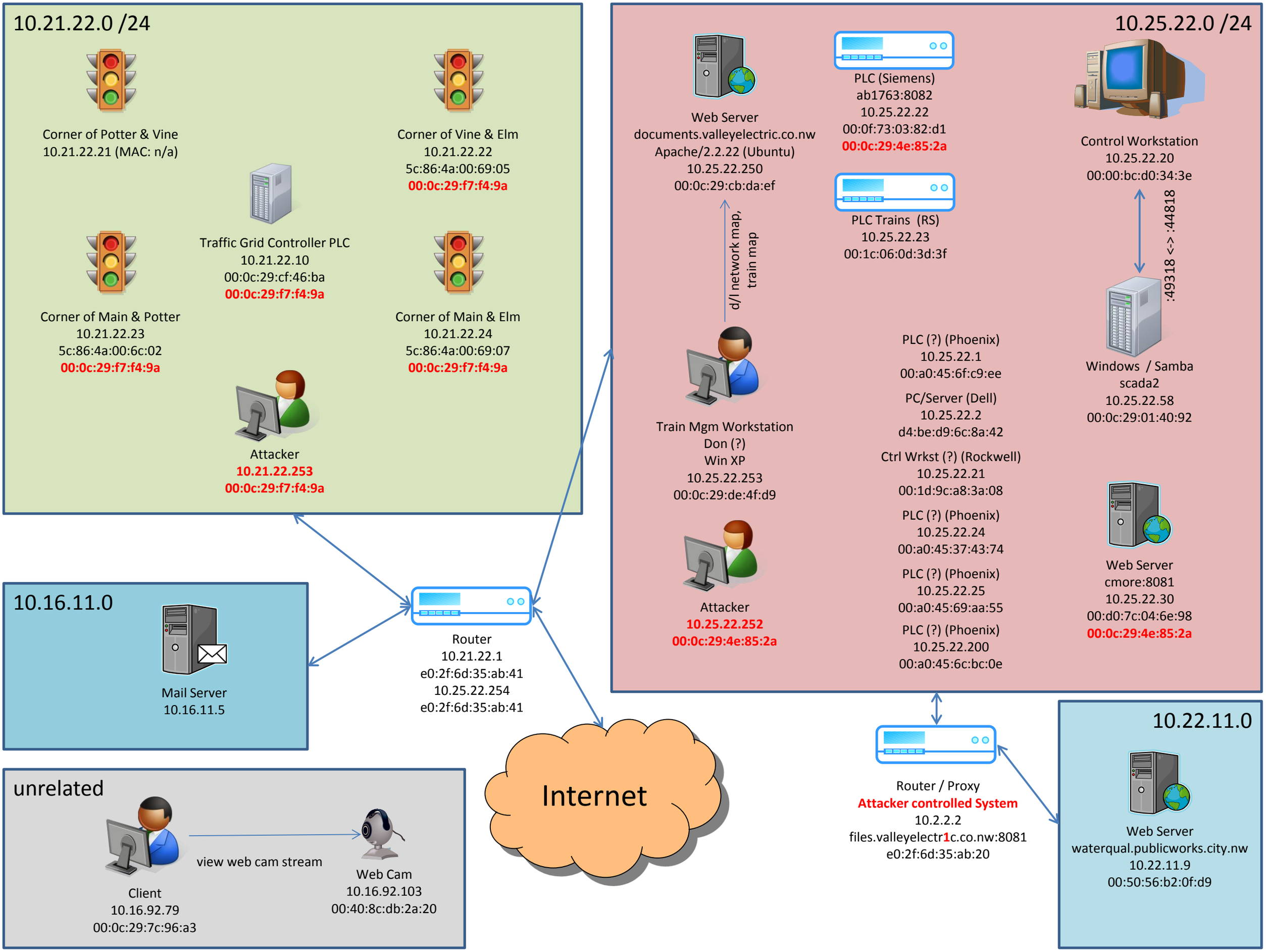
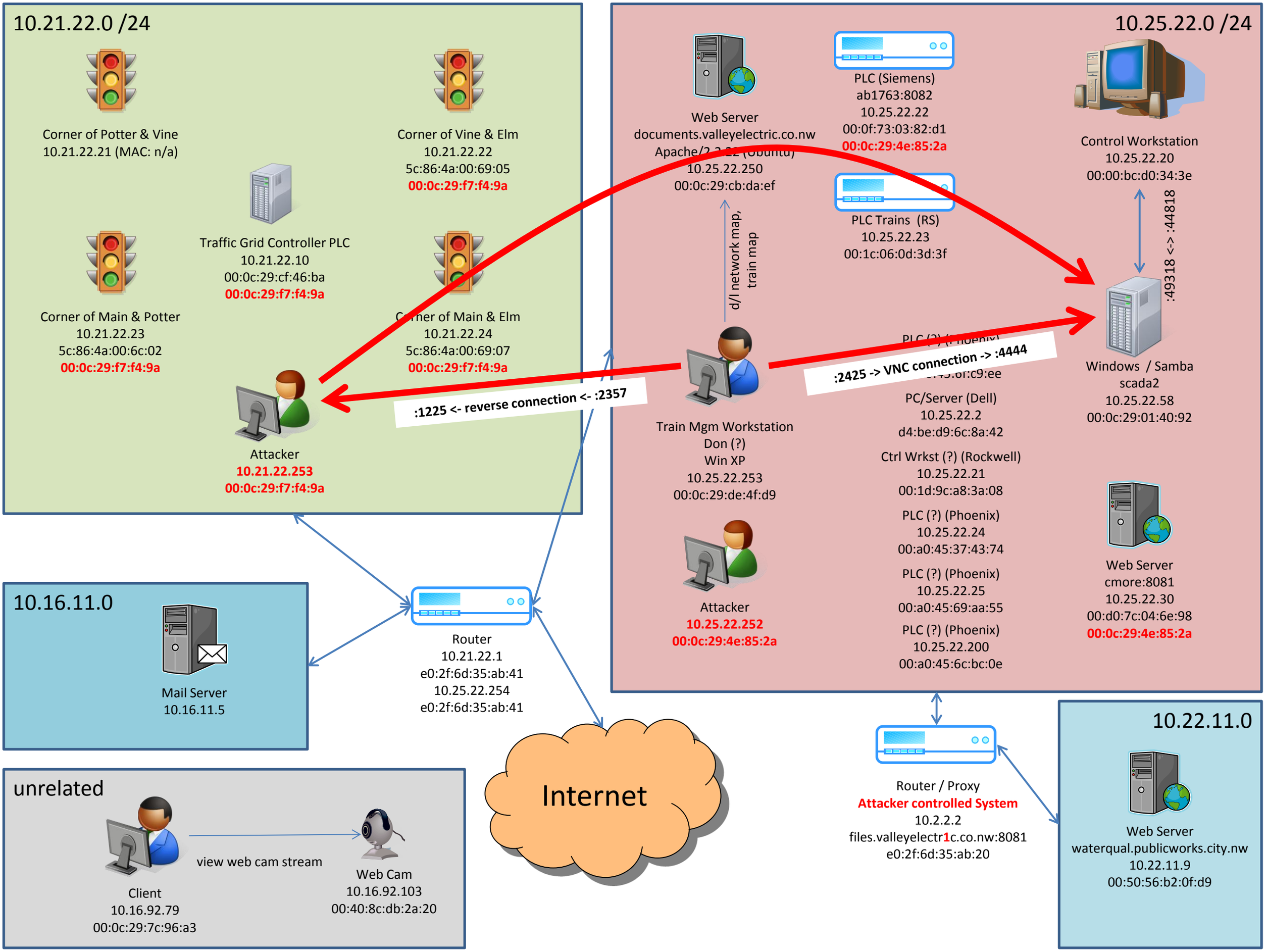

10.21.22.0 /24
Corner of Potter & Vine
10.21.22.21 (MAC: n/a)
Corner of Vine & Elm
10.21.22.22
5c:86:4a:00:69:05
00:0c:29:f7:f4:9a
Traffic Grid Controller PLC
10.21.22.10
00:0c:29:cf:46:ba
00:0c:29:f7:f4:9a
Corner of Main & Potter
10.21.22.23
5c:86:4a:00:6c:02
00:0c:29:f7:f4:9a
Corner of Main & Elm
10.21.22.24
5c:86:4a:00:69:07
00:0c:29:f7:f4:9a
Attacker
10.21.22.253
00:0c:29:f7:f4:9a
10.25.22.0 /24
Web Server
documents.valleyelectric.co.nw
Apache/2.2.22 (Ubuntu)
10.25.22.250
00:0c:29:cb:da:ef
PLC (Siemens)
ab1763:8082
10.25.22.22
00:0f:73:03:82:d1
00:0c:29:4e:85:2a
Control Workstation
10.25.22.20
00:00:bc:d0:34:3e
PLC Trains (RS)
10.25.22.23
00:1c:06:0d:3d:3f
d/l network map,
train map
:49318 <-> :44818
Windows / Samba
scada2
10.25.22.58
00:0c:29:01:40:92
PLC (?) (Phoenix)
10.25.22.1
00:a0:45:6f:c9:ee
PC/Server (Dell)
10.25.22.2
d4:be:d9:6c:8a:42
Train Mgm Workstation
Don (?)
Win XP
10.25.22.253
00:0c:29:de:4f:d9
Ctrl Wrkst (?) (Rockwell)
10.25.22.21
00:1d:9c:a8:3a:08
PLC (?) (Phoenix)
10.25.22.24
00:a0:45:37:43:74
Web Server
cmore:8081
10.25.22.30
00:d0:7c:04:6e:98
00:0c:29:4e:85:2a
Attacker
10.25.22.252
00:0c:29:4e:85:2a
PLC (?) (Phoenix)
10.25.22.25
00:a0:45:69:aa:55
PLC (?) (Phoenix)
10.25.22.200
00:a0:45:6c:bc:0e
10.16.11.0
Mail Server
10.16.11.5
Router
10.21.22.1
e0:2f:6d:35:ab:41
10.25.22.254
e0:2f:6d:35:ab:41
Internet
Router / Proxy
Attacker controlled System
10.2.2.2
files.valleyelectr1c.co.nw:8081
e0:2f:6d:35:ab:20
10.22.11.0
Web Server
waterqual.publicworks.city.nw
10.22.11.9
00:50:56:b2:0f:d9
unrelated
view web cam stream
Client
10.16.92.79
00:0c:29:7c:96:a3
Web Cam
10.16.92.103
00:40:8c:db:2a:20


10.21.22.0 /24
Corner of Potter & Vine
10.21.22.21 (MAC: n/a)
Corner of Vine & Elm
10.21.22.22
5c:86:4a:00:69:05
00:0c:29:f7:f4:9a
Traffic Grid Controller PLC
10.21.22.10
00:0c:29:cf:46:ba
00:0c:29:f7:f4:9a
Corner of Main & Potter
10.21.22.23
5c:86:4a:00:6c:02
00:0c:29:f7:f4:9a
Corner of Main & Elm
10.21.22.24
5c:86:4a:00:69:07
00:0c:29:f7:f4:9a
Attacker
10.21.22.253
00:0c:29:f7:f4:9a
:1225 <- reverse connection <- :2357
10.25.22.0 /24
Web Server
documents.valleyelectric.co.nw
Apache/2.2.22 (Ubuntu)
10.25.22.250
00:0c:29:cb:da:ef
PLC (Siemens)
ab1763:8082
10.25.22.22
00:0f:73:03:82:d1
00:0c:29:4e:85:2a
PLC Trains (RS)
10.25.22.23
00:1c:06:0d:3d:3f
Control Workstation
10.25.22.20
00:00:bc:d0:34:3e
:49318 <-> :44818
d/l network map,
train map
:2425 -> VNC connection -> :4444
Windows / Samba
scada2
10.25.22.58
00:0c:29:01:40:92
Train Mgm Workstation
Don (?)
Win XP
10.25.22.253
00:0c:29:de:4f:d9
PC/Server (Dell)
10.25.22.2
d4:be:d9:6c:8a:42
Ctrl Wrkst (?) (Rockwell)
10.25.22.21
00:1d:9c:a8:3a:08
PLC (?) (Phoenix)
10.25.22.24
00:a0:45:37:43:74
PLC (?) (Phoenix)
10.25.22.25
00:a0:45:69:aa:55
PLC (?) (Phoenix)
10.25.22.200
00:a0:45:6c:bc:0e
Attacker
10.25.22.252
00:0c:29:4e:85:2a
Web Server
cmore:8081
10.25.22.30
00:d0:7c:04:6e:98
00:0c:29:4e:85:2a
10.16.11.0
Mail Server
10.16.11.5
Router
10.21.22.1
e0:2f:6d:35:ab:41
10.25.22.254
e0:2f:6d:35:ab:41
Internet
Router / Proxy
Attacker controlled System
10.2.2.2
files.valleyelectr1c.co.nw:8081
e0:2f:6d:35:ab:20
10.22.11.0
Web Server
waterqual.publicworks.city.nw
10.22.11.9
00:50:56:b2:0f:d9
unrelated
view web cam stream
Client
10.16.92.79
00:0c:29:7c:96:a3
Web Cam
10.16.92.103
00:40:8c:db:2a:20