ICSJWG 2012 Fall Conference
Denver, Colorado
October 15-18, 2012

Networking as a Security Control

Using IP Addressing Schema for Network Isolation

SCADAhacker.com

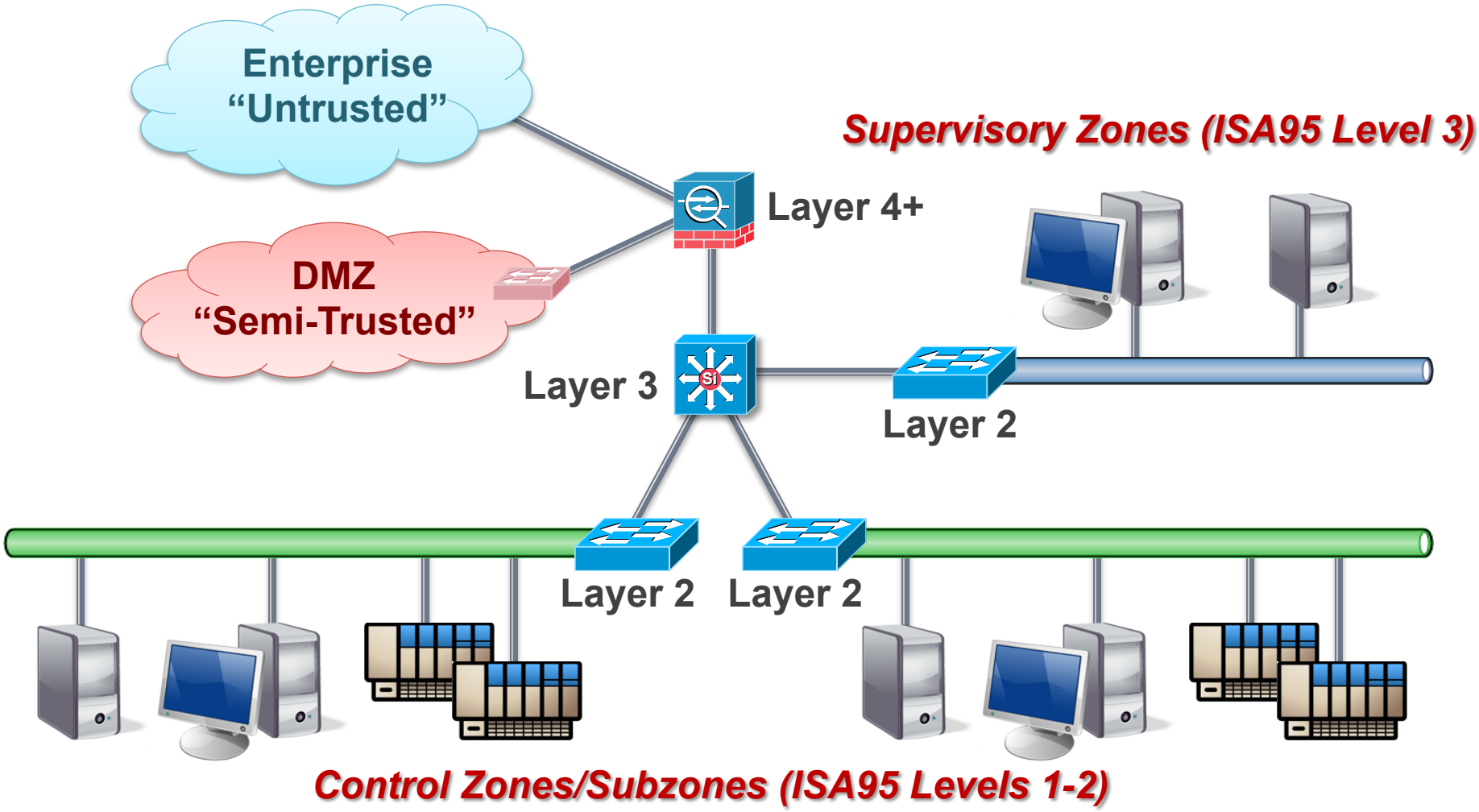
Think like a hacker ...
To secure industrial control systems and protect critical infrastructure

Discussion Points

- Network segmentation is now a part of most leading standards and best practices including ISA, ISO, NIST, SANS, etc.
- Network design is a foundation for more advanced security controls
- Risk analysis shows greatest "consequences" centered on hosts with modest ability to protect
- Habits have resulted in network architectures with inherent vulnerabilities
  - Default "classful" subnets – excessive attack surface
  - "Fully Visible" ICS networks – too much lateral ability

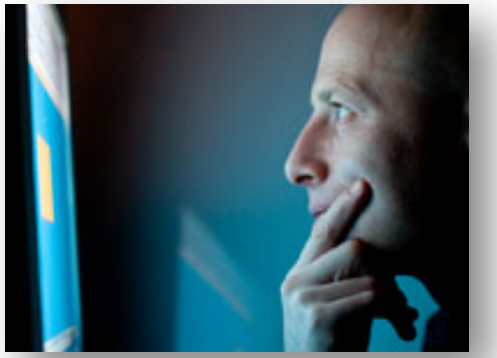
Proprietary property of SCADAhacker.com – All rights reserved.

Typical ICS Architecture



Proprietary property of SCADAhacker.com – All rights reserved.

Findings from the Field



During a recent assessment:

- **100's of Field Sites – most with less than 10 hosts**
- **"Stacked" Cisco 3750 configured to route, but interfaces not configured as Layer 3**
- **Utilized Class A private network (10.0.0.0/8)**
- **Configured hosts with subnet mask 255.255.248.0 (2,046 max hosts)**
- **Multi-homed hosts throughout network; some with VLANs**
- ***Do you think we had some problems here ???***

Proprietary property of SCADAhacker.com – All rights reserved.

Understanding an IP Address

IP Address (Network Address)

IP Address: 192.168.0.96
Subnet Mask: 255.255.255.0
CIDR: 192.168.0.96/24

Binary IP: 11000000.10101000.00000000.01100000

Binary Mask: 11111111.11111111.11111111.00000000

Network
192.168.0.0

Host
96 oo 254

IP Address: 192.168.0.96
Subnet Mask: 255.255.255.192
CIDR: 192.168.0.96/26

Binary IP: 11000000.10101000.00000000.01100000

Binary Mask: 11111111.11111111.11111111.11000000

Network
192.168.0.0

Sub-Network
1 oo 4

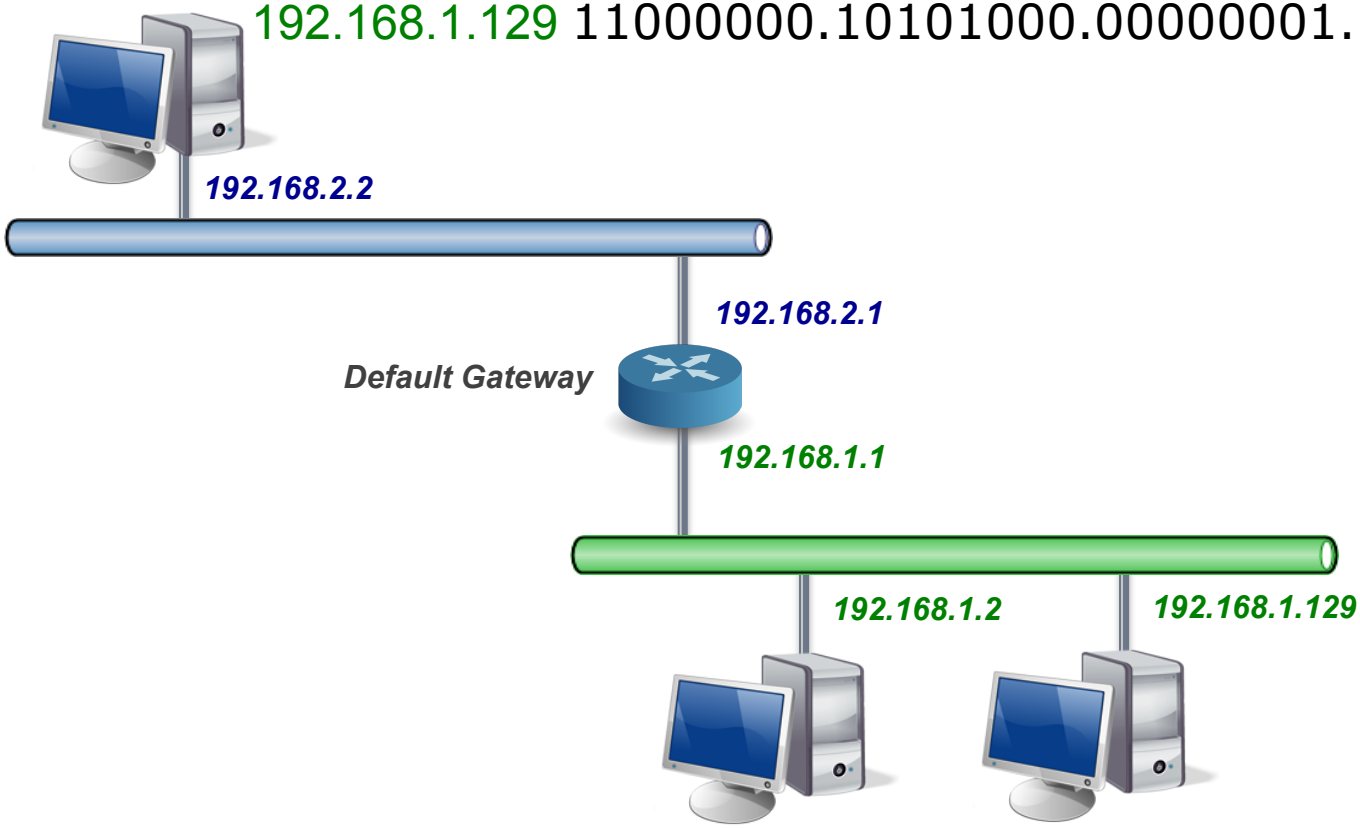
Host
32 oo 62

Increment	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1
CIDR	/17	/18	/19	/20	/21	/22	/23	/24	/25	/26	/27	/28	/29	/30	/31	/32
Mask	128	192	224	240	248	252	254	255	128	192	224	240	248	252	254	255
Hosts	32,766	16,382	8,190	4,094	2,046	1,022	510	254	126	62	30	14	6	2		
B Subnets	0	2	6	14	30	62	126	254	510	1,022	2,046	4,094	8,190	16,382		
C Subnets	1	1	1	1	1	1	1	1	0	2	6	14	30	62		

Proprietary property of SCADAhacker.com – All rights reserved.

Simple Topology

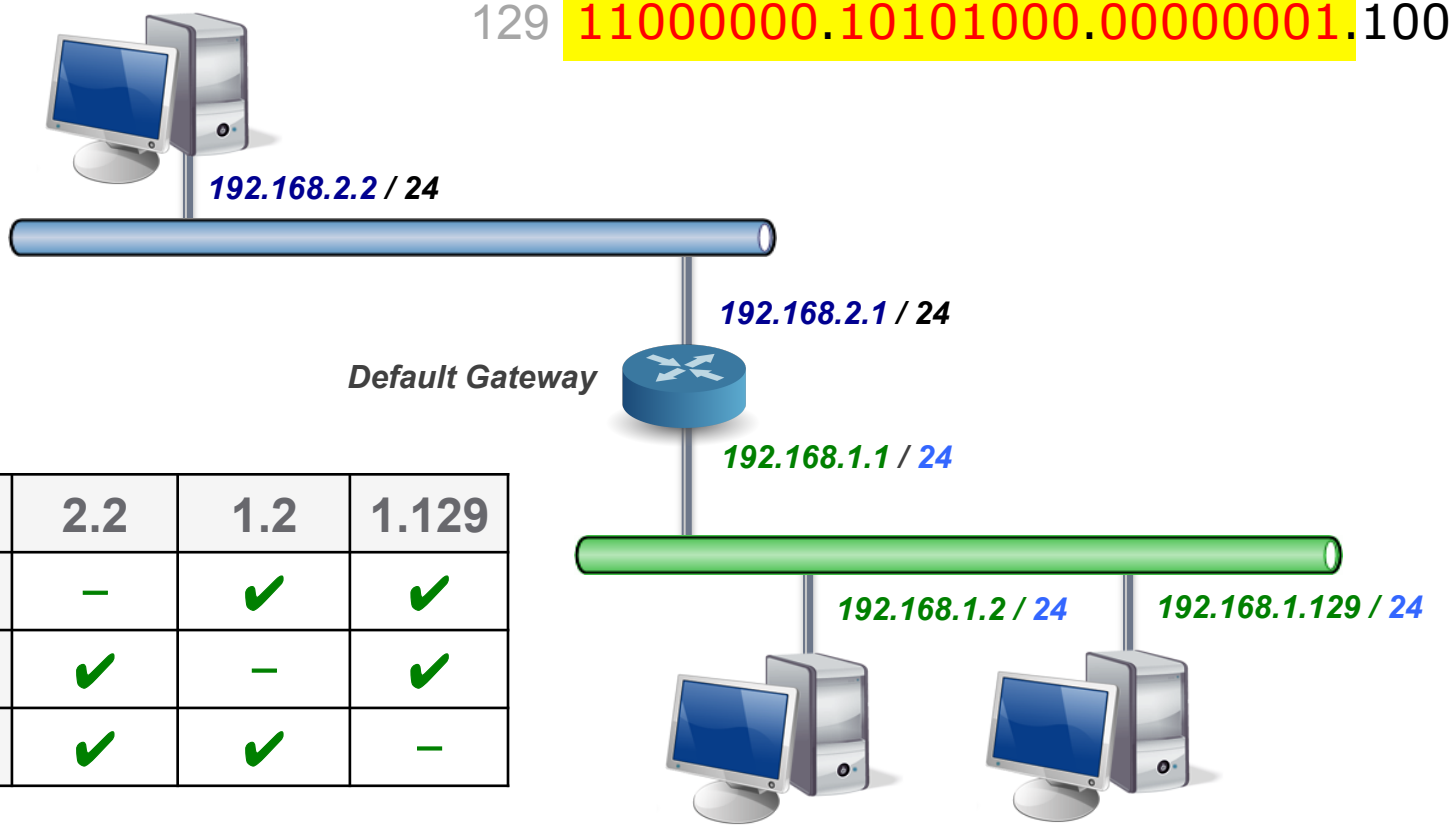
192.168.1.1 11000000.10101000.00000001.00000001
192.168.1.2 11000000.10101000.00000001.00000010
192.168.1.129 11000000.10101000.00000001.10000001



Proprietary property of SCADAhacker.com – All rights reserved.

Topology with Full Visibility

1	11000000.10101000.00000001.00000001
2	11000000.10101000.00000001.00000010
129	11000000.10101000.00000001.10000001



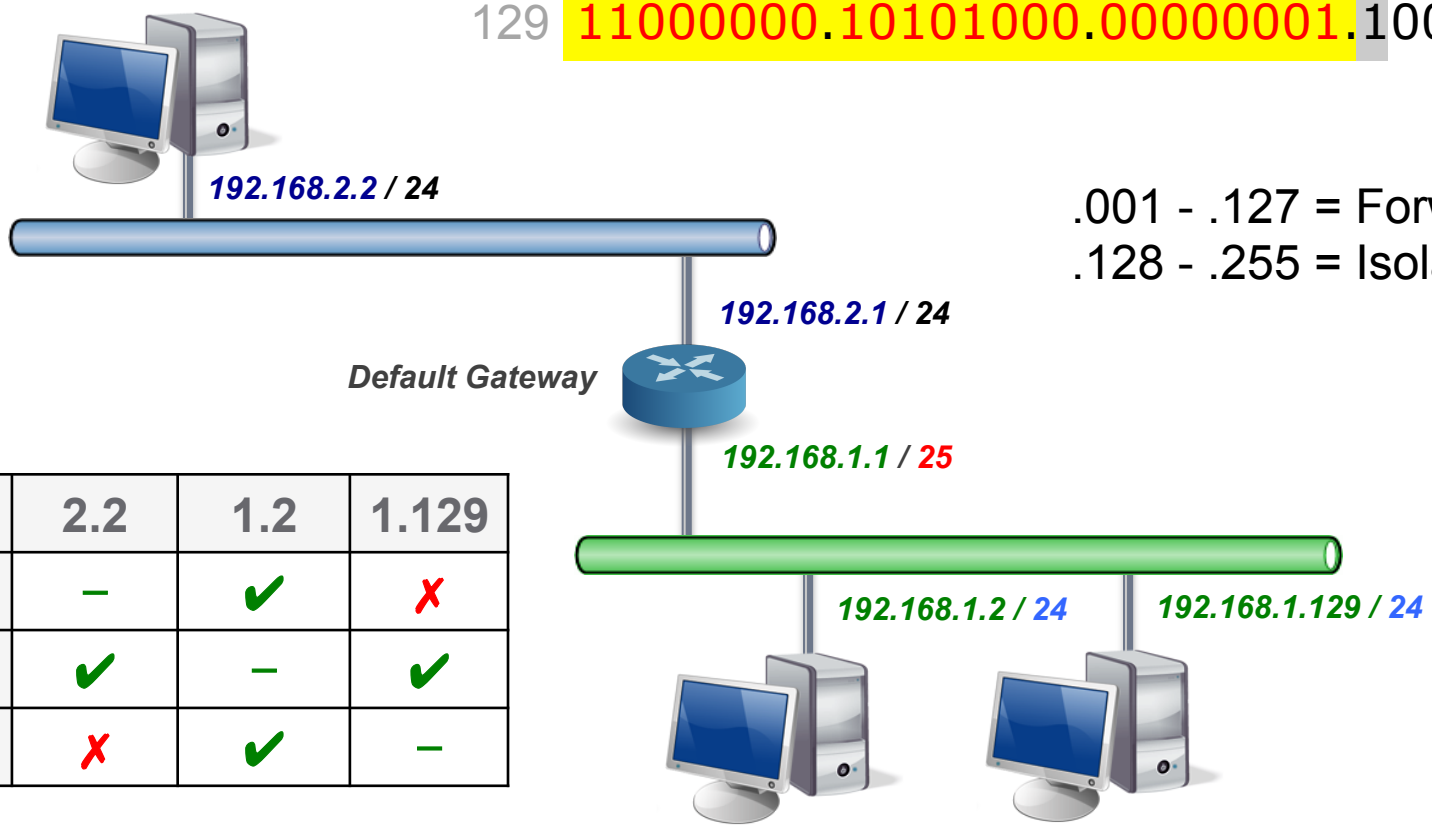
	2.2	1.2	1.129
2.2	–	✔	✔
1.2	✔	–	✔
1.129	✔	✔	–

Proprietary property of SCADAhacker.com – All rights reserved.

Topology with Split Visibility

1	11000000.10101000.00000001.00000001
2	11000000.10101000.00000001.00000010
129	11000000.10101000.00000001.10000001

.001 - .127 = Forwarded
.128 - .255 = Isolated



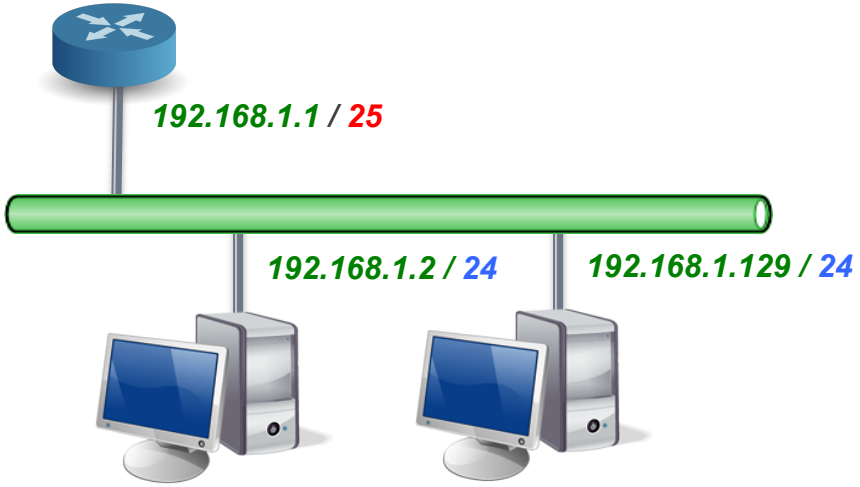
	2.2	1.2	1.129
2.2	–	✔	✗
1.2	✔	–	✔
1.129	✗	✔	–

Proprietary property of SCADAhacker.com – All rights reserved.

Topology with Split Visibility

CIDR	/24	/25	/26	/27	/28	/29	/30
Subnet Mask	255.255.255.0	255.255.255.128	255.255.255.192	255.255.255.224	255.255.255.240	255.255.255.248	255.255.255.252
# Hosts	254	126	62	30	14	6	2
1	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0
129	0	128	128	128	128	128	128

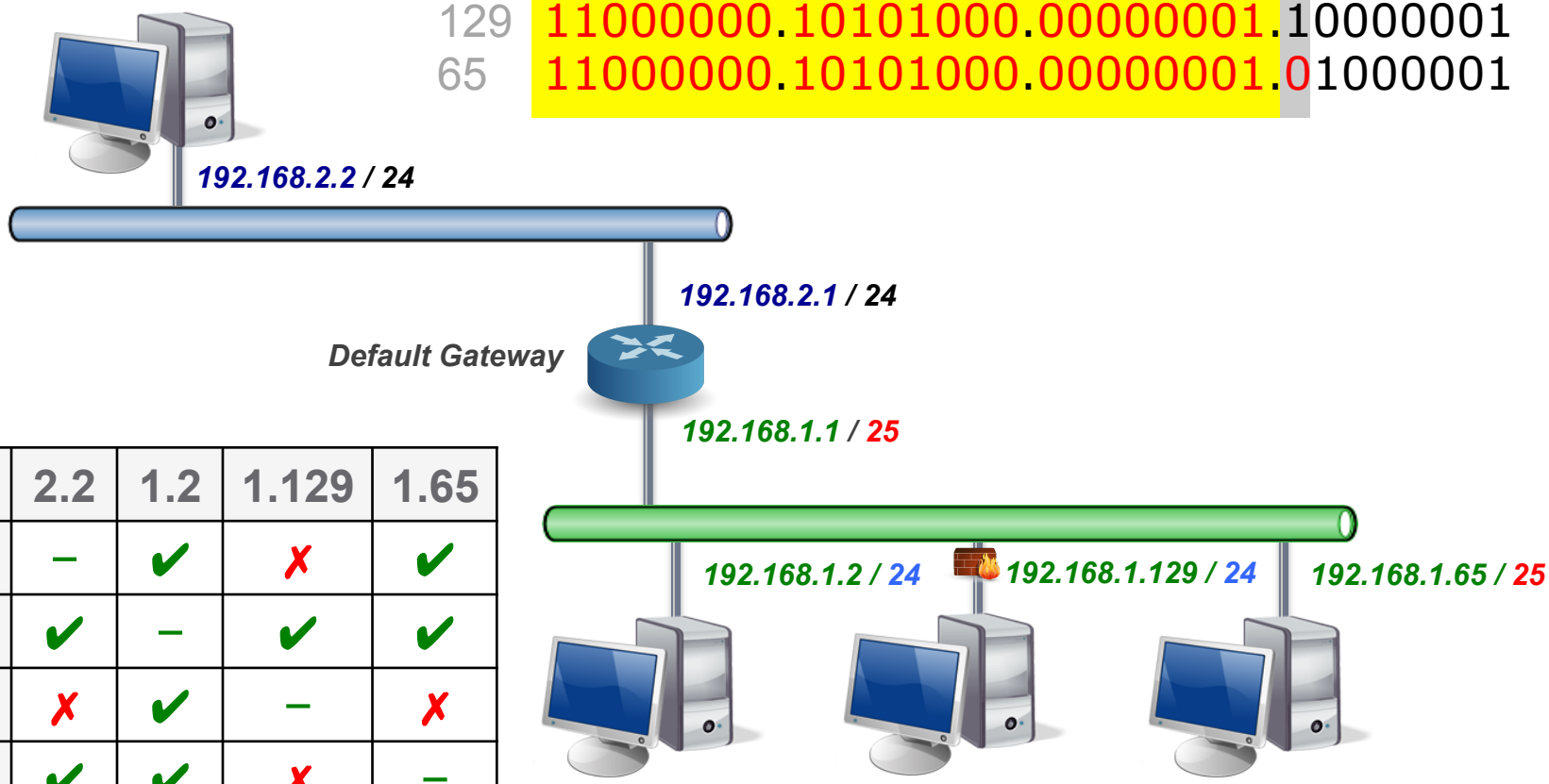
	2.2	1.2	1.129
2.2	–	✔	✗
1.2	✔	–	✔
1.129	✗	✔	–



Proprietary property of SCADAhacker.com – All rights reserved.

Topology with 3-way Split Visibility

1	11000000.10101000.00000001.00000001
2	11000000.10101000.00000001.00000010
129	11000000.10101000.00000001.10000001
65	11000000.10101000.00000001.01000001



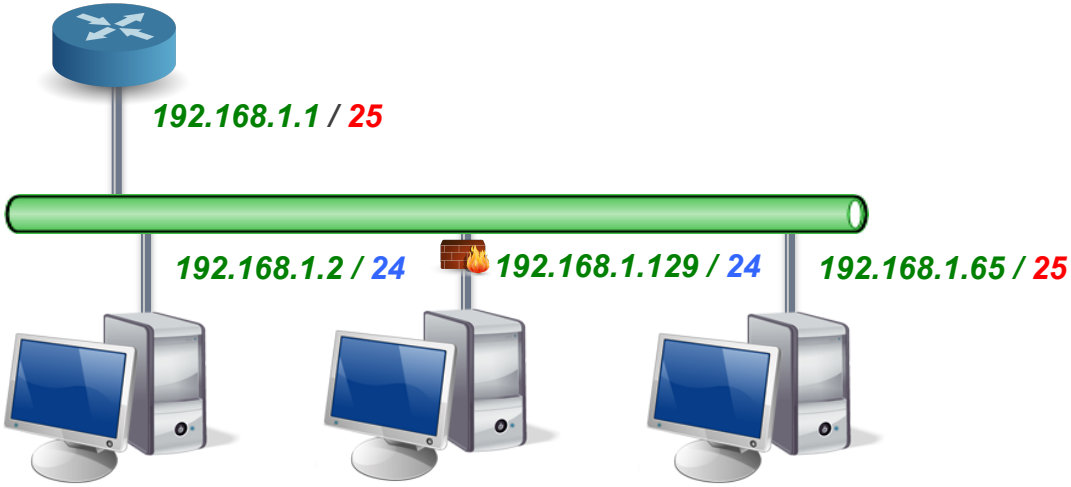
	2.2	1.2	1.129	1.65
2.2	–	✔	✗	✔
1.2	✔	–	✔	✔
1.129	✗	✔	–	✗
1.65	✔	✔	✗	–

Proprietary property of SCADAhacker.com – All rights reserved.

Topology with 3-way Split Visibility

CIDR	/24	/25	/26	/27	/28	/29	/30
Subnet Mask	255.255.255.0	255.255.255.128	255.255.255.192	255.255.255.224	255.255.255.240	255.255.255.248	255.255.255.252
# Hosts	254	126	62	30	14	6	2
1	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0
65	0	0	64	64	64	64	64
129	0	128	128	128	128	128	128

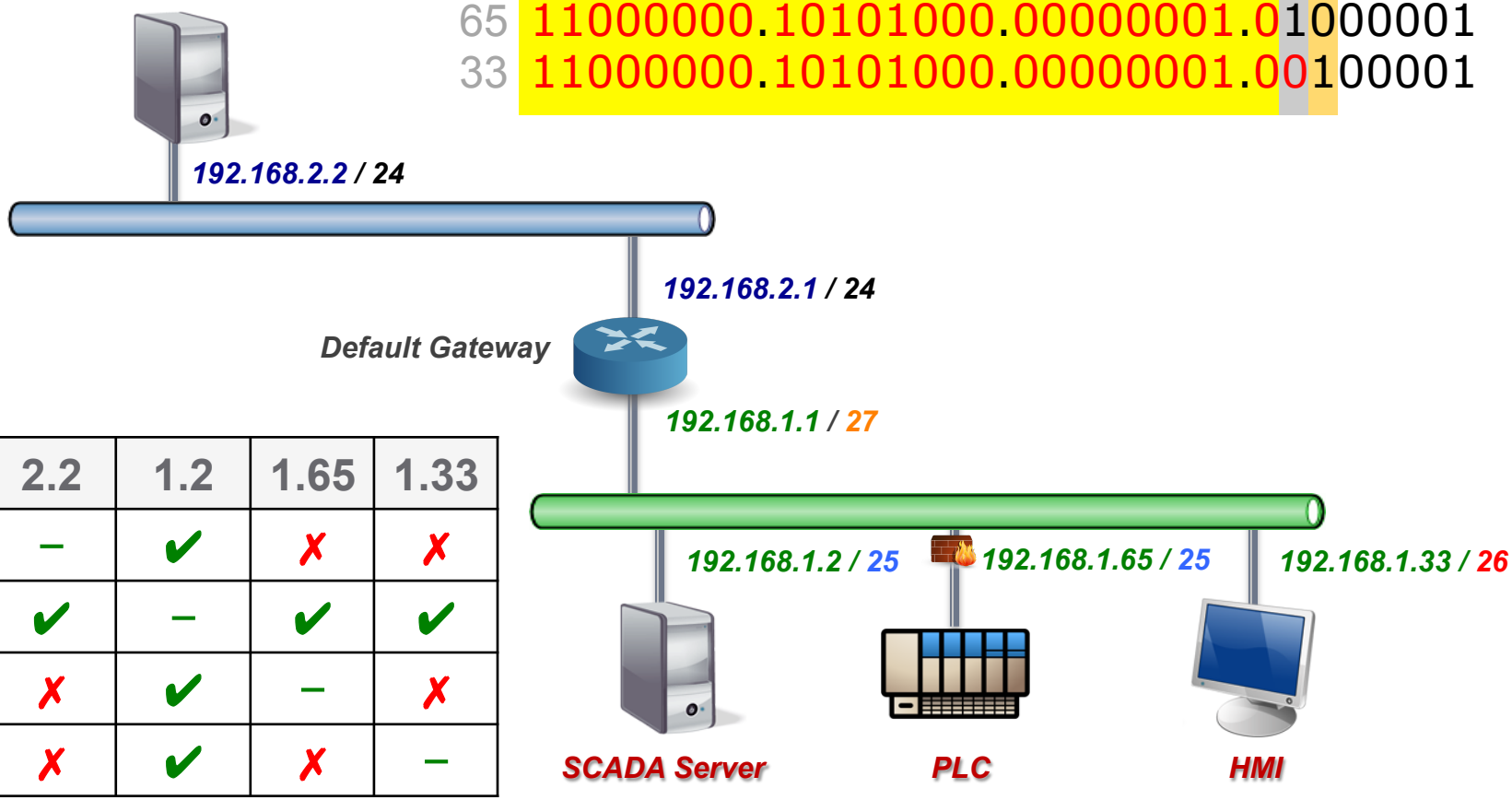
	2.2	1.2	1.129	1.65
2.2	–	✔	✗	✔
1.2	✔	–	✔	✔
1.129	✗	✔	–	✗
1.65	✔	✔	✗	–



Proprietary property of SCADAhacker.com – All rights reserved.

Advanced Topology w Split Visibility

1	11000000.10101000.00000001.00000001
2	11000000.10101000.00000001.00000010
65	11000000.10101000.00000001.01000001
33	11000000.10101000.00000001.00100001



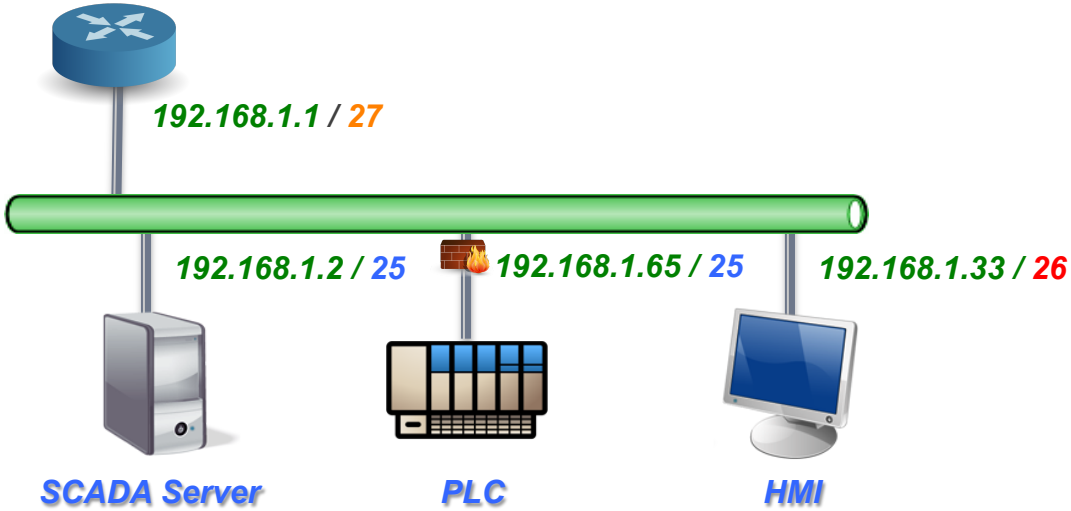
	2.2	1.2	1.65	1.33
2.2	–	✔	✗	✗
1.2	✔	–	✔	✔
1.65	✗	✔	–	✗
1.33	✗	✔	✗	–

Proprietary property of SCADAhacker.com – All rights reserved.

Advanced Topology w Split Visibility

CIDR	/24	/25	/26	/27	/28	/29	/30
Subnet Mask	255.255.255.0	255.255.255.128	255.255.255.192	255.255.255.224	255.255.255.240	255.255.255.248	255.255.255.252
# Hosts	254	126	62	30	14	6	2
1	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0
33	0	0	0	32	32	32	32
65	0	0	64	64	64	64	64

	App	Srv	PLC	HMI
App	–	✔	✗	✗
Srv	✔	–	✔	✔
PLC	✗	✔	–	✗
HMI	✗	✔	✗	–



Proprietary property of SCADAhacker.com – All rights reserved.

Variable Length Subnet Masking

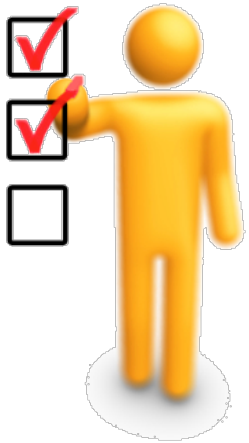
CIDR	/24	/25	/26	/27
Subnet Mask	255.255.255.0	255.255.255.128	255.255.255.192	255.255.255.224
# Hosts	254	126	62	30
Last Octet				
0	0	0	0	0
32	0	0	0	32
64	0	0	64	64
96	0	0	64	96
128	0	128	128	128
160	0	128	128	160
192	0	128	192	192
224	0	128	192	224
255	0	128	192	224

Network Number

Proprietary property of SCADAhacker.com – All rights reserved.

How this can help you

- Offers additional security controls for “hard to protect” endpoints and field devices
- Offers protection from “careless network access control”
- Improves strength and resilience of existing “logical” and “physical” segmentation strategy
- Helps simplify configuration of L3 / L4 barrier appliances
- Easy to incorporate into project design guidelines
- Well suited for typical heterogeneous ICS architectures



Proprietary property of SCADAhacker.com – All rights reserved.

SCADAhacker.com

Think like a hacker ...

Additional Information:

joel@SCADAhacker.com
www.SCADAhacker.com
@SCADAhacker
+1.855.SCADAhacker (722-3242)