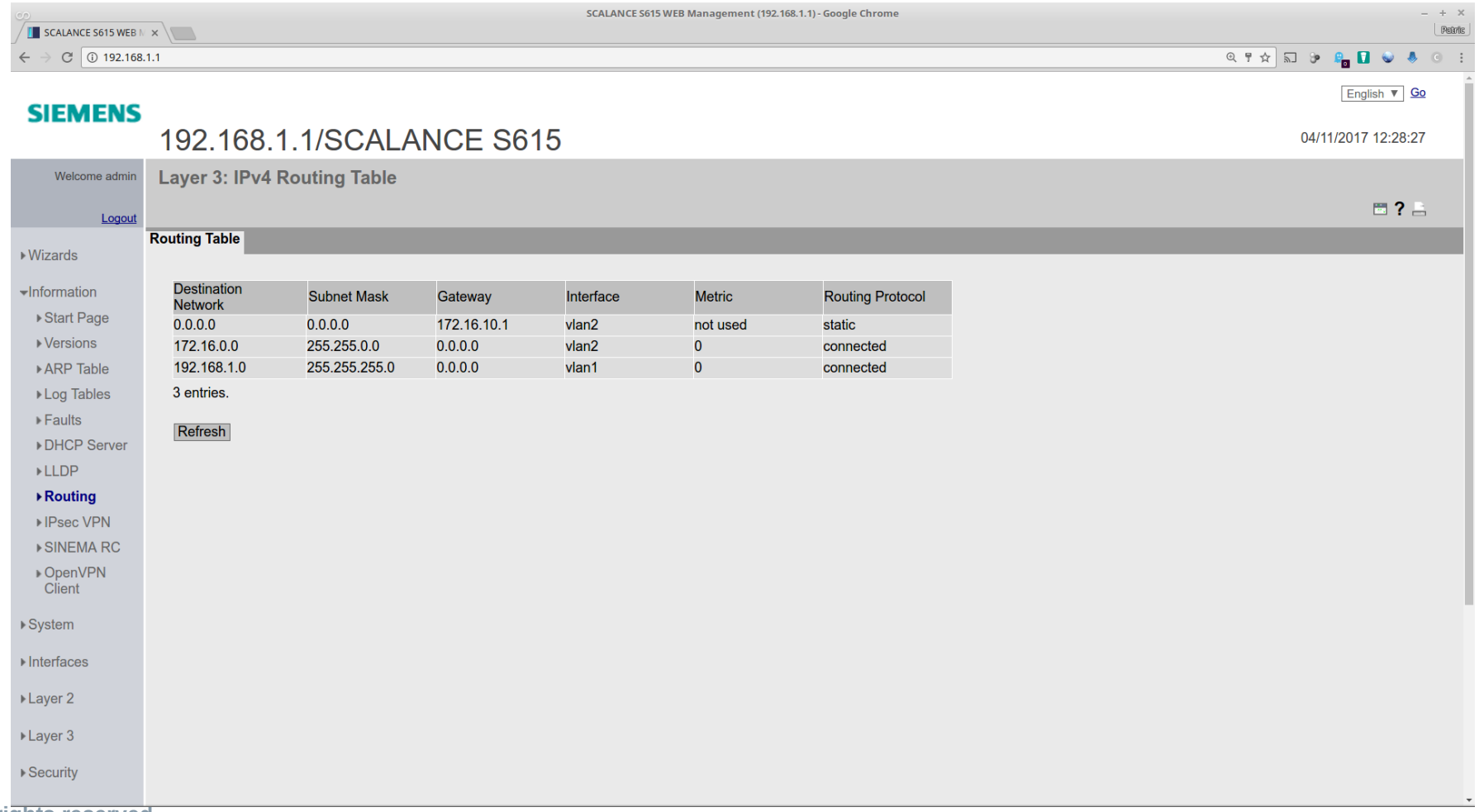
1) Navigate to and click on Layer 3
2) Navigate to and click on NAT
3) Check the Enable Masquerading for vlan2 (EXT)
4) Click Set Values



Routing / Masquerading – Examine Routing Table
Lab

1) Navigate to Information

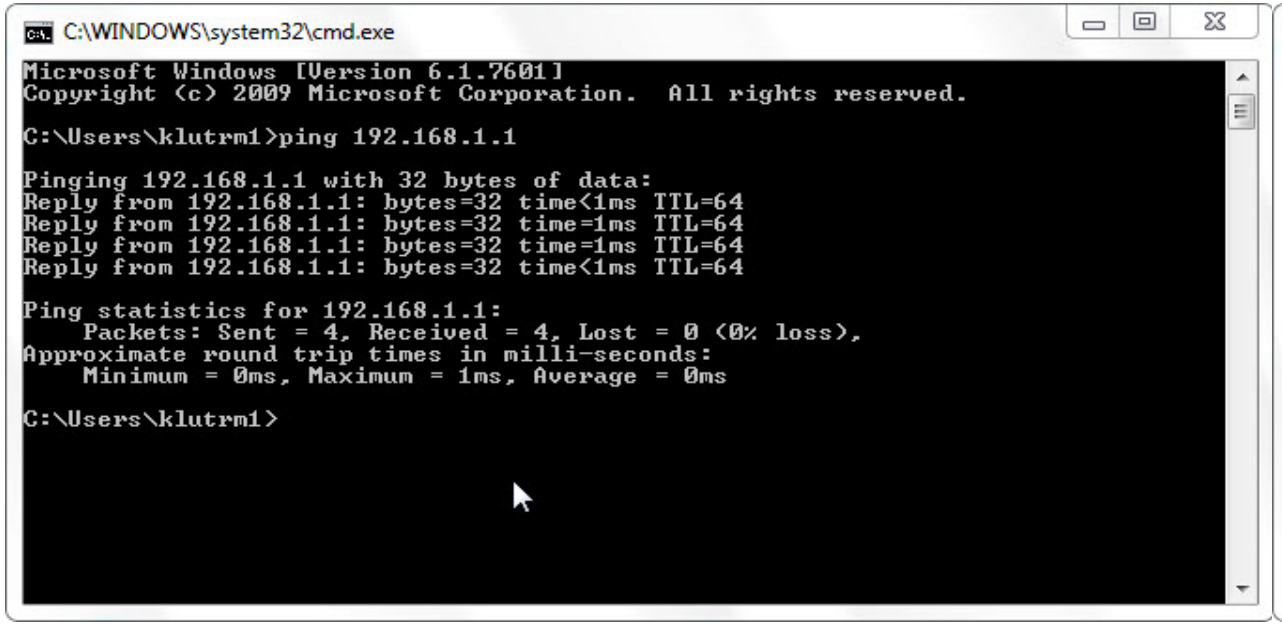
2) Navigate to Routing

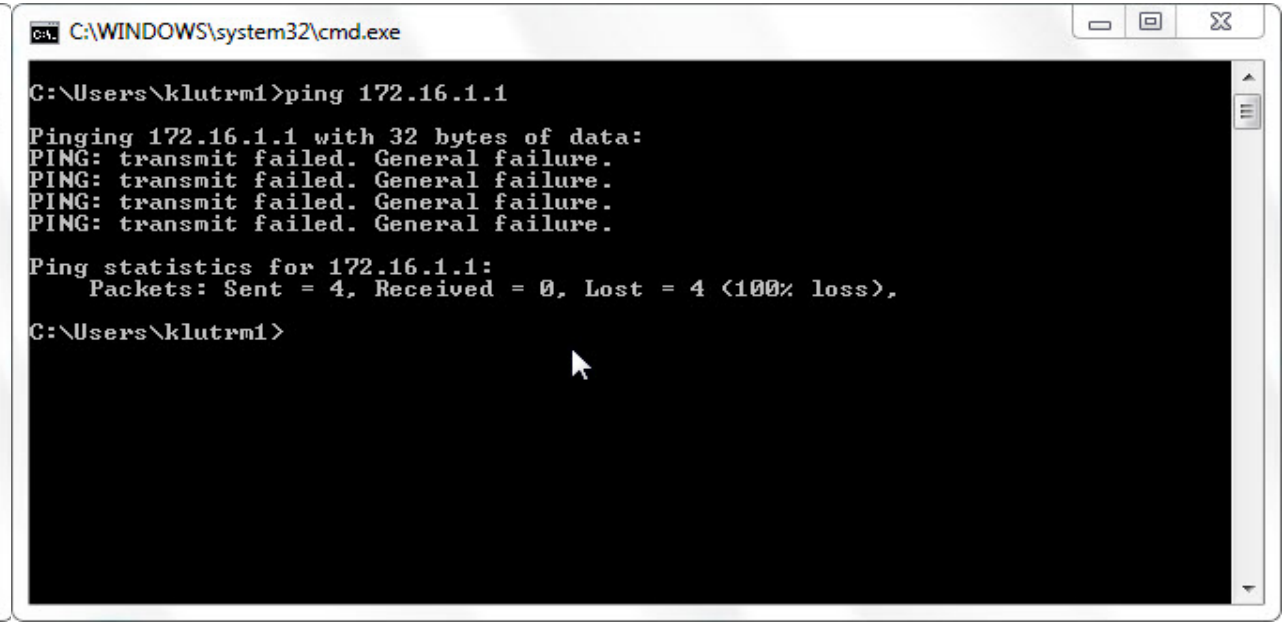


Routing / Masquerading – Ping Test
Lab

1) Ping S615 Internal Address

2) Ping S615 External Address (172.16.X.1 where X is the station number assigned to you)





Routing / Masquerading – Configure PC Gateway Address
Lab

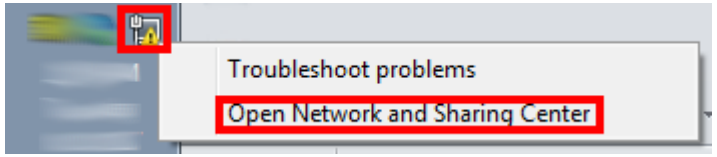
1) Right Click on the Network Icon in the Notification Area

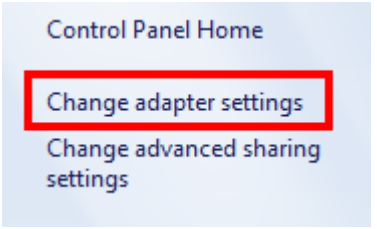
2) Click on Open Network and Sharing Center

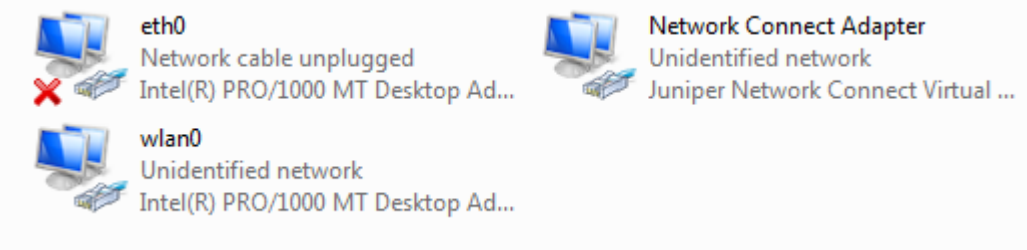
3) Click Change adapter settings

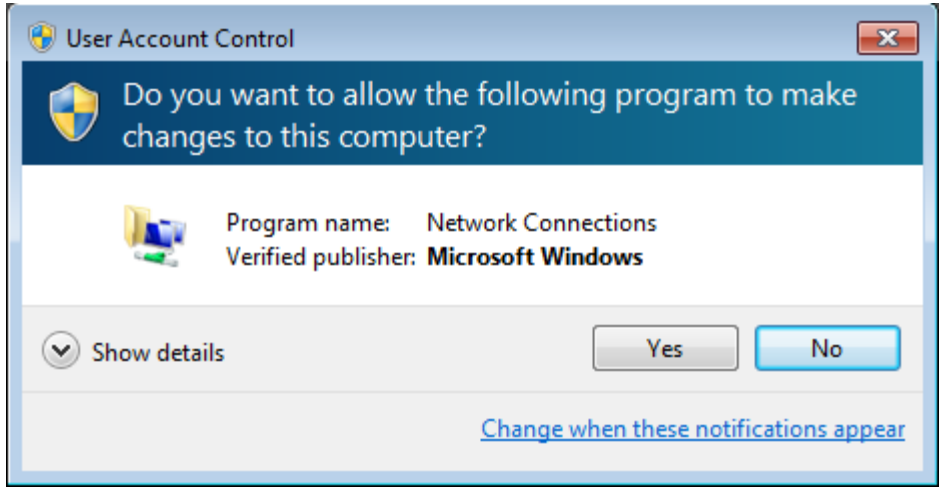
4) Select the connected network and double click

5) Accept the Windows warning by clicking Yes



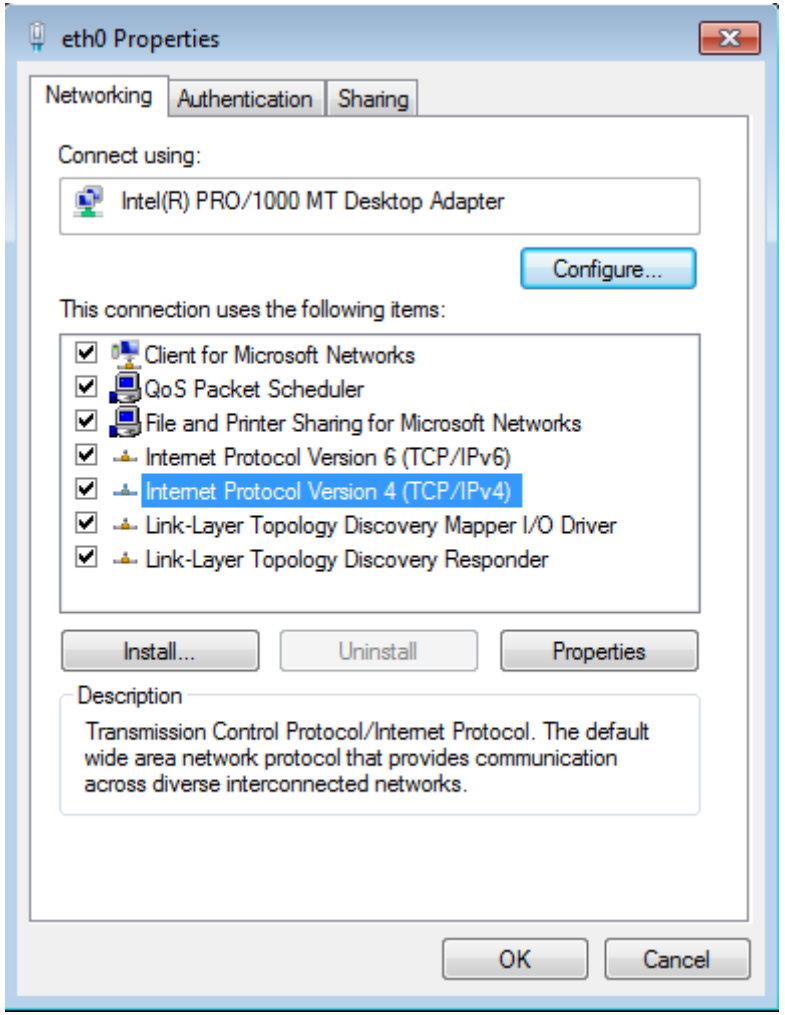


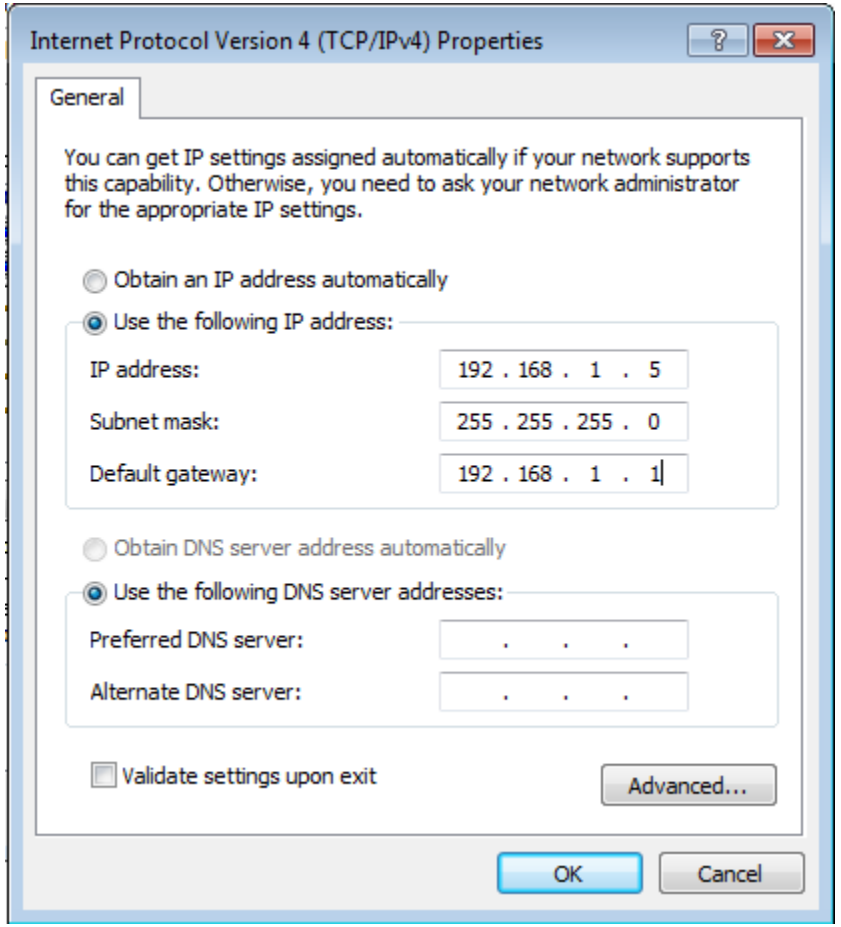




Routing / Masquerading – Configure PC Gateway Address
Lab

1) Click on Internet Protocol Version 4 (TCP/IPv4)
2) Click Properties
3) Enter Default Gateway
4) Click OK until all the way out of the network properties screens.
5) Close any remaining open screens.

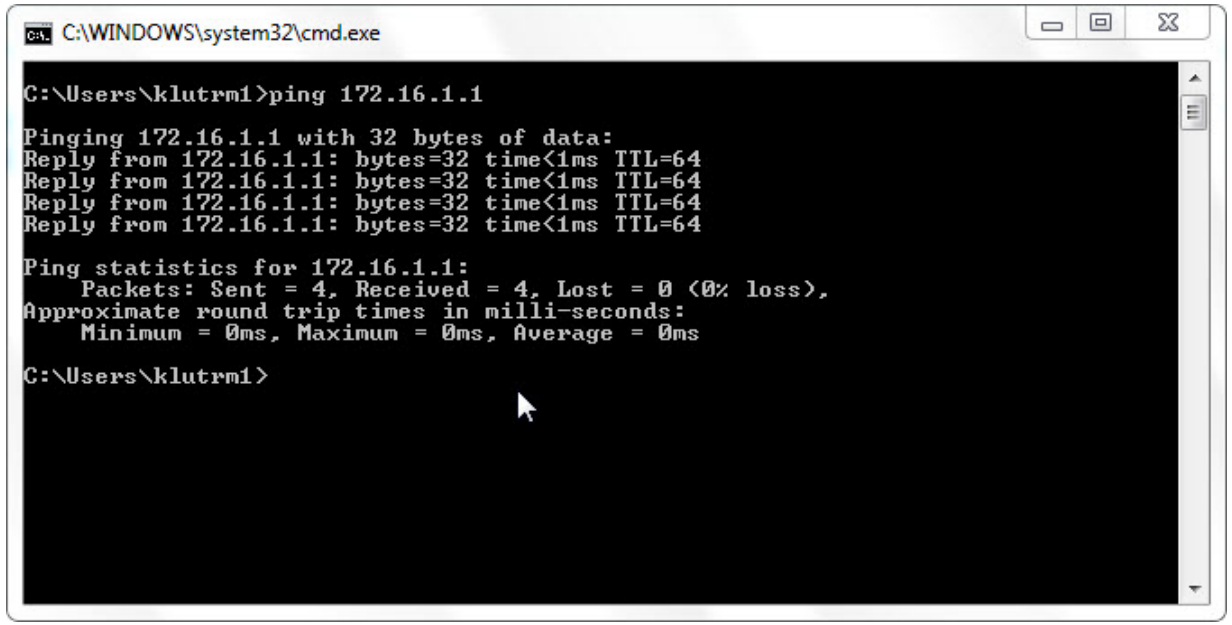


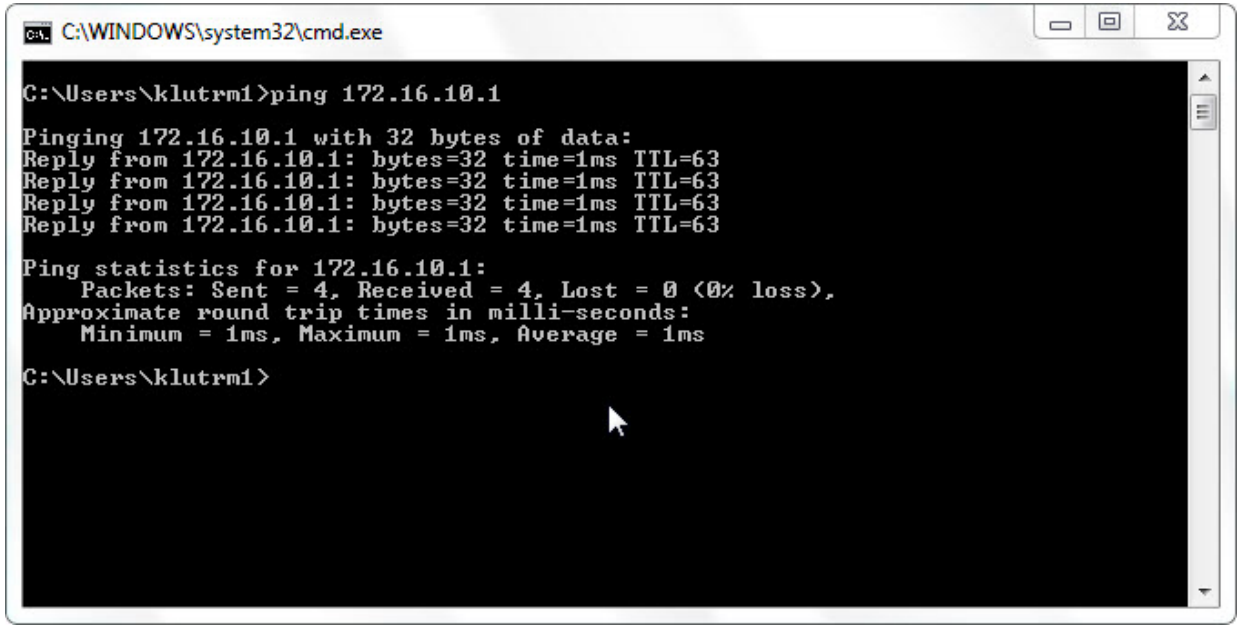


Routing / Masquerading – Ping Test
Lab

1. Ping S615 External Address (172.16.X.1 where X is the station number assigned to you)

1. Ping Instructor S615 External Address





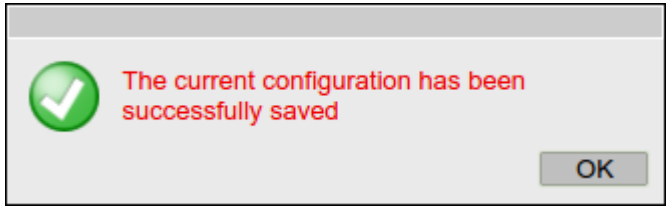
Routing / Masquerading – Write Startup Config
Lab

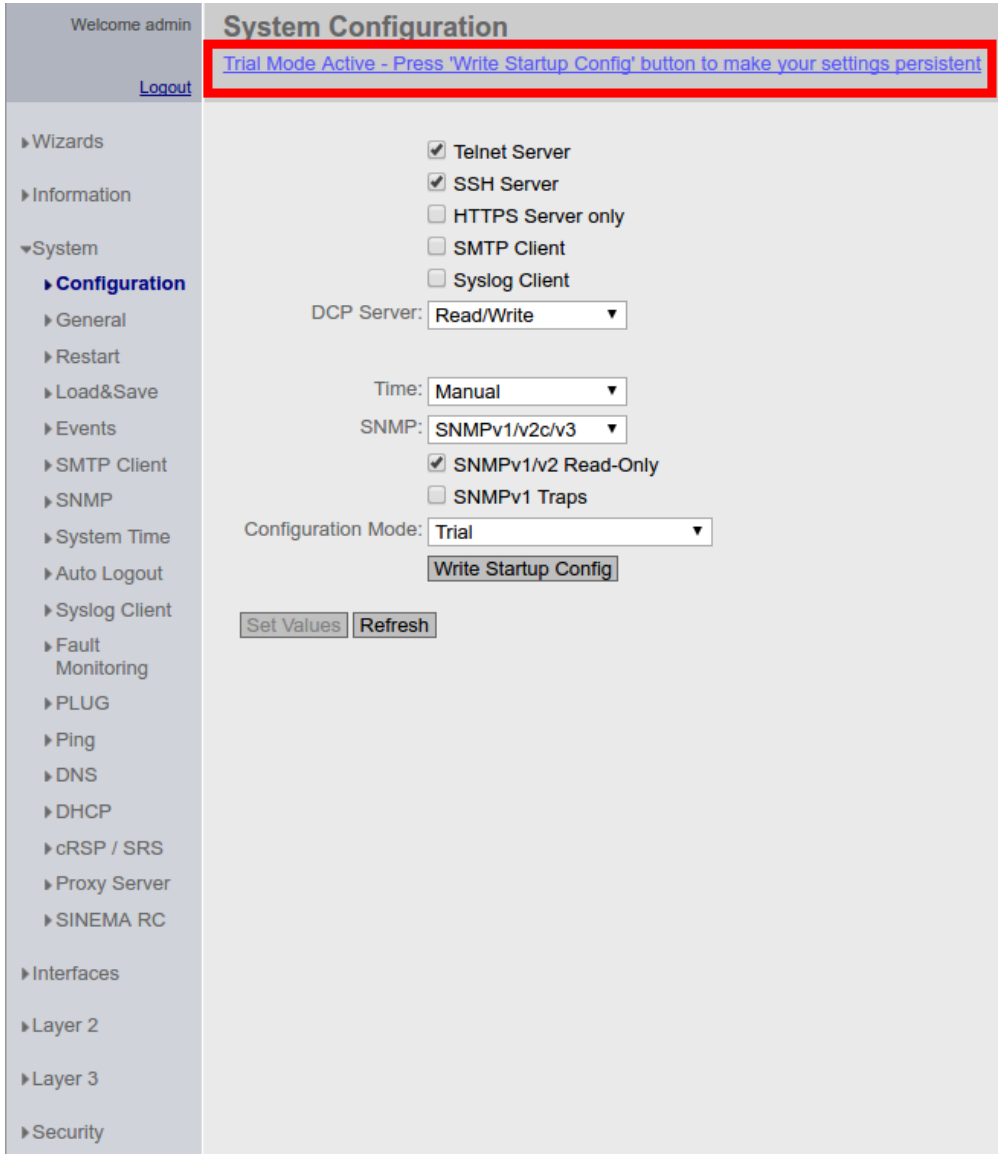
1) Navigate to and click on System

2) Navigate to and click on Configuration
   A. Alternatively, note the hot link at the top of the screen will go to the correct screen

3) Click Write Startup Config button

4) Acknowledge the Success Popup





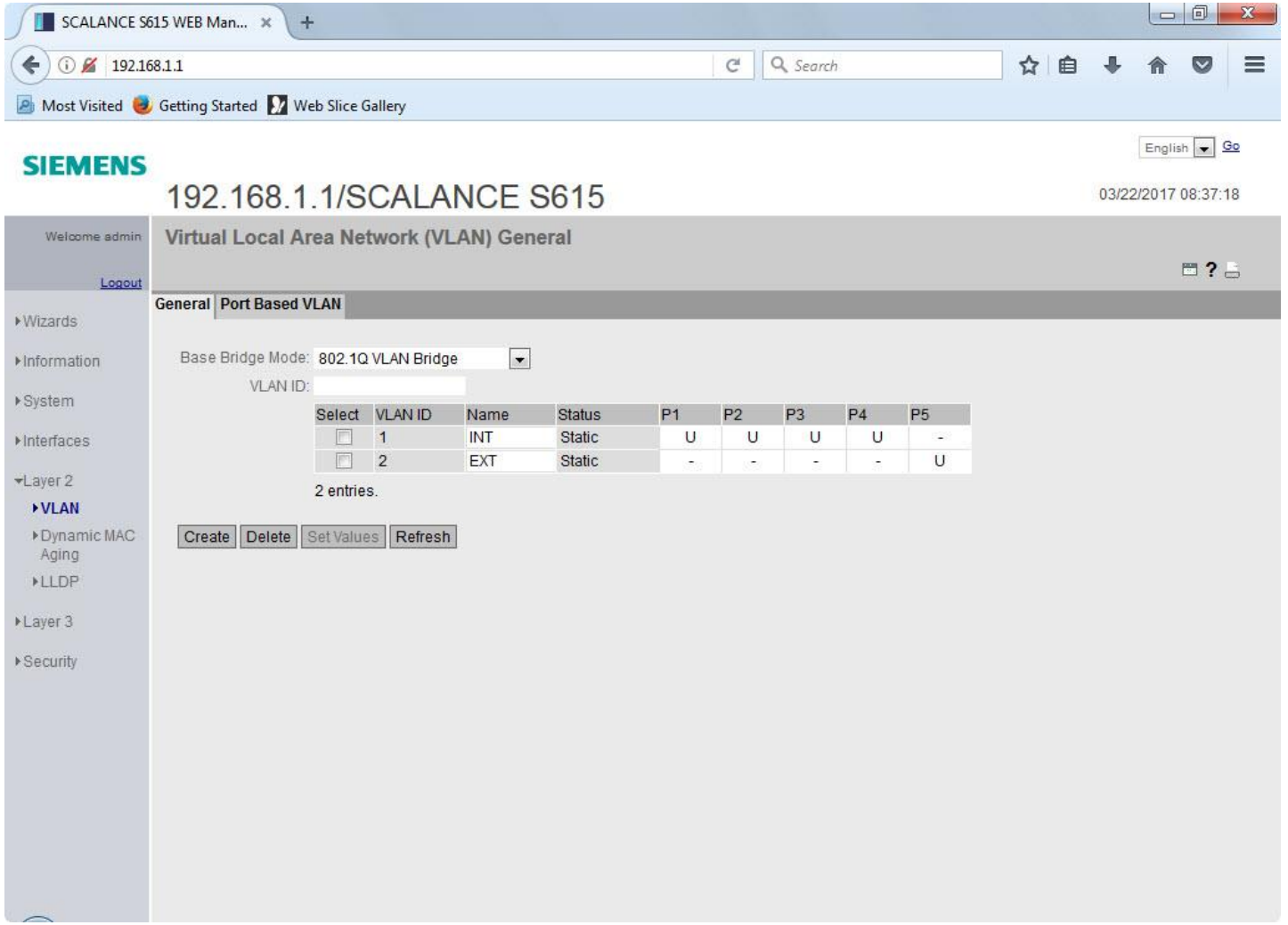
Labs

VLAN Lab

VLAN – Default Configuration
Lab

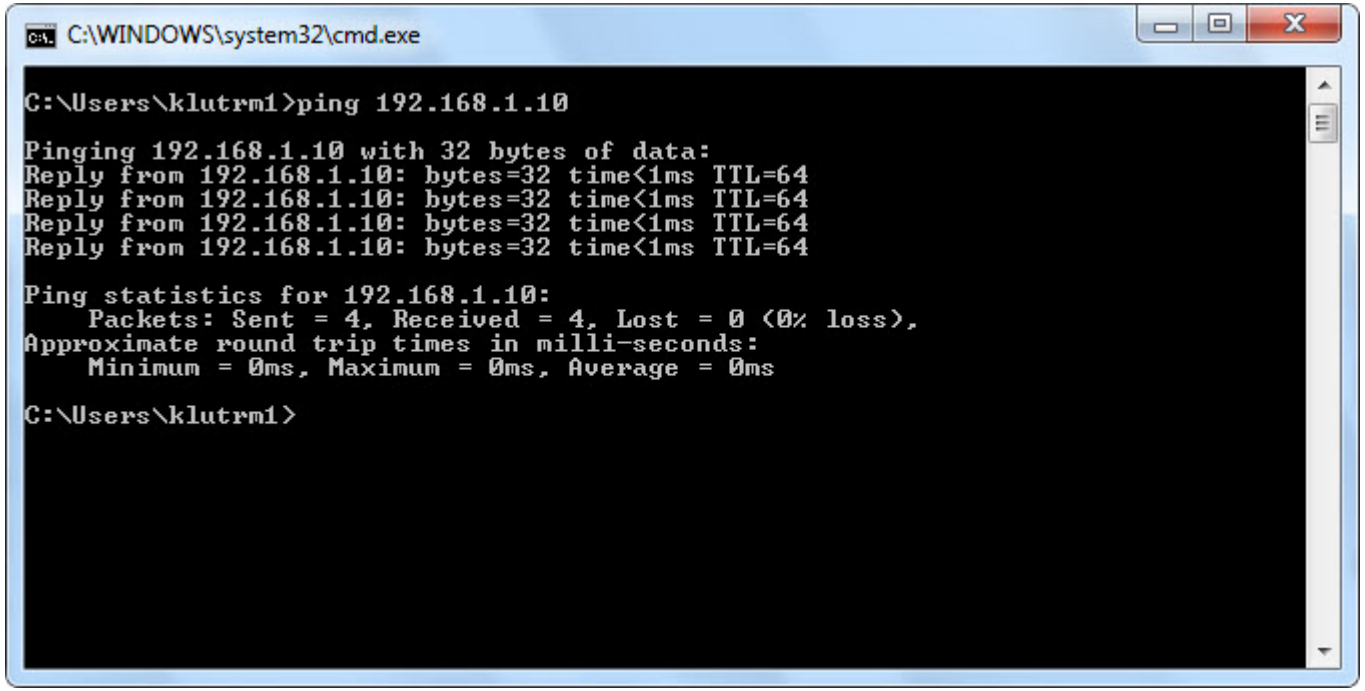
1) Navigate to and click on Layer 2

2) Navigate to and click on VLAN



VLAN – Ping Test
Lab

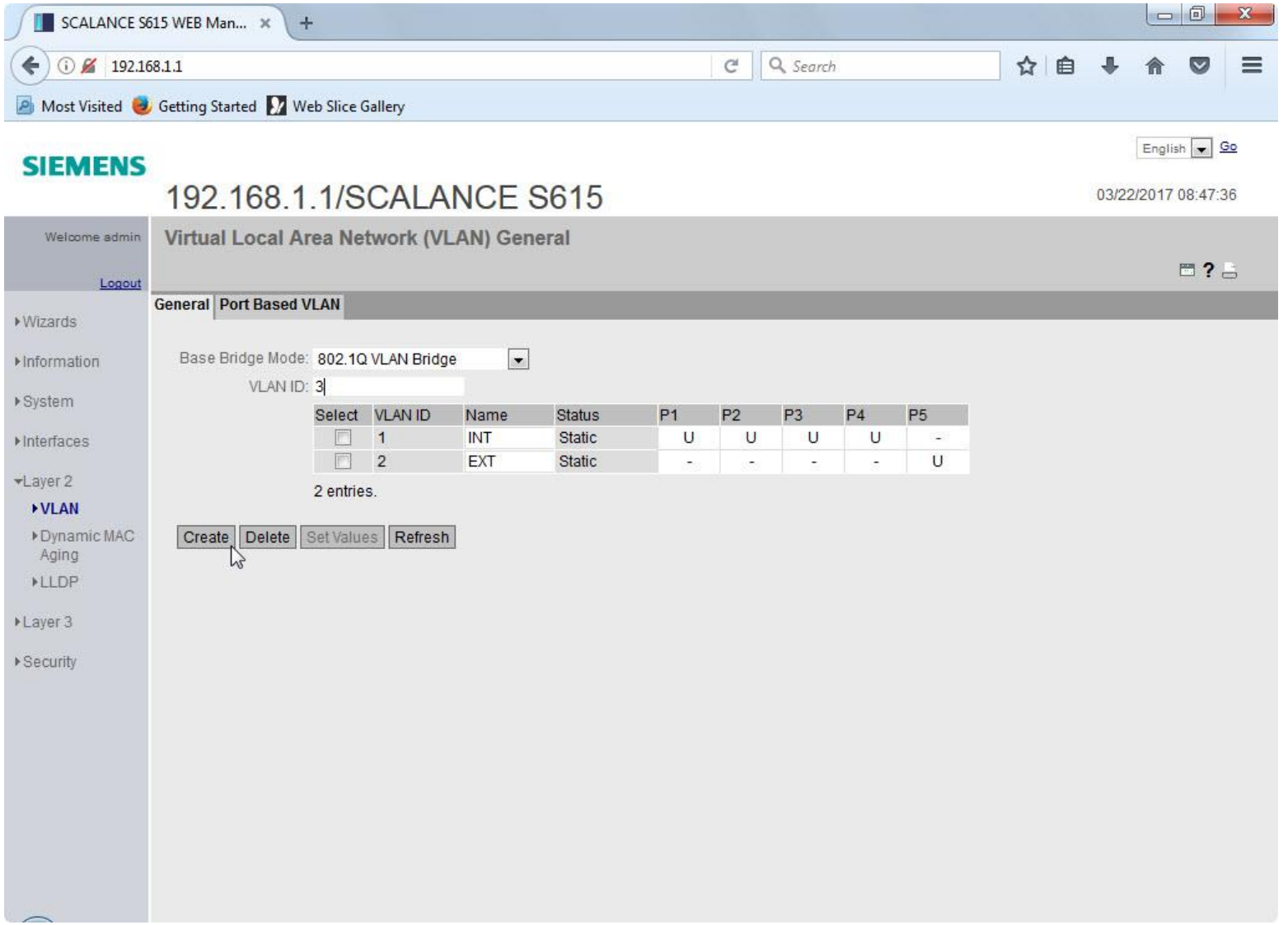
1) Ping the PLC



VLAN – VLAN ID Creation
Lab

1) In the VLAN ID box, type 3

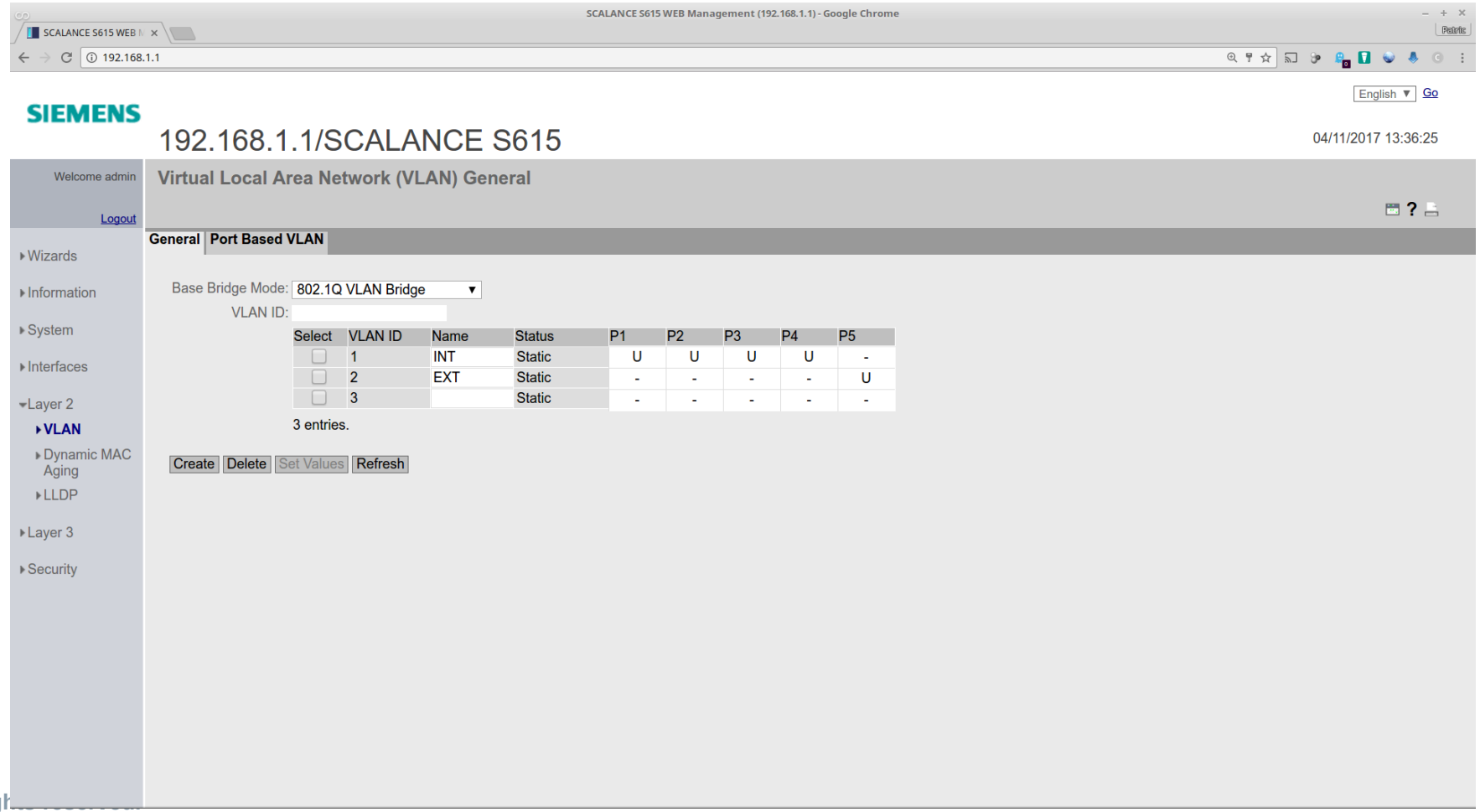
2) Click on the Create button



VLAN – VLAN ID Creation
Lab

1) The new VLAN is created

2) Click in the box under Name and next to the VLAN ID 3 and type in Controls

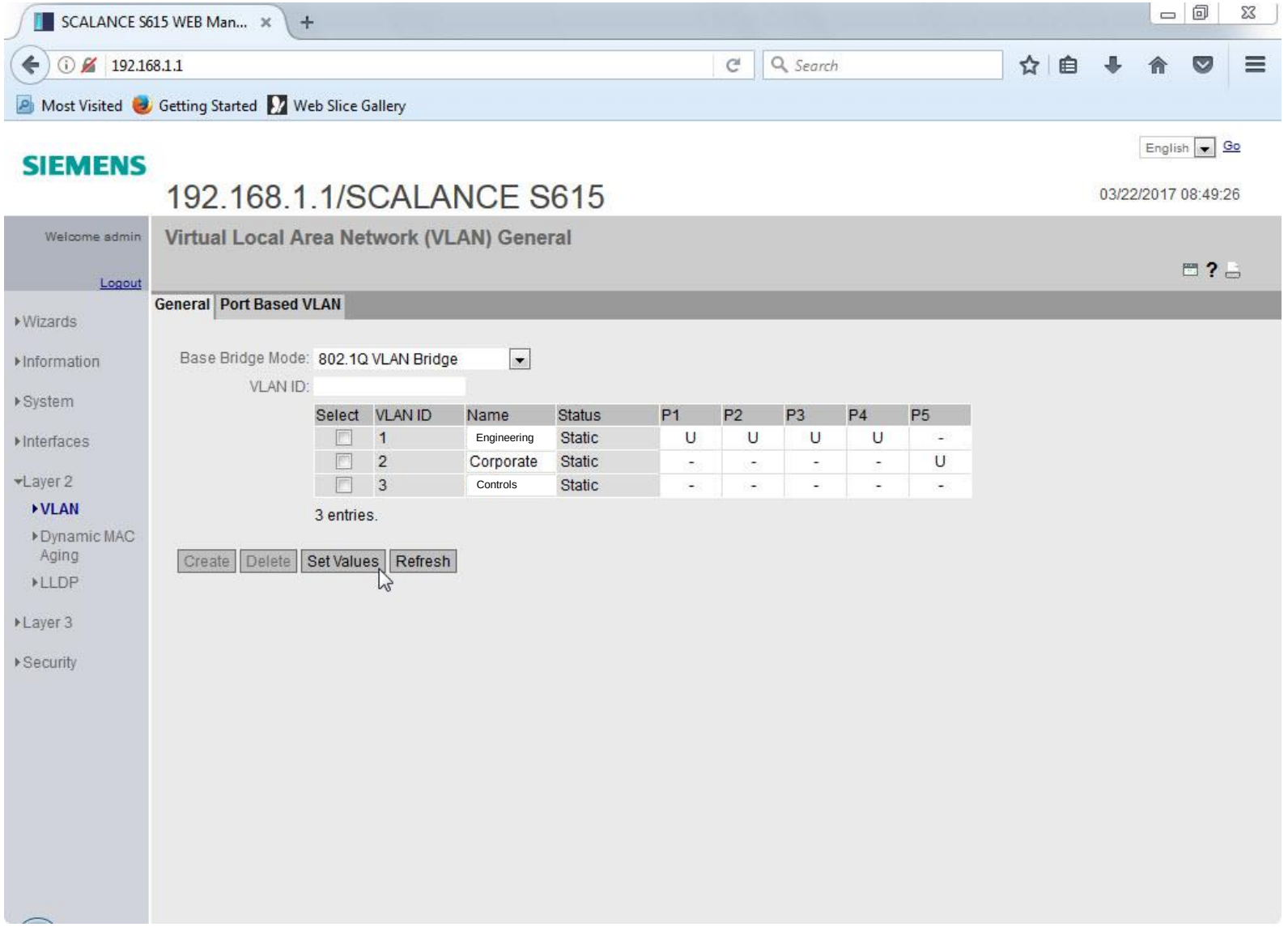


VLAN – VLAN Renaming
Lab

1) Select the box under Name and next to VLAN ID 1 and change it to Engineering

2) Select the box under Name and next to VLAN ID 2 and change it to Corporate

3) Click Set Values

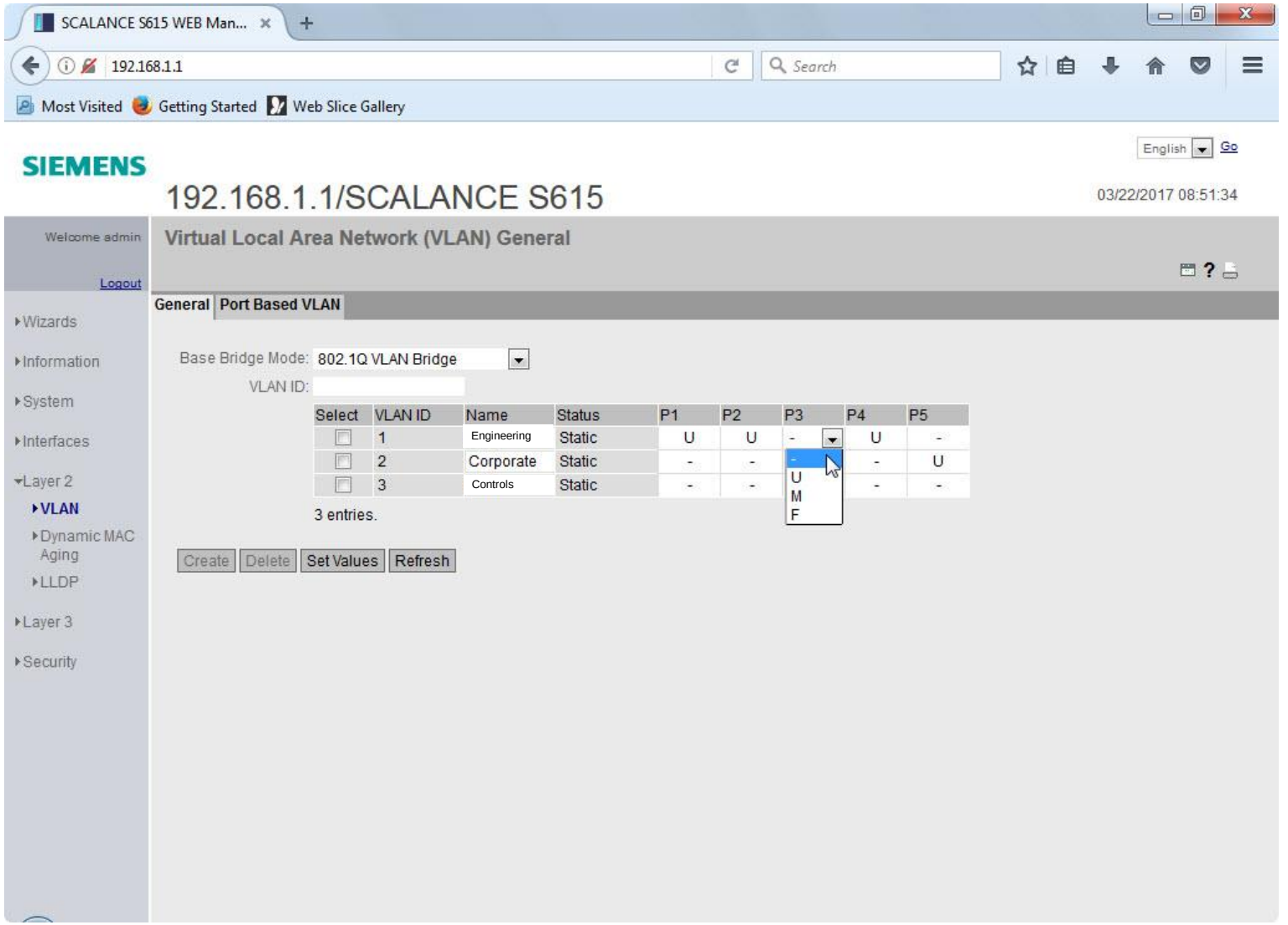


VLAN – Port Settings
Lab

1) Click on the U under P3 in the VLAN ID 1 row and change it to the “-”

2) Click on the U under P4 in the VLAN ID 1 row and change it to the “-”

3) Click Set Values

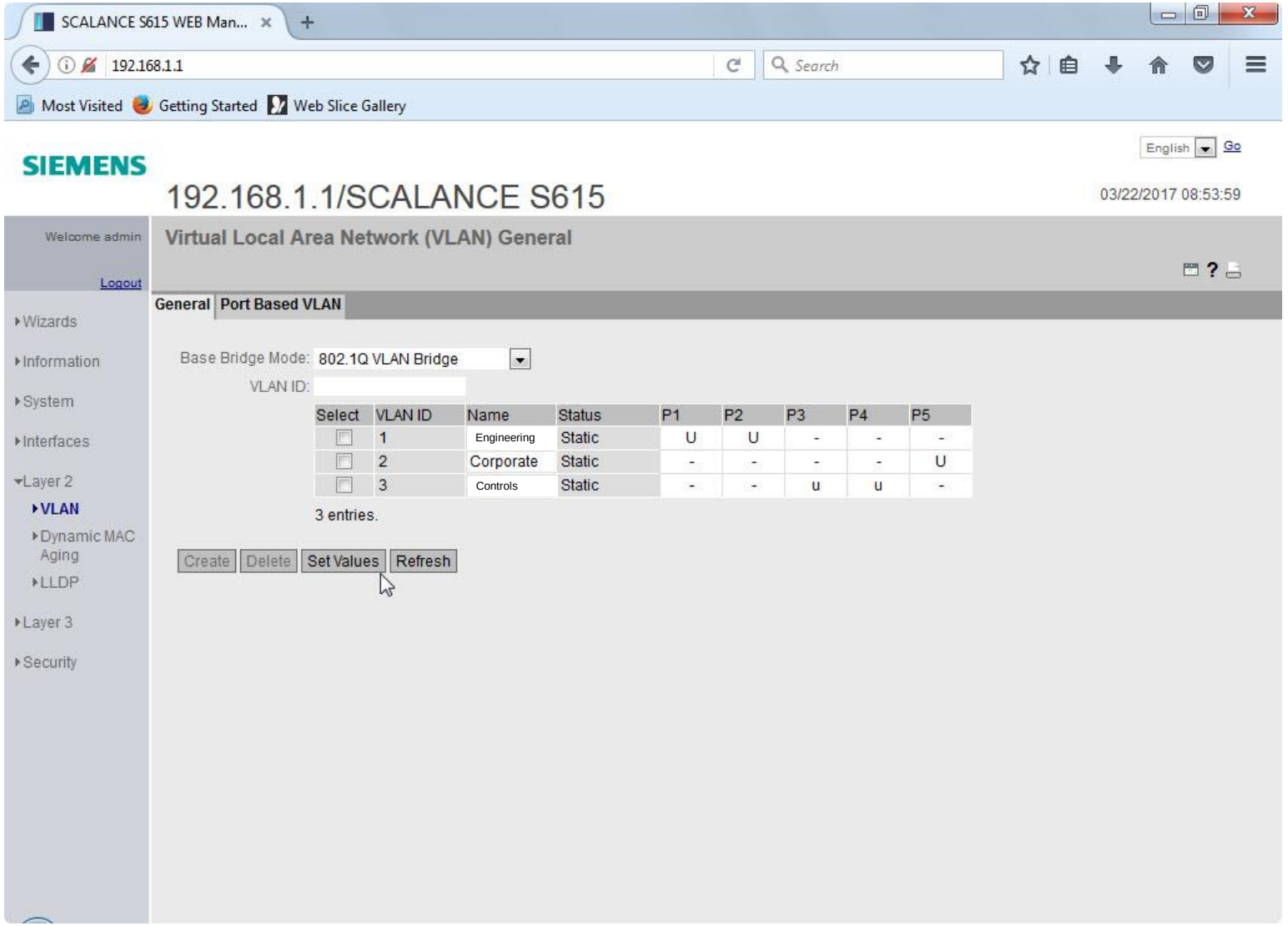


VLAN – Port Settings
Lab

1) Click on the “-” under P3 in the VLAN ID 3 row and change it to “u”

2) Click on the “-” under P4 in the VLAN ID 3 row and change it to “u”

3) Click Set Values



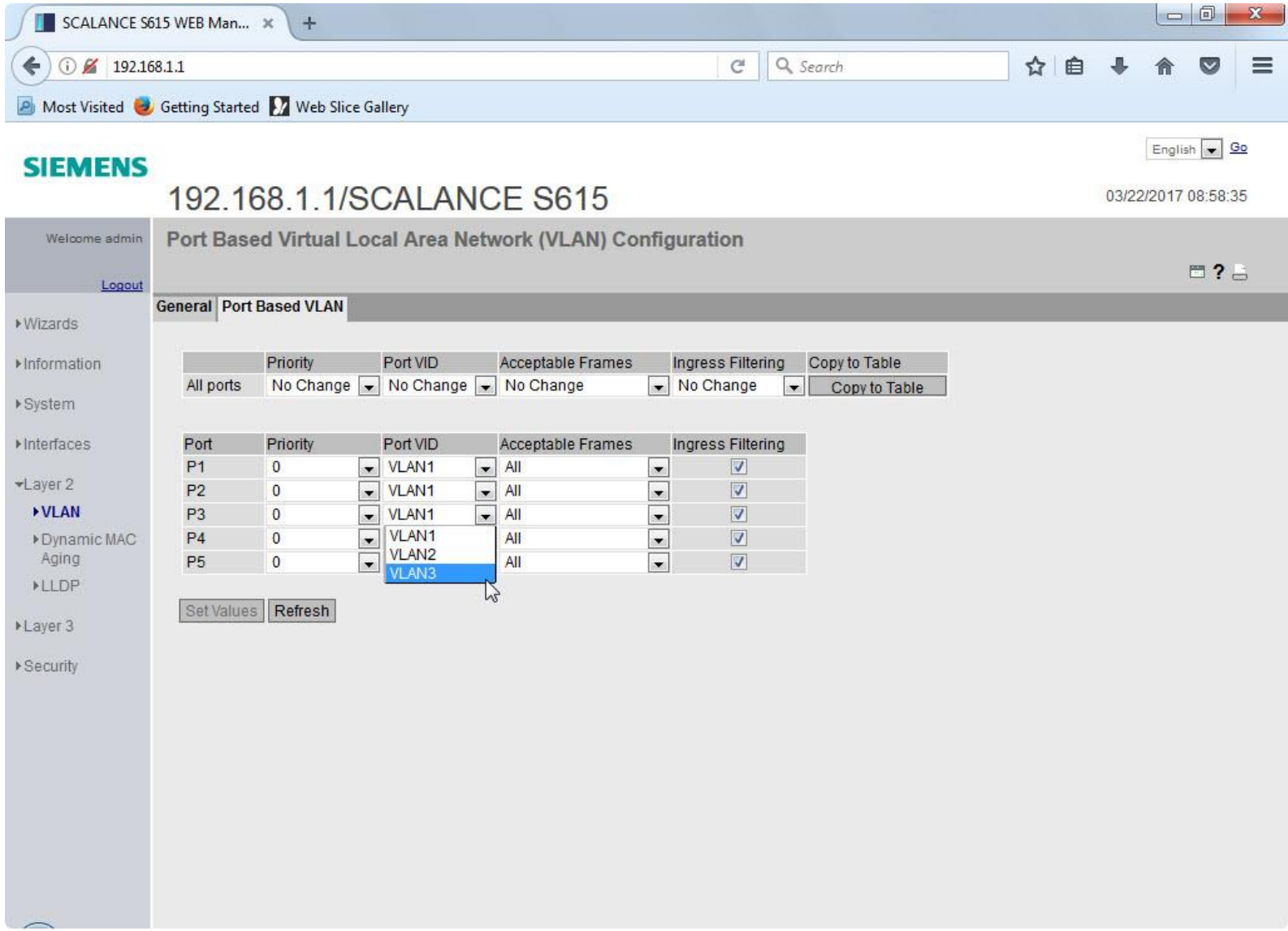
VLAN – Port Settings
Lab

1) Click on the Port Based VLAN tab

2) Click on the dropdown under Port VID in the P3 row and change it from VLAN1 to VLAN3

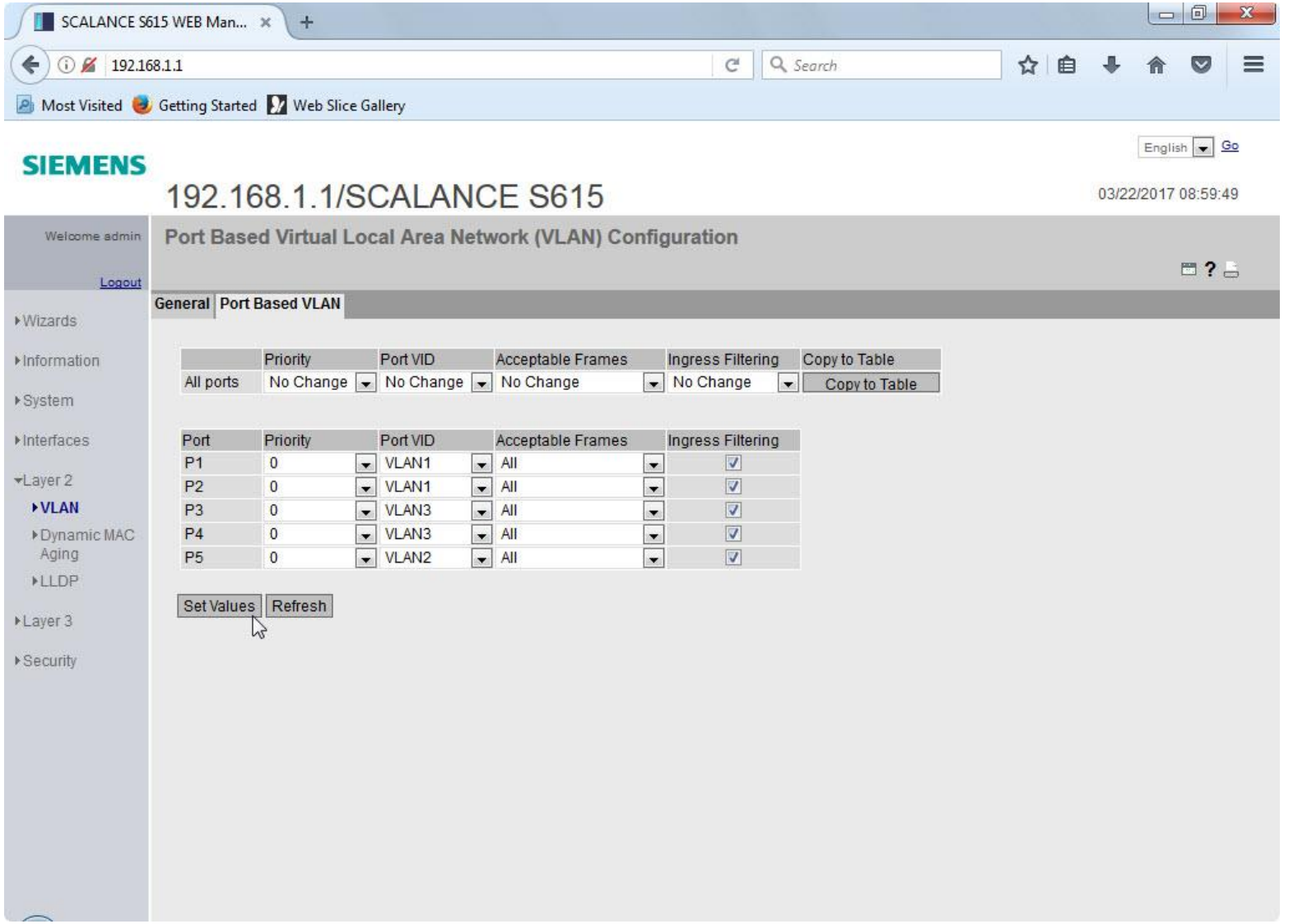
3) Click on the dropdown under Port VID in the P4 row and change it from VLAN1 to VLAN3

4) Click Set Values



VLAN – Port Settings
Lab

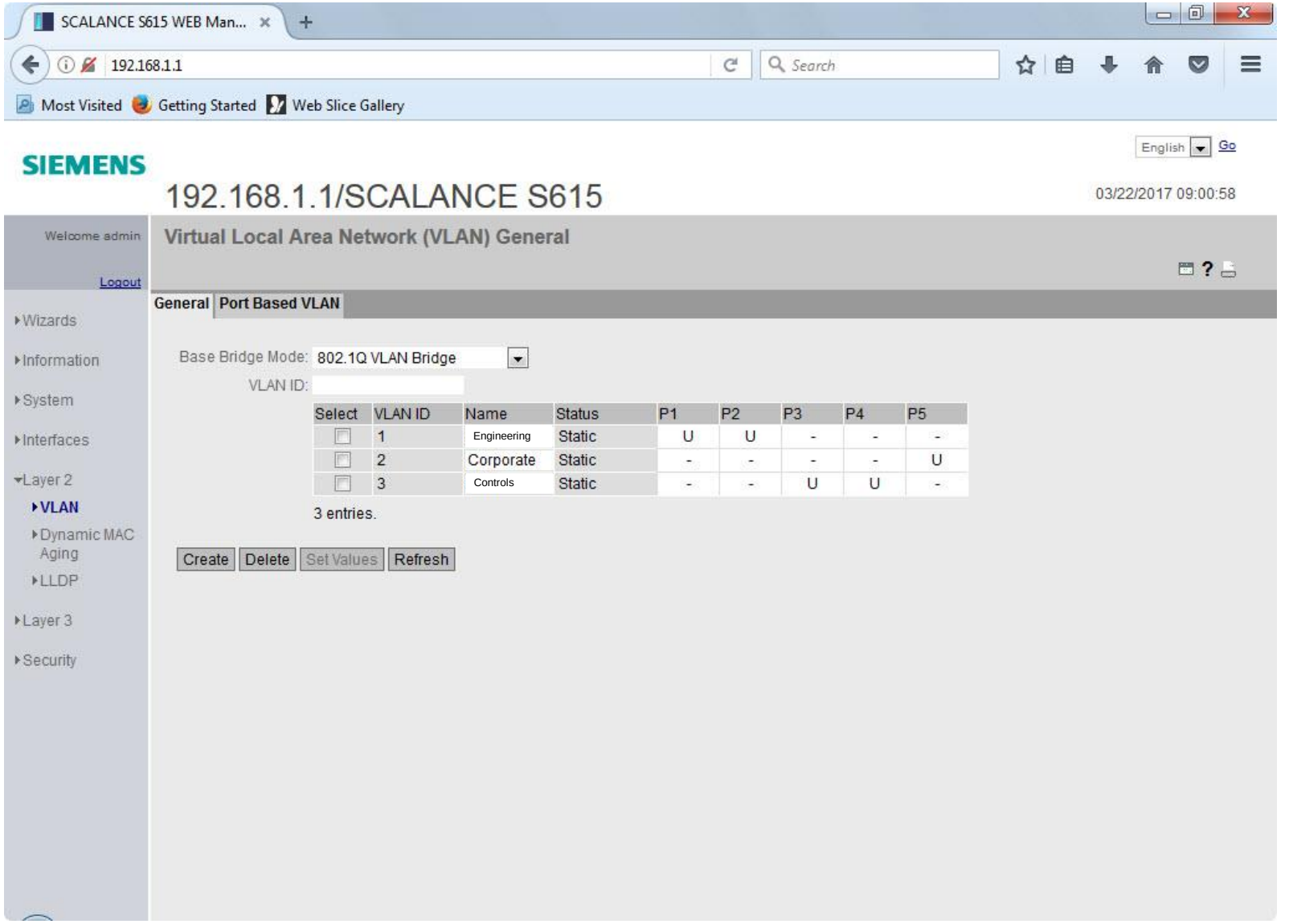
1) The Port Based VLAN screen should look like these settings



VLAN – Port Settings
Lab

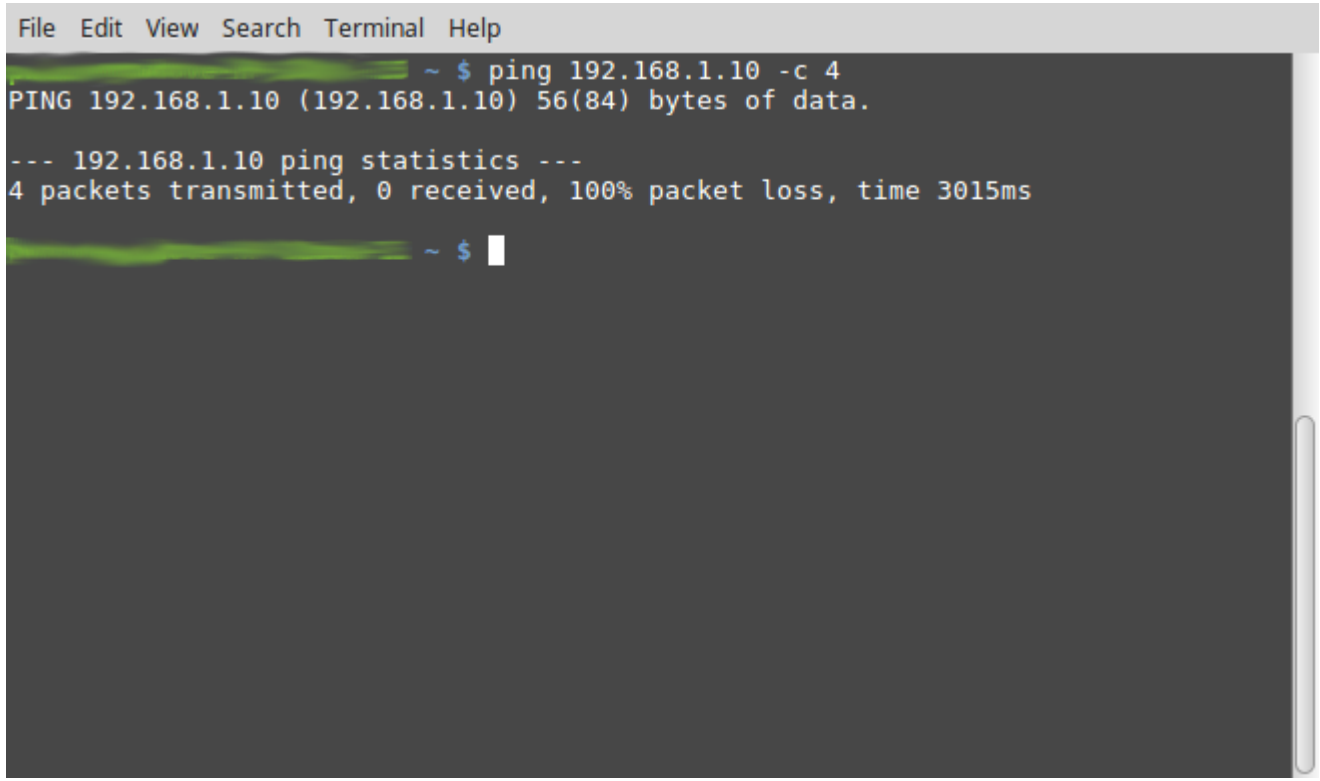
1) Click on the General tab

2) The u under P3 and P4 in the VLAN ID 3 row should now be a capital “U”



VLAN – Ping Test
Lab

1) Ping the PLC



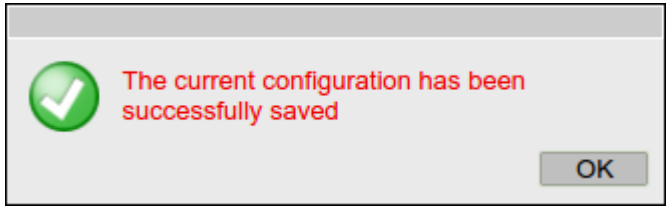
VLAN – Write Startup Config
Lab

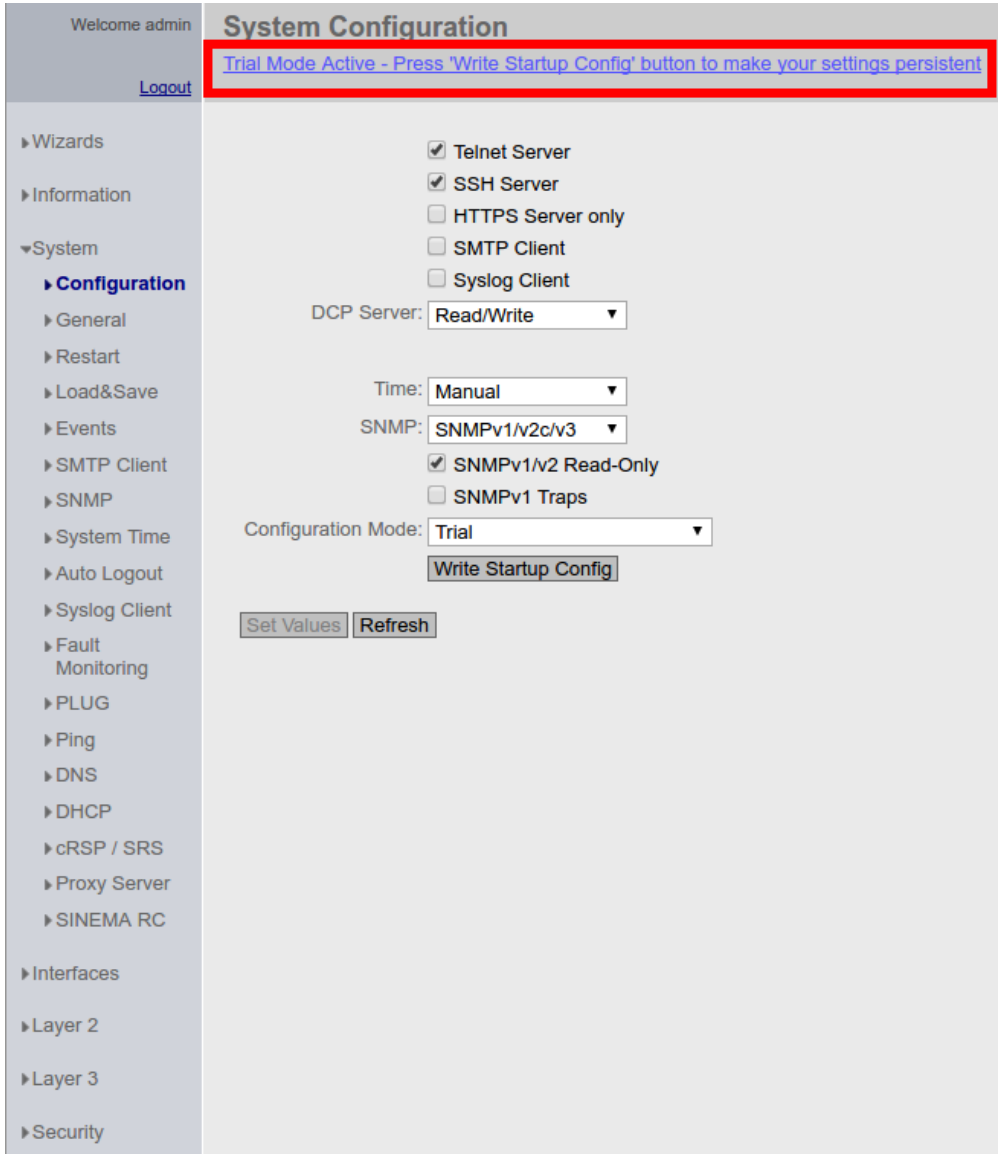
1) Navigate to and click on System

2) Navigate to and click on Configuration
   A. Alternatively, note the hot link at the top of the screen will go to the correct screen

3) Click Write Startup Config button

4) Acknowledge the Success Popup





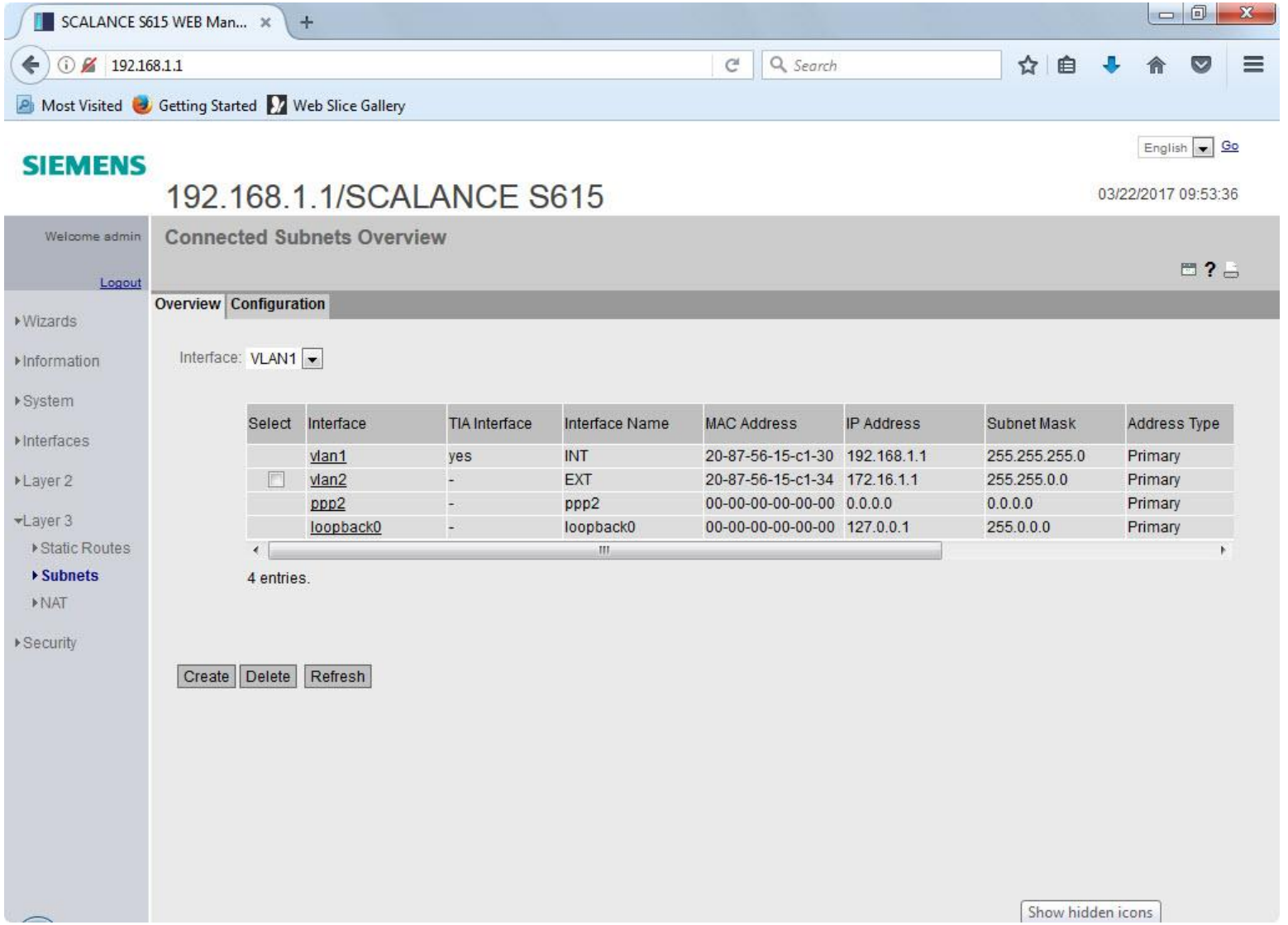
Labs

VLAN Routing Lab

VLAN Routing – Initial Screen
Lab

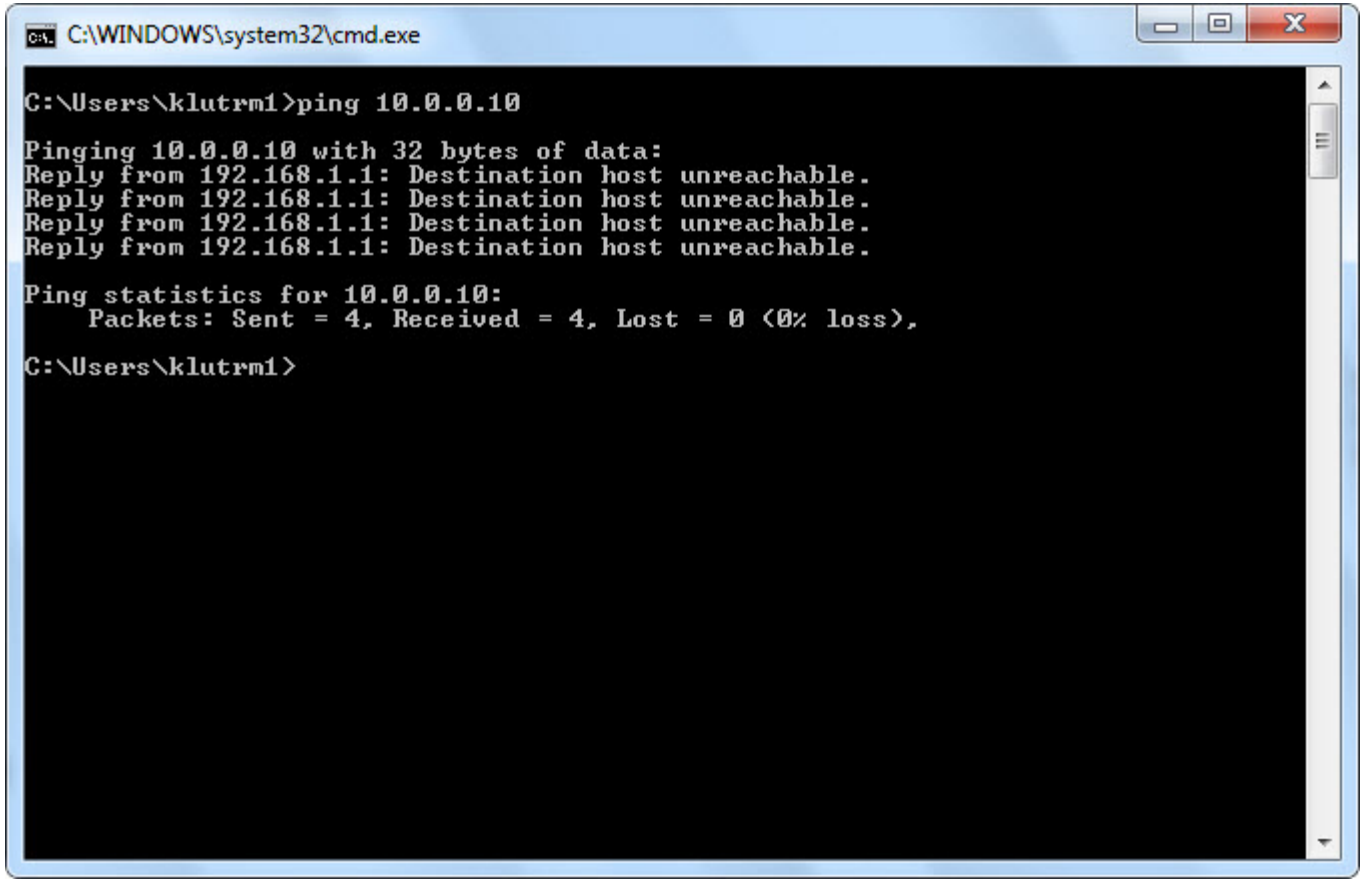
1) Navigate to and click on Layer 3

2) Navigate to and click on Subnets



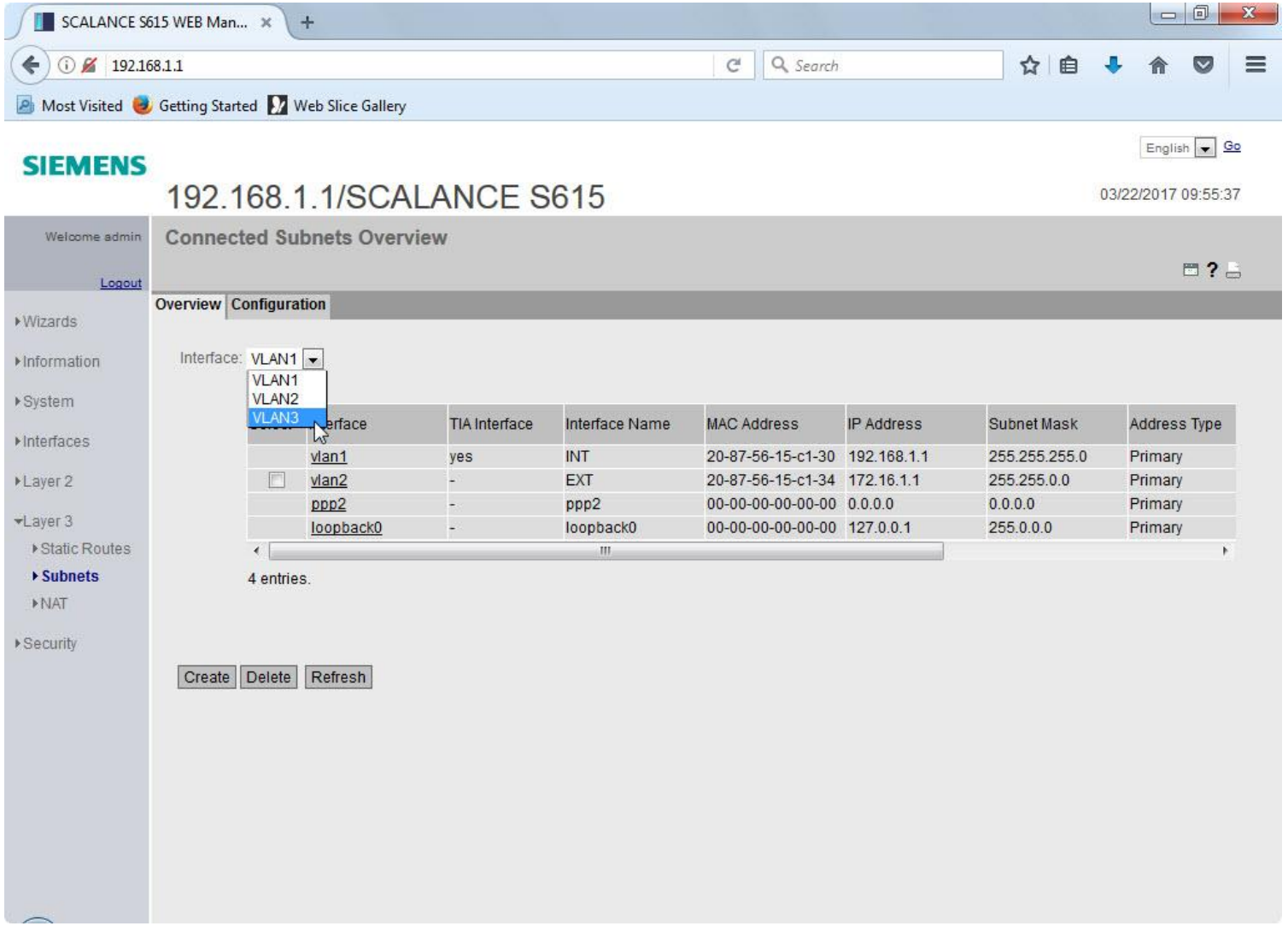
VLAN Routing – Initial Screen
Lab

1) Ping the HMI at IP Address 10.0.0.1X where X is the station number assigned to you



VLAN Routing – Interface Creation
Lab

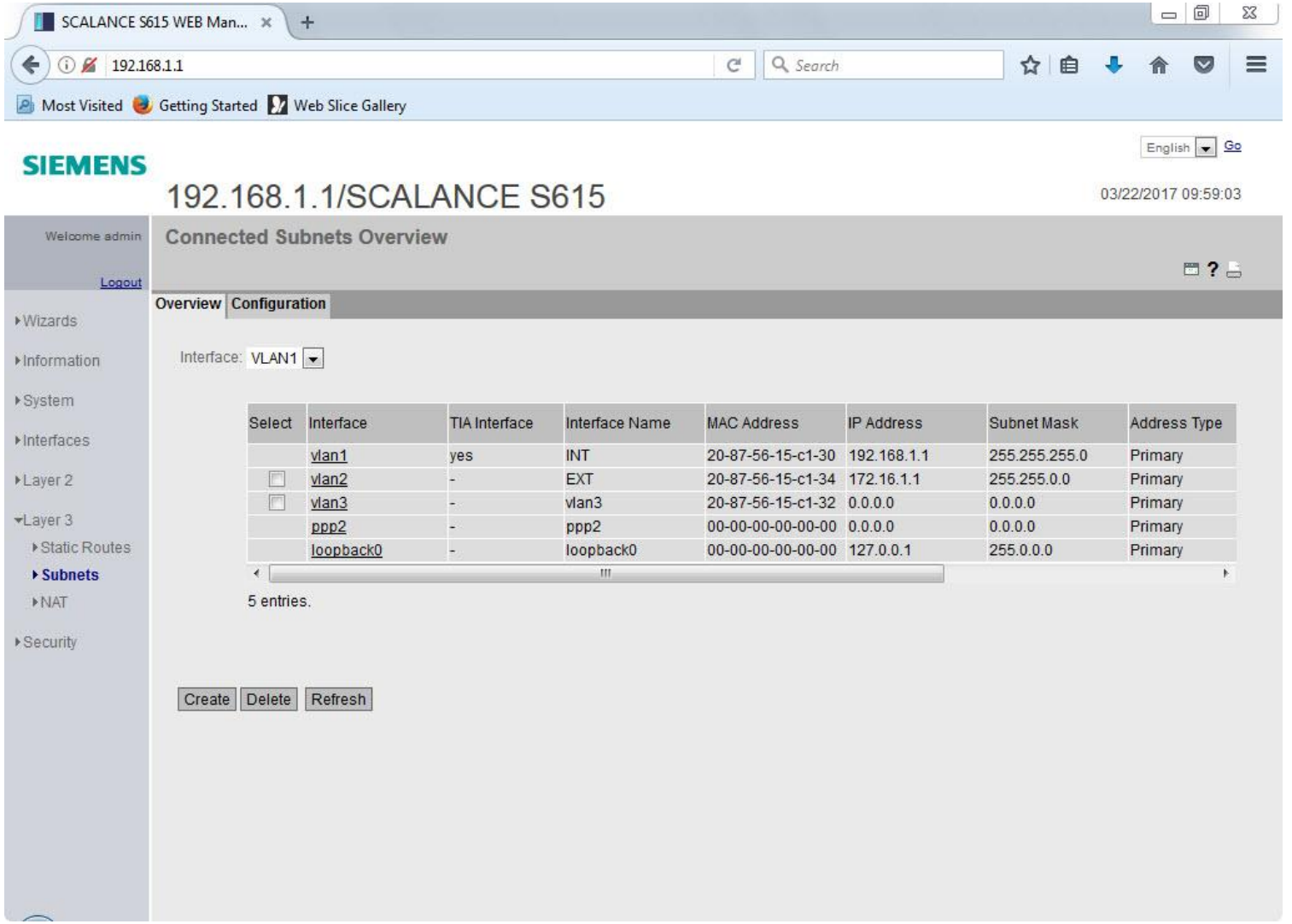
1) Navigate to and click on Layer 3
2) Navigate to and click on Subnets
3) In the Interface dropdown, select VLAN3
4) Click Create



VLAN Routing – Interface Creation
Lab

1) Note the new vlan3 interface

2) Either the Configuration tab can be clicked or the vlan3 that is underlined can be clicked to go to the configuration of the interface

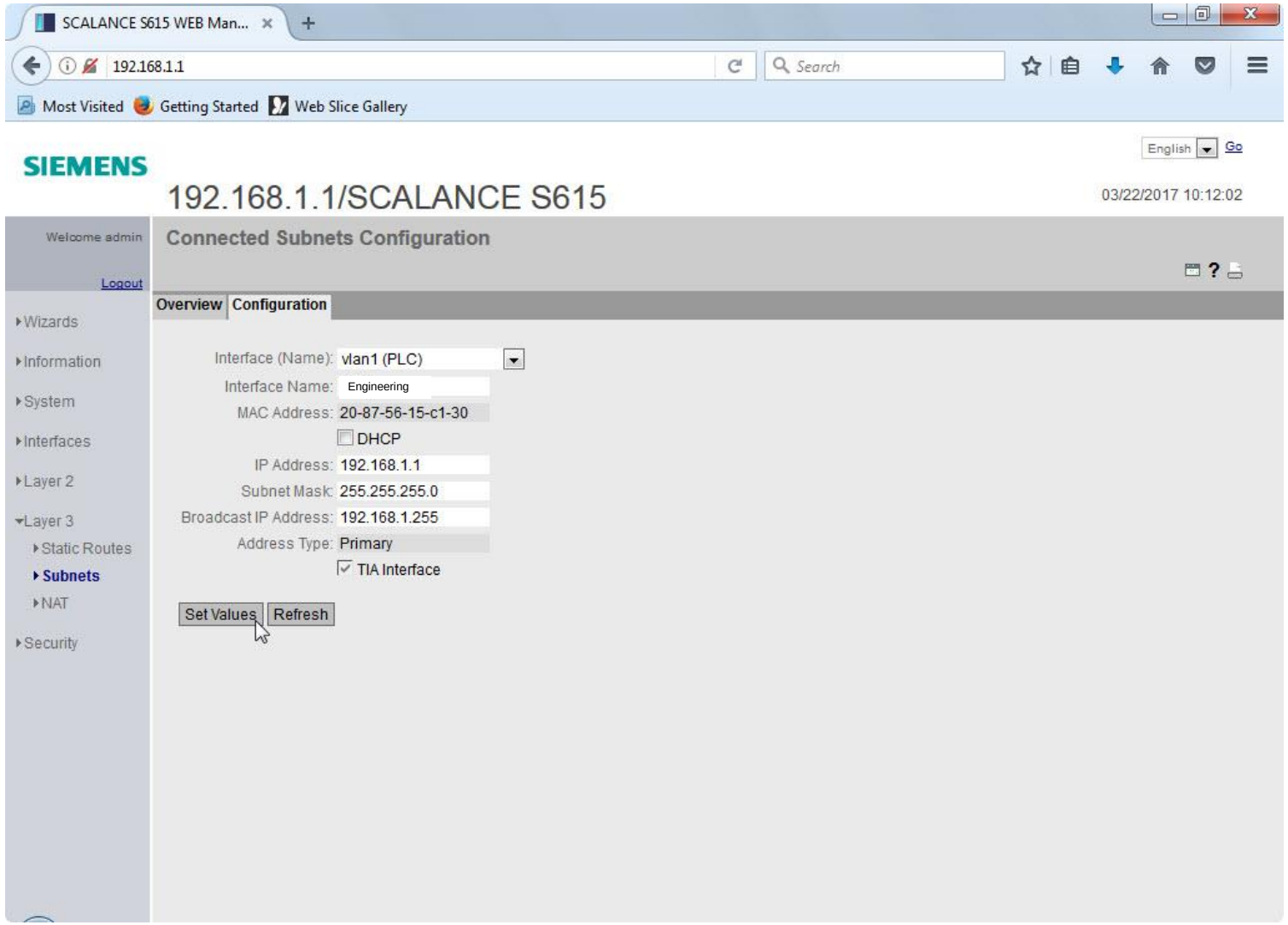


VLAN Routing – Interface Creation
Lab

1) Click on the Configuration tab

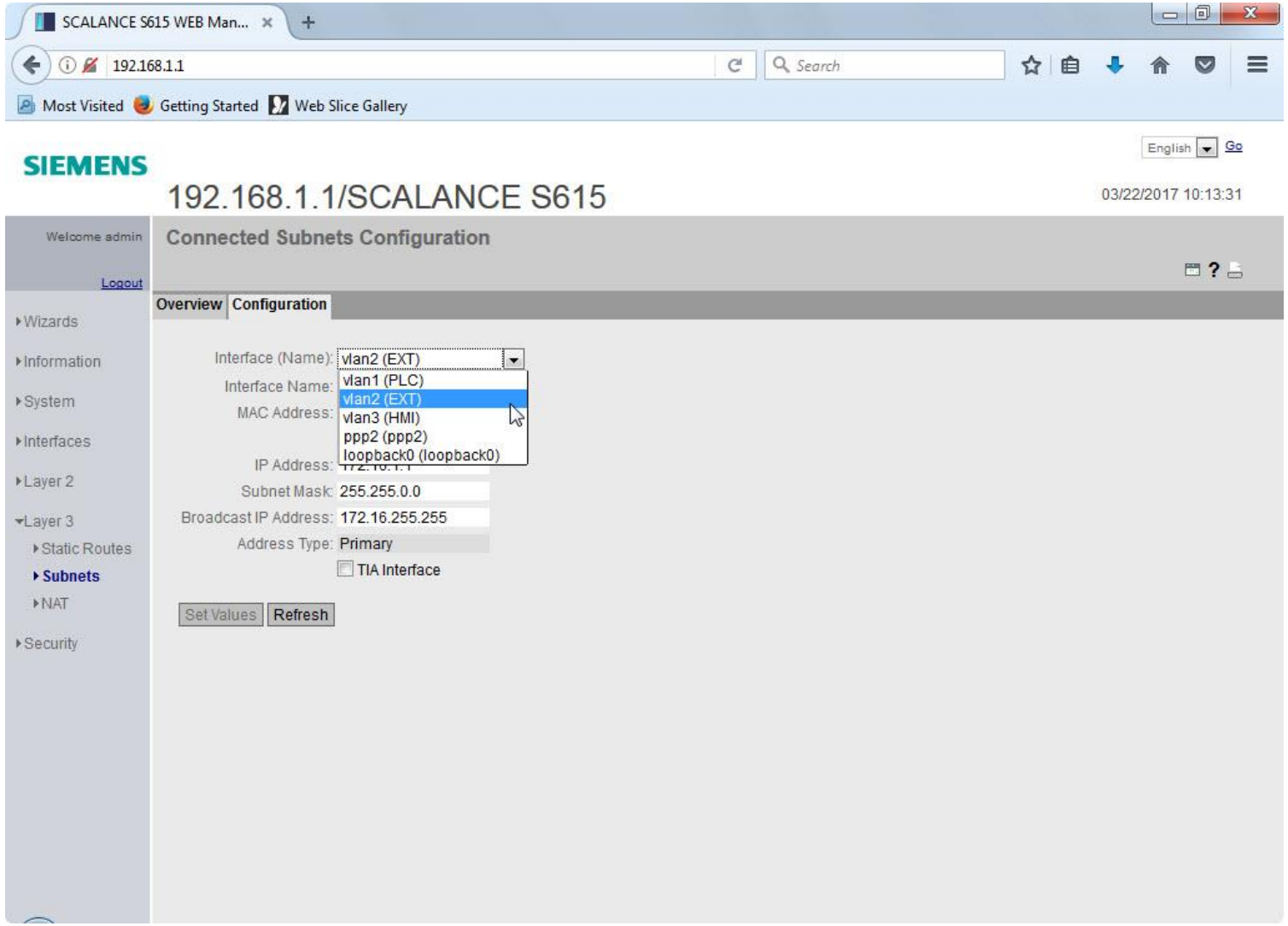
2) Click in the box next to Interface Name: and change it from INT to Engineering

3) Click Set Values



VLAN Routing – Interface Configuration
Lab

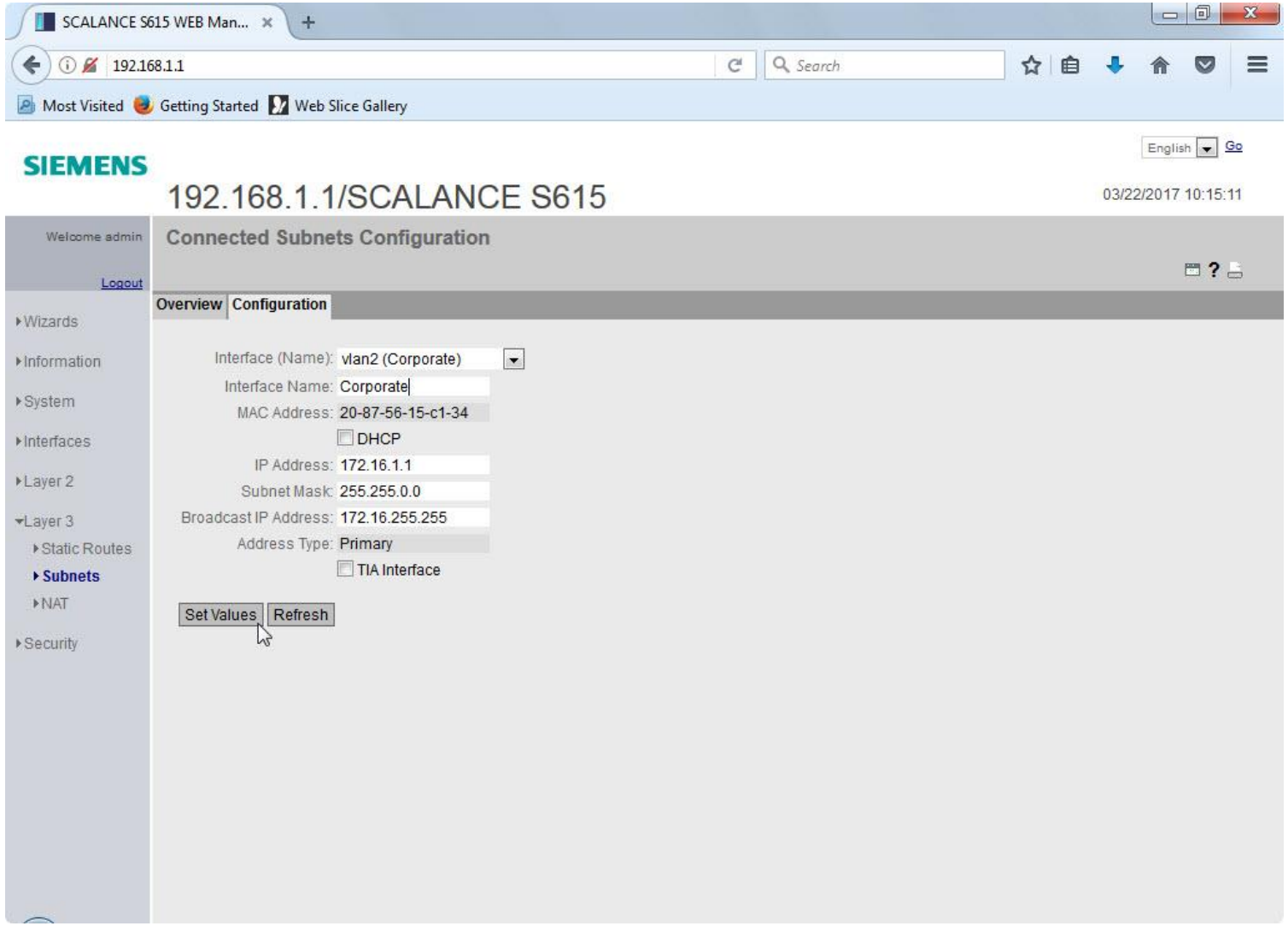
1) Click the dropdown next to Interface (Name): and select vlan2 (EXT)



VLAN Routing – Interface Configuration
Lab

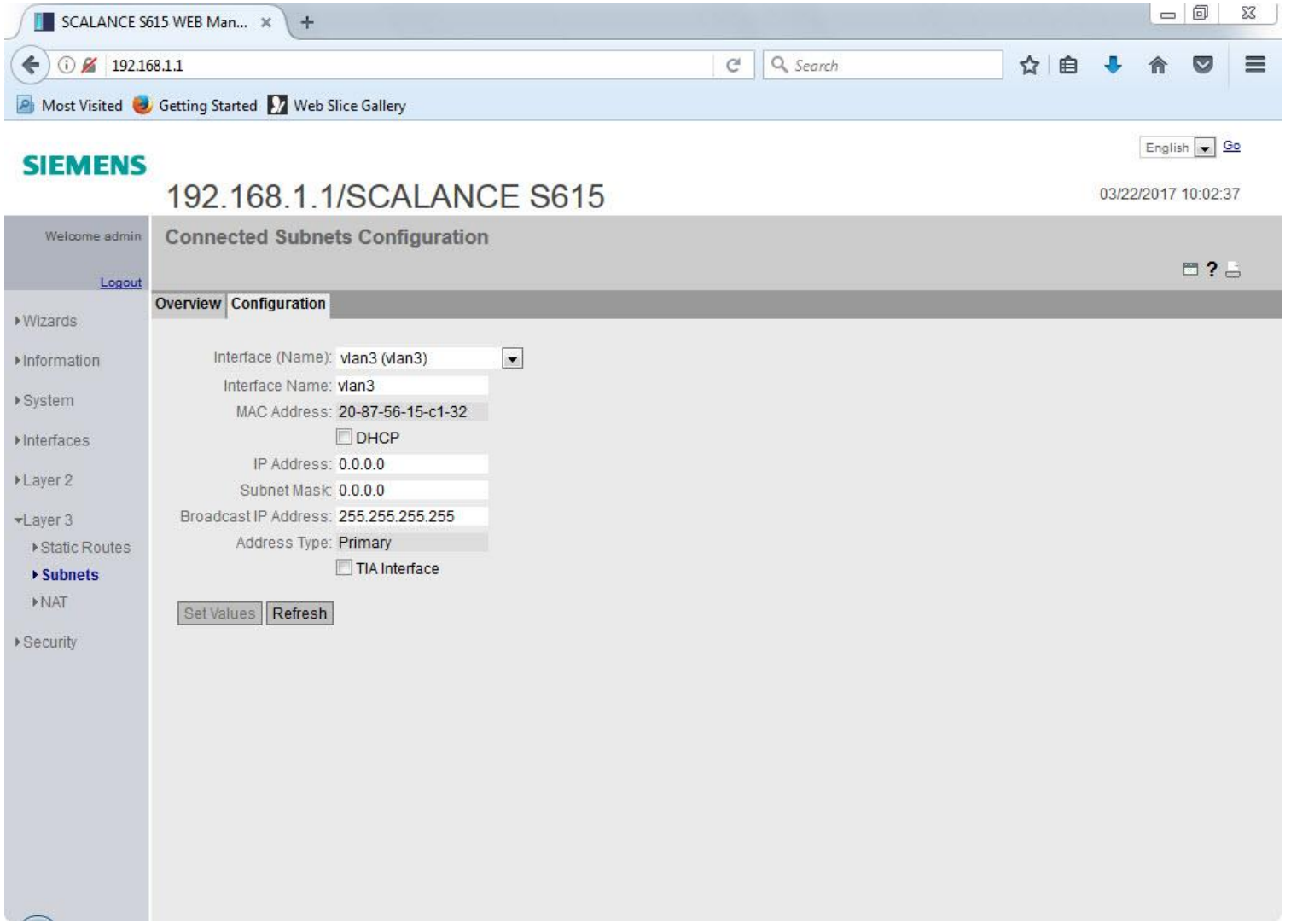
1) Click in the box next to Interface Name: and change the name from EXT to Corporate

2) Click Set Values



VLAN Routing – Interface Configuration
Lab

1) Click on the dropdown next to Interface (Name): and select vlan3



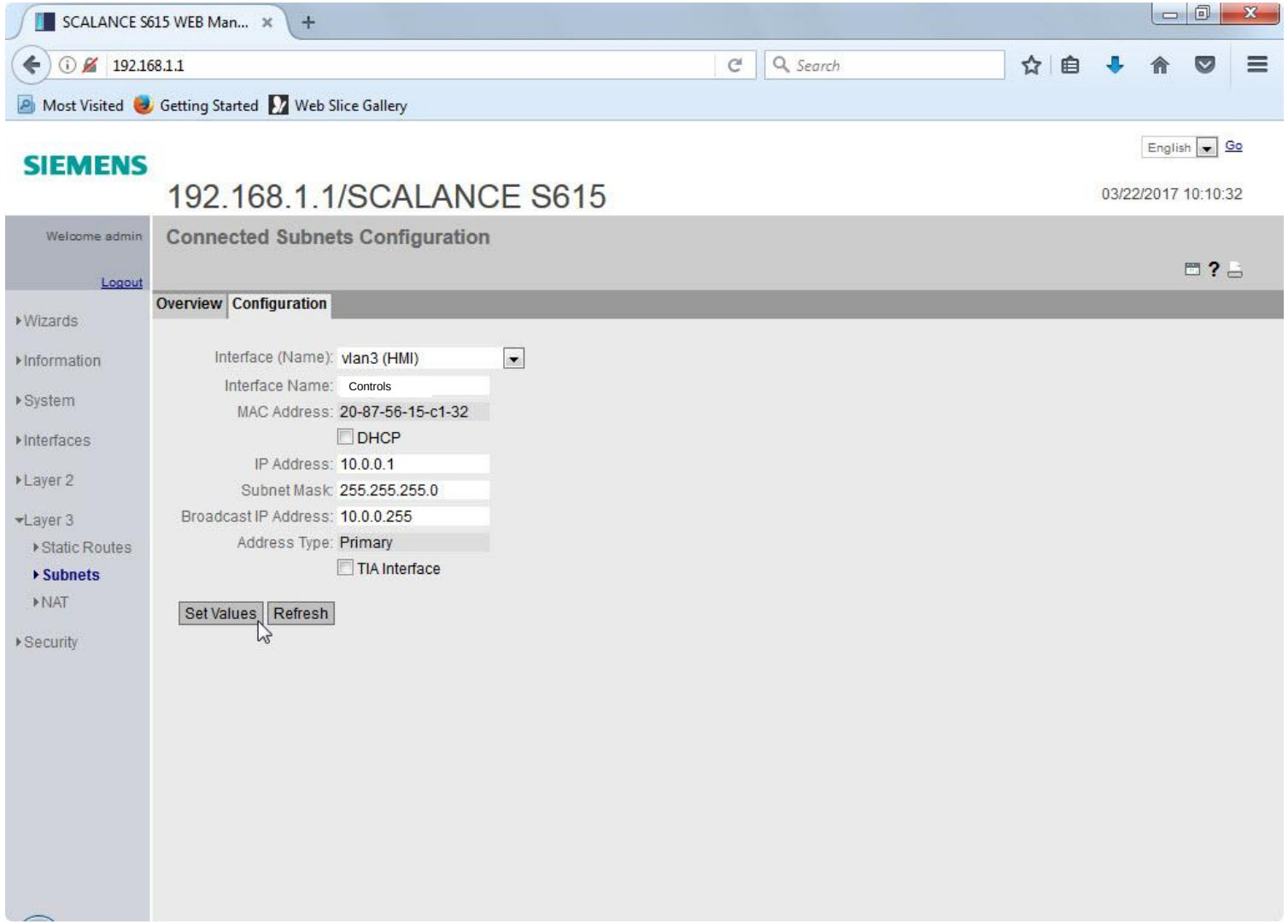
VLAN Routing – Interface Configuration
Lab

1) Click in the box next to Interface Name: and change it from vlan3 to Controls

2) Click in the box next to IP Address: and enter 10.0.0.1

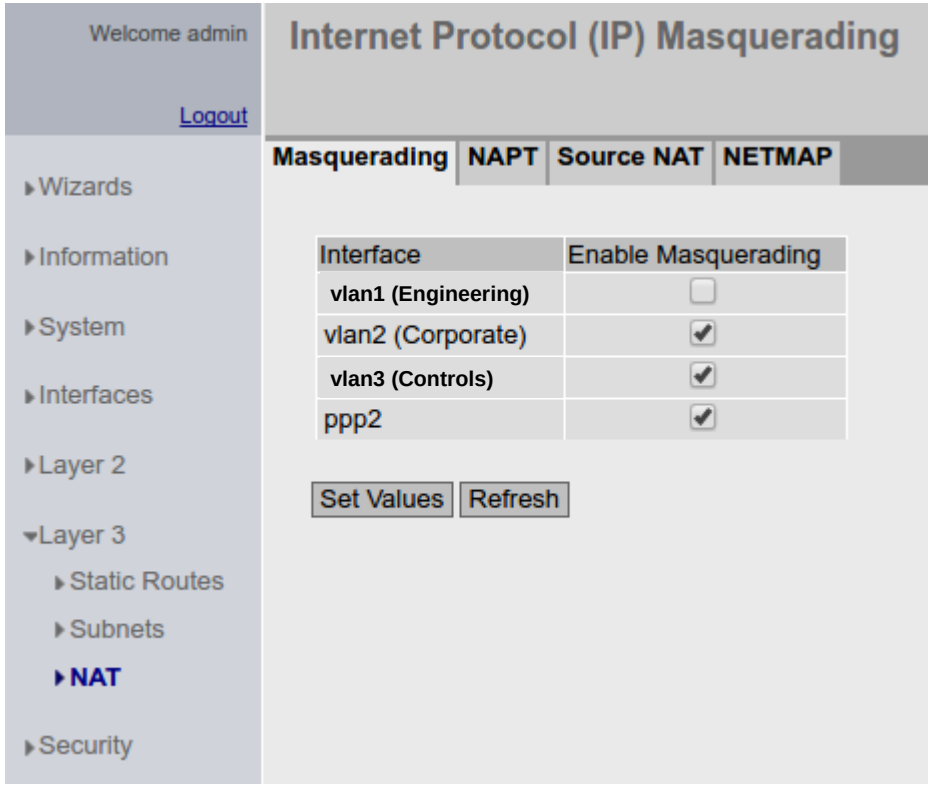
3) Click in the box next to Subnet Mask and enter in 255.255.255.0

4) Click Set Values



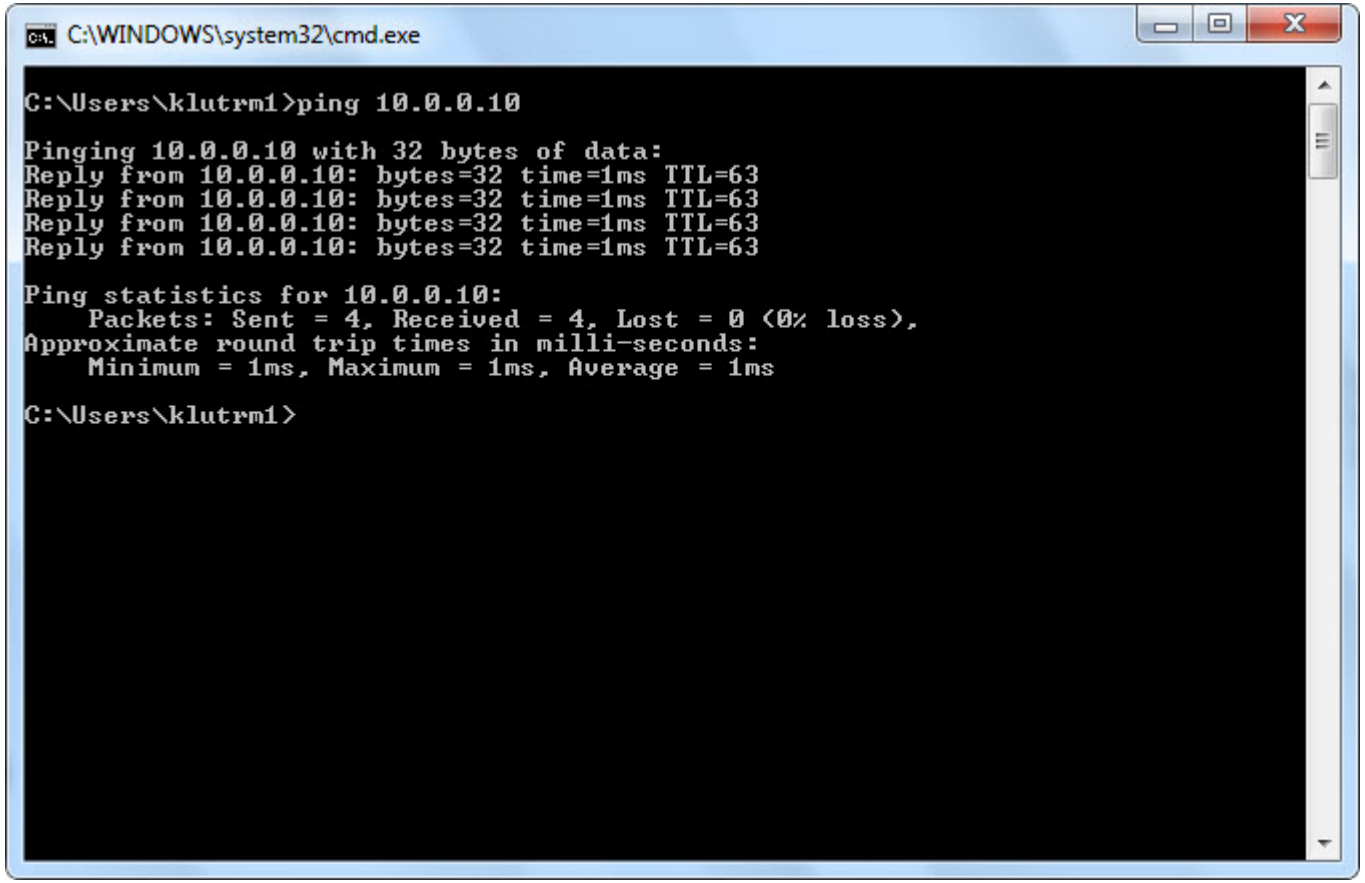
Routing / Masquerading – Enable Masquerading
Lab

1) Navigate to and click on Layer 3
2) Navigate to and click on NAT
3) Check the Enable Masquerading for vlan3 (Controls)
4) Click Set Values



VLAN Routing – Interface Configuration
Lab

1) Ping the PLC at IP Address 10.0.0.1X where X is the station number assigned to you



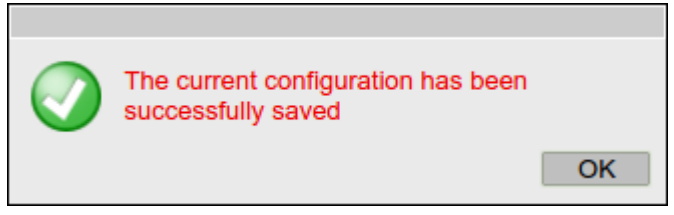
VLAN Routing – Write Startup Config
Lab

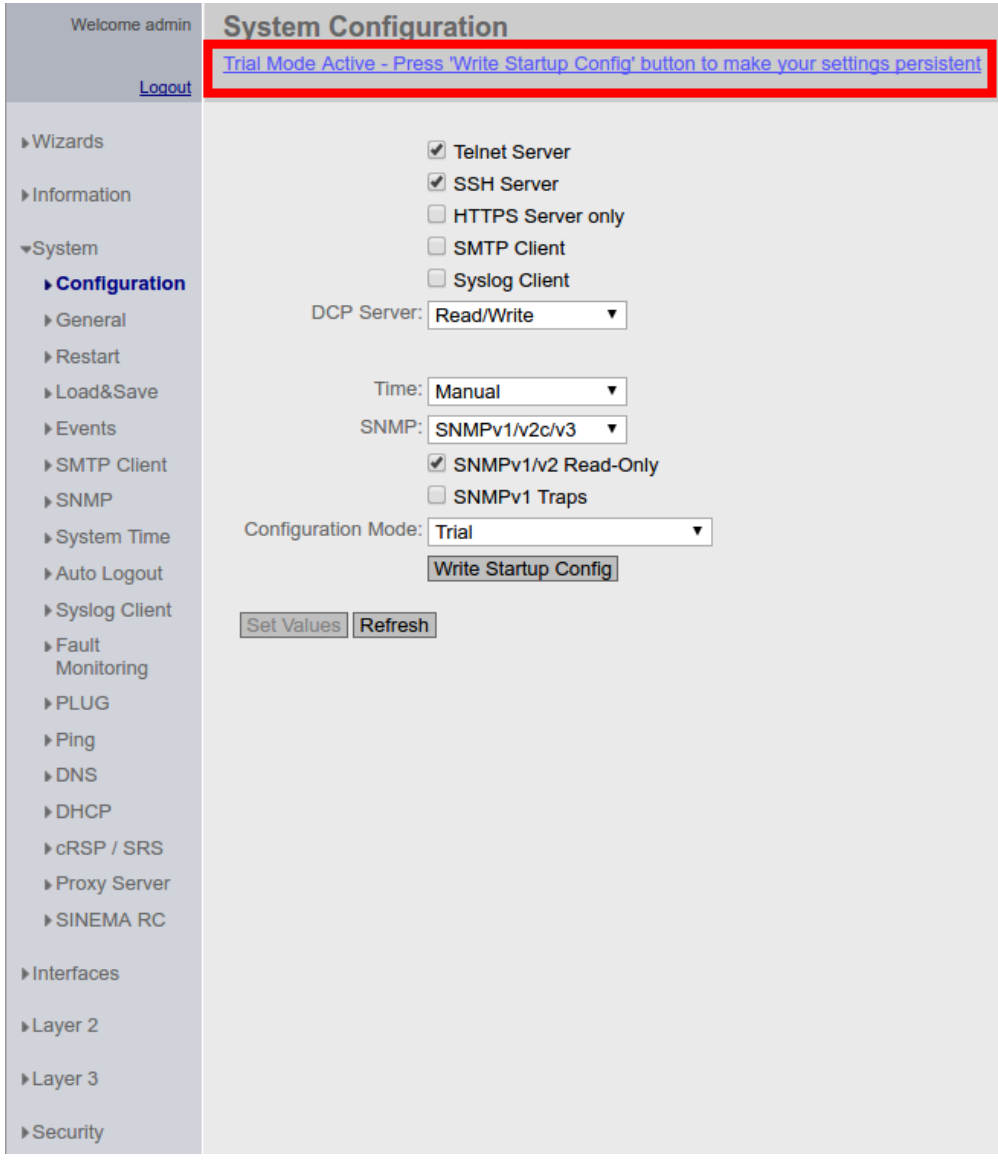
1) Navigate to and click on System

2) Navigate to and click on Configuration
   A. Alternatively, note the hot link at the top of the screen will go to the correct screen

3) Click Write Startup Config button

4) Acknowledge the Success Popup



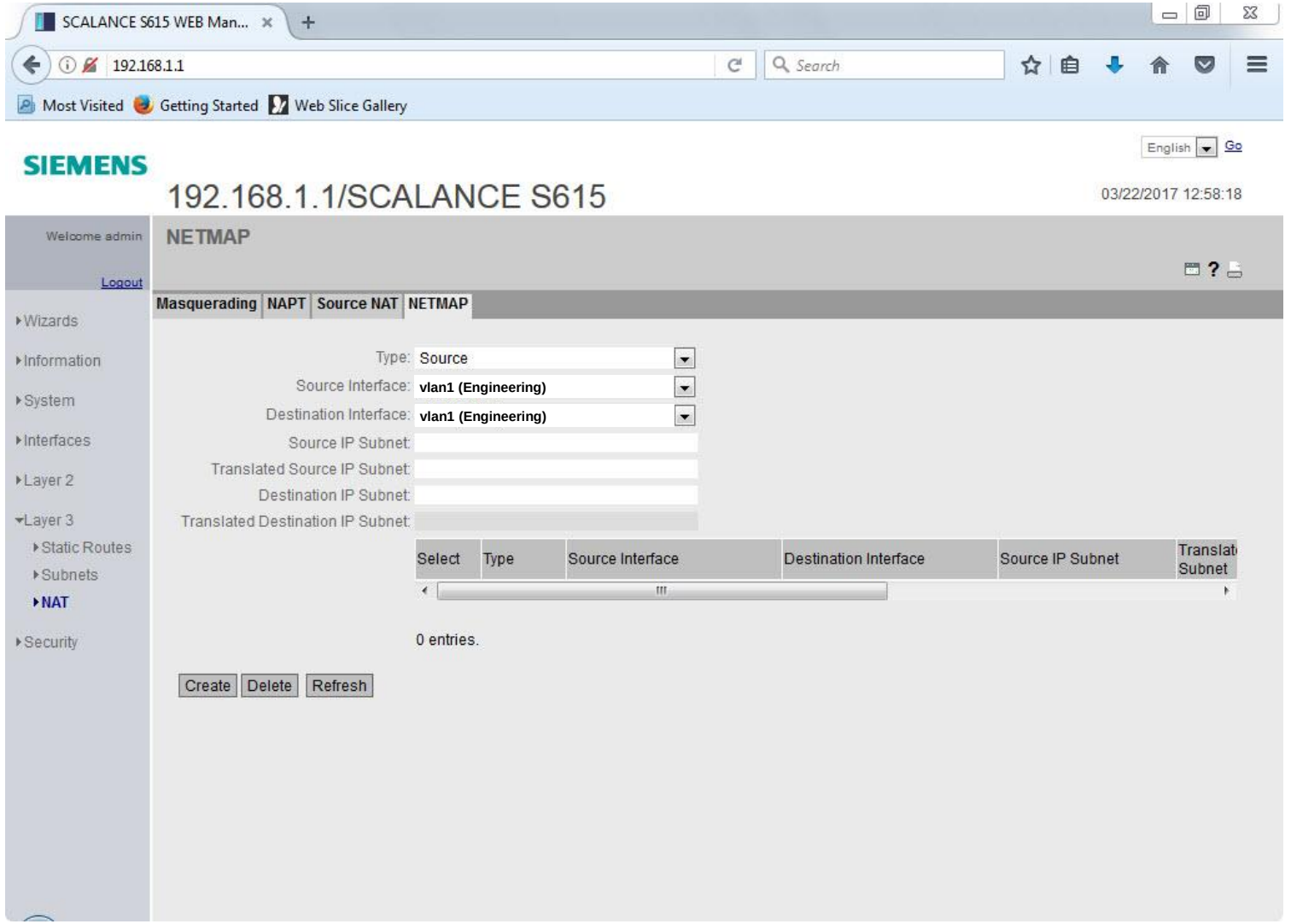


Labs

1:1 NAT Lab – DNAT

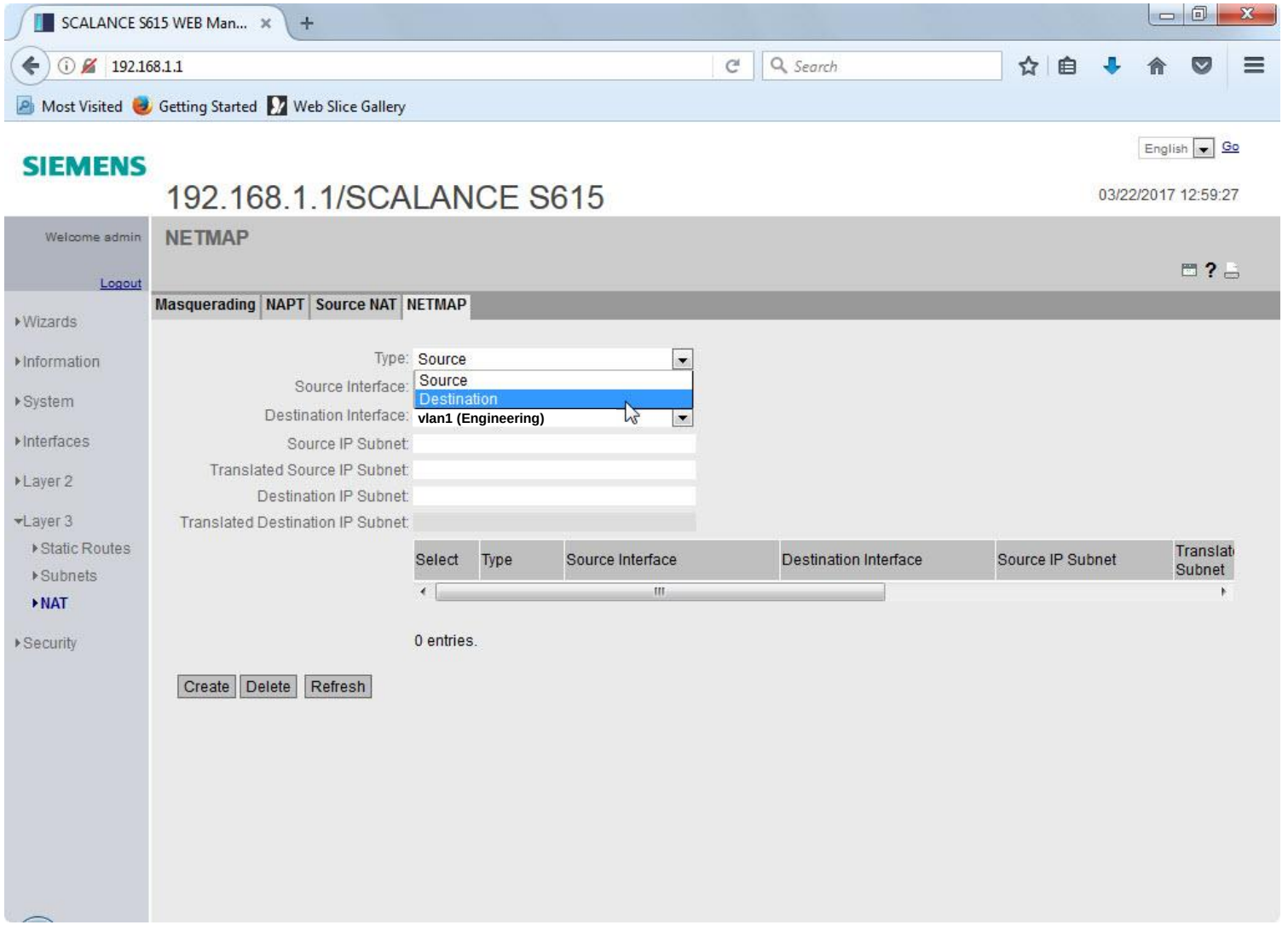
1:1 NAT – Destination NAT
Lab

1) Navigate to and click on Layer 3
2) Navigate to and click on NAT
3) Click on the NETMAP tab



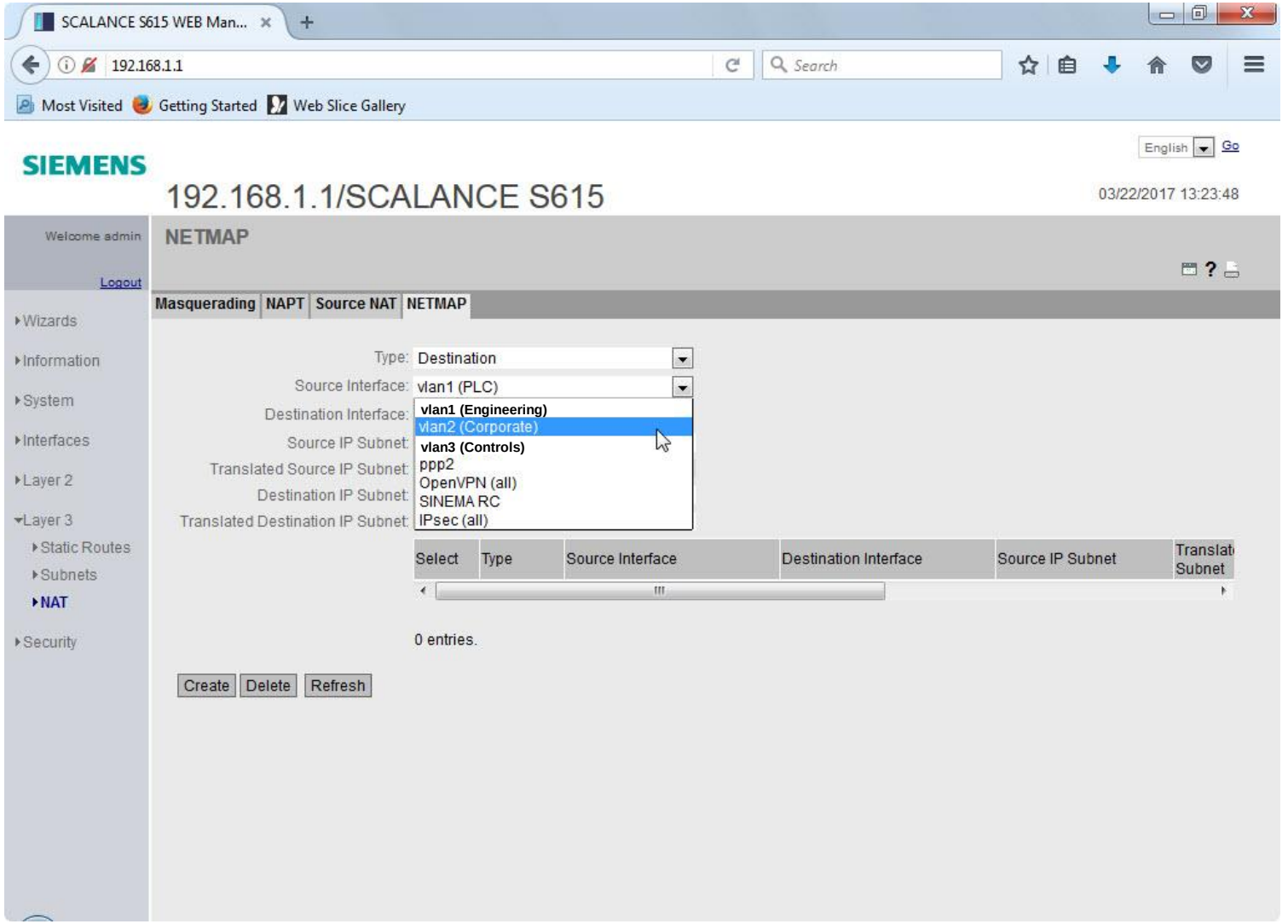
1:1 NAT – Destination NAT
Lab

1) Click the dropdown next to Type: and select Destination



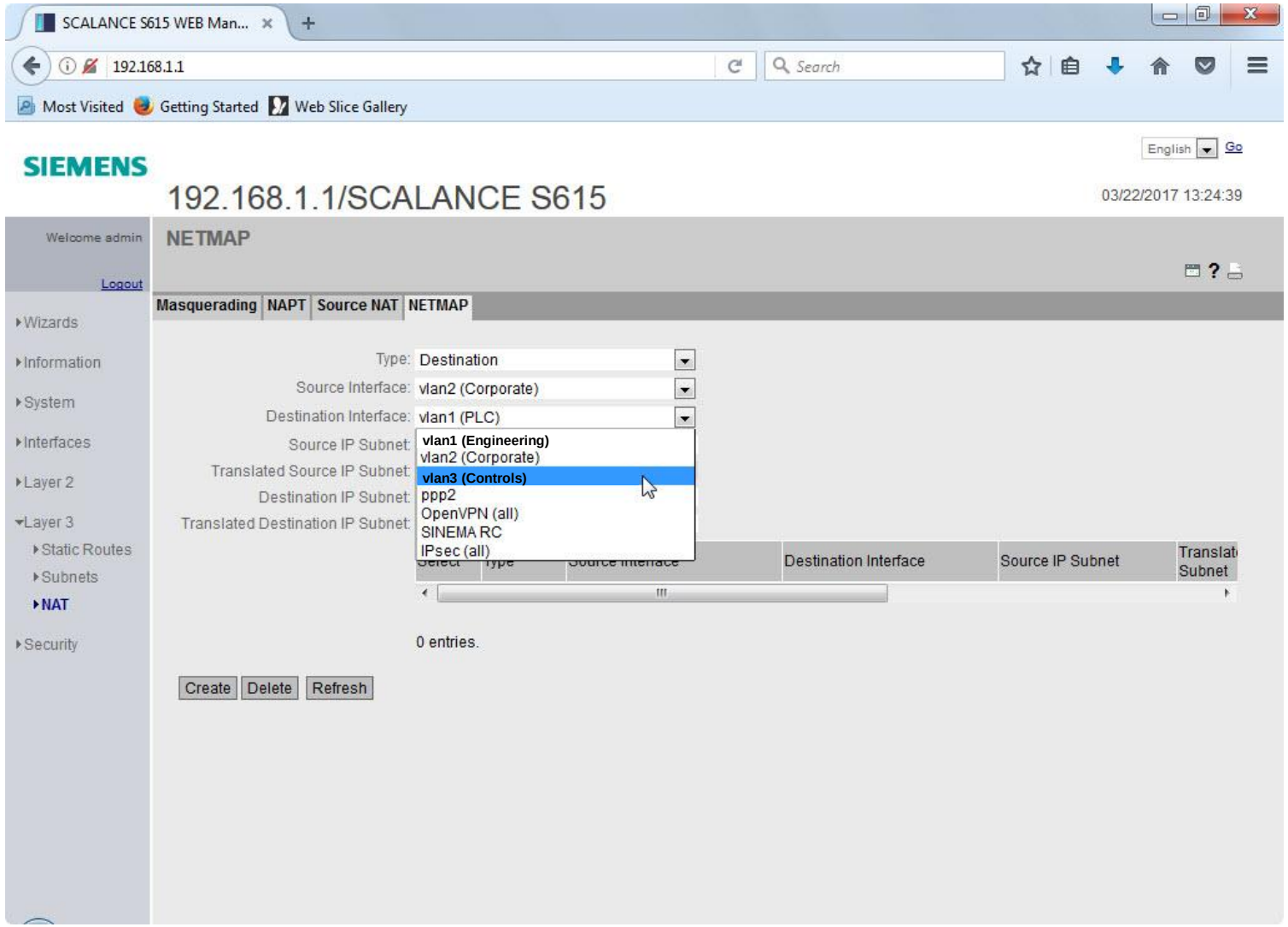
1:1 NAT – Destination NAT
Lab

1) Click the dropdown next to Source Interface: and select vlan2 (Corporate)



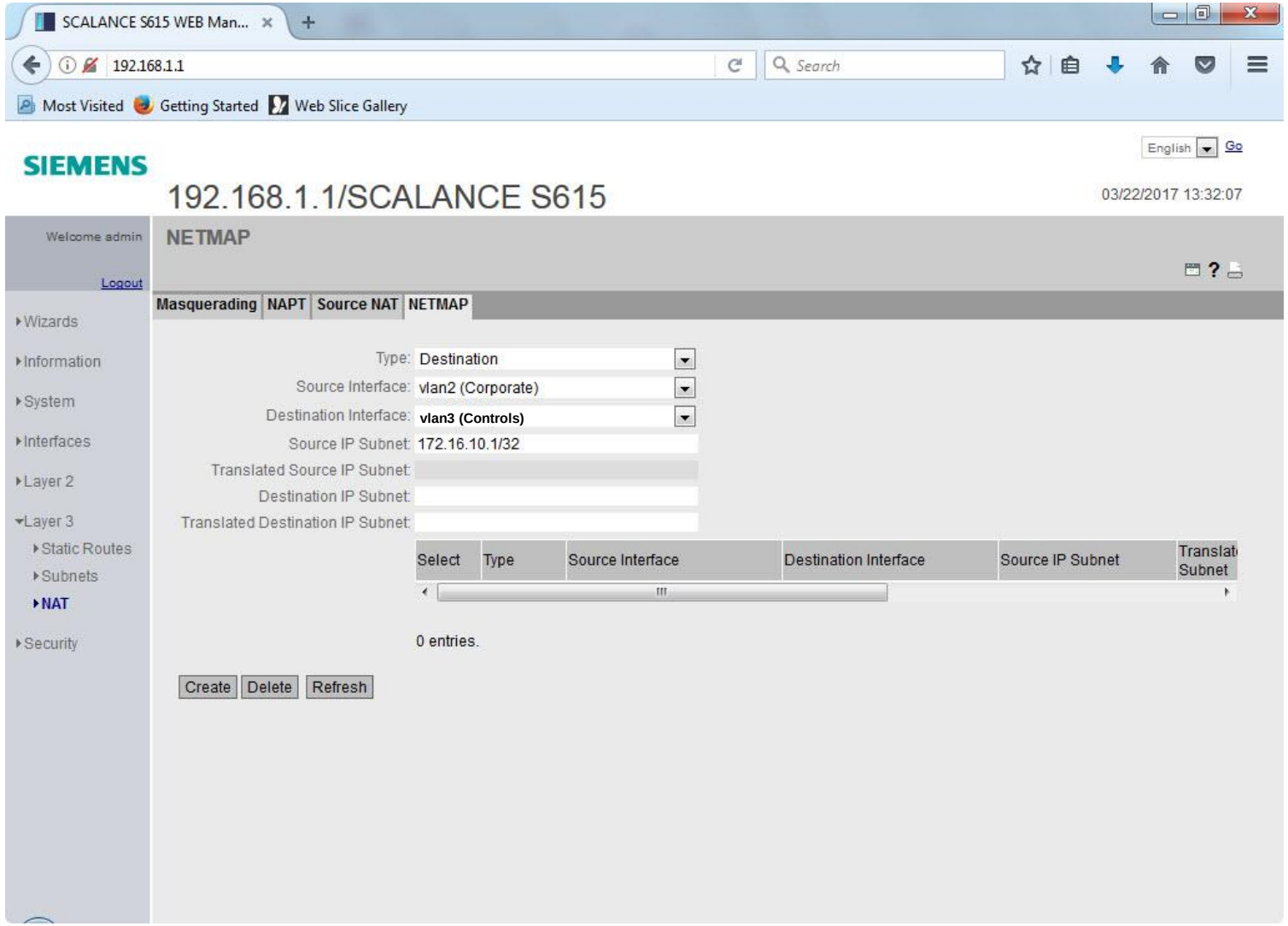
1:1 NAT – Destination NAT
Lab

1) Click the dropdown next to Destination Interface: and select vlan3 (Controls)



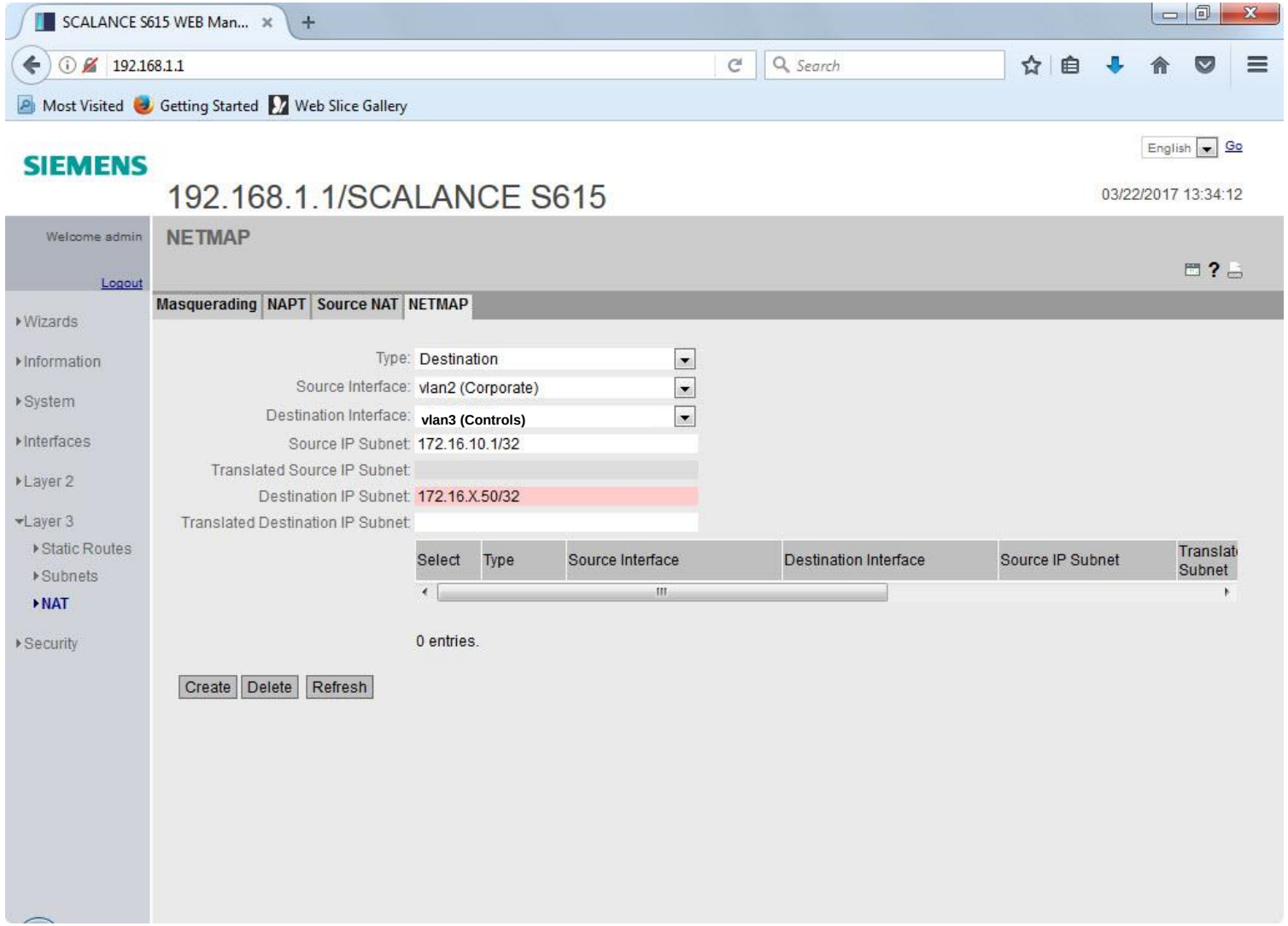
1:1 NAT – Destination NAT
Lab

1) Click the box next to Source IP Subnet: and type in 172.16.10.1/32



1:1 NAT – Destination NAT
Lab

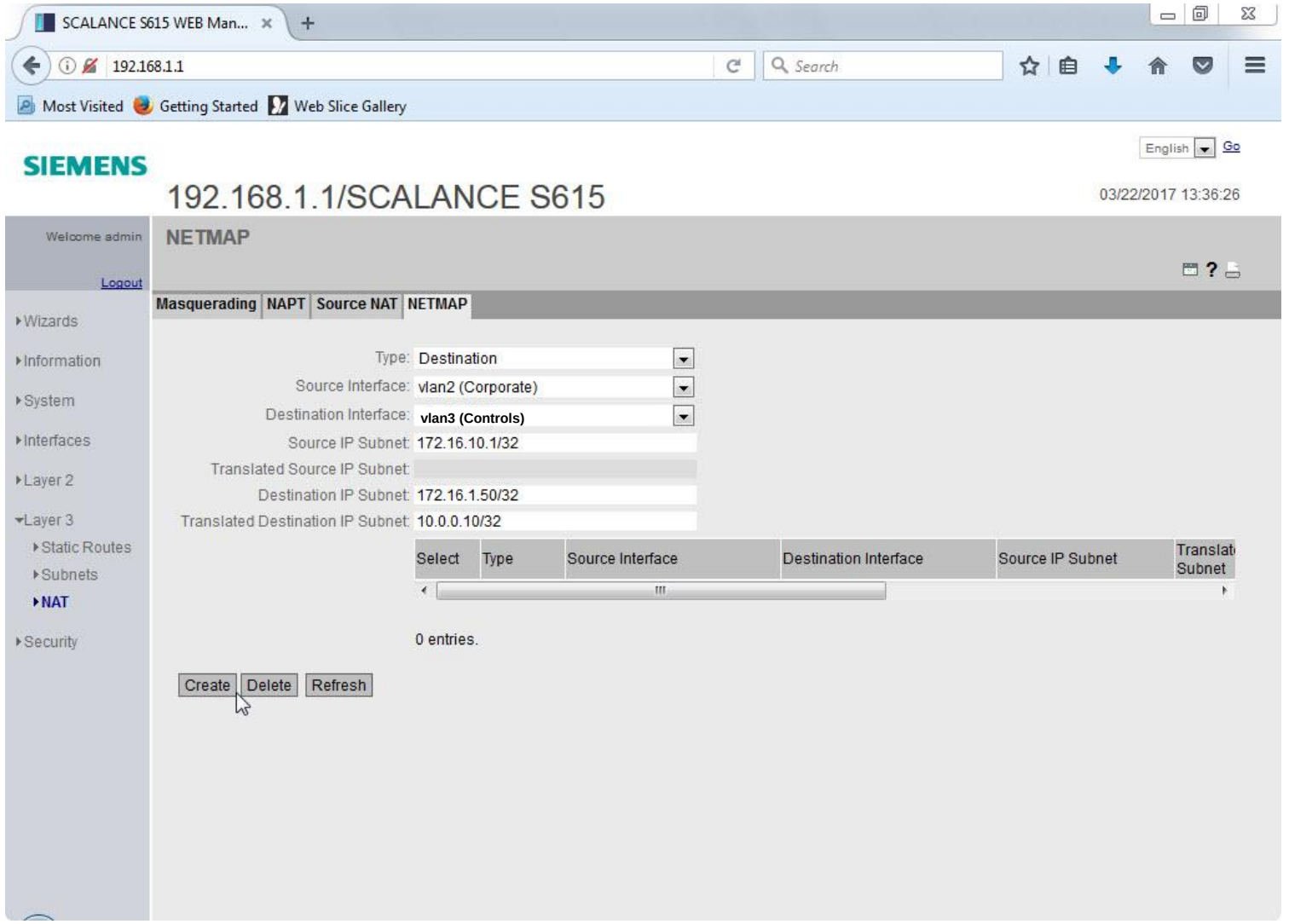
1) Click the box next to Destination IP Subnet: and type in 172.16.X.50/32 where X is the number of the station assigned to you



1:1 NAT – Destination NAT
Lab

1) Click the box next to Translated Destination IP Subnet: and type in 10.0.0.1X/32 where X is the number of the station assigned to you

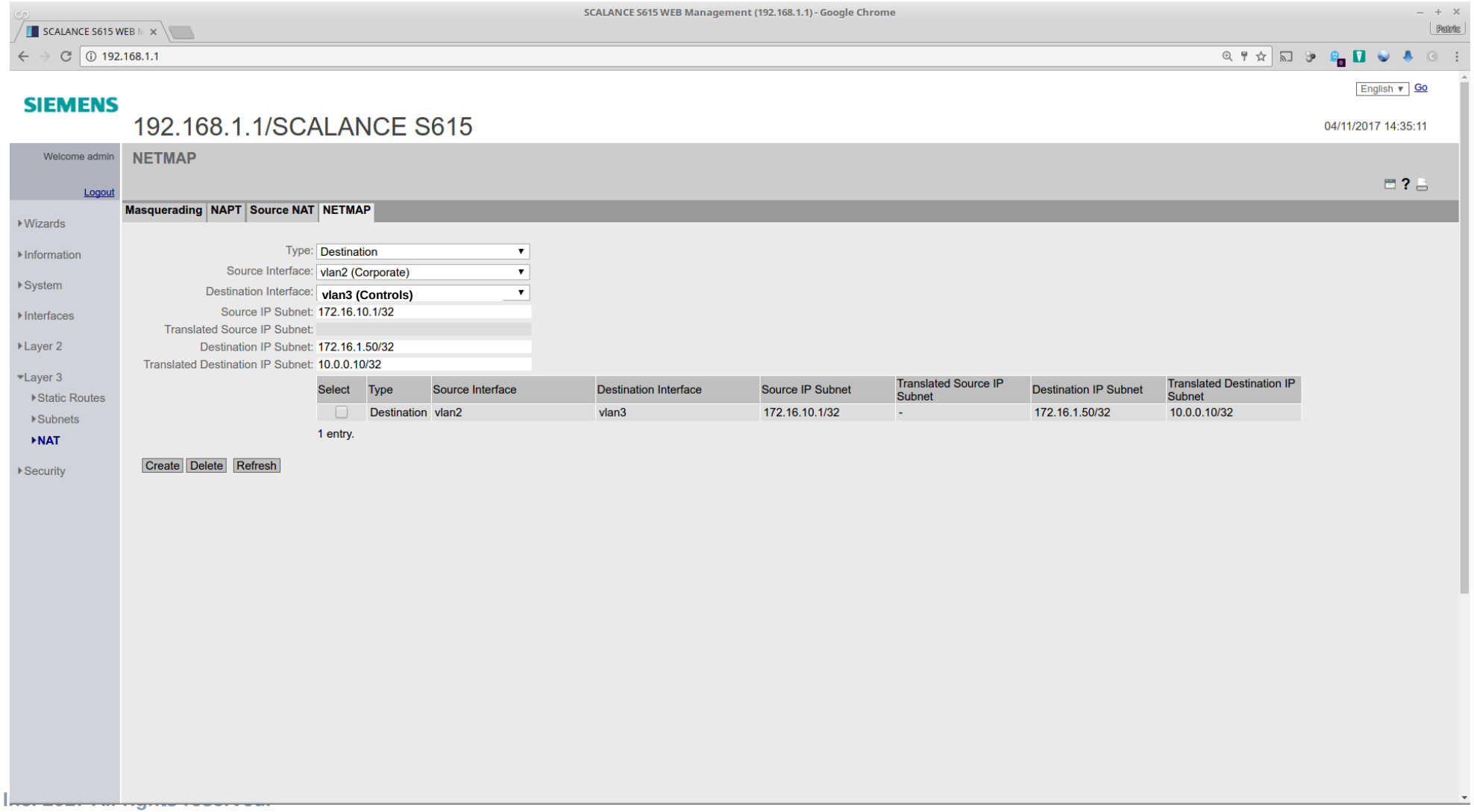
2) Click Create



1:1 NAT – Destination NAT
Lab

1) Note the entry for Destination NAT

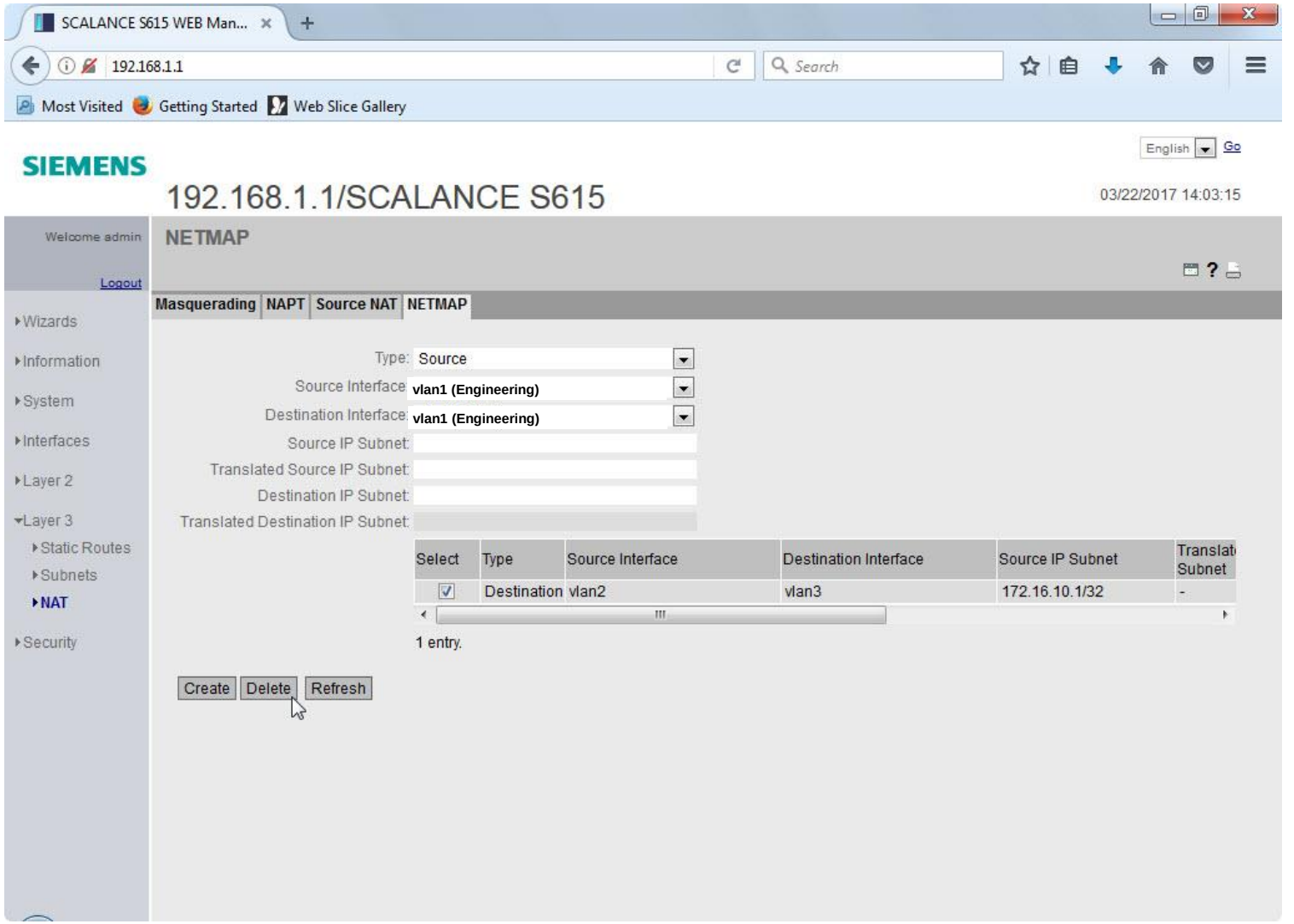
2) The instructor will perform a ping test



1:1 NAT – Destination NAT
Lab

1) Click the check box next to the NAT rule in the Select column

2) Click Delete

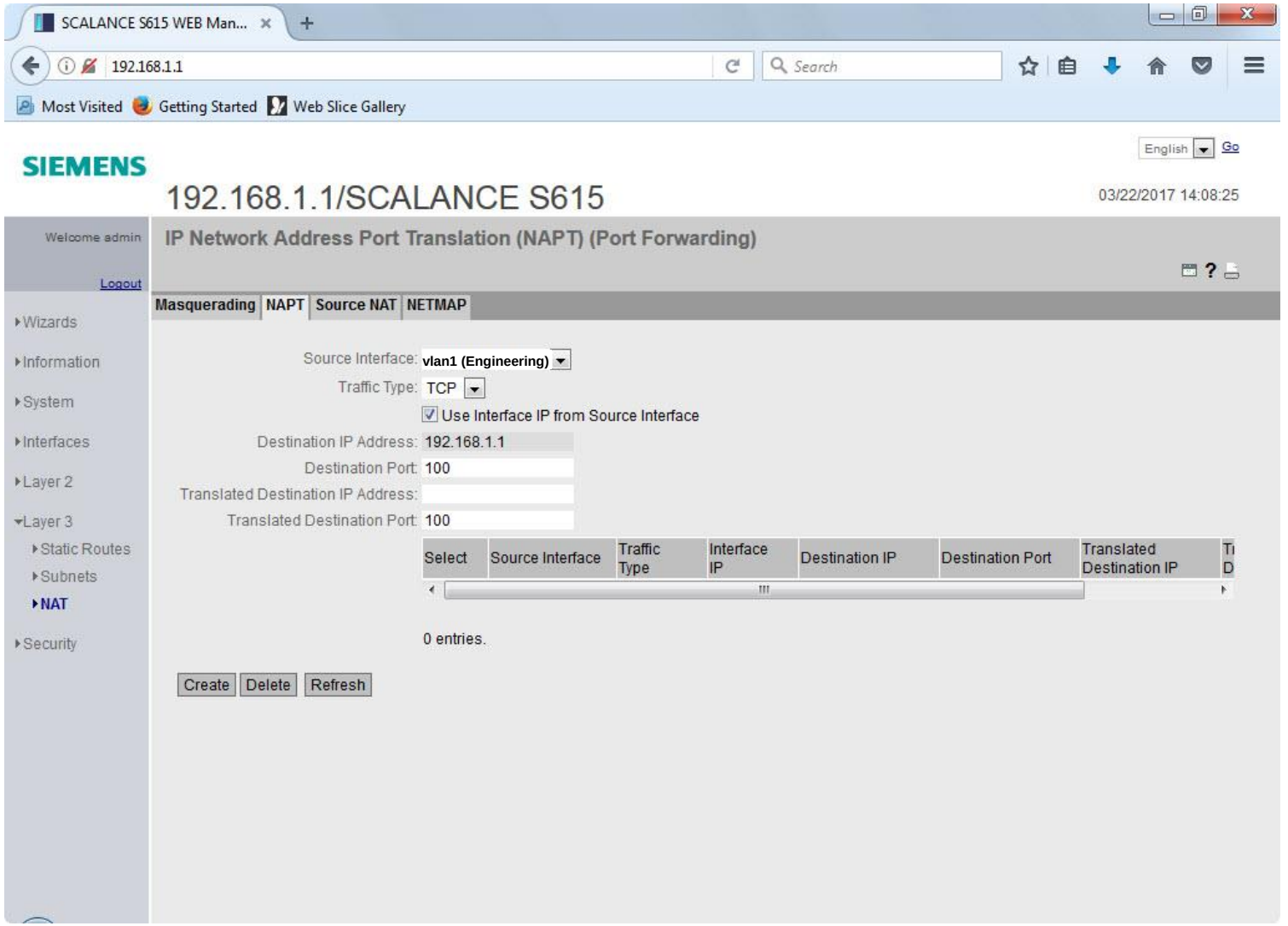


Labs

1:1 NAT Lab – NAPT

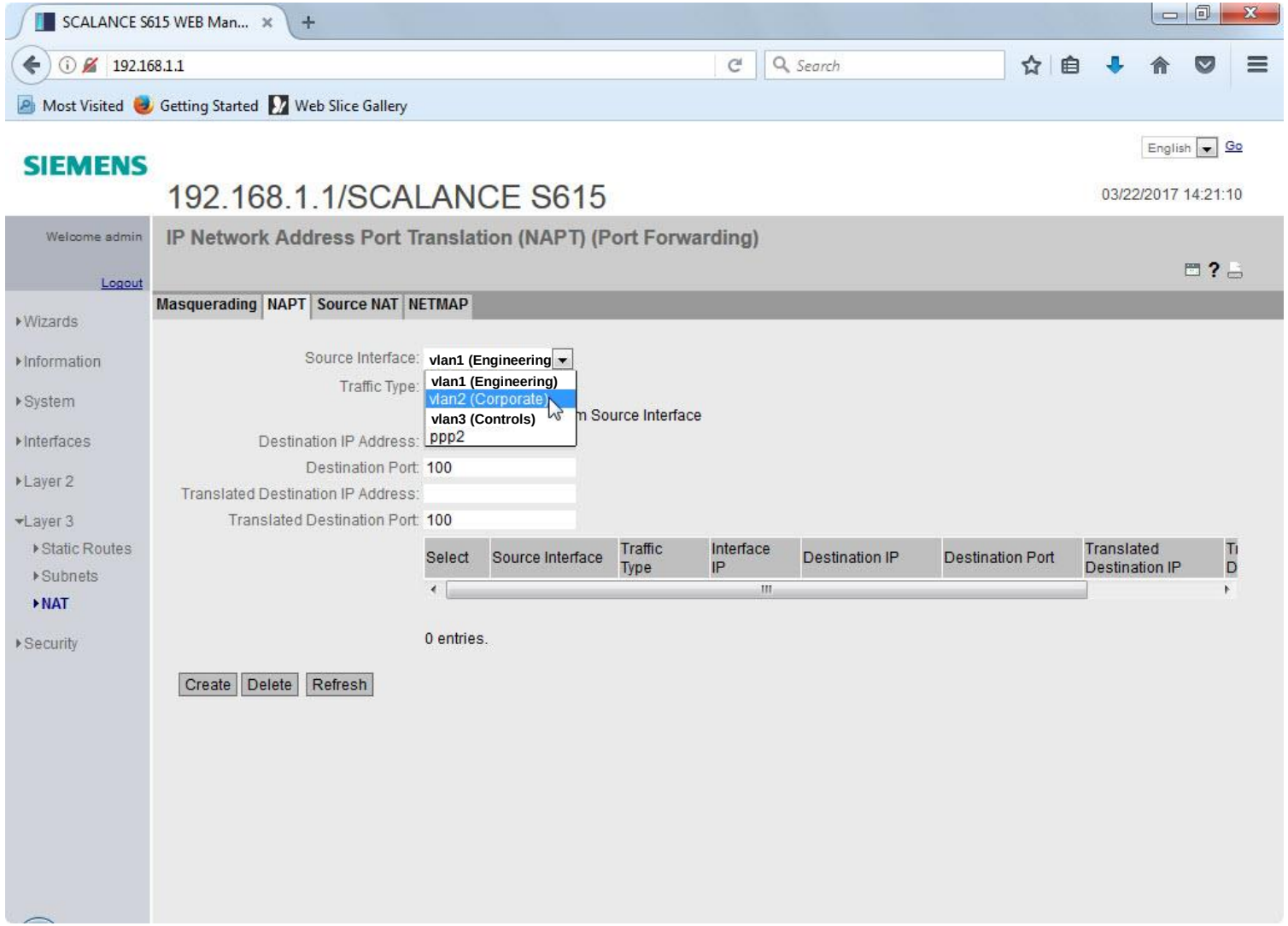
1:1 NAT – NAPT
Lab

1) Click the NAPT Tab



1:1 NAT – NAPT
Lab

1) Click the dropdown next to the Source Interface: and select vlan2 (Corporate)



1:1 NAT – NAPT
Lab

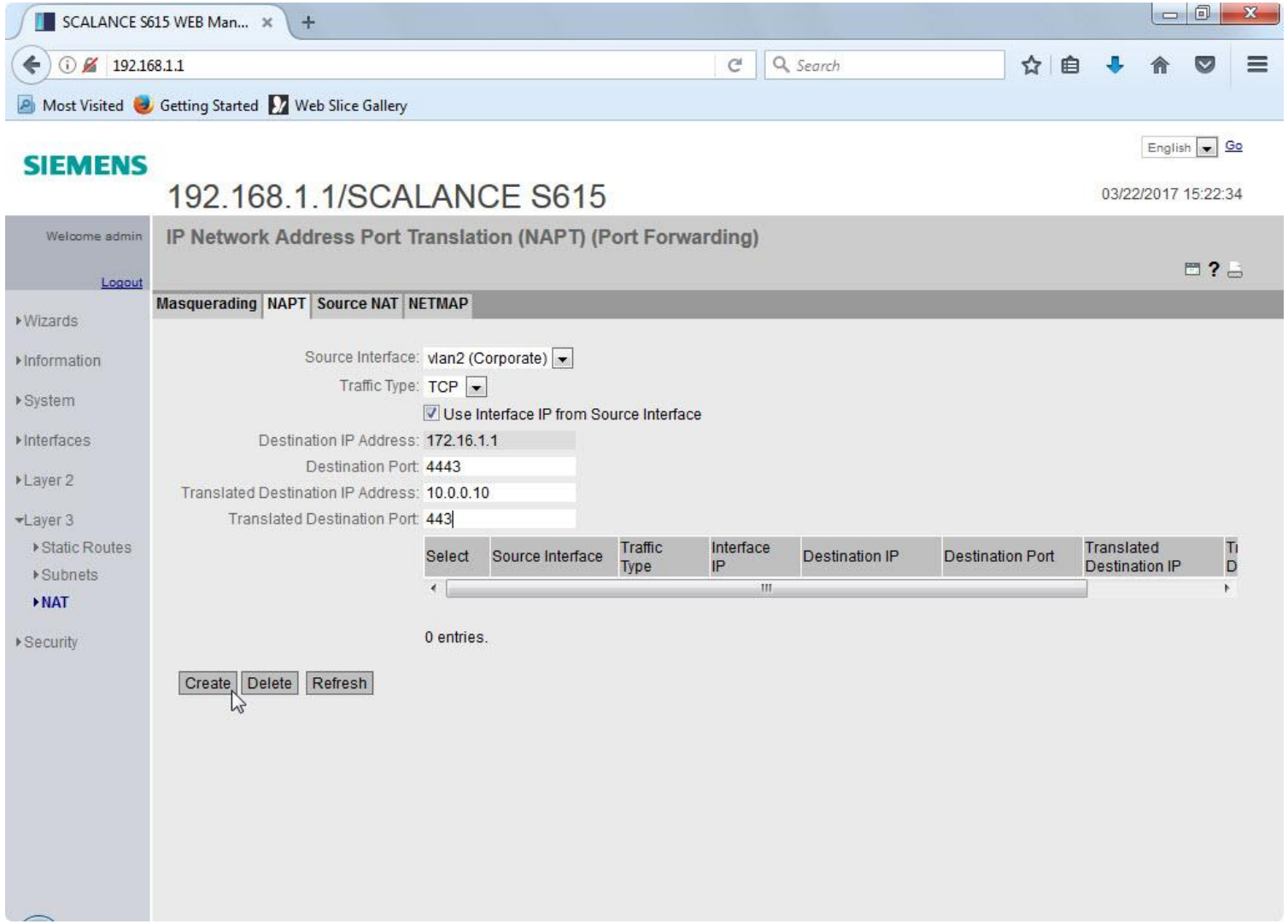
1) Make sure there is a check in the box next to User Interface IP from Source Interface

2) In the box next to Destination Port: enter the value 4443

3) In the box next to Translated Destination IP Address: enter the IP Address 10.0.0.1X where X is the number of the station assigned to you

4) In the box next to Translated Destination Port: enter the value 443

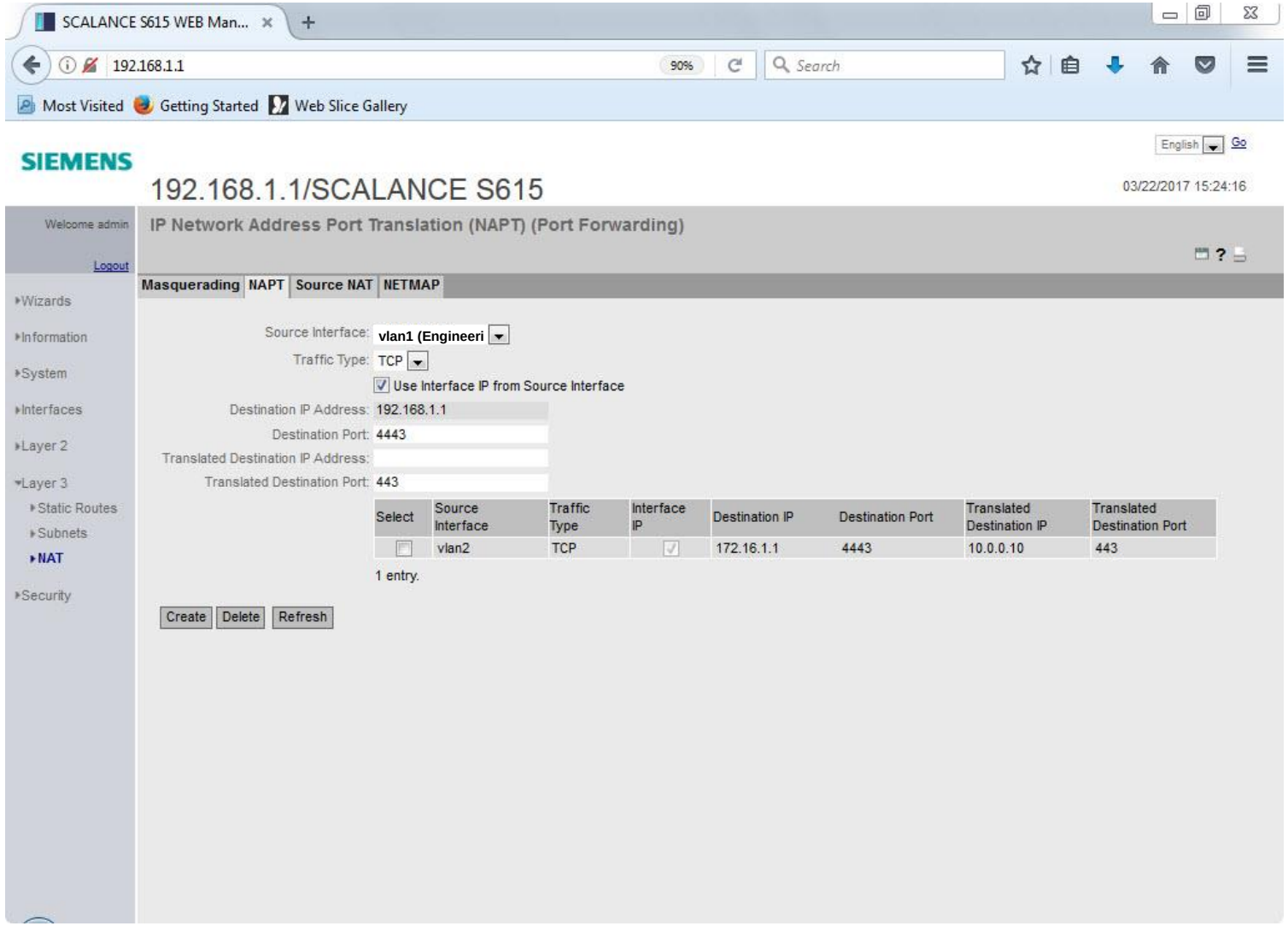
5) Click Create



1:1 NAT – NAPT
Lab

1) Note the final entry

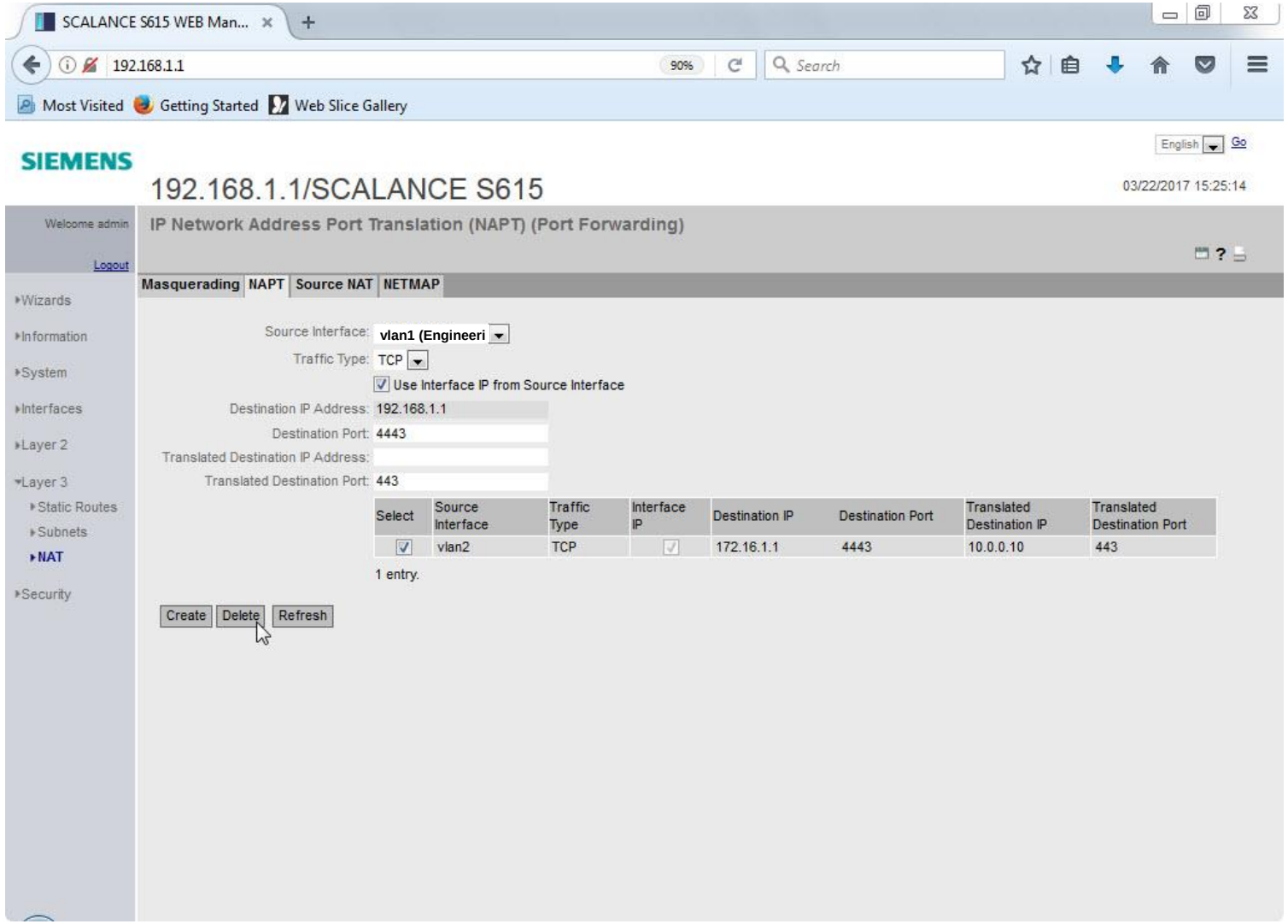
2) Instructor will test by browsing to the IP Address of the station utilizing port 4443.



1:1 NAT – NAPT
Lab

1) Click the check box next to the NAPT rule in the Select column

2) Click Delete

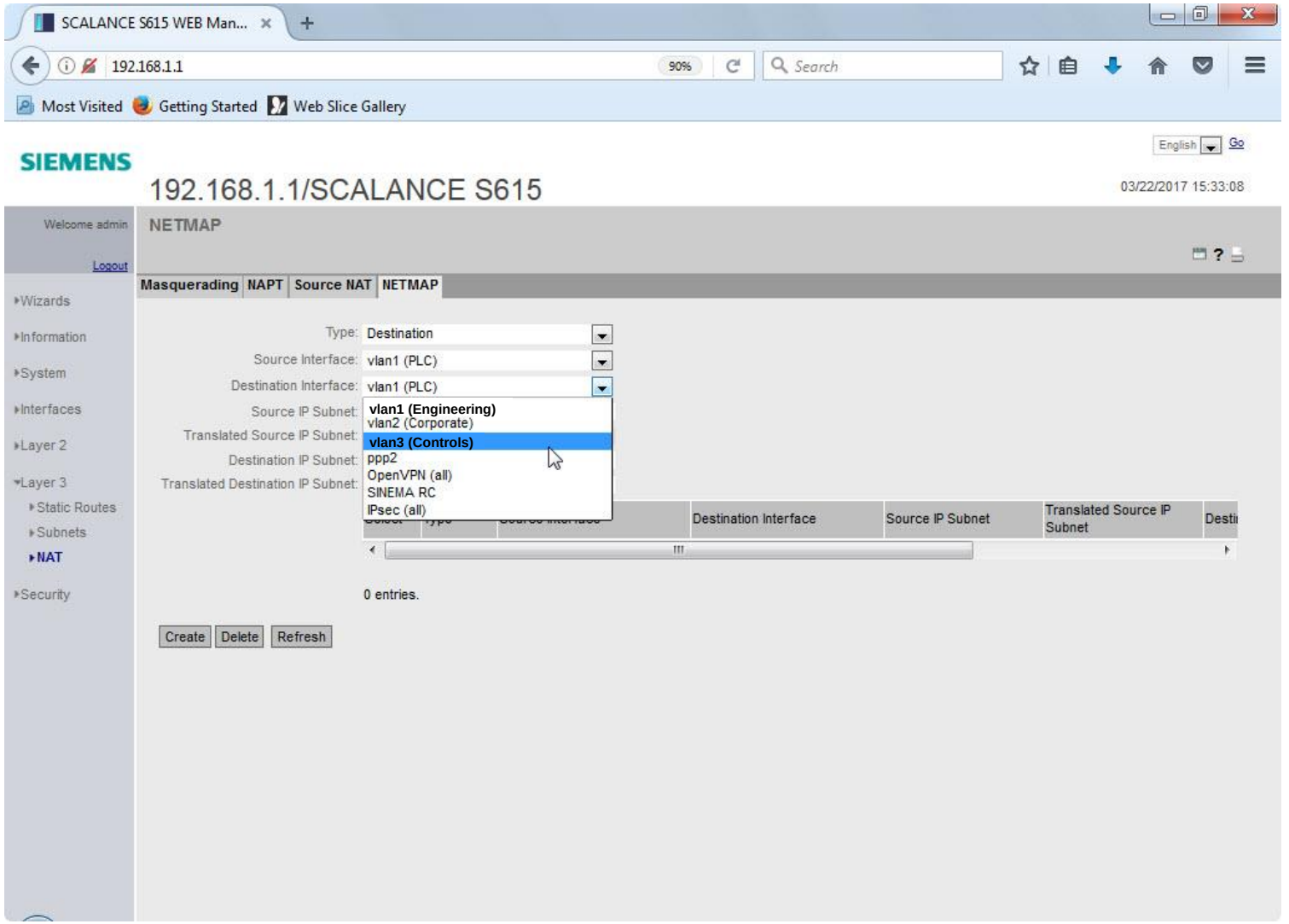


Labs

1:1 NAT Lab – Double NAT

1:1 NAT – Double NAT
Lab

1) Click the NETMAP tab
2) Select Type: Destination
3) Source Interface: vlan1 (Engineering)
4) Destination Interface: vlan3 (Controls)



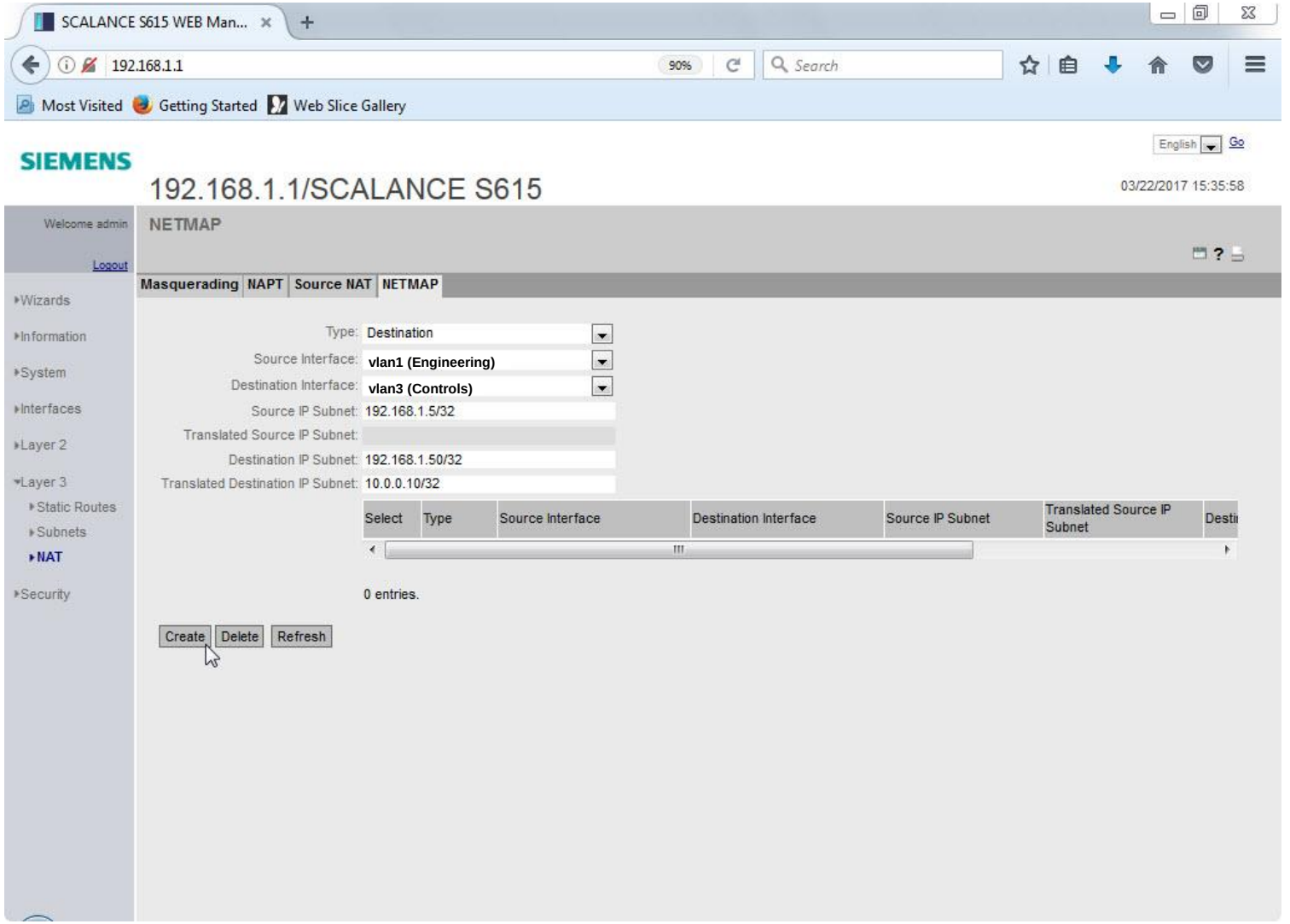
1:1 NAT – Double NAT
Lab

1) In the box next to Source IP Subnet: enter 192.168.1.5/32

2) In the box next to Destination IP Subnet: enter 192.168.1.50/32

3) In the box next to Translated Destination IP Subnet: enter 10.0.0.1X/32 where X is the number of the station assigned to you

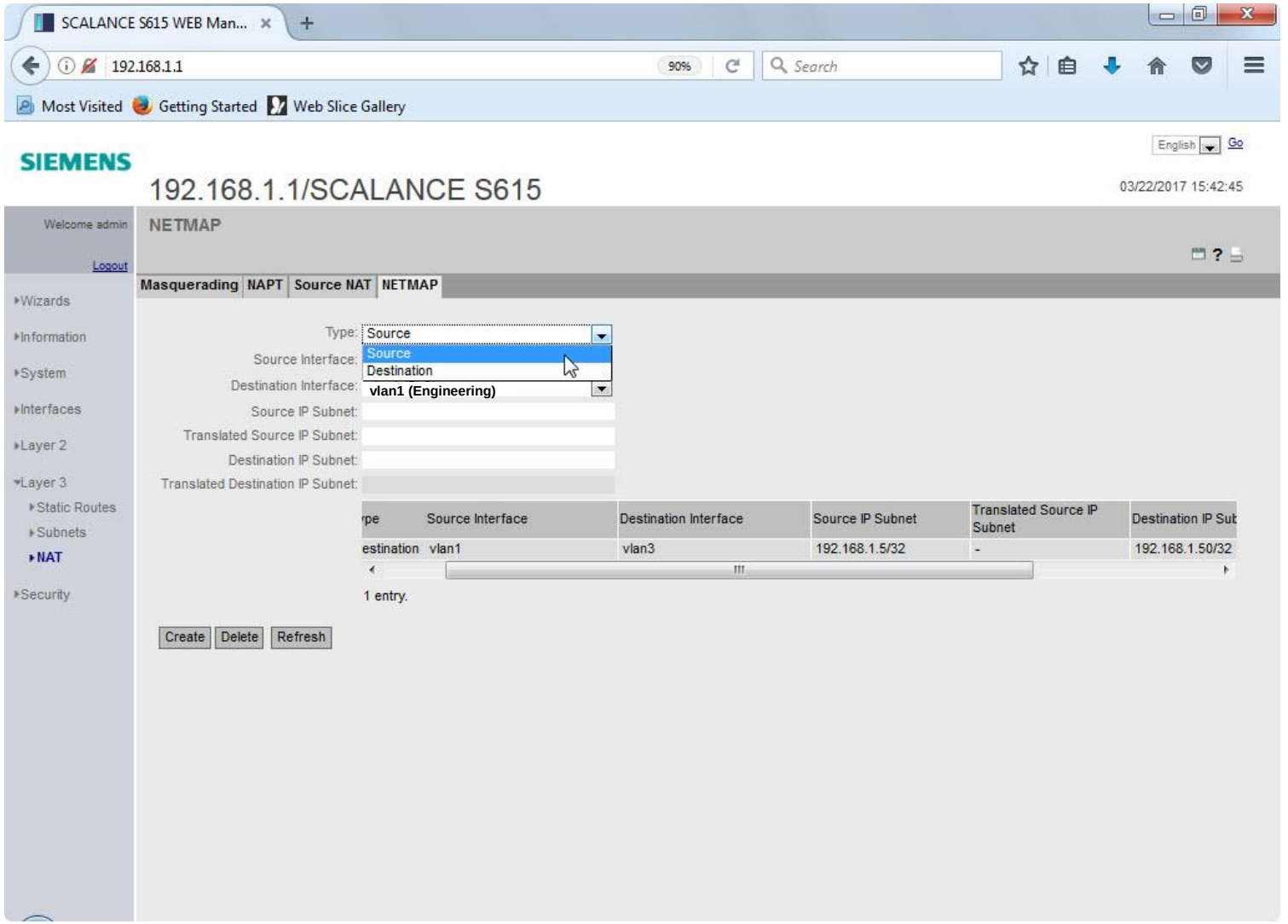
4) Click Create



1:1 NAT – Double NAT
Lab

1) Note the newly added Destination NAT rule

2) Select Type: Source



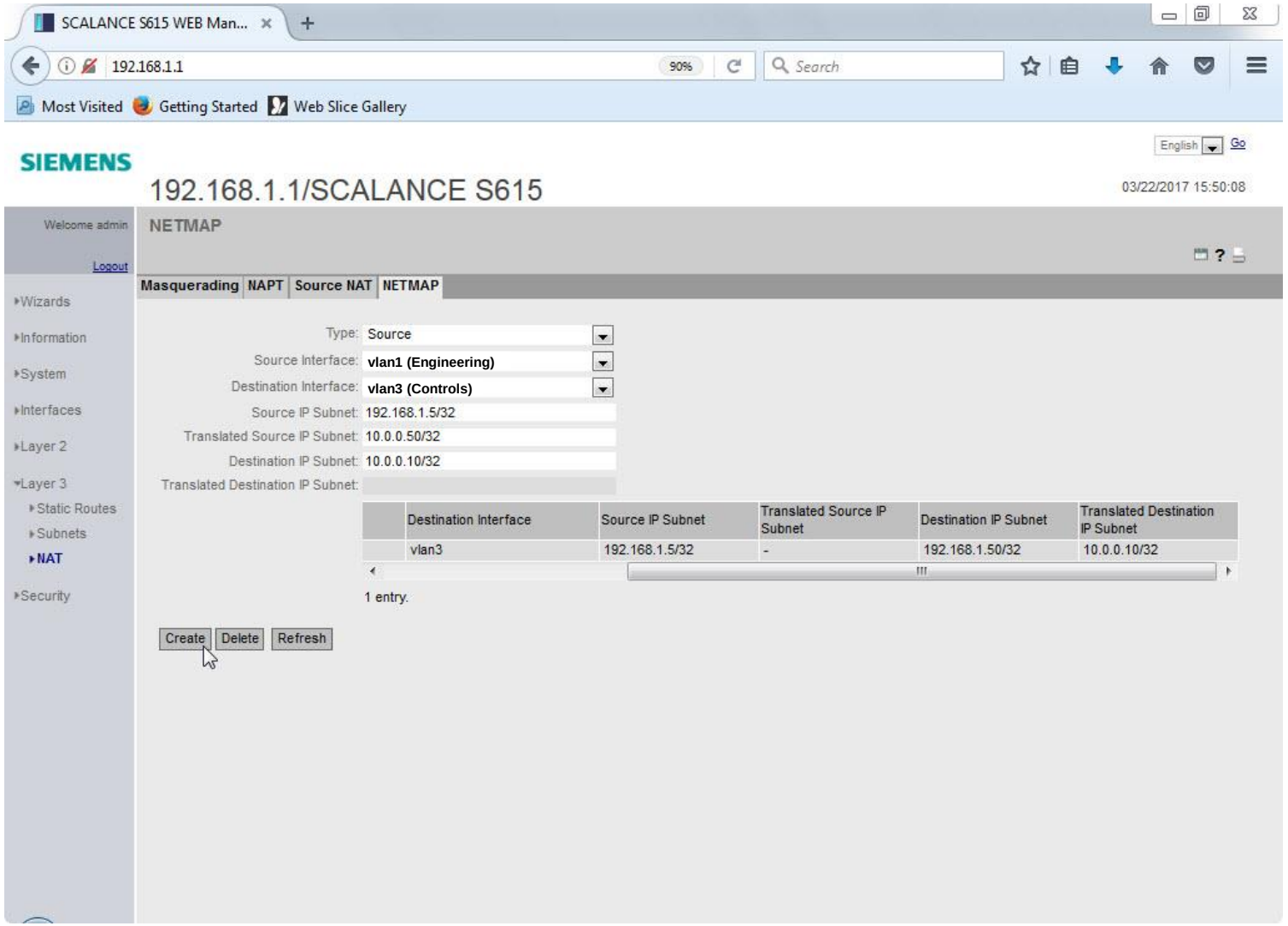
1:1 NAT – Double NAT
Lab

1) In the box next to Source IP Subnet: enter 192.168.1.5/32

2) In the box next to Translated Source IP Subnet: enter 10.0.0.50/32

3) In the box next to Destination IP Subnet: enter 10.0.0.1X/32 where X is the number of the station assigned to you

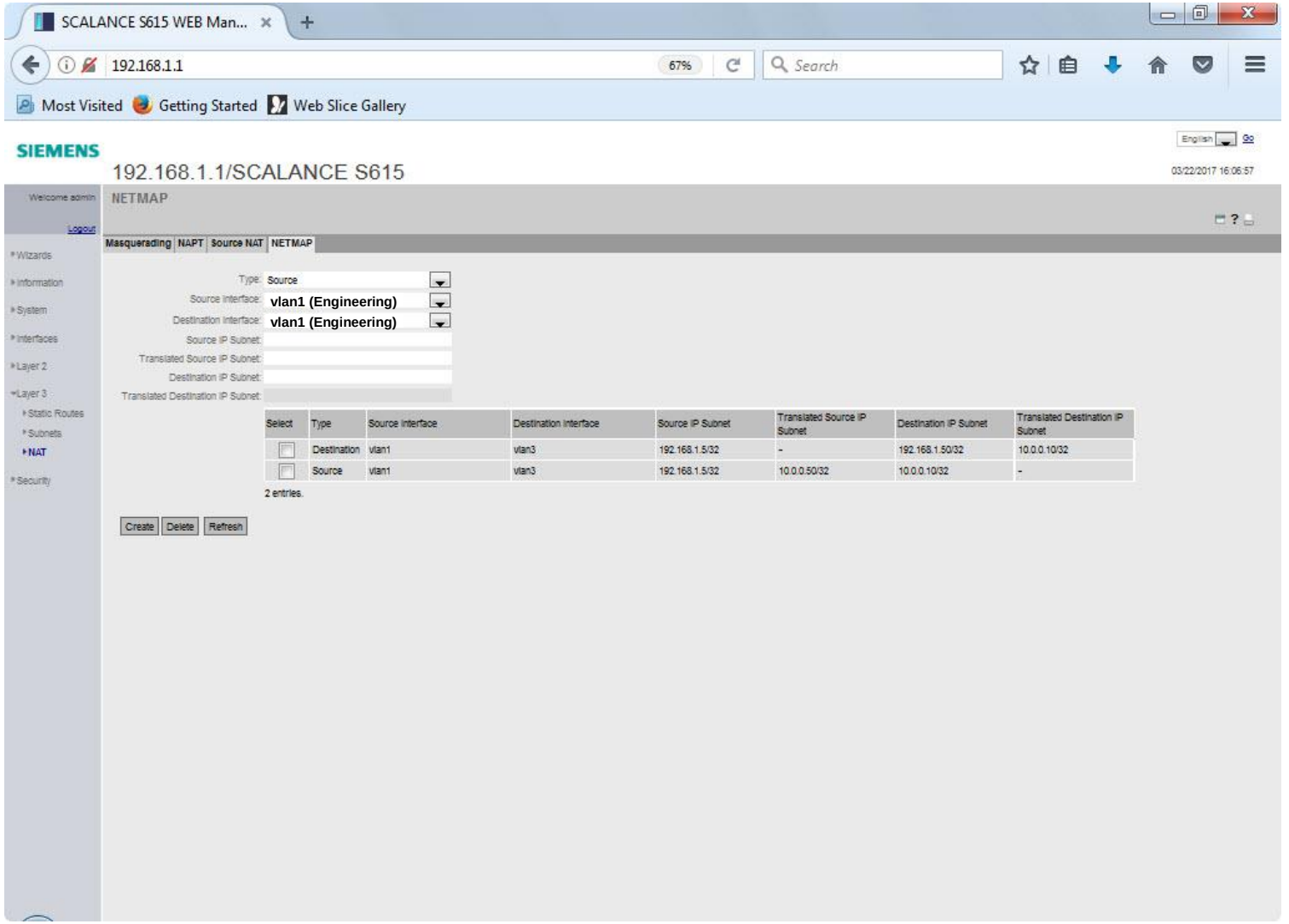
4) Click Create



1:1 NAT – Double NAT
Lab

1) Note final configuration

2) Test configuration by trying to ping 192.168.1.50



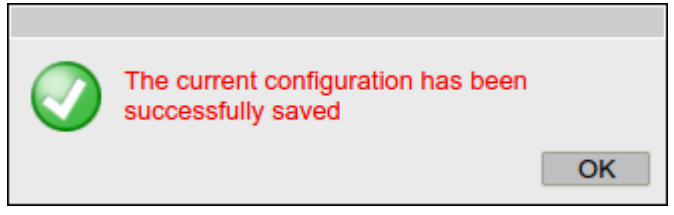
1:1 NAT – Write Startup Config
Lab

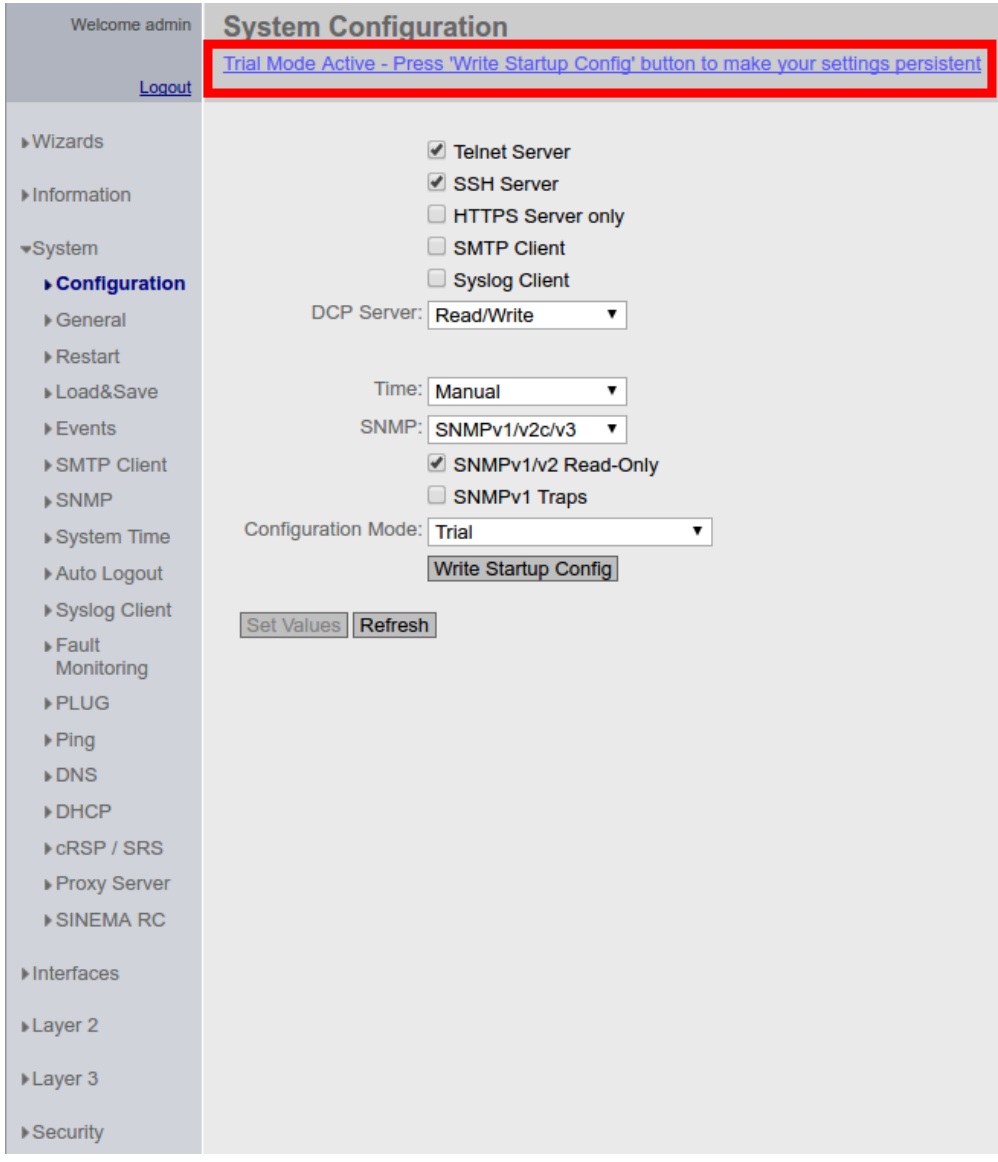
1) Navigate to and click on System

2) Navigate to and click on Configuration
   A. Alternatively, note the hot link at the top of the screen will go to the correct screen

3) Click Write Startup Config button

4) Acknowledge the Success Popup



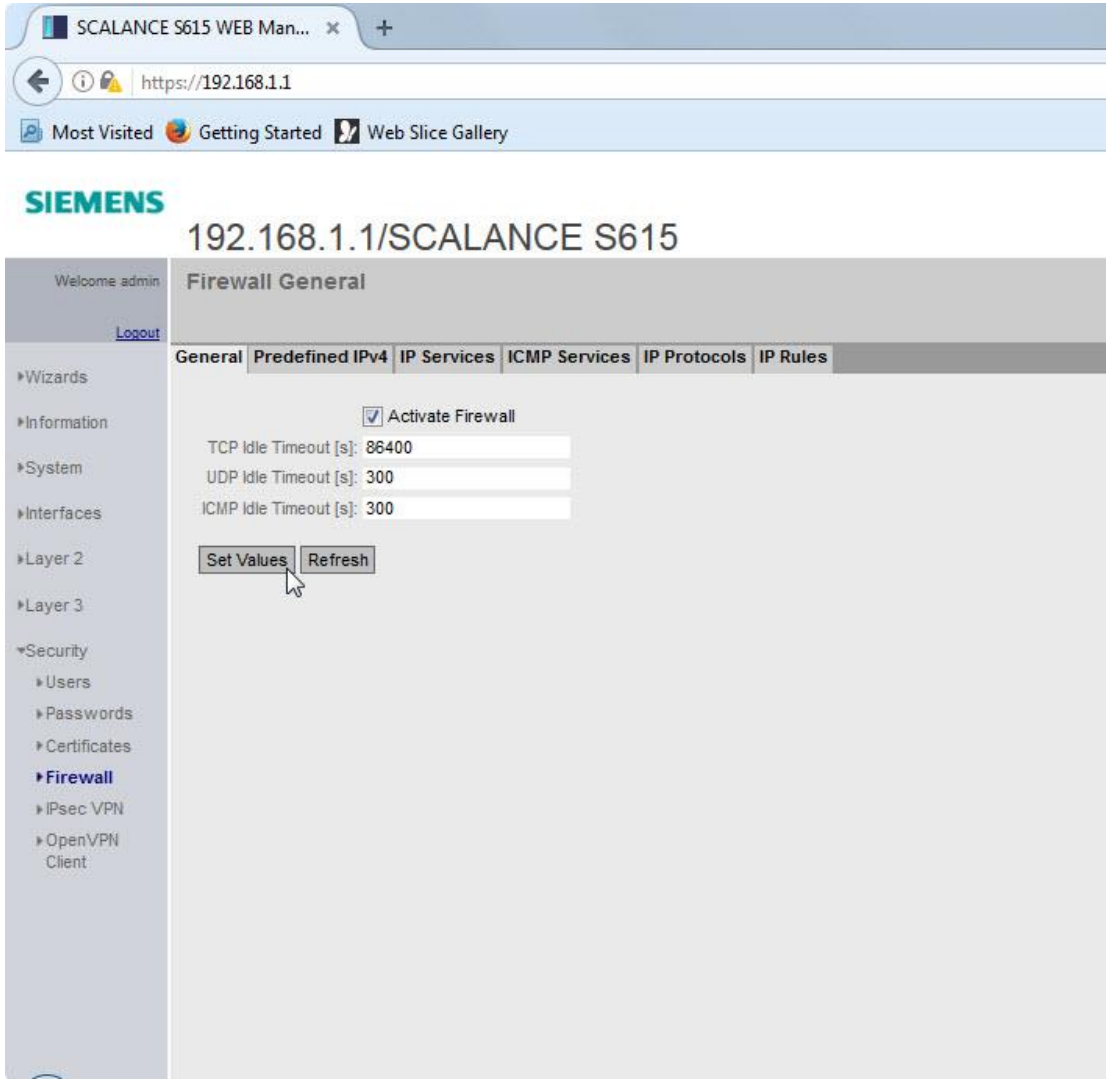


Labs

Firewall Lab

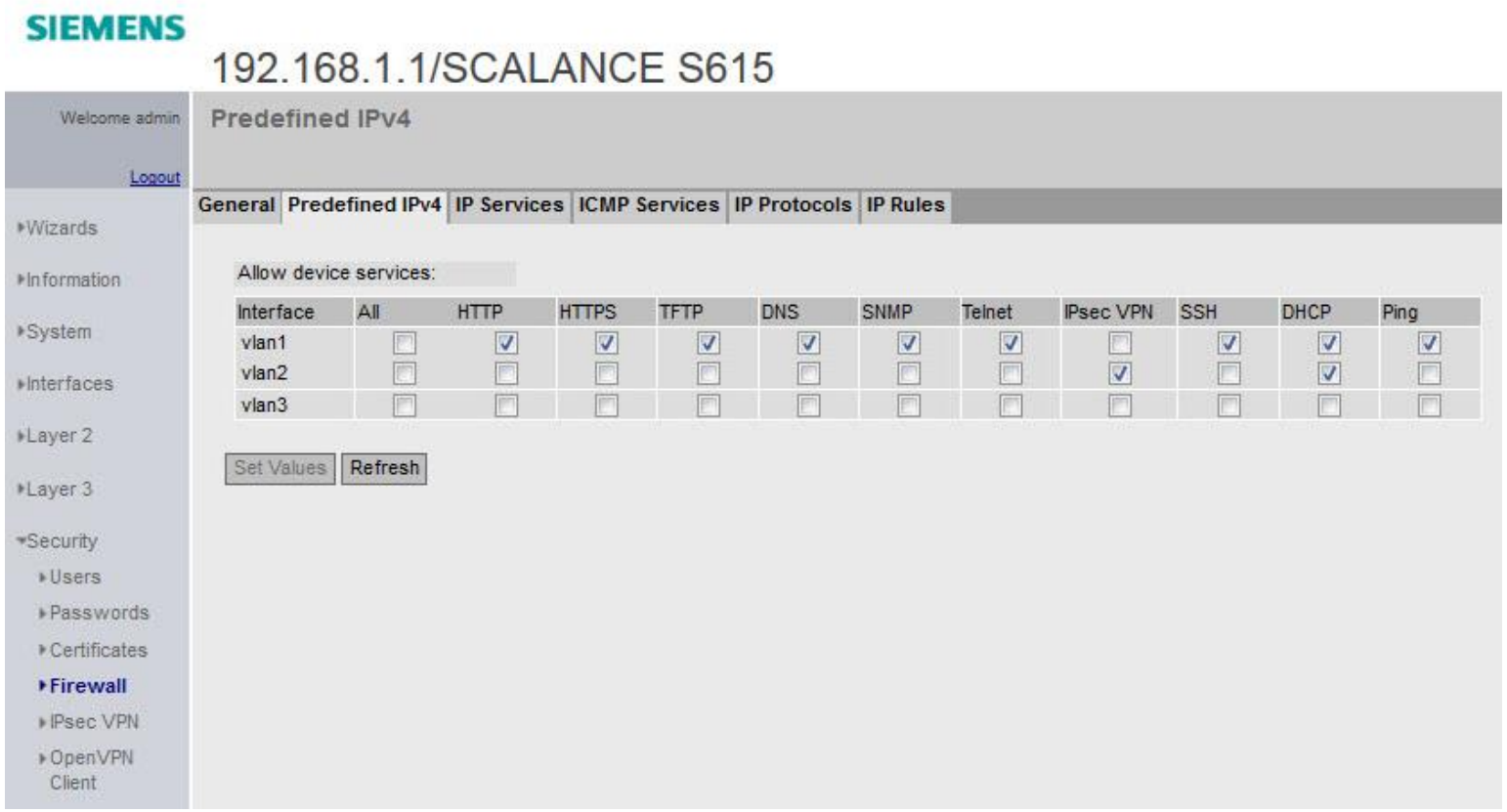
Firewall - Initial
Lab

1) Navigate to and click on Security
2) Navigate to and click on Firewall
3) Click the box next to Activate Firewall
4) Click Set Values



Firewall – Predefined Rules
Lab

1) Note the predefined firewall rules

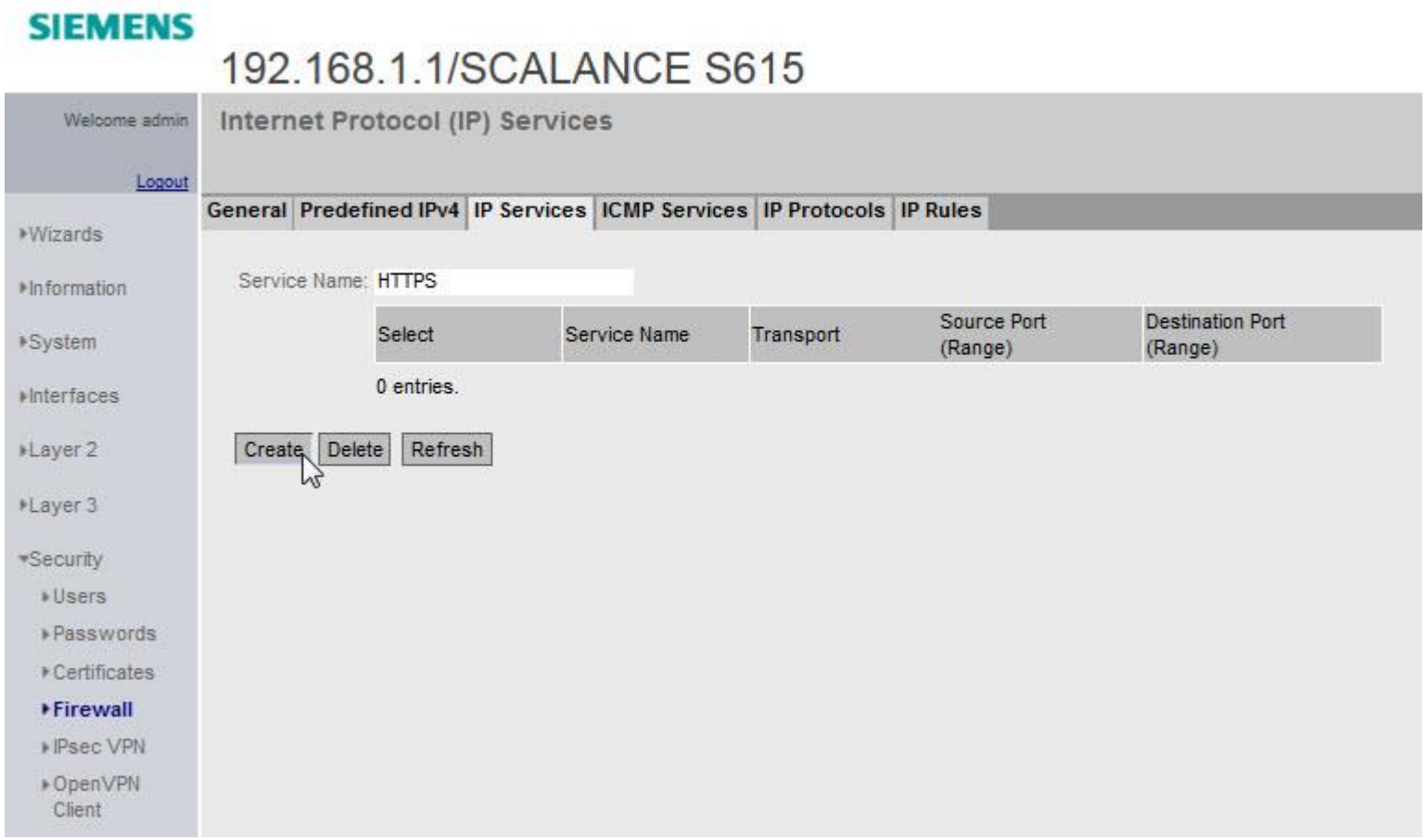


Firewall – IP Services
Lab

1) Click the IP Services tab

2) In the box next to Service Name: enter HTTPS

3) Click Create



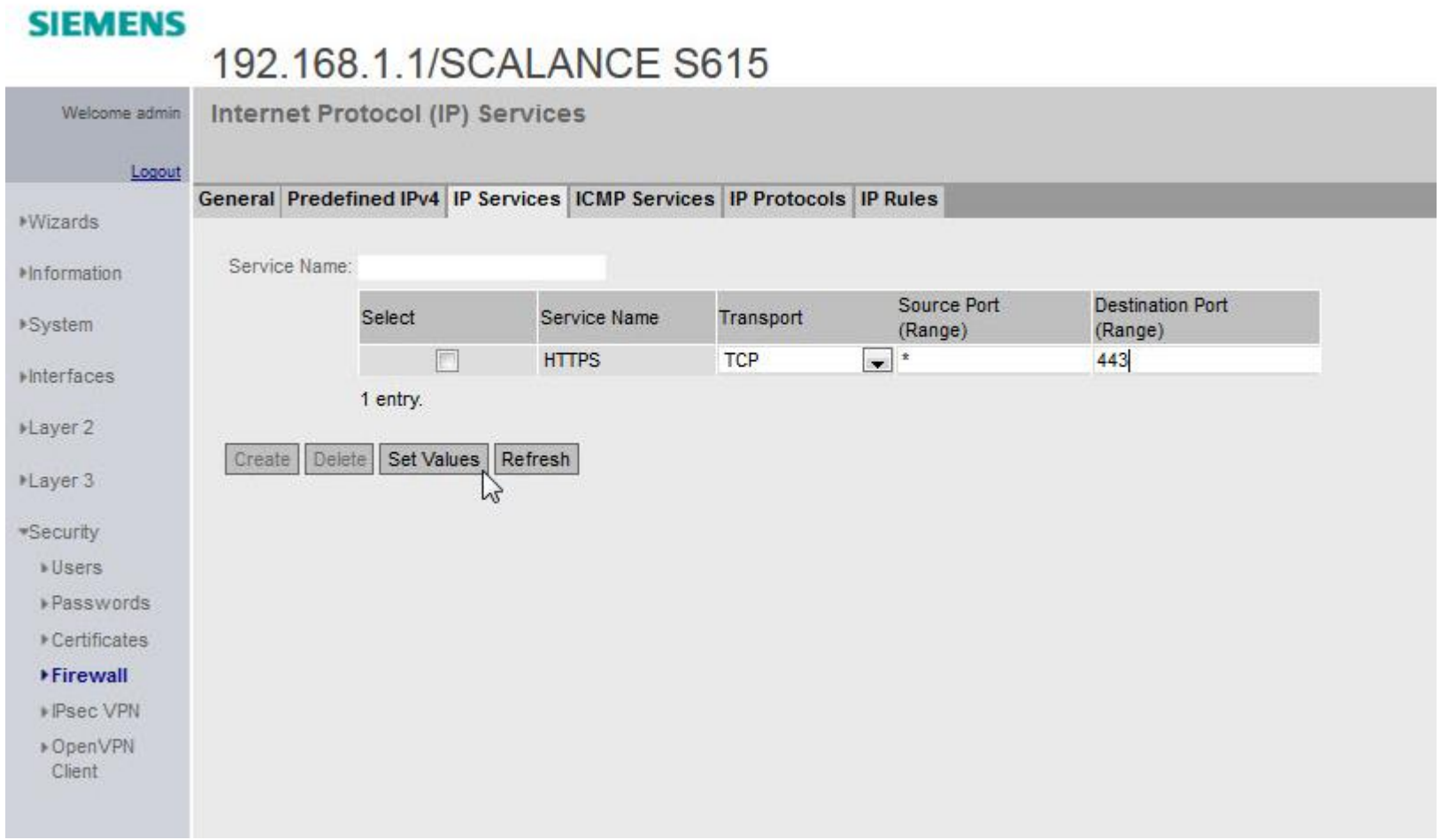
Firewall – IP Services
Lab

1) Ensure that the dropdown for Transport shows TCP

2) Ensure the Source Port (Range) box shows *

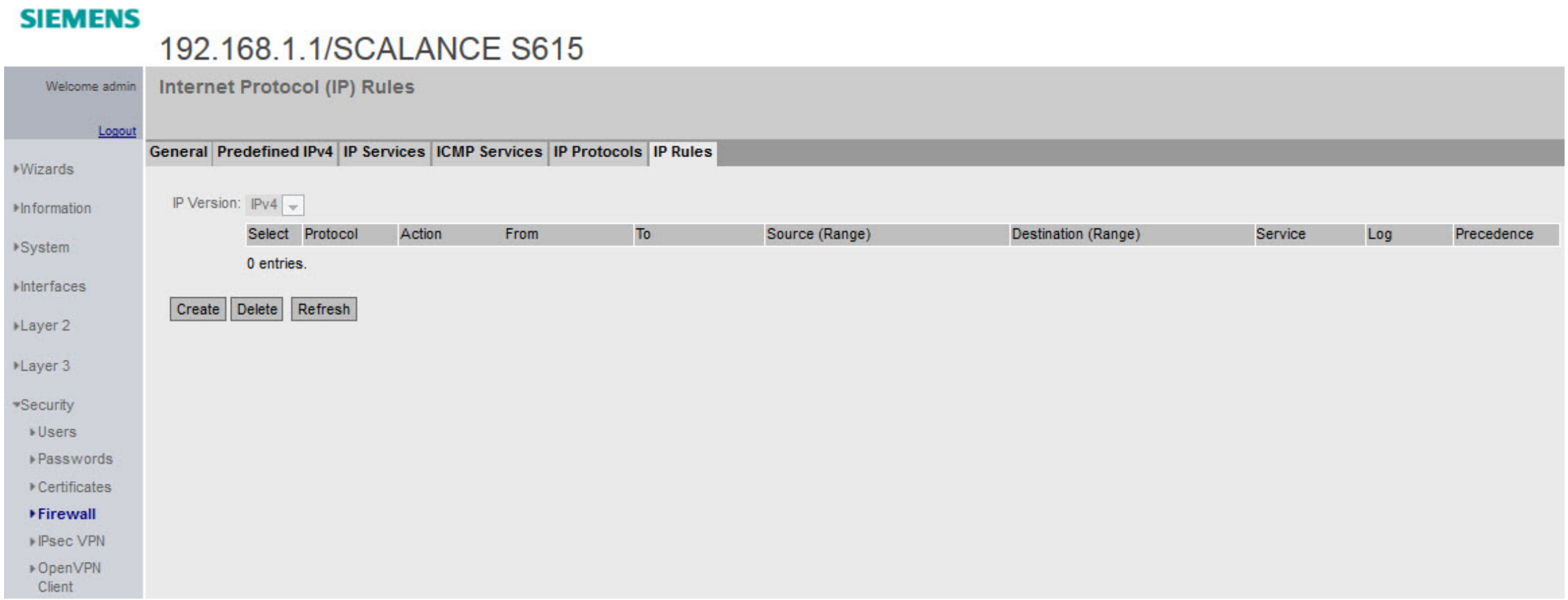
3) In the box under Destination Port (Range) enter the value 443

4) Click Set Values



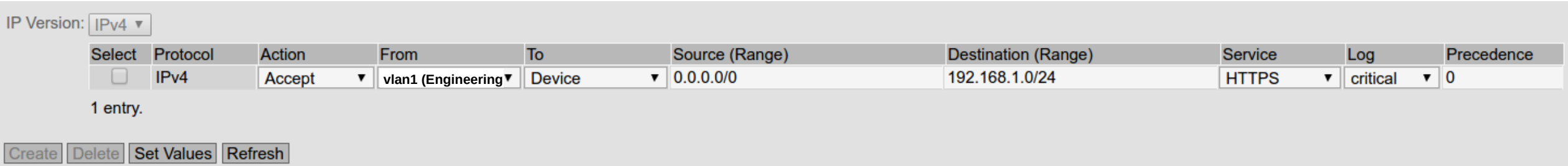
Firewall – IP Rules
Lab

1) Click on the IP Rules Tab



Firewall – IP Rules
Lab

1) Click Create
2) Set Action to Accept
3) Set From to vlan1 (Engineering)
4) Set To as Device
5) Enter Source (Range) as 0.0.0.0/0
6) Enter Destination (Range) as 192.168.1.0/24
7) Set Service as HTTPS
8) Set Log as critical
9) Click Set Values

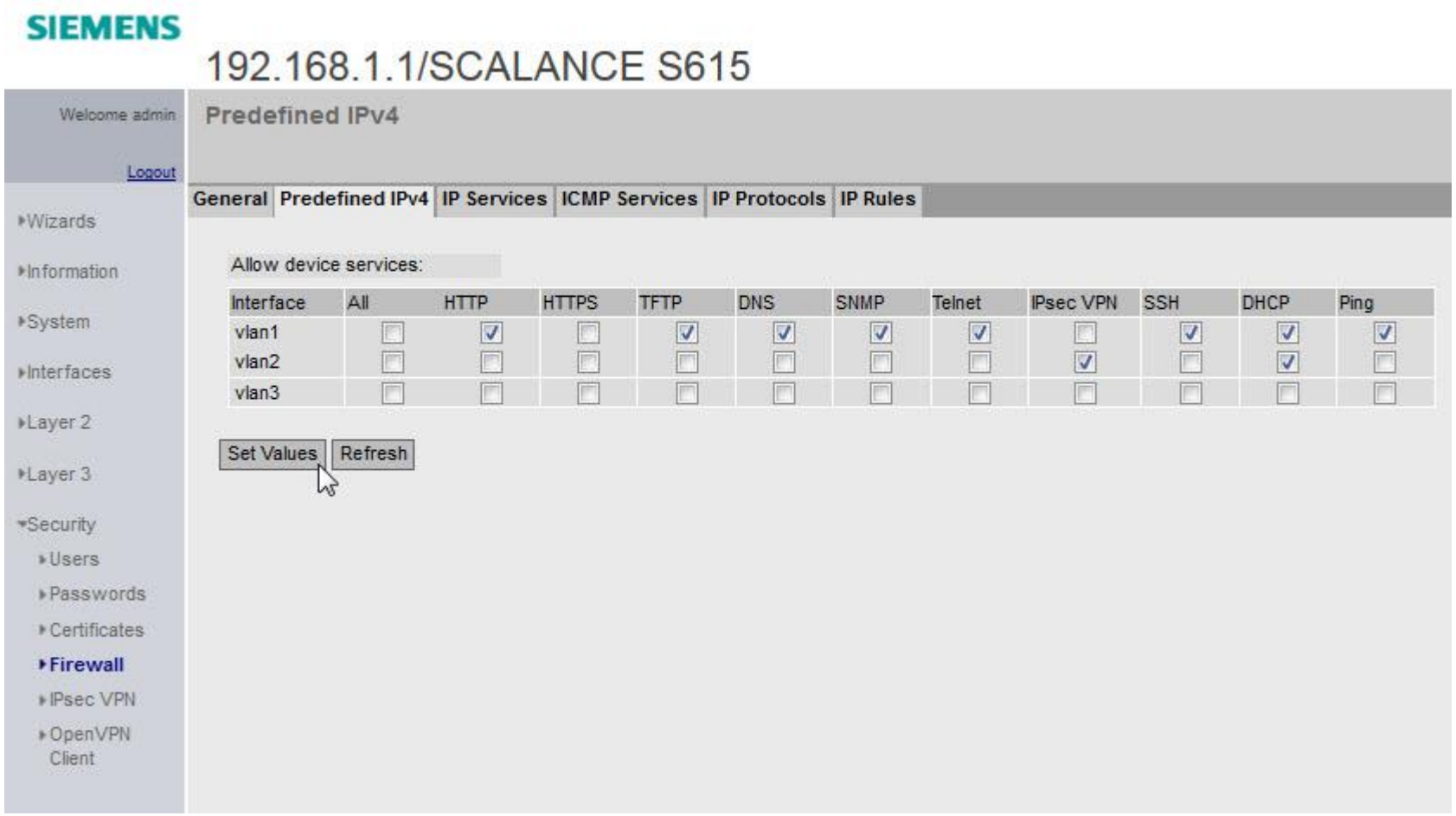


Firewall – Disable Predefined IPv4 HTTPS
Lab

1) Click on the Predefined IPv4 tab

2) Under the HTTPS column in the vlan1 row **uncheck** the box

3) Click Set Values

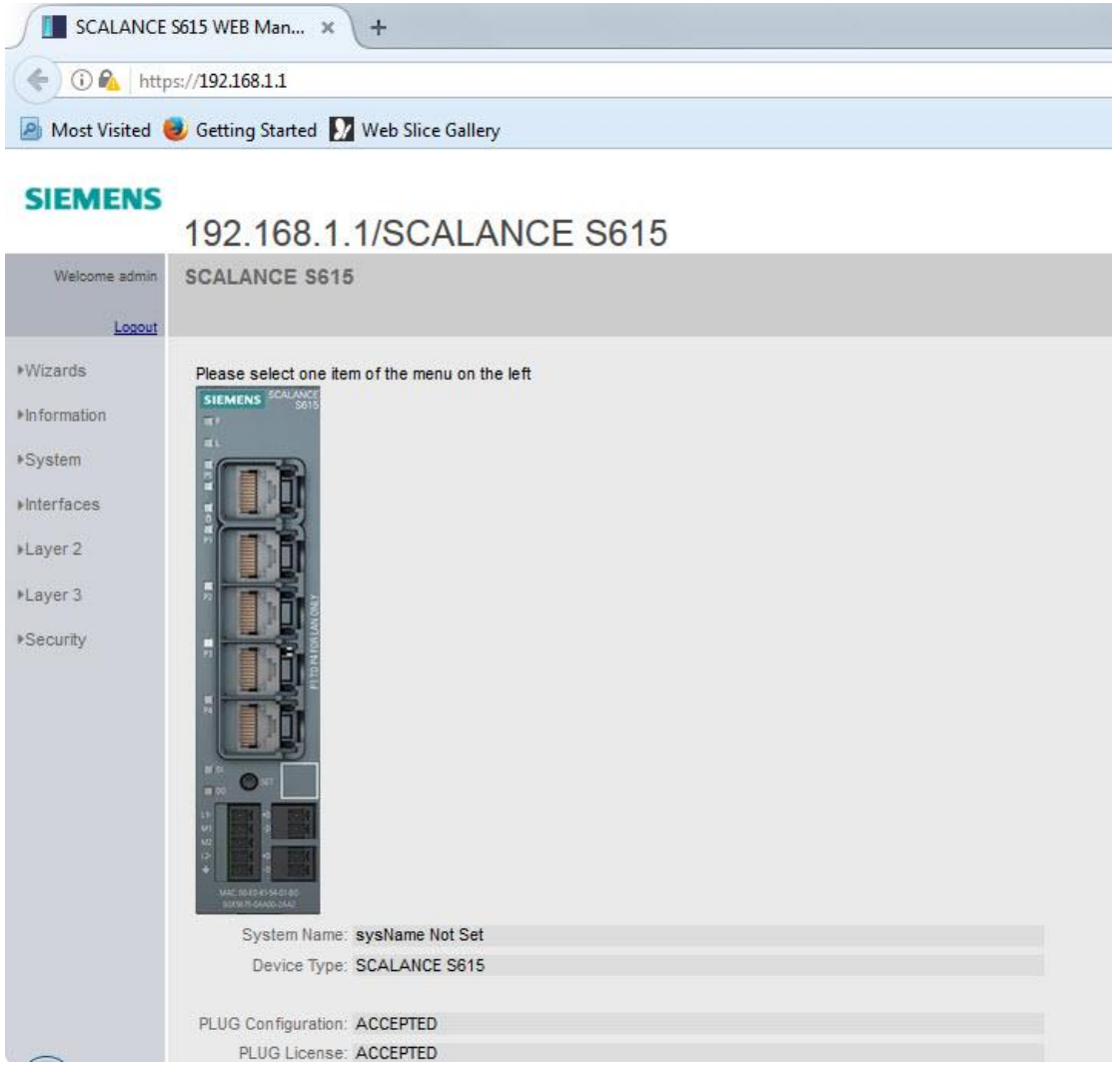


Firewall – Test HTTPS
Lab

1) Navigate to **https**://192.168.1.1

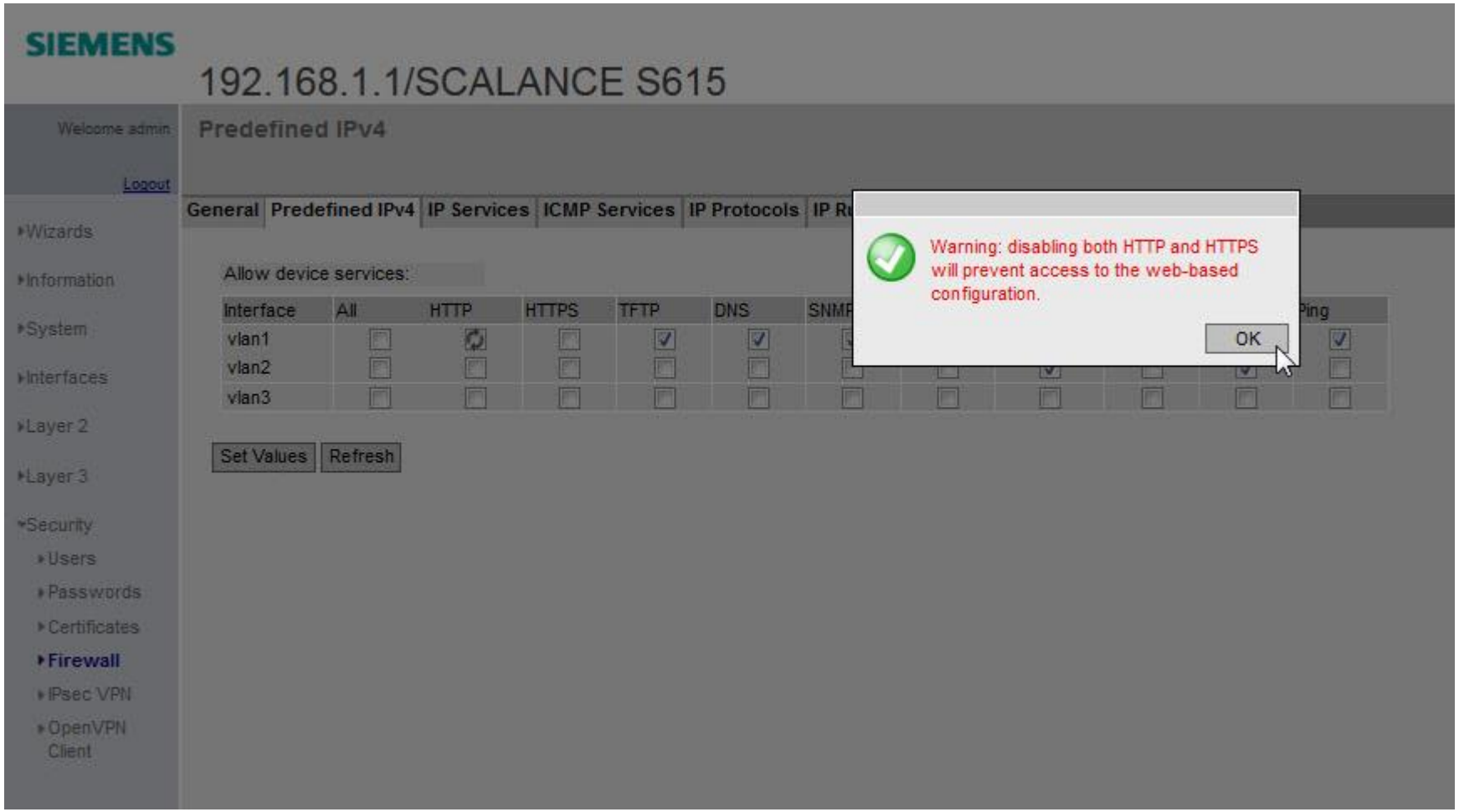
2) There will be a security exception that will need to be confirmed

3) You should be taken to the secure web page for the S615



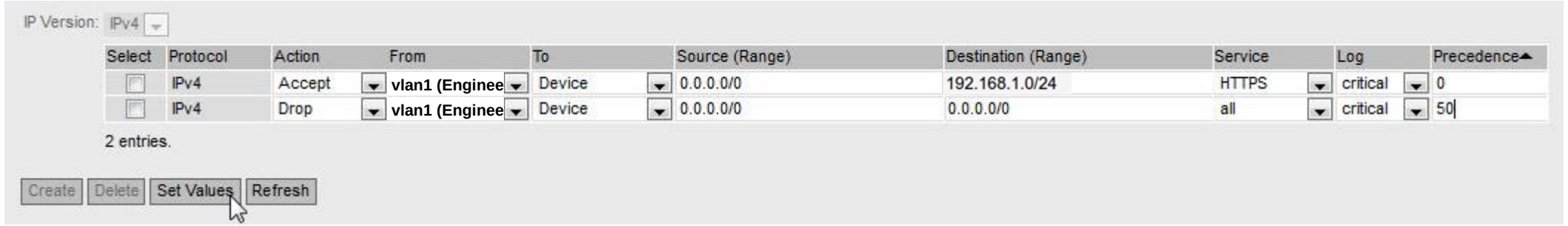
Firewall – Disable Predefined IPv4 Rules
Lab

1) **If HTTPS succeeded, navigate back to the Predefined IPv4 tab**
2) Under the HTTP column in the vlan1 row uncheck the box
3) Acknowledge the Warning
4) Uncheck all of the other boxes for vlan1
5) Click Set Values



Firewall – Create Drop Rule
Lab

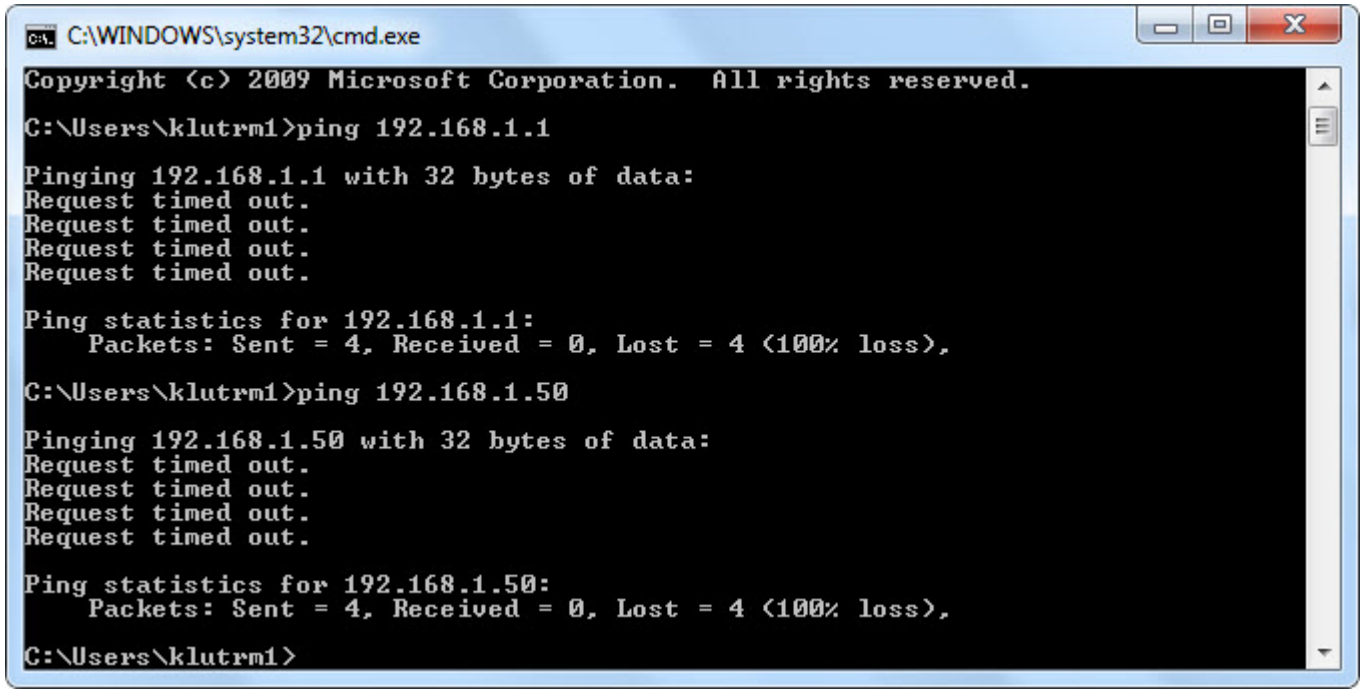
1) Click on the IP Rules tab
2) Click Create
3) Set Action to Drop
4) Set From to vlan1 (Engineering)
5) Set To as Device
6) Set Source (Range) as 0.0.0.0/0
7) Set Destination (Range) as 0.0.0.0/0
8) Set Service to all
9) Set Log to critical
10) Set Precedence to 50
11) Click Set Values



Firewall – Ping Test
Lab

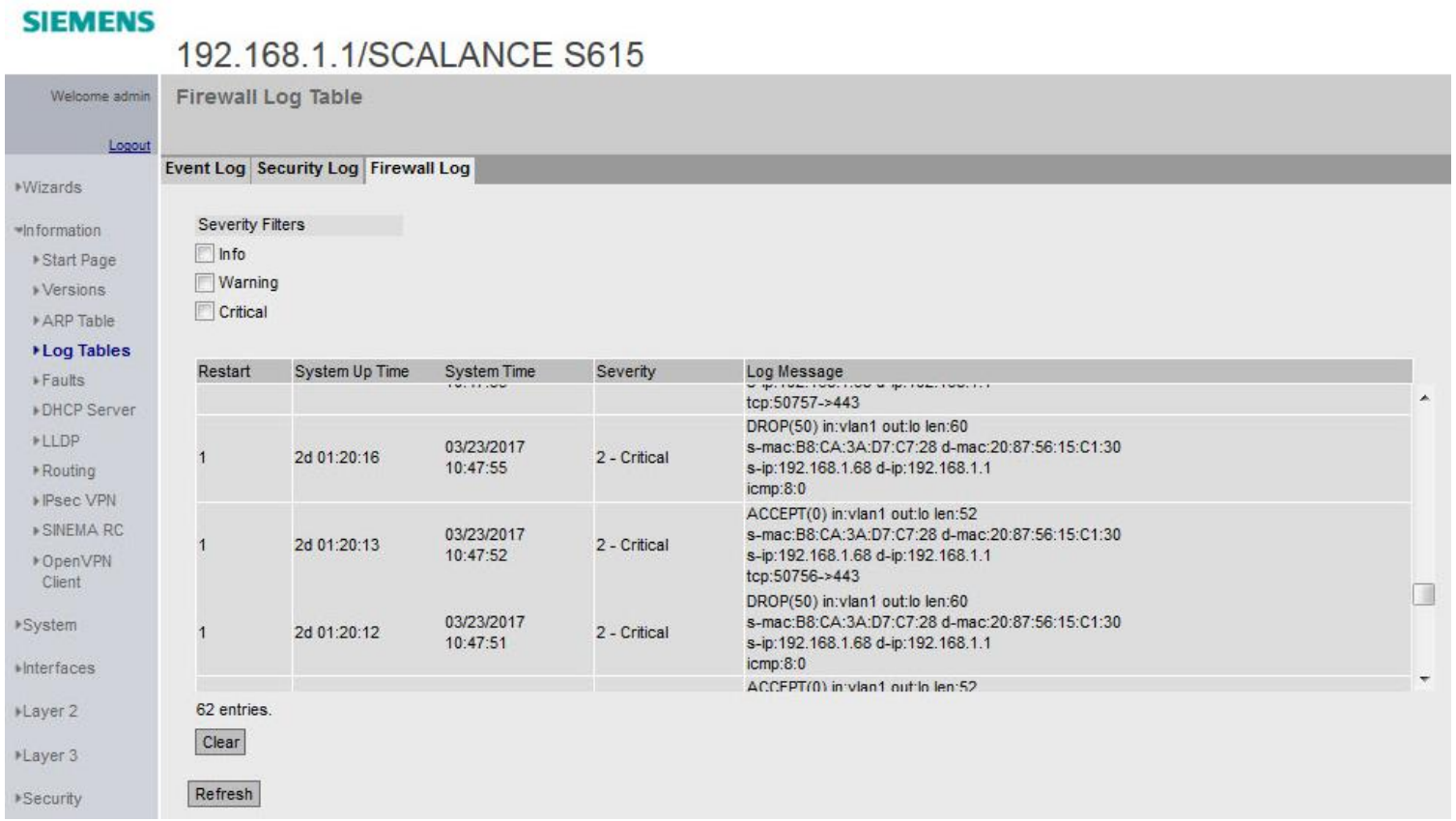
1) Ping 192.168.1.1

2) Ping 192.168.1.50



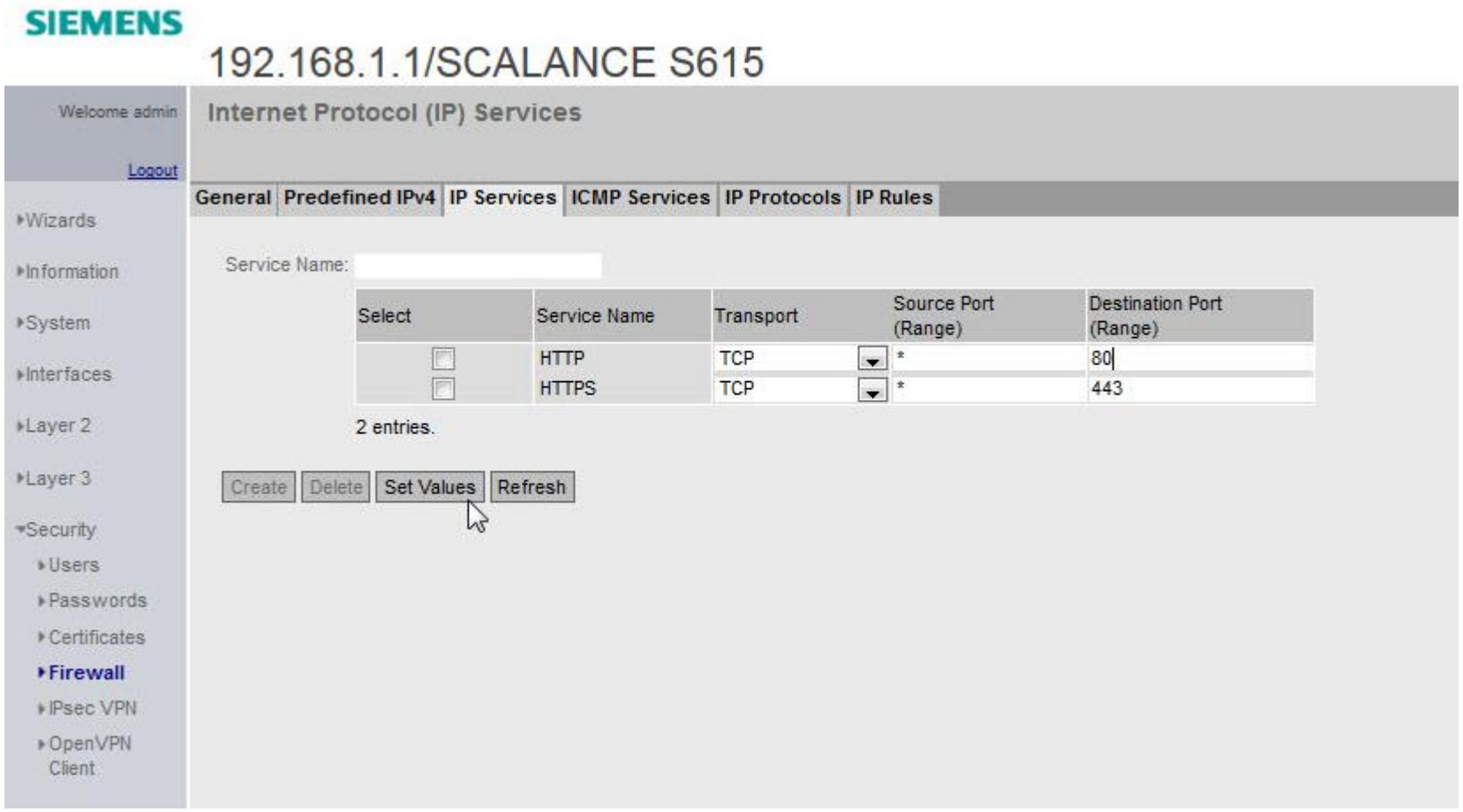
Firewall – Analyze Firewall Log
Lab

1) Navigate to and click on Information
2) Navigate to and click on Log Tables
3) Click on the Firewall Log tab
4) Identify the ACCEPT and DROP messages



Firewall – Create HTTP Service
Lab

1) Navigate to and click on Security
2) Navigate to and click on Firewall
3) Click on the IP Services tab
4) Enter HTTP in the box next to Service Name:
5) Click Create
6) Ensure Transport is TCP
7) Ensure Source Port (Range) is *
8) Enter the value 80 in the box under Destination port on the HTTP row

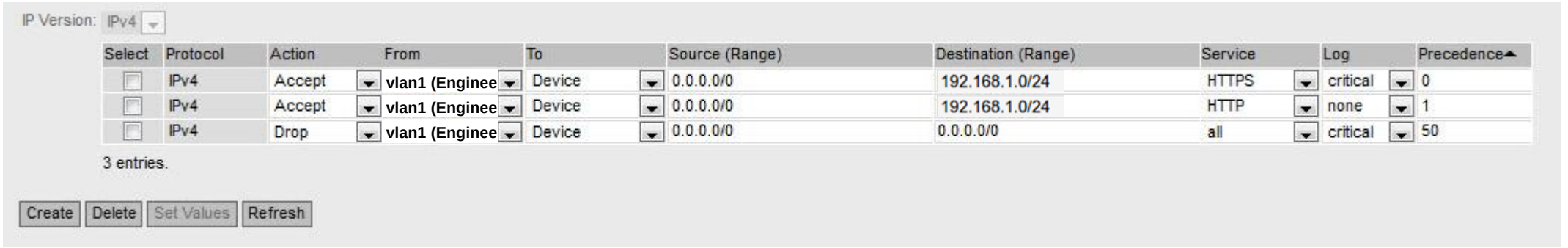


Firewall – Create HTTP Rule
Lab

1) Click on the IP Rules tab

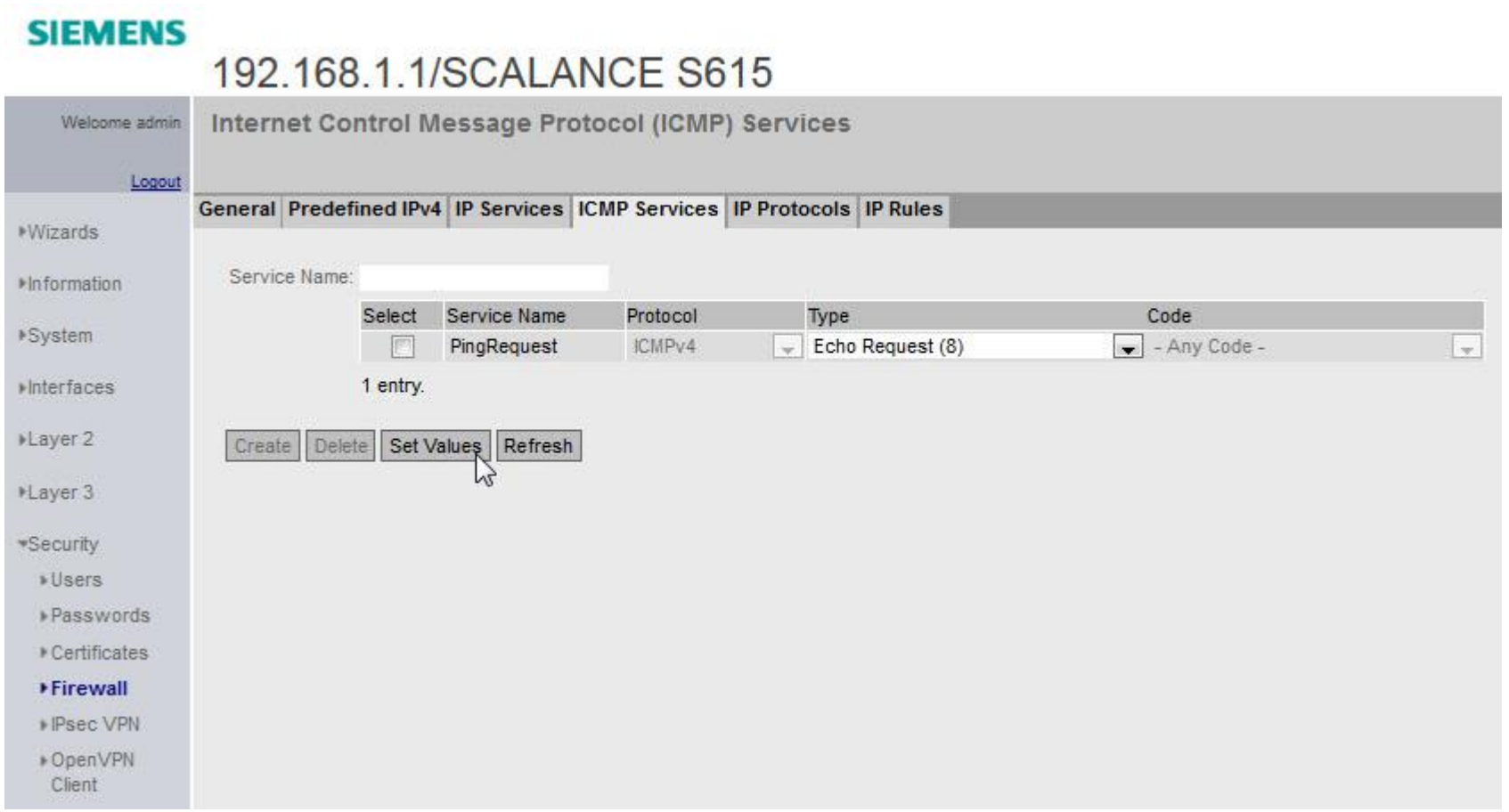
2) Click on Create to create a new rule

3) Enter the parameters below for an HTTP rule (shown on the second line)



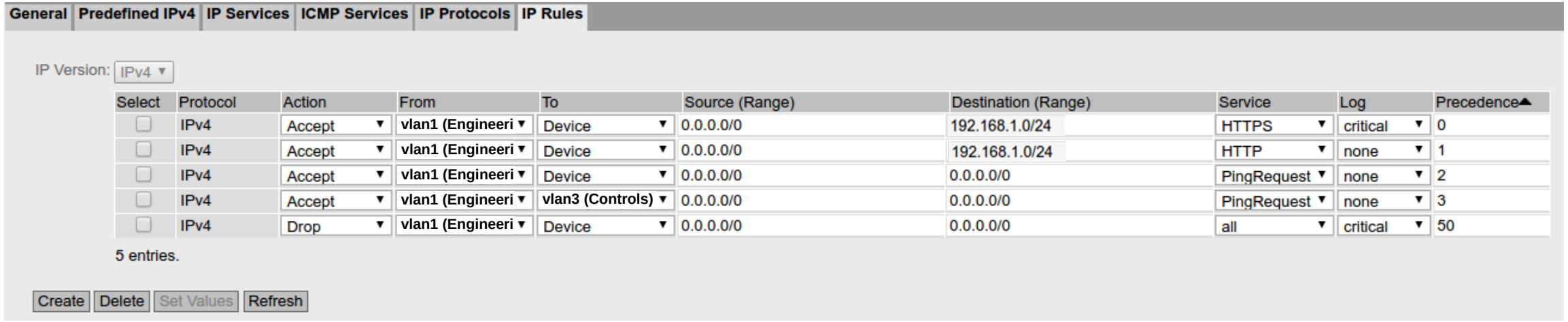
Firewall – Create ICMP Service
Lab

1) Click on the ICMP Services tab
2) Enter PingRequest in the box next to Service Name:
3) Click Create
4) Select Echo Request (8) from the dropdown under Type
5) Click Set Values



Firewall – Create Ping Rule
Lab

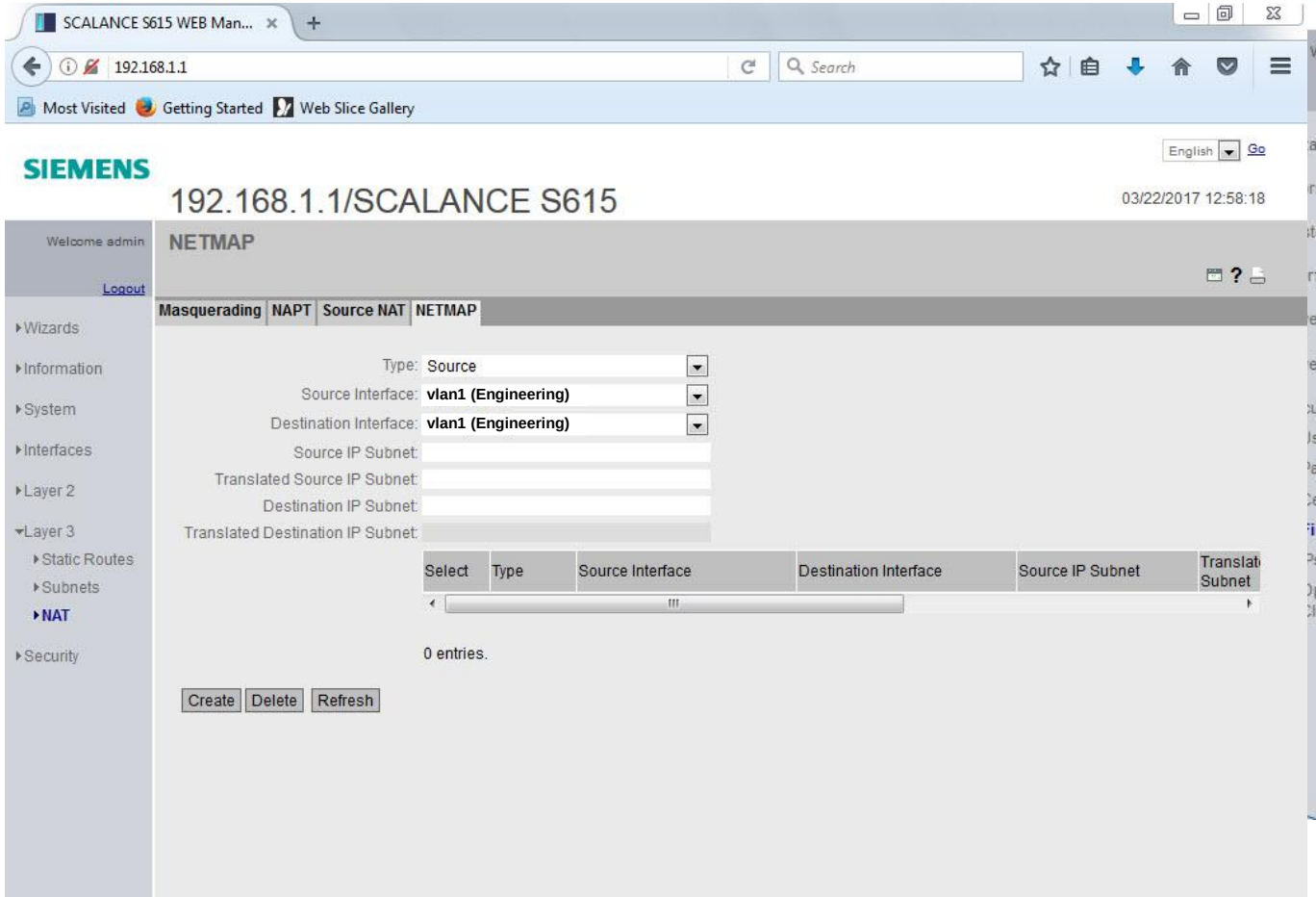
1) Click on the IP Rules tab
2) Click on Create to create a new rule
3) Enter the parameters below for a PingRequest rule for vlan1 to Device and vlan1 to vlan3
4) Click Set Values
5) Test both HTTP and Ping

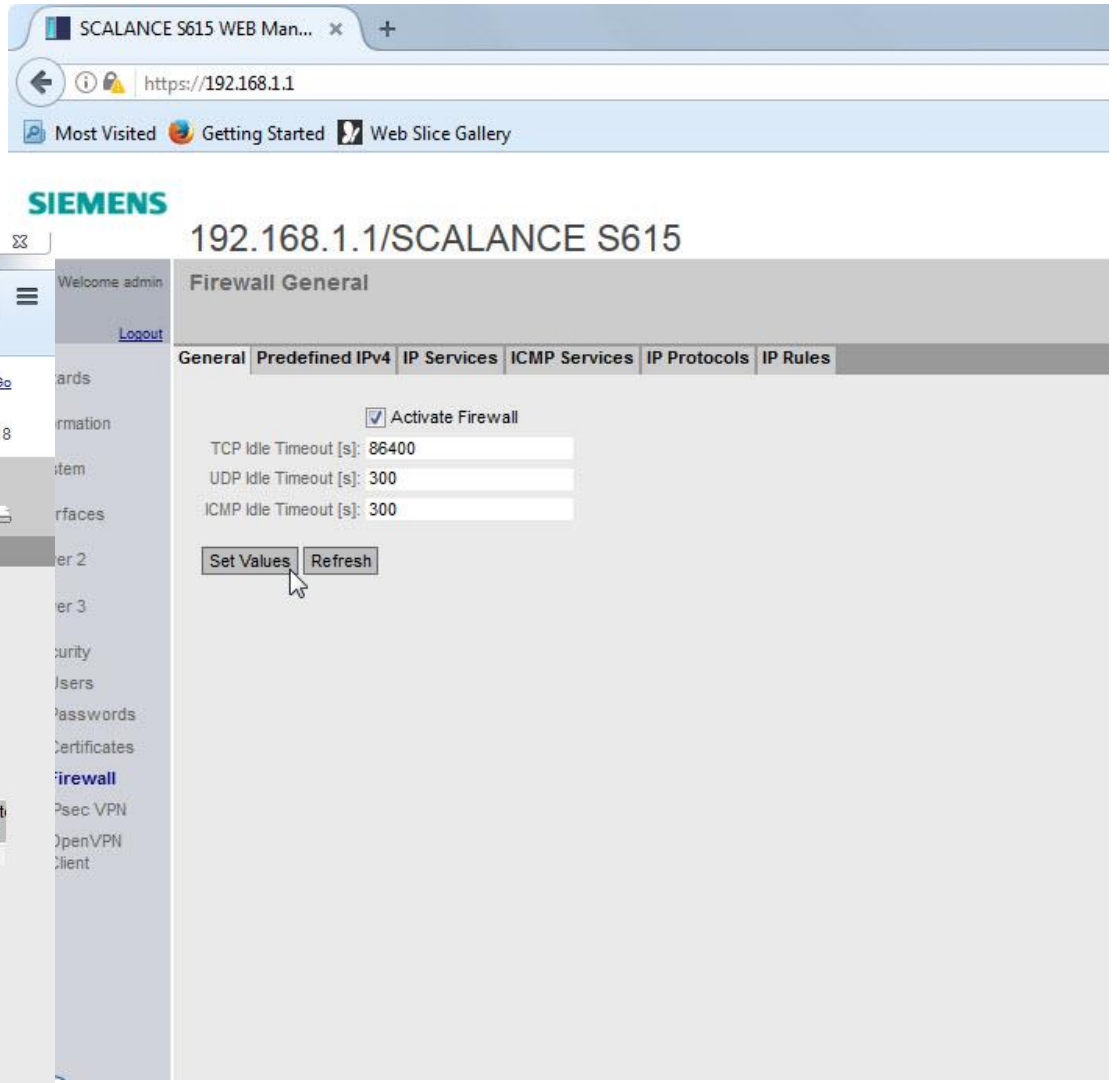


Firewall – Reset
Lab

1) Delete all NETMAP Entries

2) Disable Firewall





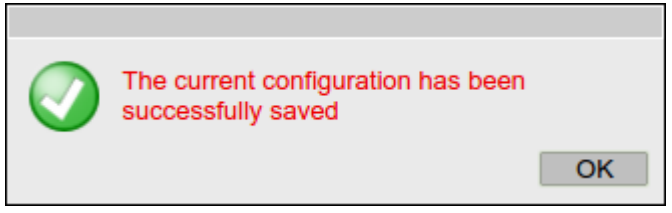
Firewall – Write Startup Config
Lab

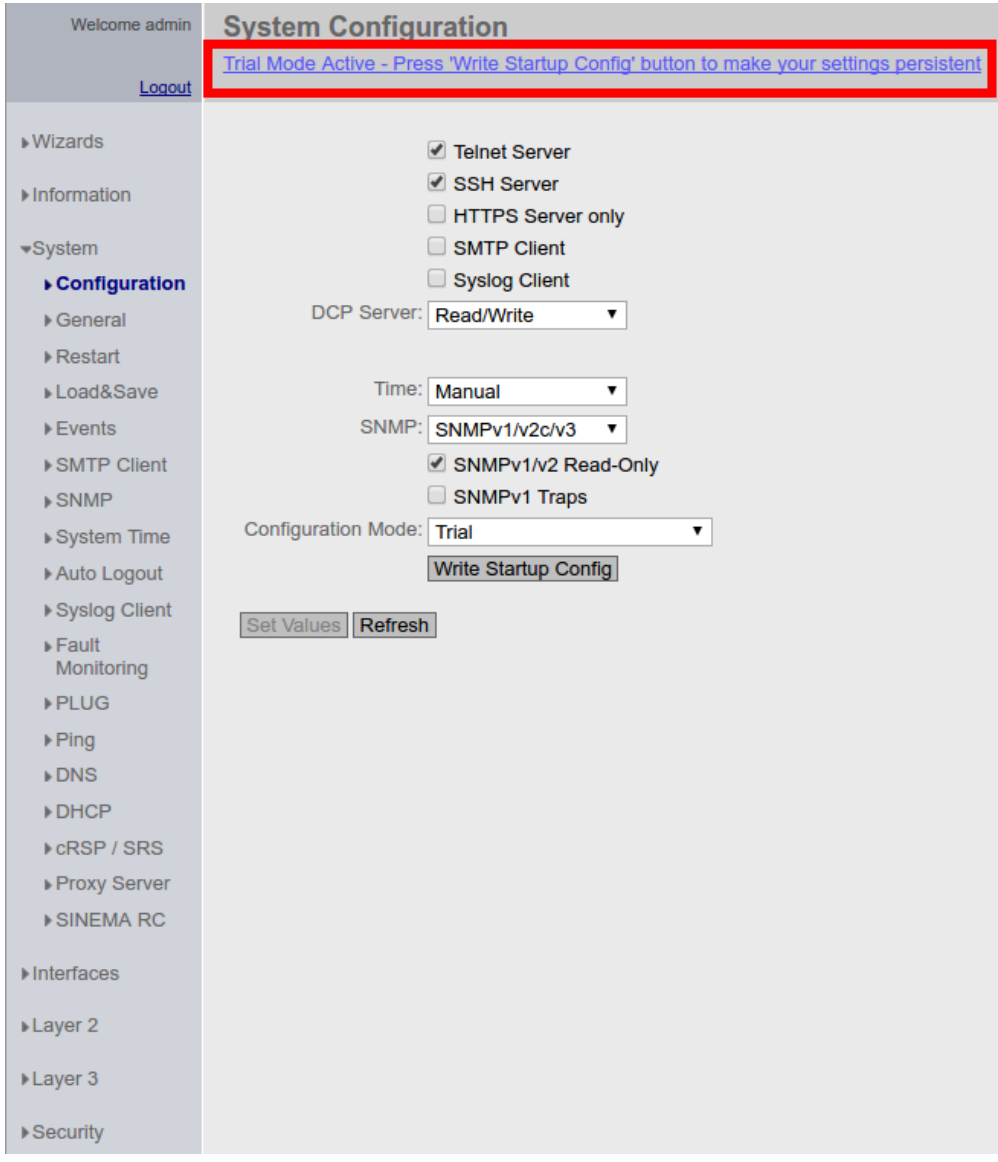
1) Navigate to and click on System

2) Navigate to and click on Configuration
   A. Alternatively, note the hot link at the top of the screen will go to the correct screen

3) Click Write Startup Config button

4) Acknowledge the Success Popup



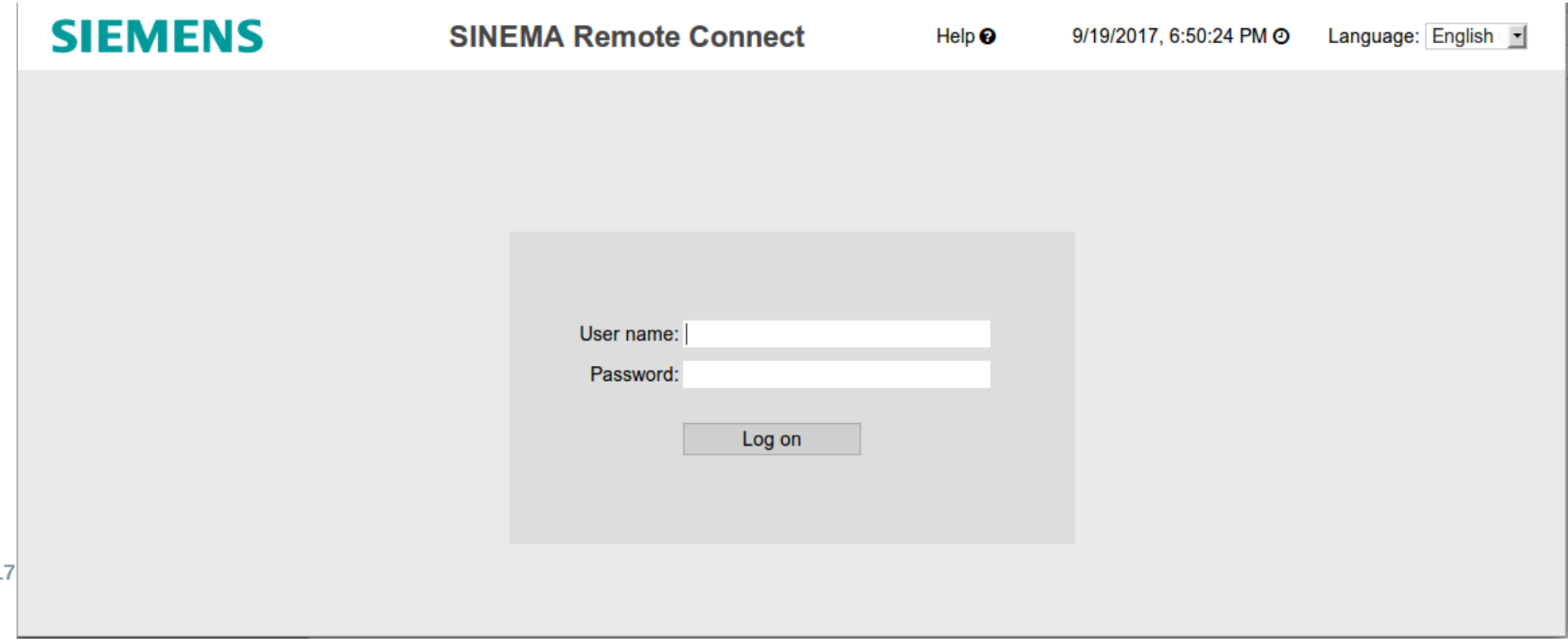


Labs

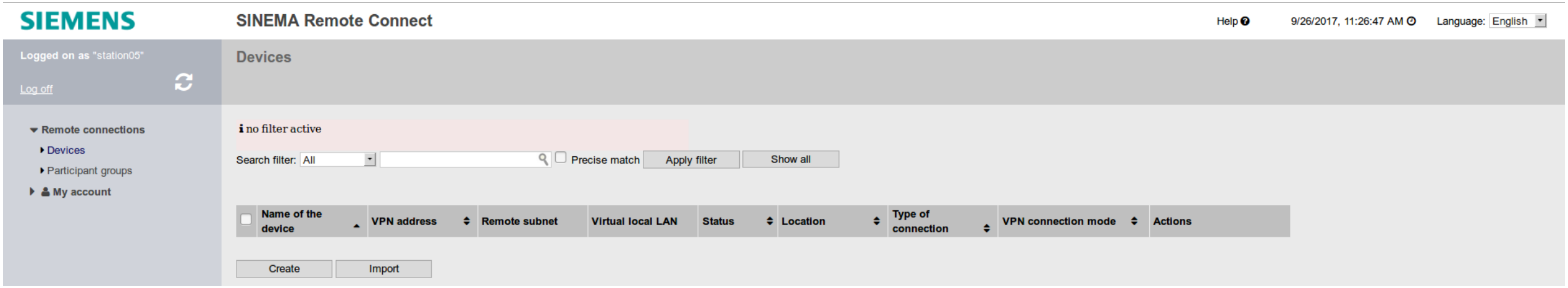
SINEMA Remote Connect Lab

1) Browse to https://172.16.10.250

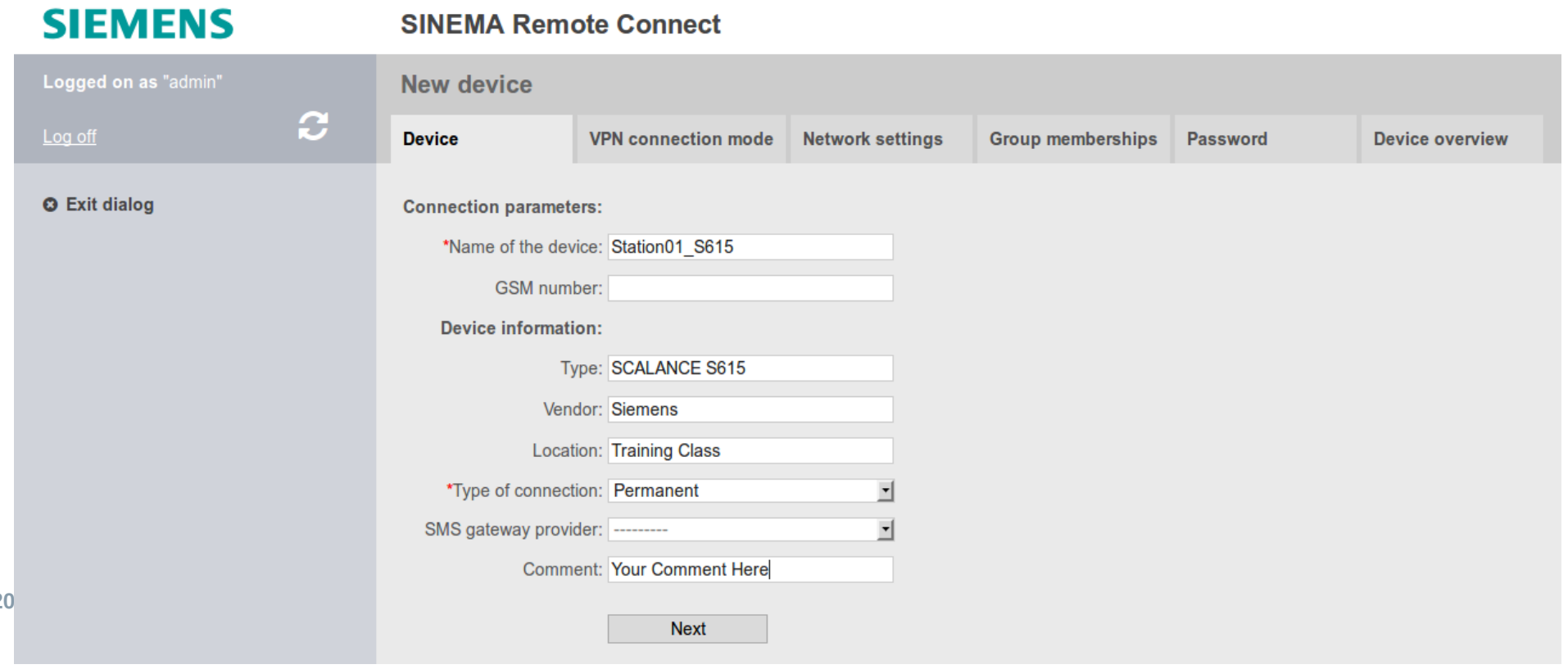
2) Login using the appropriate credentials
   A. username: station0X (where X is the station number)
   B. password: Admin!123



1) Click on Create

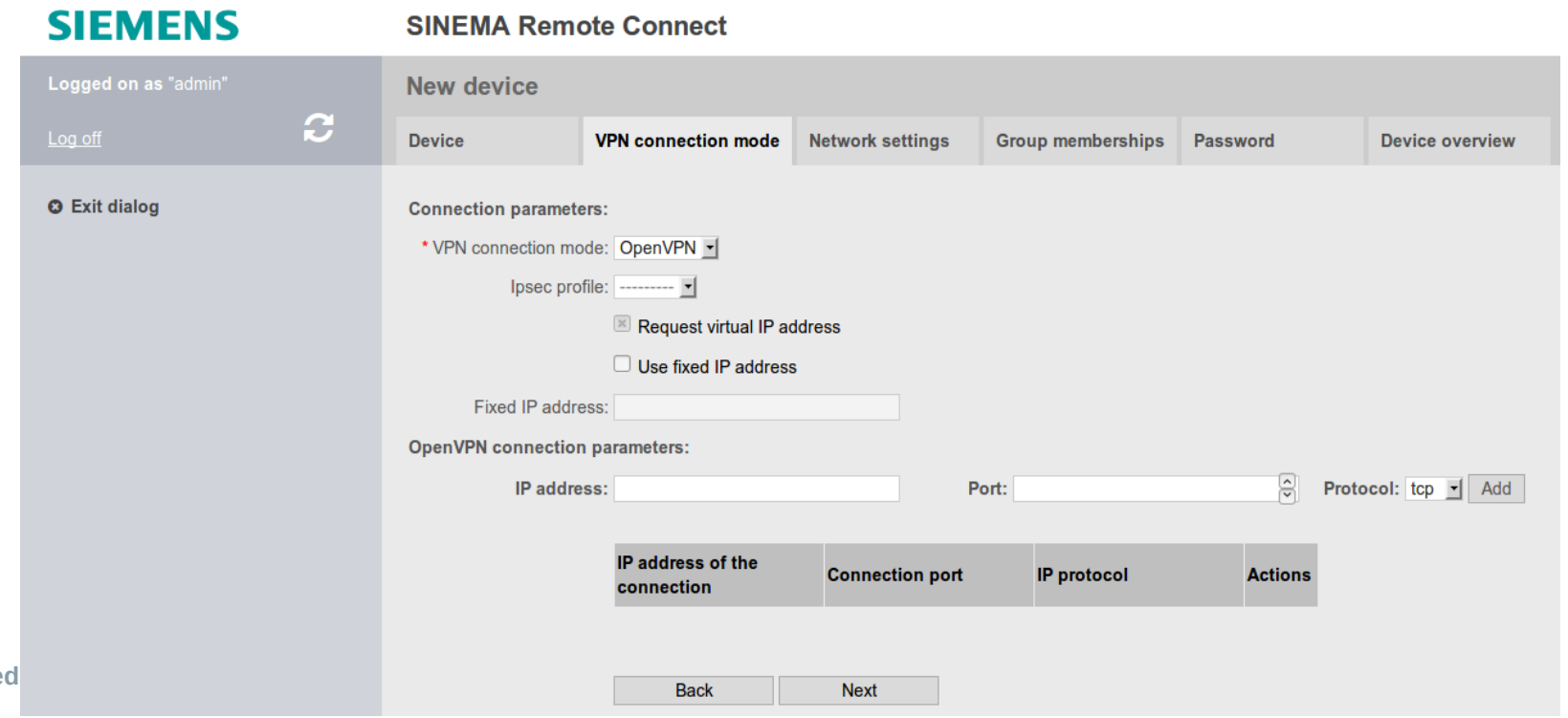


1) Enter a Station0X_S615 (where X is the station number)
2) Enter additional (optional) information
3) Select the Type of connection as Permanent
4) Click Next



1) Leave the default settings

2) Click Next



SINEMA Remote Connect

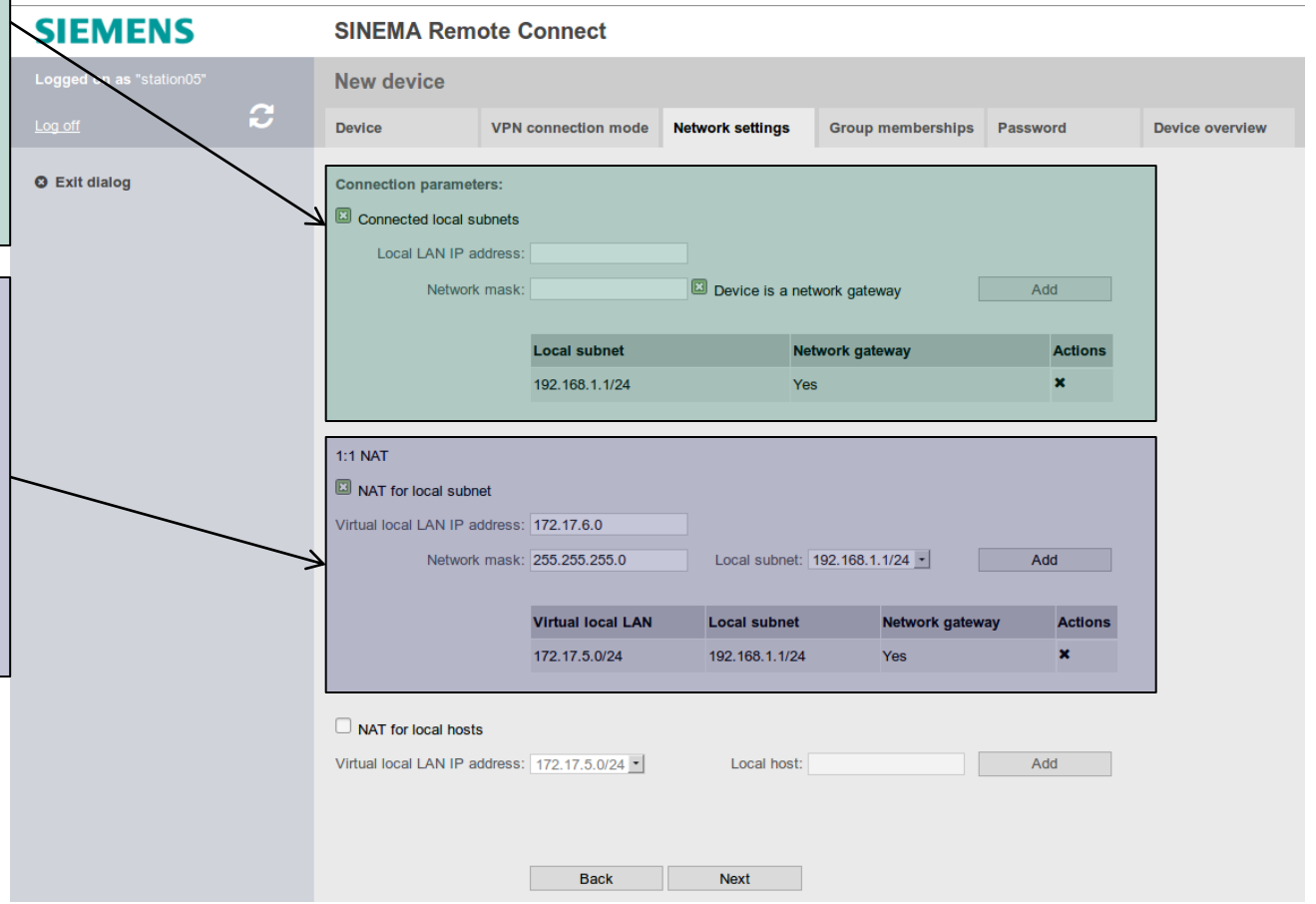
Lab – Device Creation

1) Check box next to Connected local subnets
   A. Local LAN IP address
      I. 192.168.1.1
   B. Network mask
      I. 255.255.255.0
   C. Check next to Device is a network gateway.

2) Click Add

3) Check box next to NAT for local subnet
   A. Virtual local LAN IP address
      I. 172.17.X.1(where X is the station number)
   B. Network mask
      I. 255.255.255.0

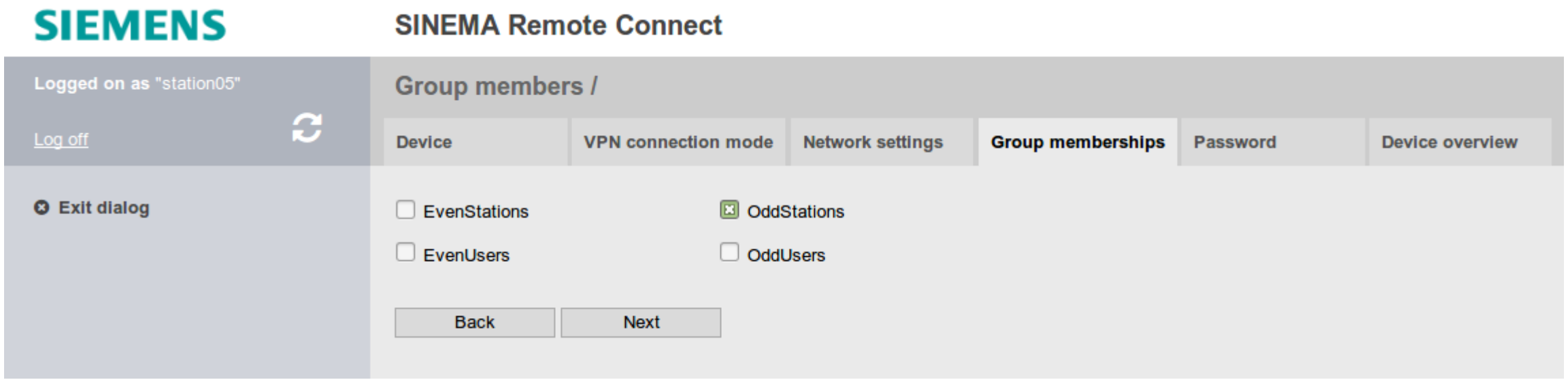
4) Click Next



1) Check the appropriate Group membership based on station number (EvenStations or OddStations)

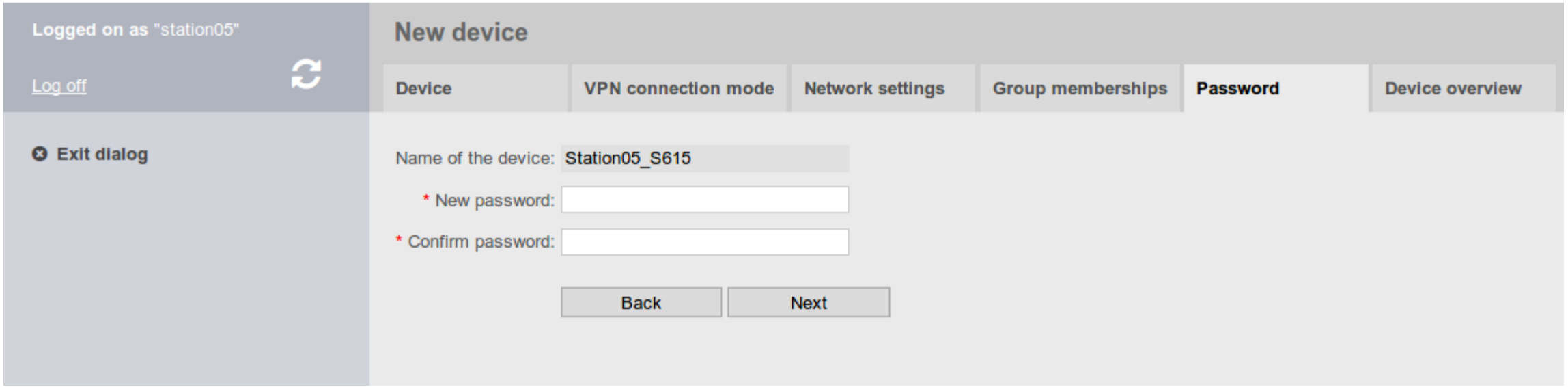
   - Do not click on the EvenUsers or OddUsers

2) Click Next



1) Enter and confirm password
   A. Admin!123

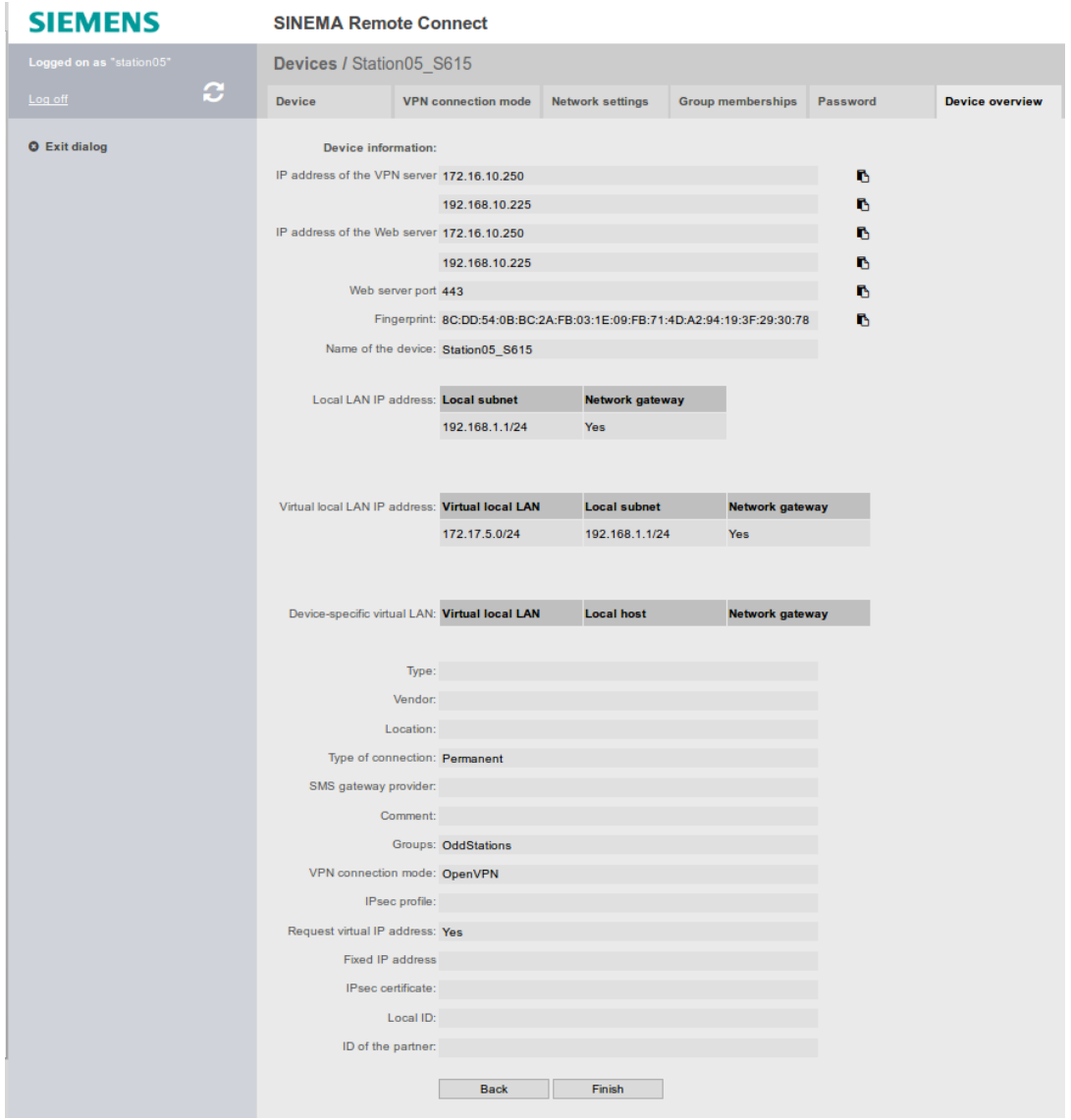
2) Click Next



SINEMA Remote Connect
Lab – Device Creation

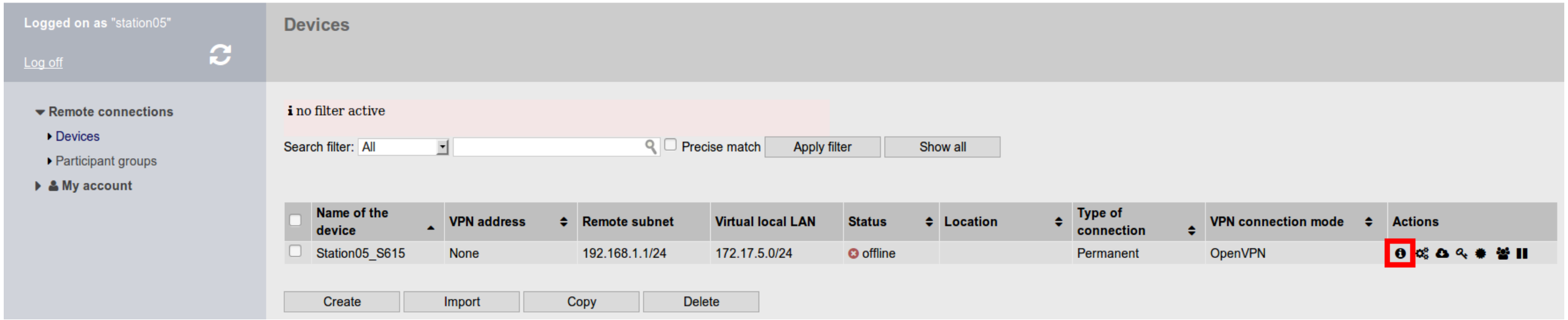
1) Confirm settings are correct

2) Click Finish



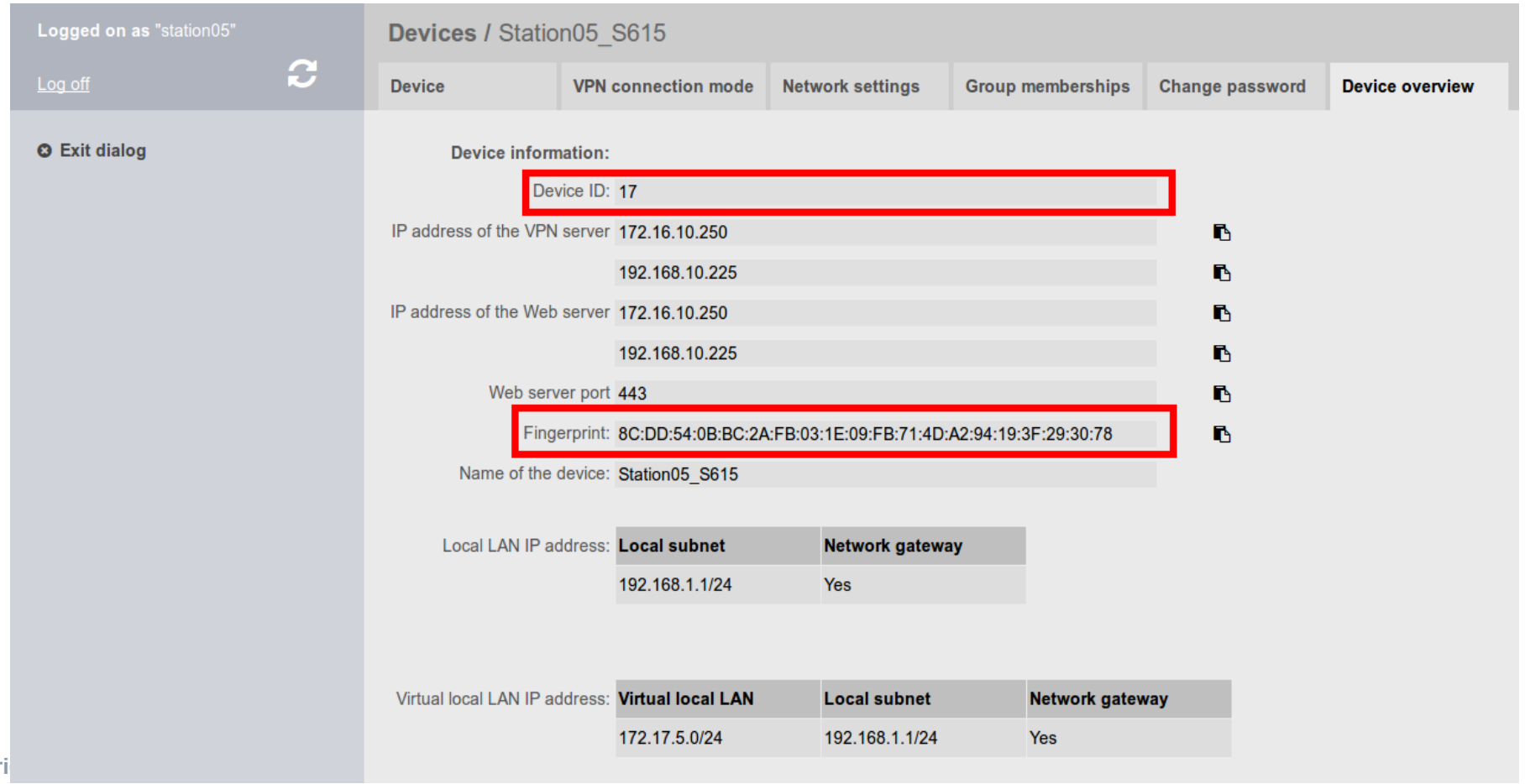
SIEMENS

1) Click on the information button

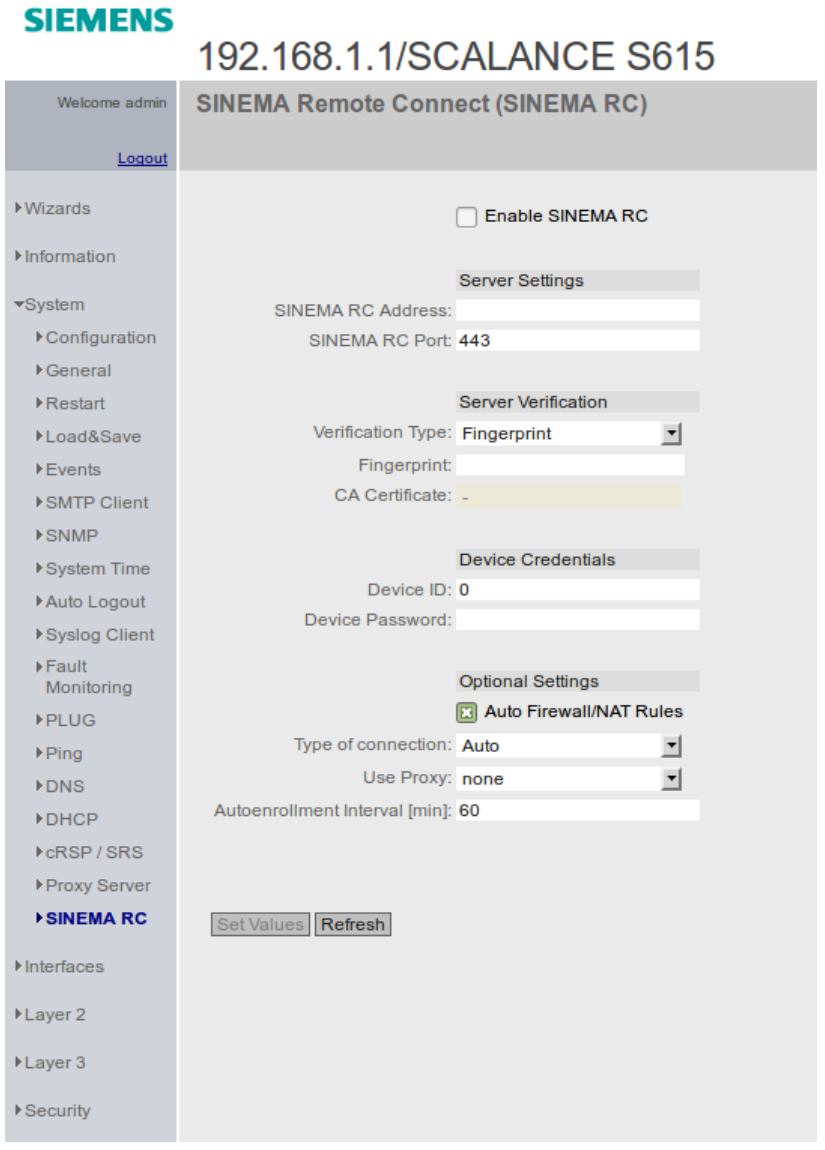


SIEMENS

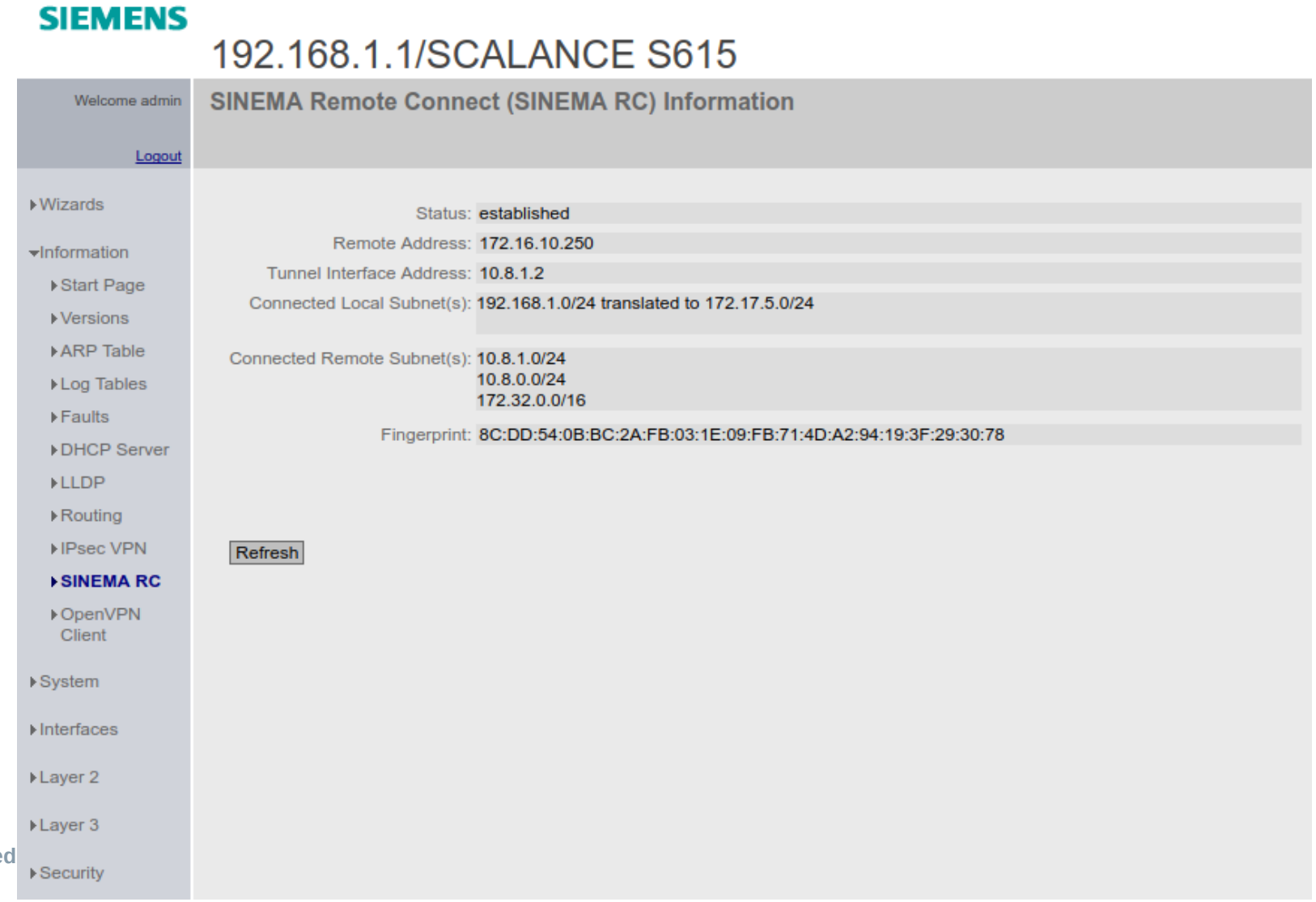
1) Note the Device ID and Fingerprint
   A. These are needed to set up the S615



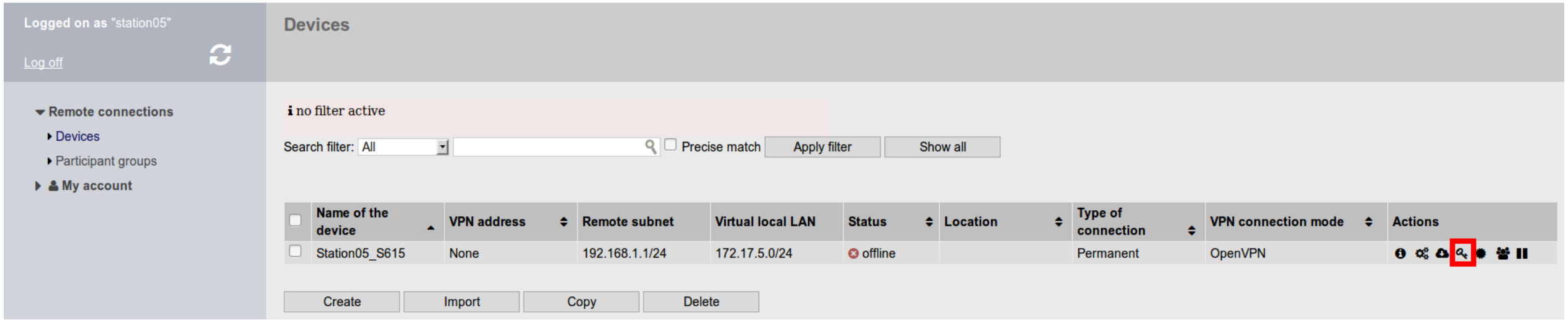
1) SINEMA RC Address
   A. 172.16.10.250
2) SINEMA RC Port
   A. 443
3) Verification Type
   A. Fingerprint
4) Fingerprint
   A. Enter noted fingerprint from SRC information page (recommend to copy and paste)
5) Device ID
   A. Enter noted Device ID from SRC information page
6) Device Password
   A. Password entered when configuring device in SRC
7) Leave Optional Settings as default
8) Click Set Values
9) Click Check Box to Enable SINEMA RC
10) Click Set Values



1) Browse to Information > SINEMA RC
2) Verify the Status is established



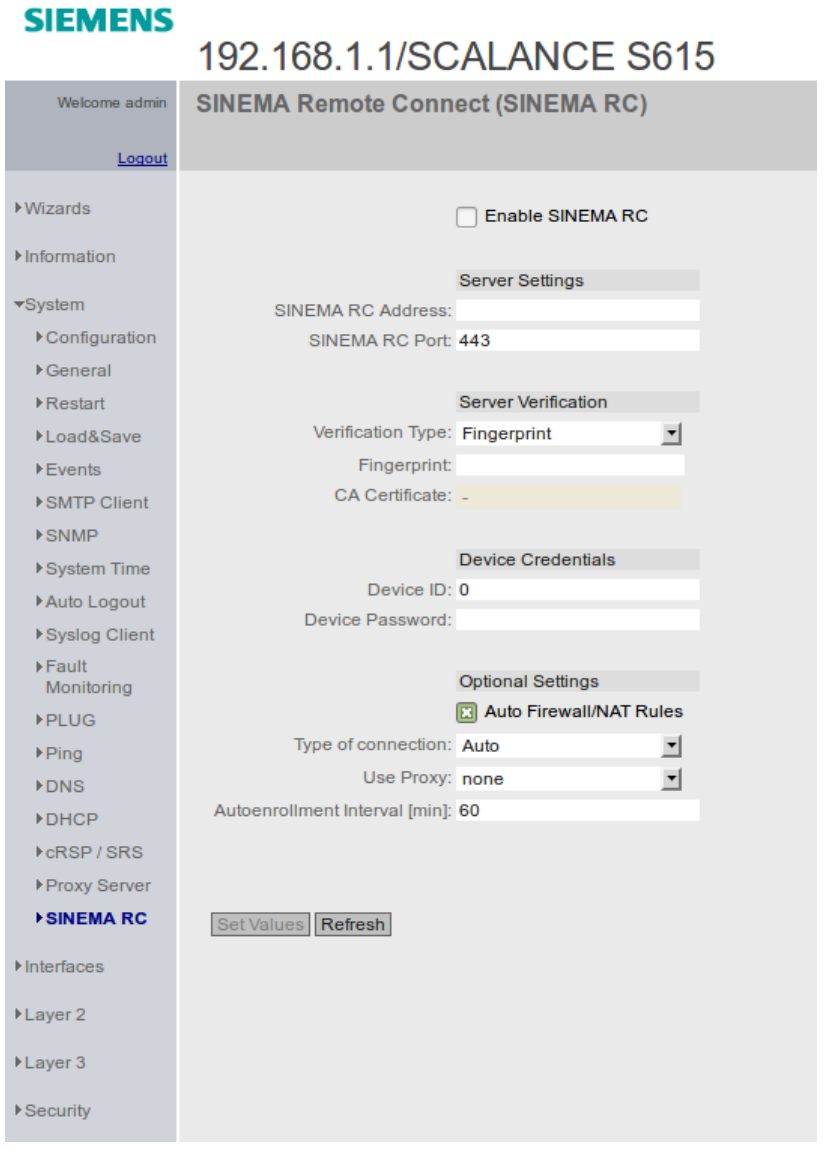
1) Go back to SINEMA Remote Connect (log back in if necessary)
   A. Click the key icon on the line of the device for the correct station.
   B. Save file to Desktop



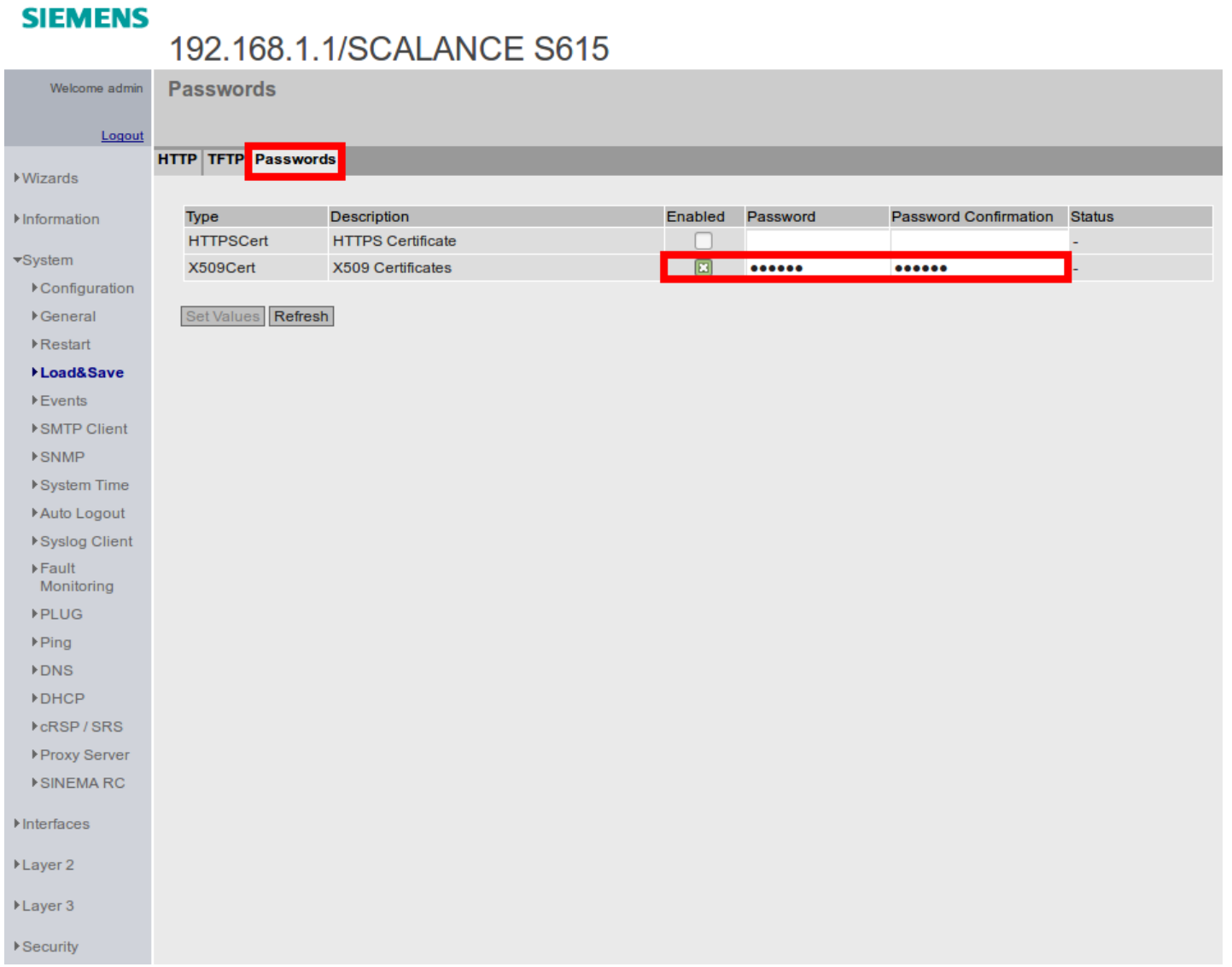
1) Log back in to the S615

2) Uncheck box next to Enable SINEMA RC
   A. SINEMA RC needs to be disabled to make modifications

3) Set Values



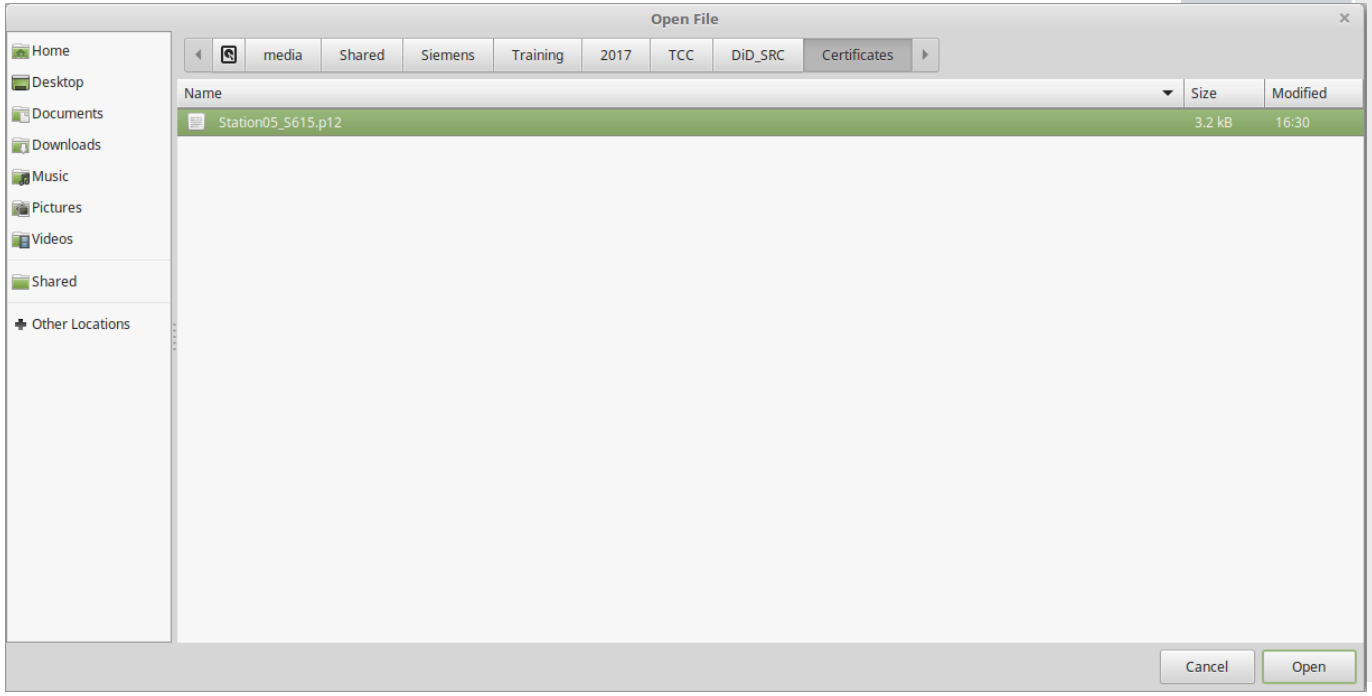
1) Browse to System > Load&Save
2) Click on the Passwords tab
3) X509Cert
   A. Enter the password used for the device and again in the confirmation space
   B. Click the check box under Enabled
4) Click Set Values

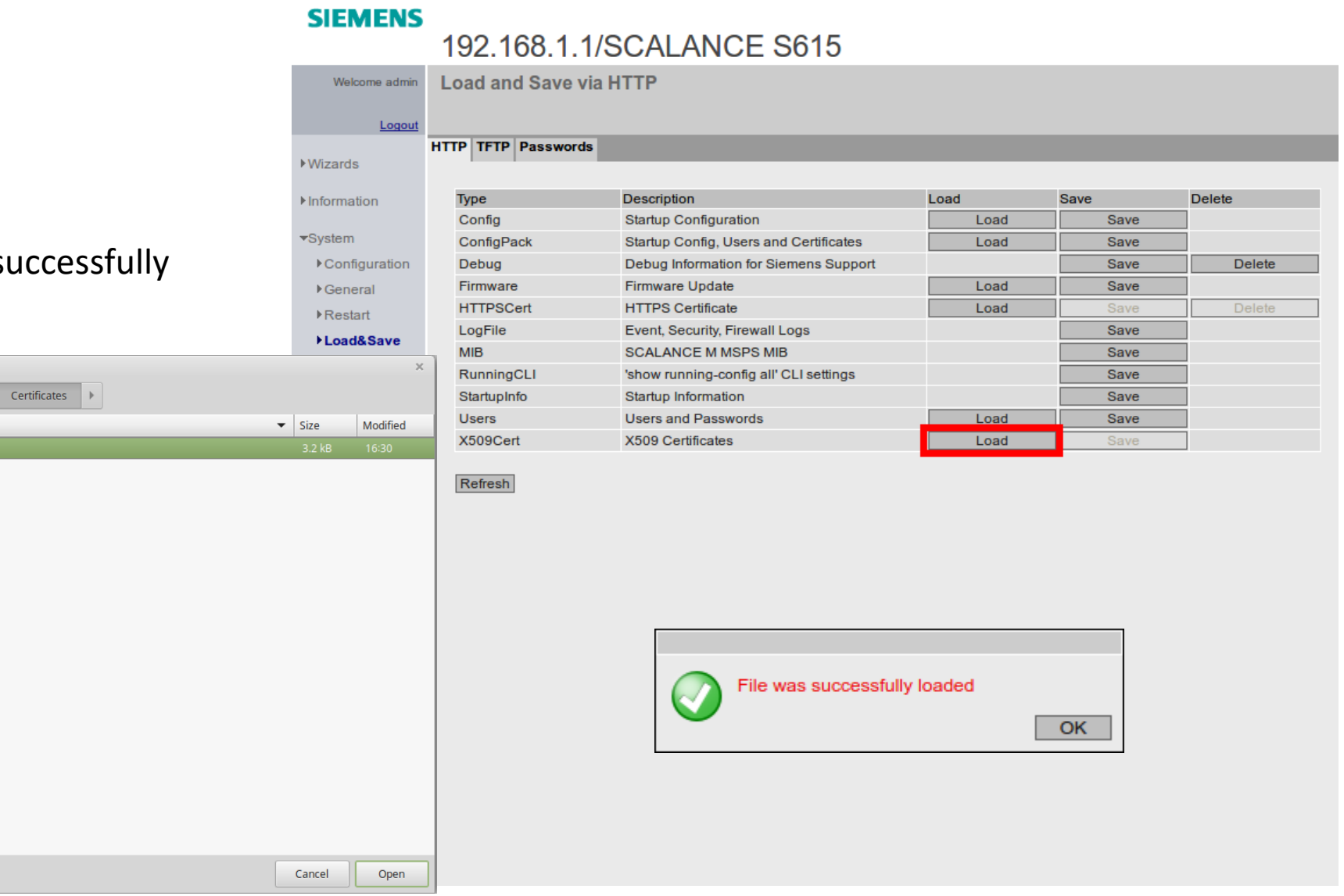


SINEMA Remote Connect

Lab – S615 Configuration - Certificate

1) Browse to System > Load&Save
2) Click on the HTTP tab
3) X509Cert
   A. Click Load
   B. Select the file and click Open
   C. Acknowledge that the File was successfully loaded

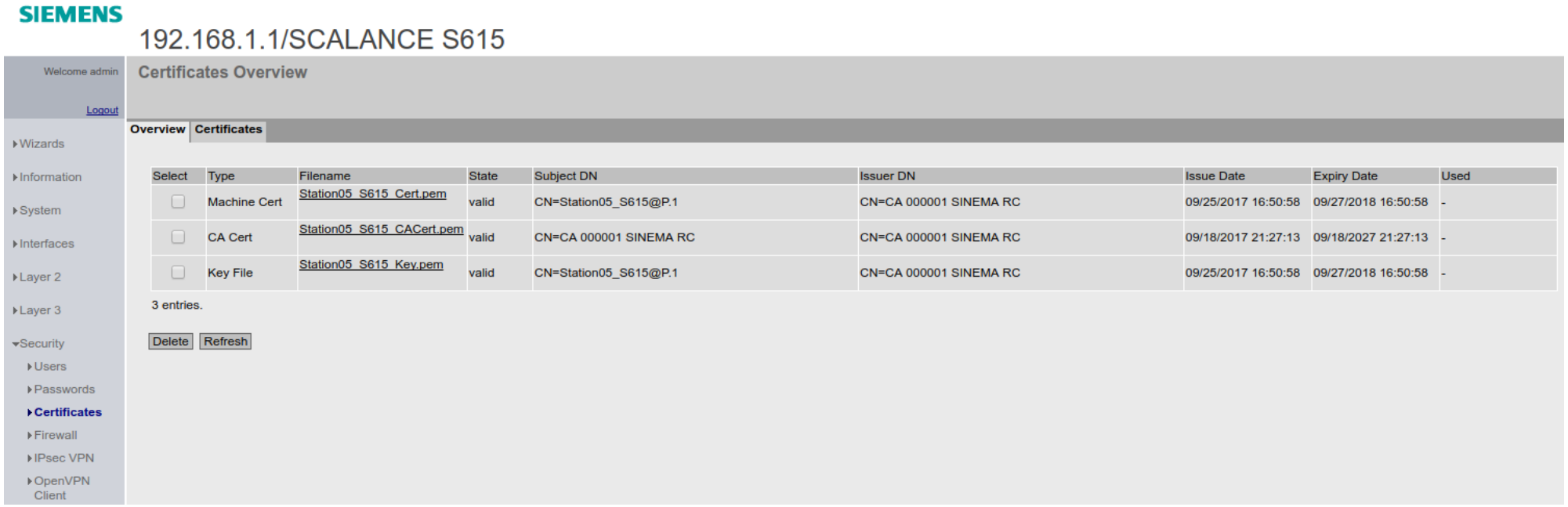




1) Browse to Security > Certificates

2) Verify the Certificates Exist

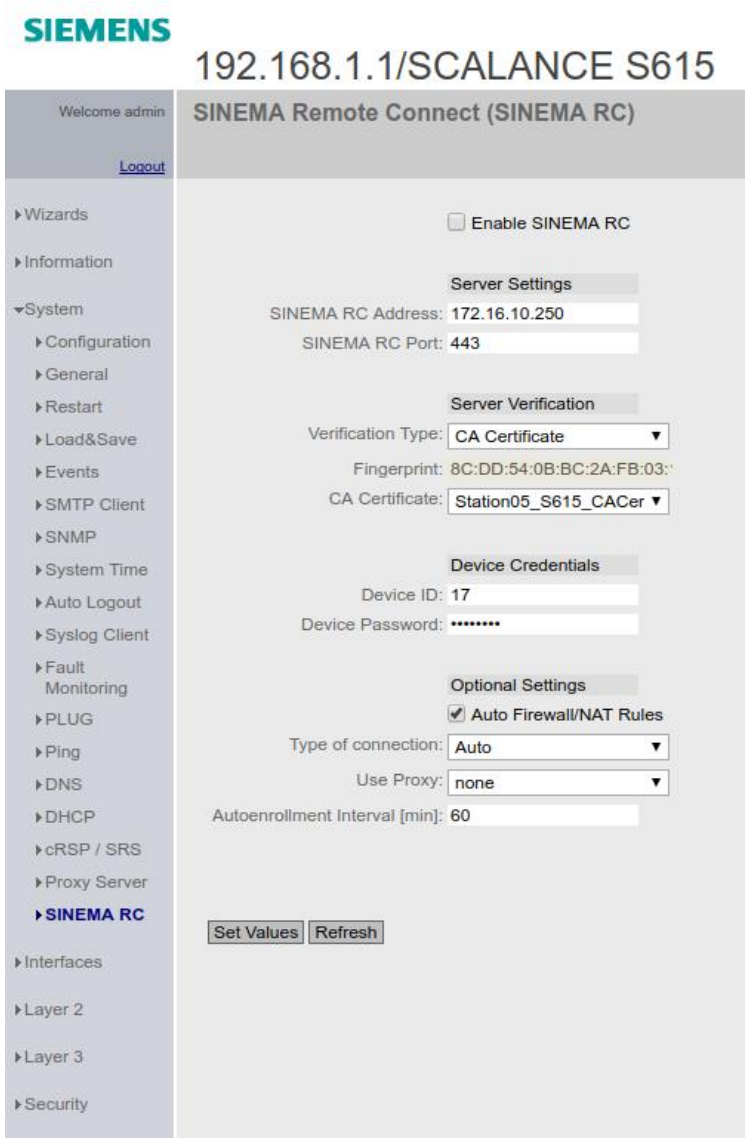
   - Note the certificates all have a .pem extension



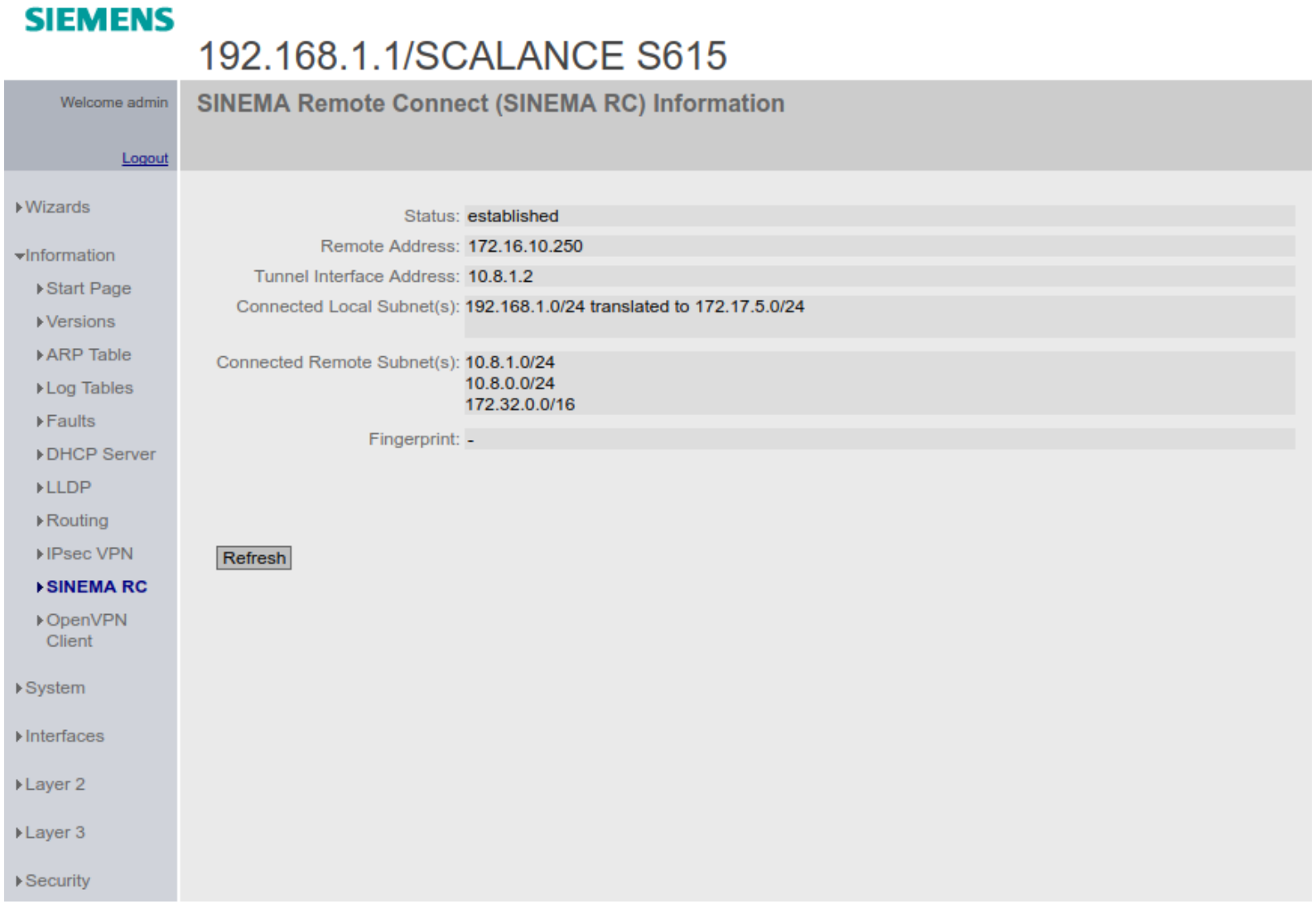
SINEMA Remote Connect

Lab – S615 Configuration - Certificate

1) SINEMA RC Address
   A. 172.16.10.250
2) SINEMA RC Port
   A. 443
3) Verification Type
   A. CA Certificate
4) CA Certificate
   A. certificate file (*.pem) in the dropdown (there should only be one file available for selection)
5) Device ID
   A. Enter noted Device ID from SRC information page
6) Device Password
   A. Password entered when configuring device in SRC
7) Leave Optional Settings as default
8) Click Set Values
9) Click Check Box to Enable SINEMA RC
10) Click Set Values



1) Browse to Information > SINEMA RC
2) Verify the Status is established



Thank you for attending!

Help us to better serve you! Please take a moment for our survey.

Add Survey Monkey Link and QR code to follow

Rick Kluth

Rick Kluth
Network Solutions Consultant

Murfreesboro, TN USA

Phone (919) 600-3029

Email: richard.kluth@siemens.com

Answers for industry.

Patric Dove

Patric Dove
Network Solutions Consultant

8850 Fallbrook Dr
Houston, TX 77064

Phone (713) 855-7491

Email: patric.dove@siemens.com

Answers for industry.