

4/19/18

Group 4

~~Manoacan, JP~~

~~Martin, Jasper~~

~~Moreno, Marivette~~

~~Manuel, Kyle~~

~~Absent~~

~~Pahutan, Luis~~

~~Racho, Charlene Nicola~~

~~Parraluman, Eldridge~~

~~Fabru, Shane~~

Merge with

Group 3

~~Jimenez, Almita~~

~~Lintag, Christopher~~

~~Magallanes, Jenico~~

~~Pela Cruz, John~~

~~Go, Cristine~~

~~Guimatay, Diane~~

~~Fajardo, Ivan~~

~~Lopez, Marvin~~

356 419  
100%

1. 192.168.1.1 192.168.2.1 192.168.13

2. Shows the same reflection

Reflection

1. Remotely monitor network activities and open-ended
2. SNMP v2 only supports unencrypted community strings  
this would risk since its unencrypted anyone would be able to edit,
3. It is more secure and has encryption unlike SNMP v3.

4/26/18

Group 3

Lintag, Christopher John A.  
Fajardo, John Van A.  
Cumatay, Dianne L.  
Magallanes, Jencho Isaac R.  
Cio, Christine Jane B.  
Jimenez, Almikka  
Lopez, Martin + James  
Dela Cruz, John Michael V.

Sk-426

5.3.2.3 Implement a local span

Verify connectivity

d. were the pings from R1 to PC-C, S1 and S3 successfully copied & forwarded out 10/6 to R2-A?

- yes

e. was the traffic monitored and copied in both directions?

- yes

Reflection

In this scenario, instead of using PC-A and a packet sniffer would on IDS or on ICS be more appropriate?

- IDS



Wintag	Magnolius
Dayada	gw
Gumatay	Lopes
finere2	detacore



### 5.2.2.6 Configuring snmp

#### Reflection

④ it may point to the ability of snmp as an open and cross platform protocol to work with many different devices including host computer in the network. snmp benefits a network administrator whose job is to monitor the status and configuration of network host across the entire network.

② because snmpv2 support only unencrypted community strings, using write access would be a greater security risks.

100  
426  
SK