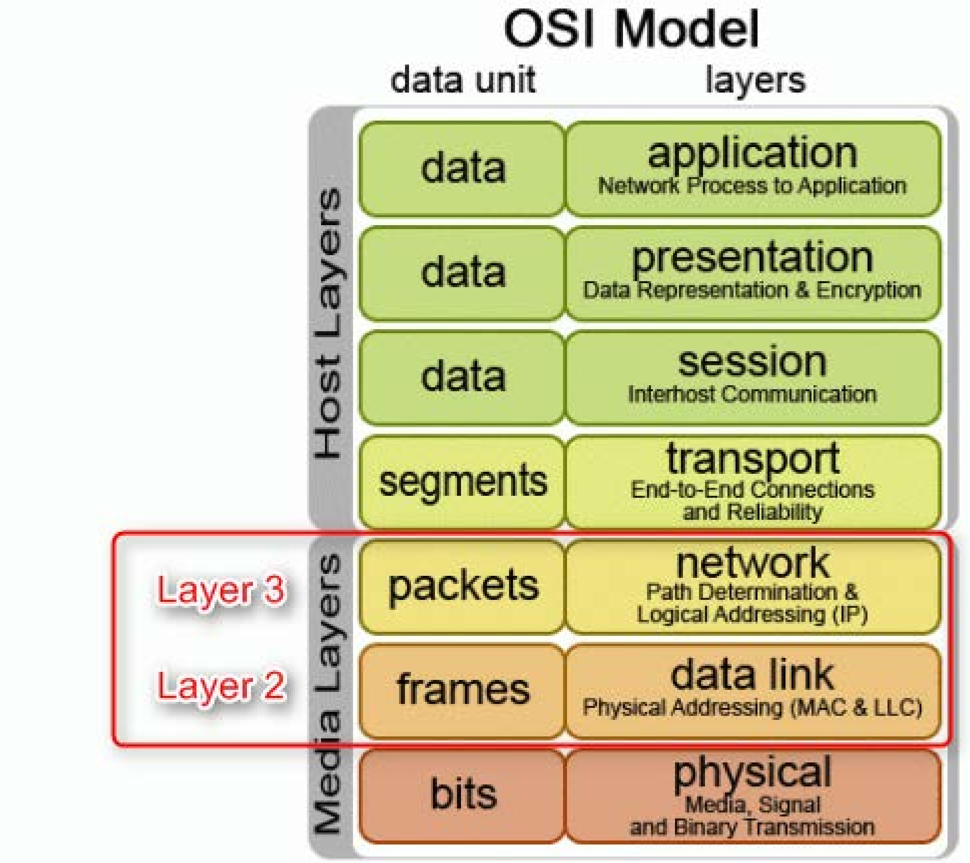
Remote access at Layer2
Using the Secomea Layer2 agent

Layer2 versus Layer3

An Ethernet connected device typically has two distinct addresses: an IP address such as 192.168.0.1, and a MAC address such as 11:22:33:44:55:66. Normally, you can configure the device's IP address to your liking, while the MAC address is a globally unique fixed address assigned to the device's Ethernet port by the manufacturer.

In network terms, the IP address is a so-called Layer3 (logical) address, and the MAC address is a so-called Layer2 (physical) address.

The layer numbers are defined in the OSI model, but we will not go further into that here, as you can easily find more information about that on e.g. Wikipedia.


OSI Model
data unit
layers
Host Layers
Media Layers
data
application
Network Process to Application
data
presentation
Data Representation & Encryption
data
session
Interhost Communication
segments
transport
End-to-End Connections and Reliability
Layer 3
packets
network
Path Determination & Logical Addressing (IP)
Layer 2
frames
data link
Physical Addressing (MAC & LLC)
bits
physical
Media, Signal and Binary Transmission

Let us instead focus on the differences between MAC/Layer2 and IP/Layer3 in the context of the automation industry and remote device management.

Typically, a program (running on your PC) only needs to know the IP address of a device to connect to it.

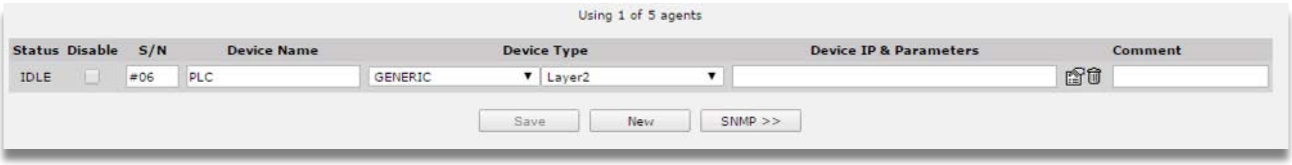
However (as we will see later), many automation programs have a feature which enables them to discover -

and communicate with - devices connected to the same Ethernet as the PC without knowing their IP address. To do this, the PC and the devices communicate using their MAC addresses and using so-called Layer2 broadcasts.

Using MAC addresses for communicating between the PC and the devices on Layer2 is by design confined to the physical Ethernet where the devices are interconnected (typically through an Ethernet switch). This is fine as long as the technician operating the PC is onsite with the device, but it becomes highly challenging when you want to do utilize remote device management, since it conflicts with the very nature of Layer2 communication being "physically confined to the same Ethernet".

This is where Secomea's Layer2 agent comes into the picture; it seamlessly removes the barrier between your PC and the remote physical Ethernet, and virtually plugs the PC into a switch port on the remote Ethernet.

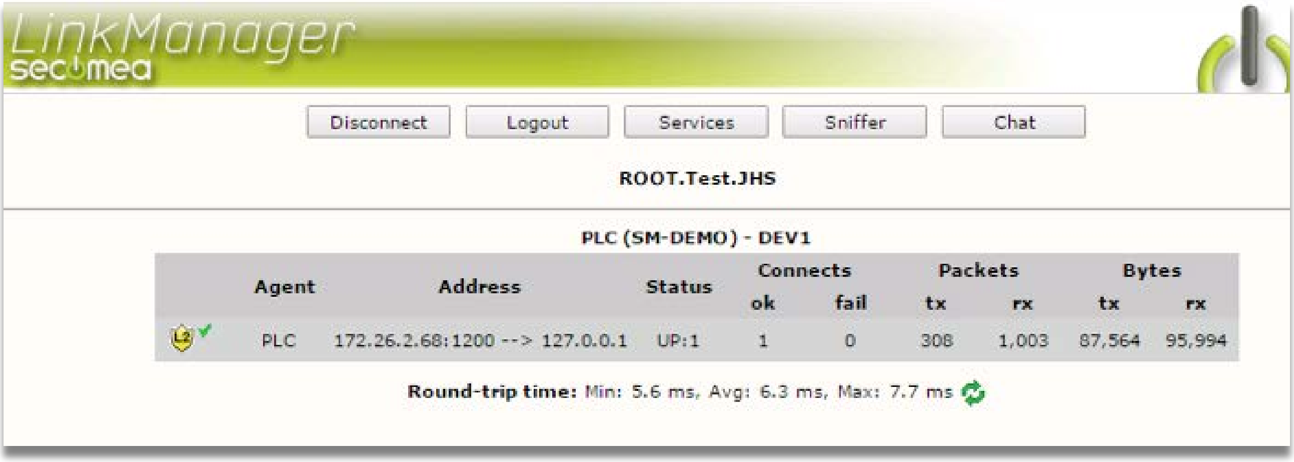
Layer2 agent configuration in the SiteManager:



Using 1 of 5 agents

Status	Disable	S/N	Device Name	Device Type		Device IP & Parameters	Comment
IDLE	□	#06	PLC	GENERIC ▼	Layer2 ▼		

Connection established to the Layer2 agent via LinkManager:



ROOT.Test.JHS

PLC (SM-DEMO) - DEV1

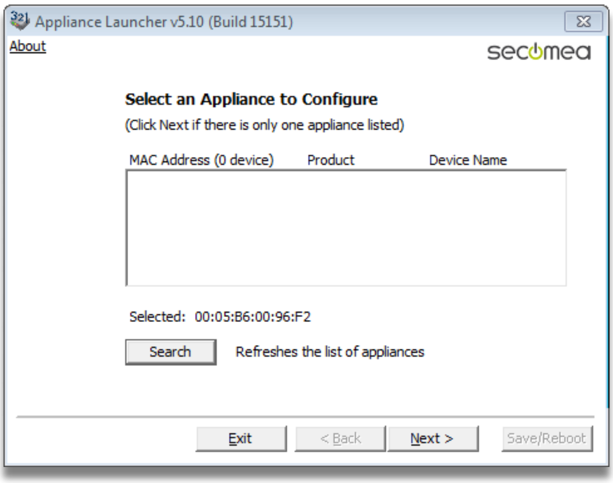
	Agent	Address	Status	Connects		Packets		Bytes	
				ok	fail	tx	rx	tx	rx
✓	PLC	172.26.2.68:1200 --> 127.0.0.1	UP:1	1	0	308	1,003	87,564	95,994

Round-trip time: Min: 5.6 ms, Avg: 6.3 ms, Max: 7.7 ms

Examples of Layer2 dependant application features

An example of a well known Secomea utility depending on Layer2 is the Secomea Appliance Launcher. This utility is designed specifically for applying network and GateManager settings to Secomea appliances, such as SiteManagers and TrustGates. Since such an appliance may not have IP address, or its IP address may not match the IP network your PC is connected to, the only option is to reach it on the physical address (MAC).

If you connected with a LinkManager via a traditional agent working at Layer3 to a remote Device network with a number of Secomea appliances, and you started the Appliance Launcher on your PC, you would get this result:



Select an Appliance to Configure

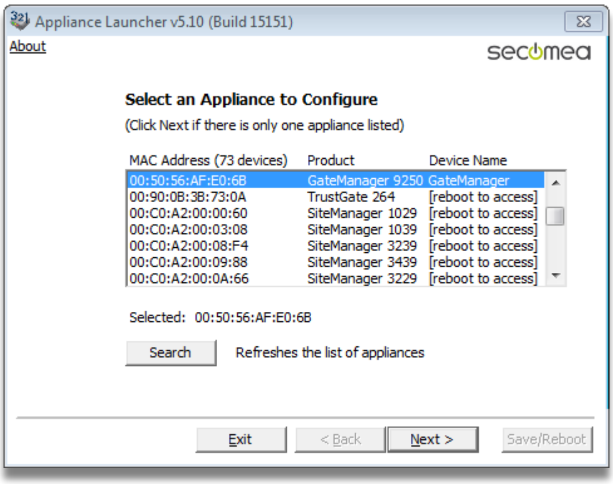
(Click Next if there is only one appliance listed)

MAC Address (0 device)	Product	Device Name

Selected: 00:05:B6:00:96:F2

Refreshes the list of appliances

Connecting remotely to the same network using the Layer2 agent would discover all devices in the remote network, and have them all becoming fully accessible by the Appliance Launcher:



Select an Appliance to Configure

(Click Next if there is only one appliance listed)

MAC Address (73 devices)	Product	Device Name
00:50:56:AF:E0:6B	GateManager 9250	GateManager
00:90:0B:3B:73:0A	TrustGate 264	[reboot to access]
00:C0:A2:00:00:60	SiteManager 1029	[reboot to access]
00:C0:A2:00:03:08	SiteManager 1039	[reboot to access]
00:C0:A2:00:08:F4	SiteManager 3239	[reboot to access]
00:C0:A2:00:09:88	SiteManager 3439	[reboot to access]
00:C0:A2:00:0A:66	SiteManager 3229	[reboot to access]

Selected: 00:50:56:AF:E0:6B

Refreshes the list of appliances

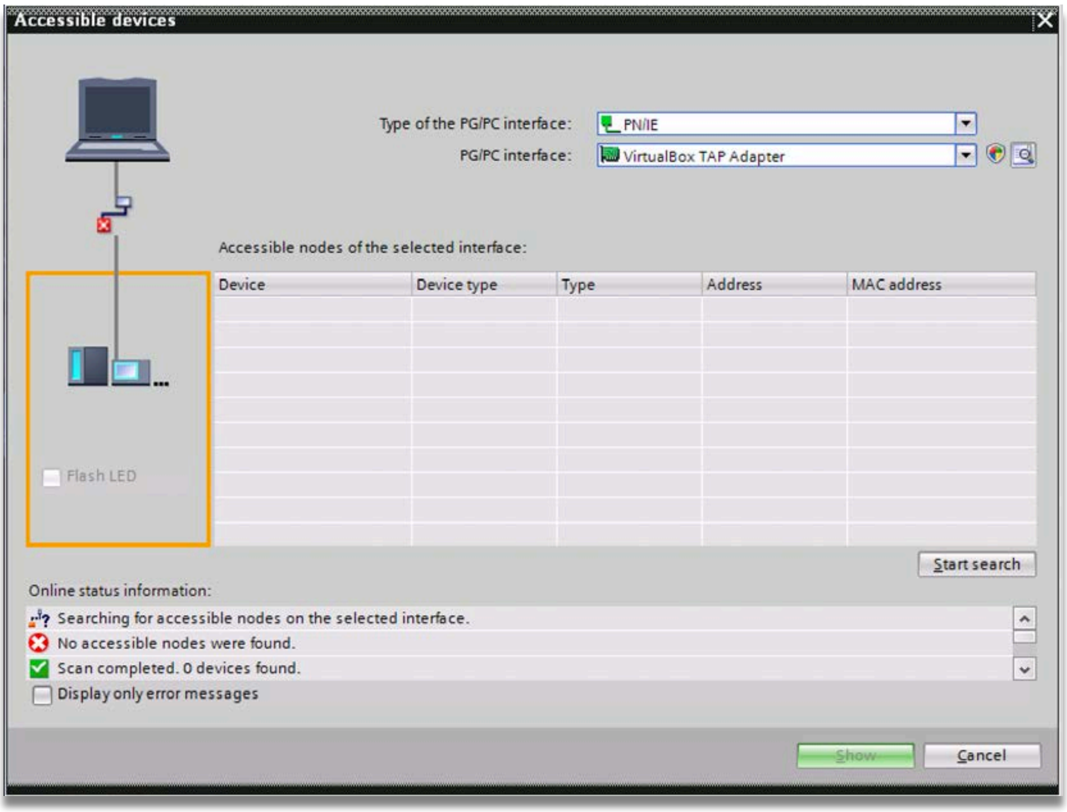
In reality no one would have a need for this specific scenario, as the Appliance Launcher utility is designed for first time setup, which typically also means it is done by the same person that physically installs and connects power to the appliance, and that person would therefore be on site and connected to the same network.

Especially within the automation industry it is often seen that applications relies on Layer2 access to the devices. This is not necessarily sign of bad protocol design, but could be because the design assumed that the application user, such as the PLC programmer, would always be at the physical location in order to verify that the machine is operating according to changes applied. In recent years, however, the abilities for trouble shooting and debugging from within the application without needing physical access to the automation devices has improved; concurrently with remote access becoming an standard part of an OEMs maintenance offering.

Siemens for example, has evolved their Step7 PLC program into the Total Integrated Automation (TIA) portal along with features of their PLCs and HMIs becoming more advanced. The device communication protocol has, however, not changed as the TIA portal needs to stay backwards compatible, and the communication protocol itself still does the job.

The Secomea solution has supported both Step7 and the TIA portal for many years. You just have to specifically state in the Siemens program which IP address you want to access.

But attempting to let the TIA portal scan for available devices after connecting with the LinkManager to the standard Siemens agent, would result in this:



Accessible devices

Type of the PG/PC interface: PN/IE

PG/PC interface: VirtualBox TAP Adapter

Accessible nodes of the selected interface:

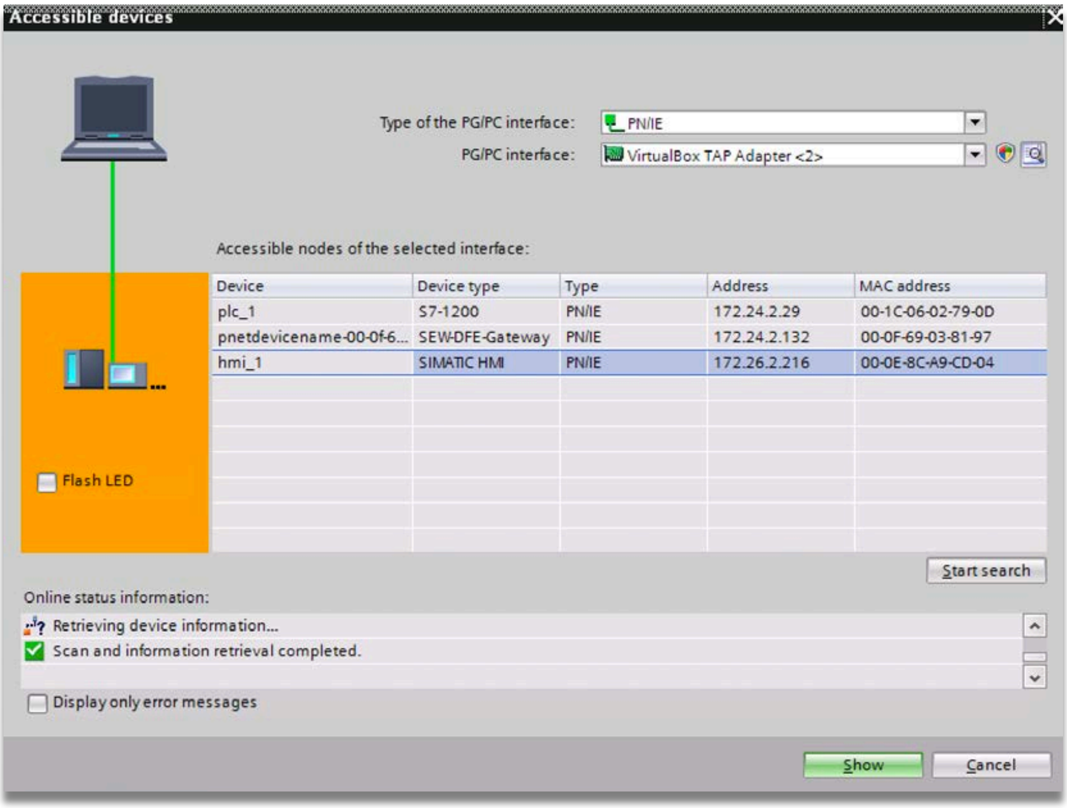
Device	Device type	Type	Address	MAC address

Online status information:

- Searching for accessible nodes on the selected interface.
- No accessible nodes were found.
- Scan completed. 0 devices found.

☐ Display only error messages

With the new Layer2 agent you will now experience that the TIA portal can scan and detect all Siemens devices in the DEV network of the SiteManager:



Accessible devices

Type of the PG/PC interface: PN/IE

PG/PC interface: VirtualBox TAP Adapter <2>

Accessible nodes of the selected interface:

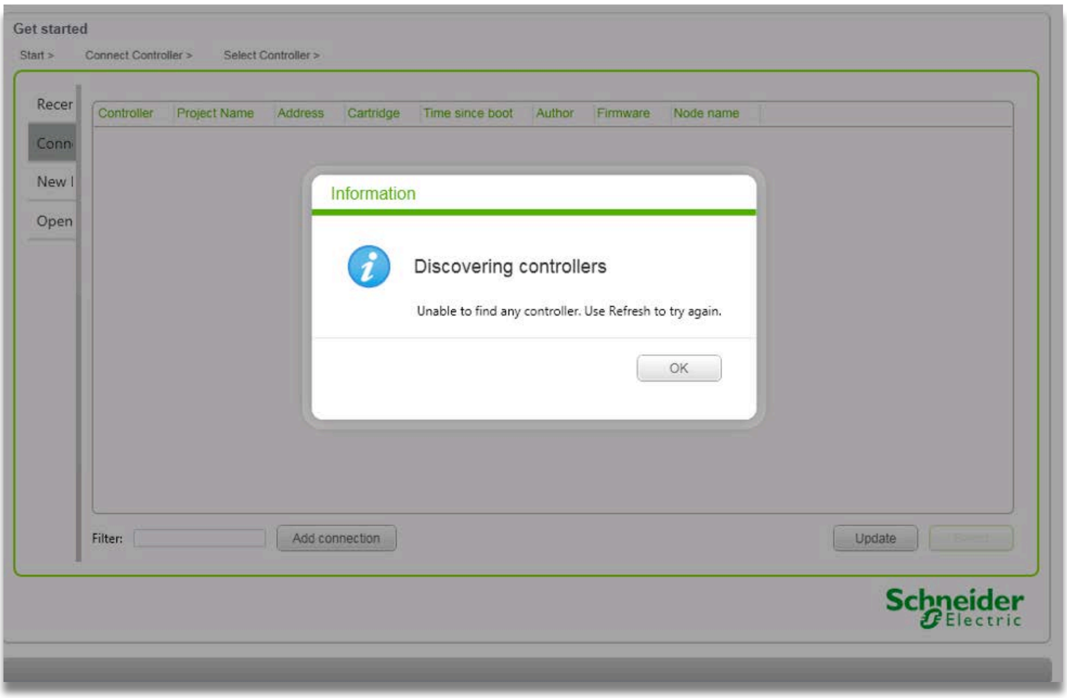
Device	Device type	Type	Address	MAC address
plc_1	S7-1200	PN/IE	172.24.2.29	00-1C-06-02-79-0D
pnetdevicename-00-0f-6...	SEW-DFE-Gateway	PN/IE	172.24.2.132	00-0F-69-03-81-97
hmi_1	SIMATIC HMI	PN/IE	172.26.2.216	00-0E-8C-A9-CD-04

Online status information:

- Retrieving device information...
- Scan and information retrieval completed.

☐ Display only error messages

Another example is Schneider Electric's SoMachine, which has similar functionality for discovering devices. The standard Secomea agents already support remote access to Schneider equipment, but invoking the discovery feature of SoMachine 4.1 via the standard agent would give this result:



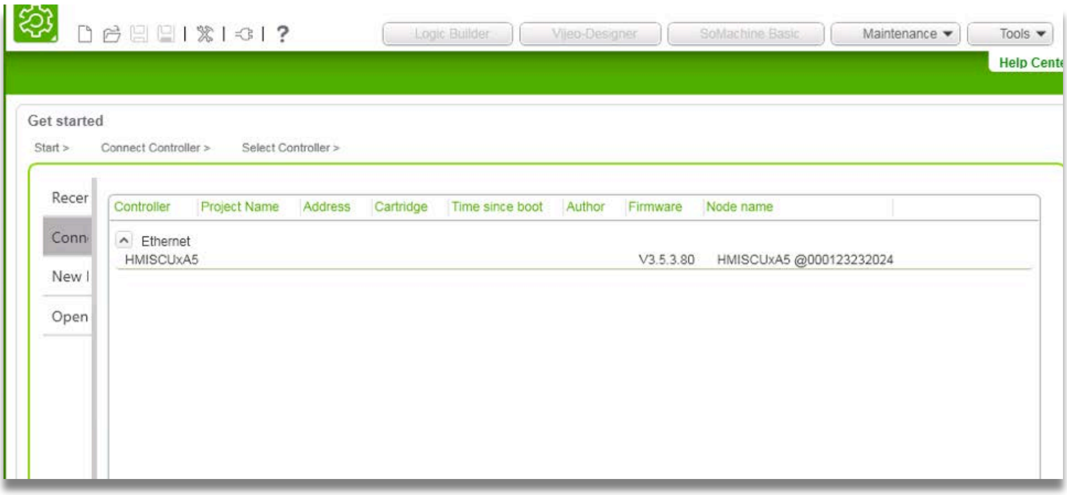
Controller	Project Name	Address	Cartridge	Time since boot	Author	Firmware	Node name

Information

Discovering controllers

Unable to find any controller. Use Refresh to try again.

The same action performed via the new Layer2 agent, will give this much richer result:



Controller	Project Name	Address	Cartridge	Time since boot	Author	Firmware	Node name
Ethernet							
HMISCUxA5						V3.5.3.80	HMISCUxA5 @000123232024

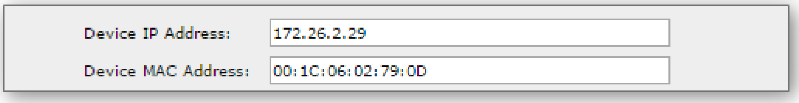
Bottom line is that with the Layer2 agent, the application and the devices sees each other as if they were located in the very same physical network, connected to the same physical switch.

Security aspects

Traditional IP access via the SiteManager agents typically involves limiting the access to a specific IP address, and specific ports.

The Layer2 agent will by default provide the LinkManager access to the entire DEV network of the SiteManager - and to any device in that network at both Layer2 and Layer3 level.

For IT security reasons this may not be desirable, and therefore the agent offers filtering on the IP address, MAC address and even a combination of both:



Device IP Address: 172.26.2.29

Device MAC Address: 00:1C:06:02:79:0D

If stating both the IP address and the MAC address, the security is in fact increased considerably. If the PLC was incidentally replaced by another type device but with the same IP address, the SiteManager would actively prevent access to it.

And if your intention is to have Layer2 access to multiple devices in the network, but want to limit the access to specific users by the domain structures and account management in the GateManager Portal, you simply create separate Layer2 agents for each device.

Performance aspects

Layer2 communication would typically represent a bigger overhead than Layer3 traffic, since also less relevant broadcast messages could risk consuming bandwidth. The Layer2 agent will, however, actively drop some types of packets that are deemed irrelevant for this purpose, such as STP and IGMP multicast.

From the LinkManager side, it would typically only be the Windows PC's NetBIOS announcement messages that would travel to the DEV net end. This is not blocked, as there may be a desire of the remote device to identify the remote PC based on this, and also the amount of data related to this is limited.

More important is to prevent broadcasts from devices in the DEV network to flood the connection back to the LinkManager PC. The best way to prevent this is to use the above mentioned filters, so broadcast messages are limited to those that the device may send, and which may be relevant to the application.

It should also be noted that Layer2 traffic is encapsulated in TCP packets in order to ensure retransmission and correct packet order of broadcast frames. This also means that Layer2 connections could suffer more from high latency connections than ordinary IP based agents.

Final notes

It should be noted that the Layer2 agent does not solve all problems, and should only be used if needed. The general recommendation is to use the standard vendor agents based on IP addresses.

The Layer2 feature is, however, an extremely important step to not only make the Secomea solution 100% complete in aspect of supporting secure and complete access to any type of network device, but also to effectively differentiate the Secomea solution from other remote access solutions.