



Access Gateway Switch



Eran Bar

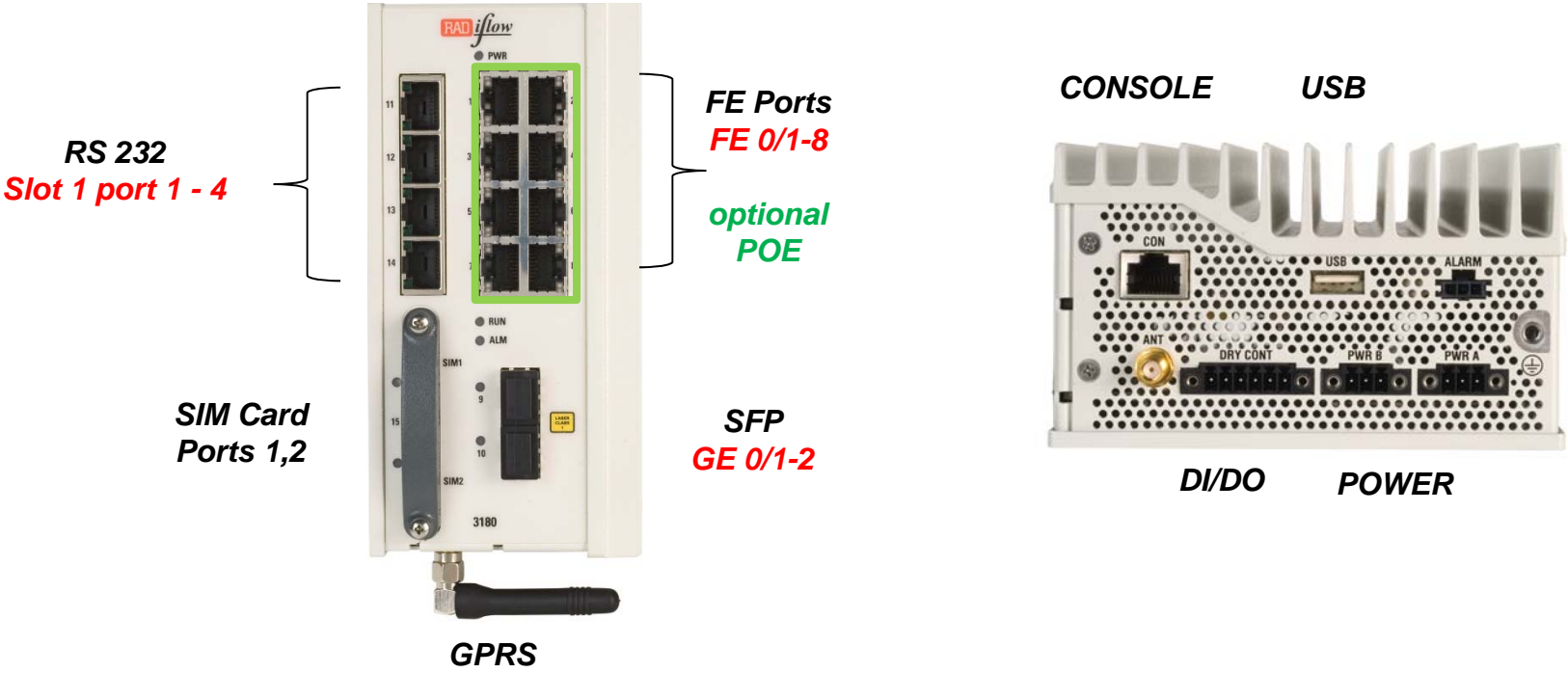
Portfolio Overview

- **Industrial design**
 - Modular DIN rail switches (7 I/O slots) or Compact system
 - Harsh environment - IP30, - 40 ÷ +75° C, IEC 61850-3 EMI
 - ETH or RS-232/RS-485 serial interface modules
- **Networking**
 - Advanced Ethernet switching and IP routing functionality
 - Serial Tunneling or Service translation
 - Physical Interface :
 - Copper – Fast Ethernet / Gigabit Ethernet
 - Fiber – Single Mode / Multi Mode.
 - Cellular – GPRS /UMTS
- **Integrated security mechanisms**
 - MAC/IP filtering per port
 - Distributed app-aware firewall
 - Remote access and Inter-site connectivity



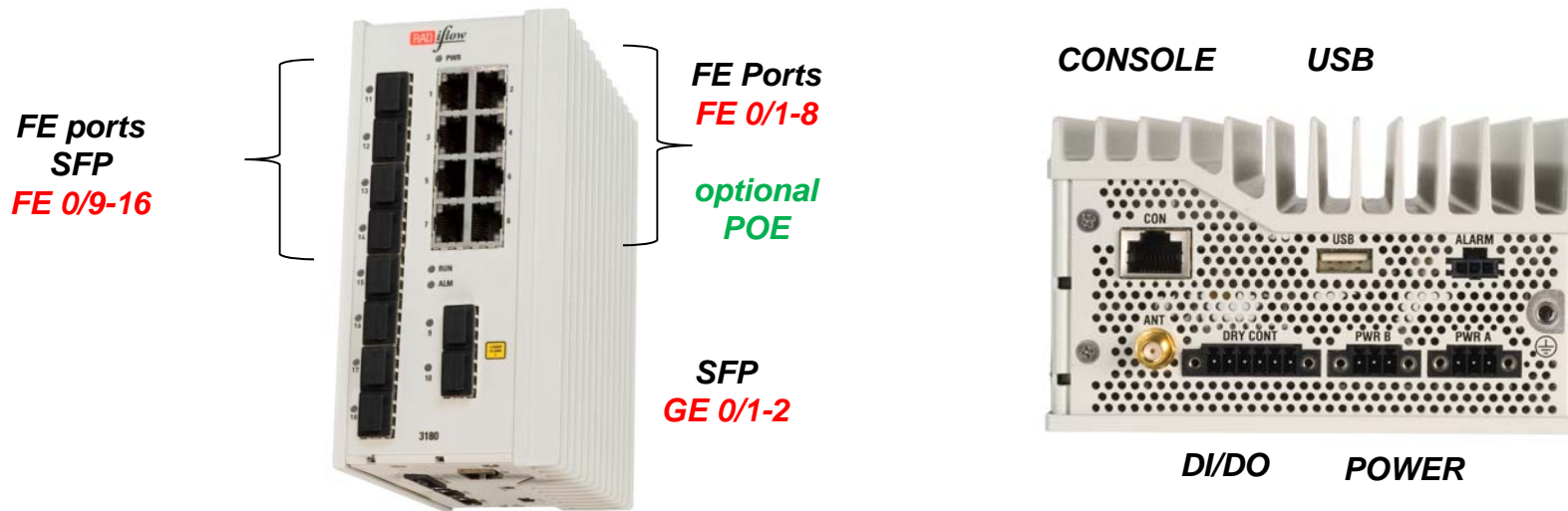
Access and Network Interfaces

RF-3180-[PS]-ET28/POE/4RS2/CEL1

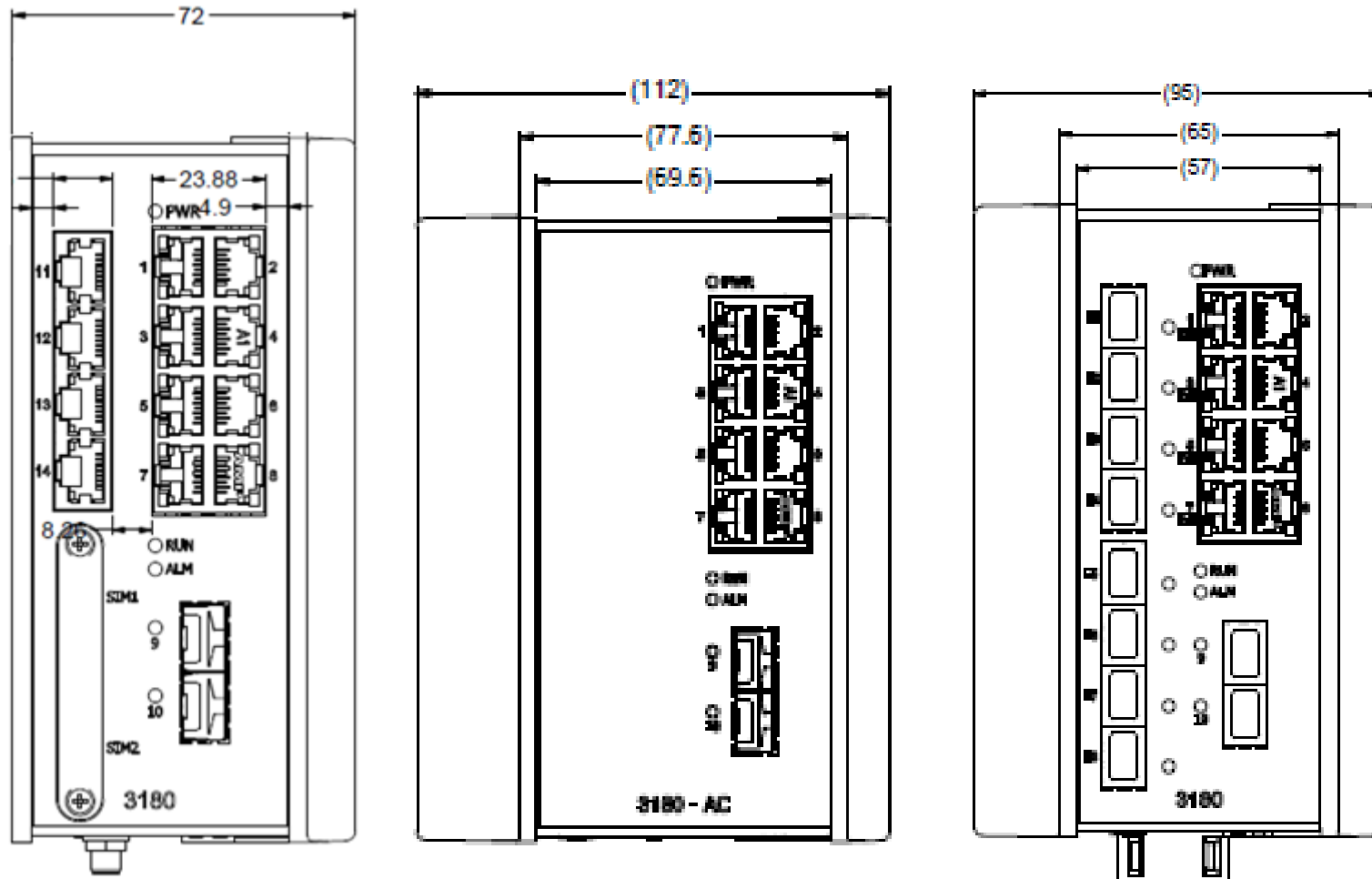


Access and Network Interfaces

RF-3180-[PS]-ET288/POE



Enhanced compact switch – 3180



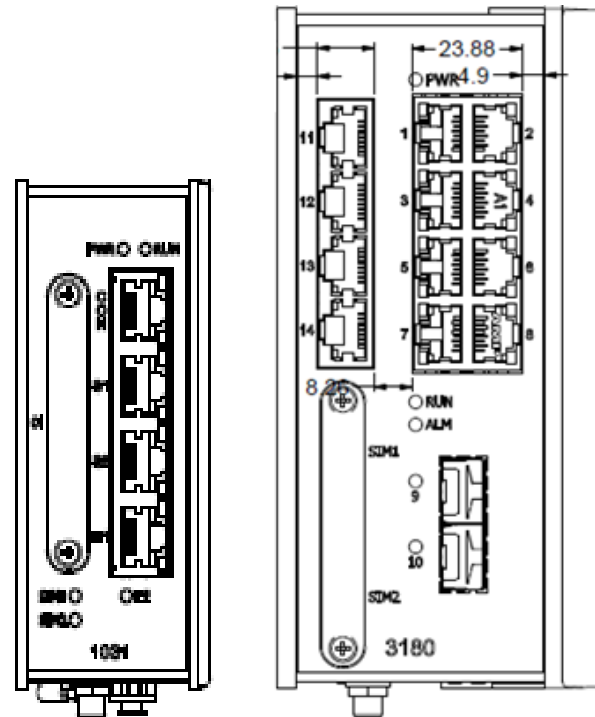
Secure Utility Gateway - 1031

- Launch planned R4.0 June 2014
- Interfaces
 - 1xETH 10/100BaseT
 - 1xETH100/1000 SFP (second phase)
 - 1xRS-232/RS-485 + 1xRS-232
 - Dual SIM 2G/3G Cellular modem
 - 2+2 Discrete I/O
- Dimensions (HxWxD) [mm] - 110x40x120



1031 vs. 3180

- -25% in height
- -38% in width

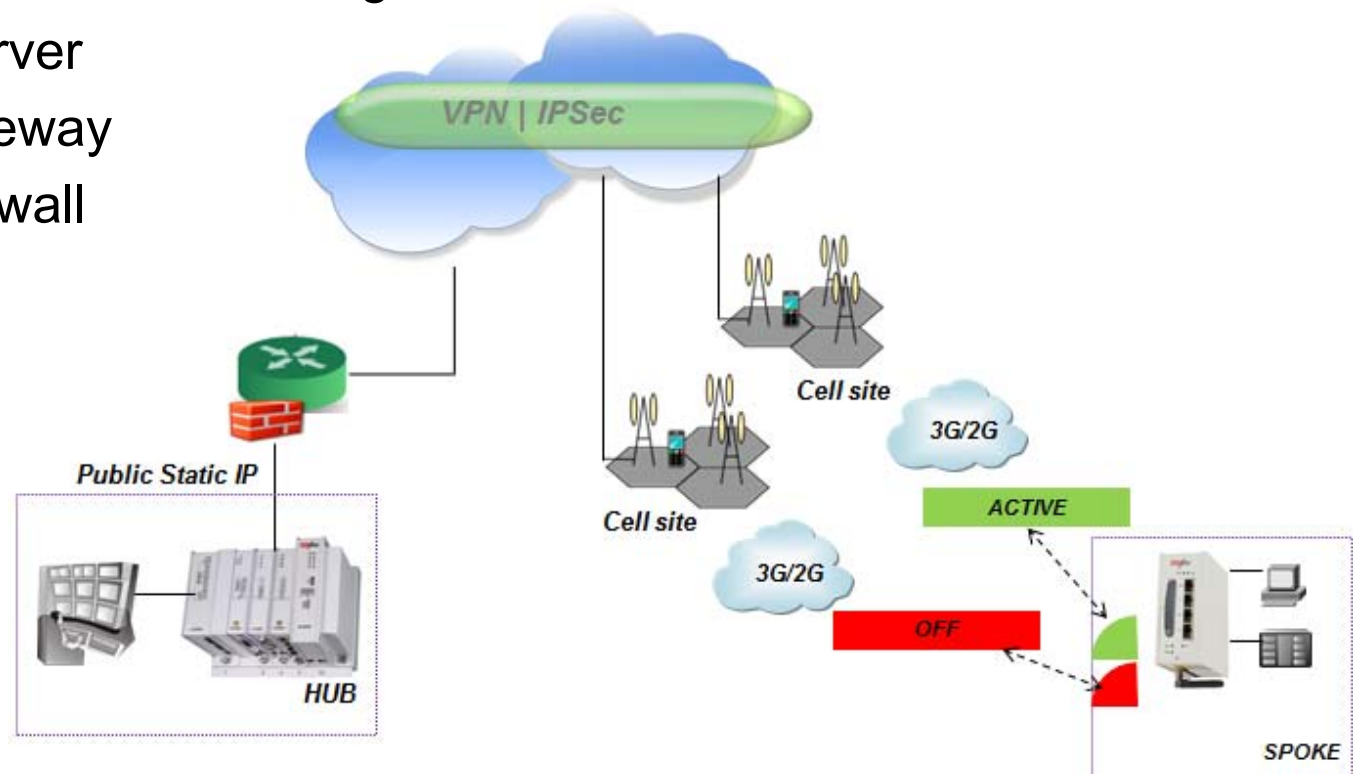


Secure Utility Gateway - 1031

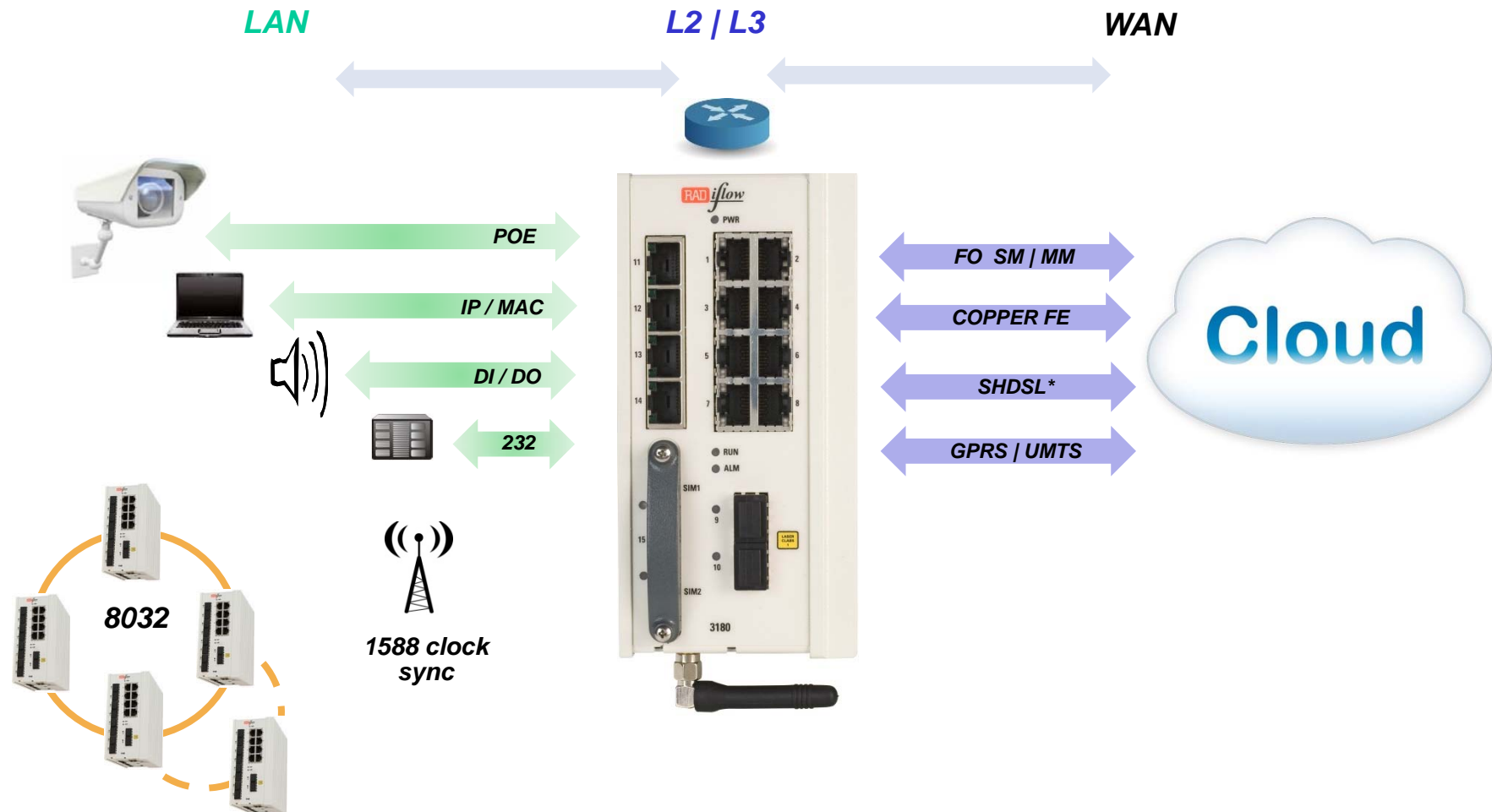


- Services

- Transparent Serial Tunneling
- Terminal Server
- SCADA Gateway
- SCADA Firewall
- L2 VPN
- L3 VPN
- IPSec
- NAT



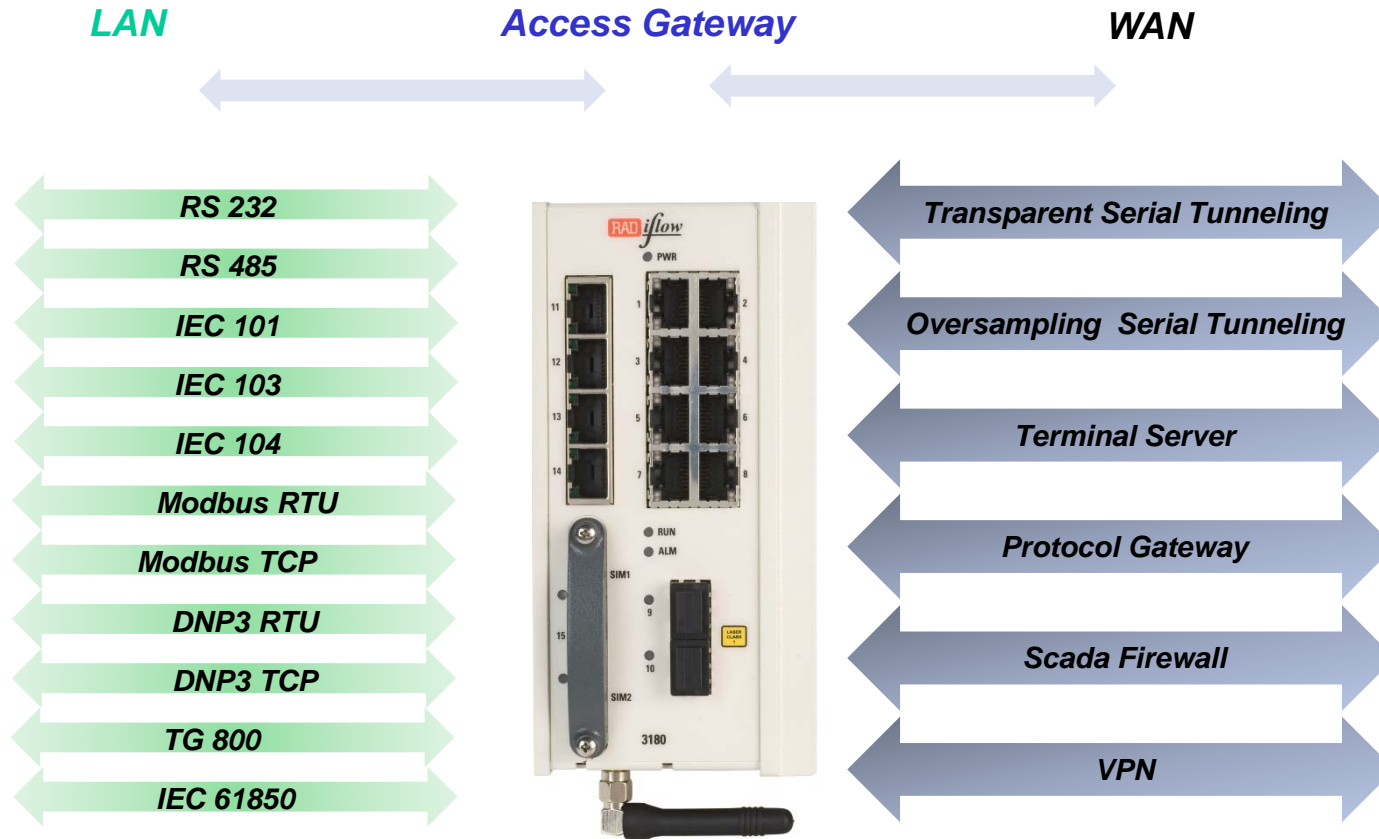
LAN Services



Networking - Comprehensive L2 /L3 Capabilities

- **Resilient networking**
 - xSTP
 - Ethernet Ring (Sub Ring)
 - LAG (LACP)
- **Quality of service**
 - Prioritization , shaping ,Scheduling
- **OAM**
 - EFM ,CFM
- **VLAN**
 - QinQ ,Private Vlan
- **DHCP Relay**
 - OPTION 82
- **IGMP snooping**
- **Port based network access control (802.1x)**
 - 802.1 PROXY
- **SNTP**
- **TFTP /SFTP**
- **SNMP**
- **Layer 3 dynamic Routing**
 - OSPF
 - RIP
 - VRRP
 - NAT*
- **Multi Access interfaces**
- **Extensive authentication**
 - Multi-level user access approvals
 - Radius & Tacacs+ servers
- **Port blocking**
- **MAC based port security**
- **SSHv2**

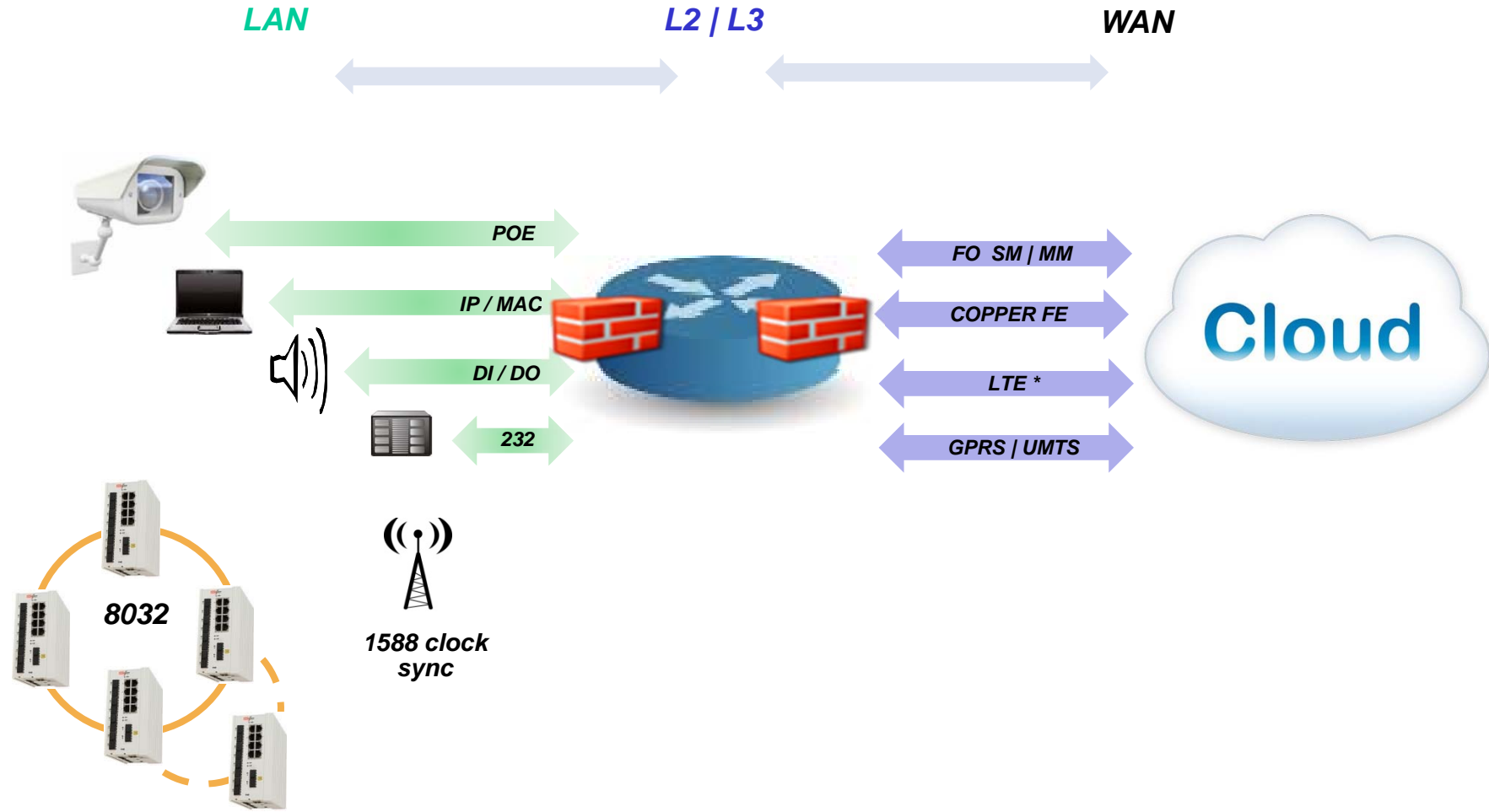
Access Gateway



Access Gateway

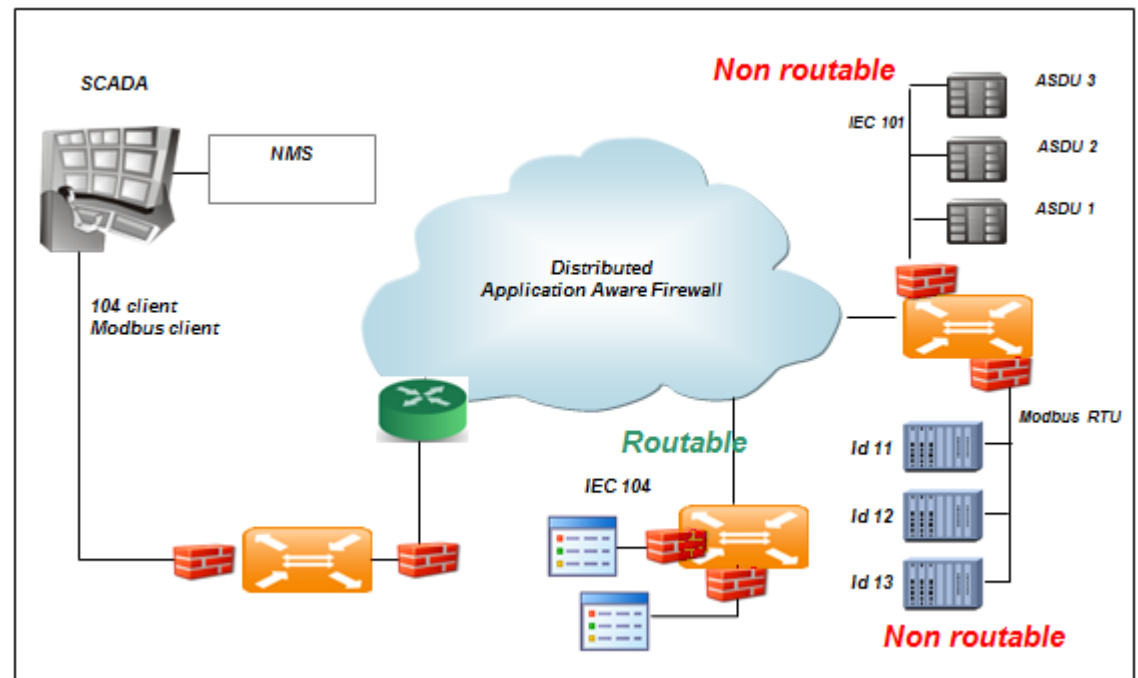
- IP Sec
- L2 VPN
- L3 Route based VPNs
- Firewall
 - IEC 104
 - DNP3
 - Modbus
- Serial Tunneling
- Terminal Server
- Gateway
 - 101/104
 - DNP3
- Cellular GPRS interface

LAN Services



Industrial Security Planning

- Access control
 - managing users and their roles
 - Mapping to services and devices
- Network types
 - Routable
 - Ethernet
 - IP
 - SCADA ICS
 - Non Routable
 - Serial field bus
 - SCADA protocols



Security Measures Supported

- Interfaces
 - FO ports : resiliency to tapping
 - Serial ports and services : less susceptible to sniffing
 - USB : file authentication to a designated node
- File transfer
 - SFTP
 - USB
 - Over a secure VPN
- Authentication
 - Local
 - Centralized

LAN Substation Services & Security

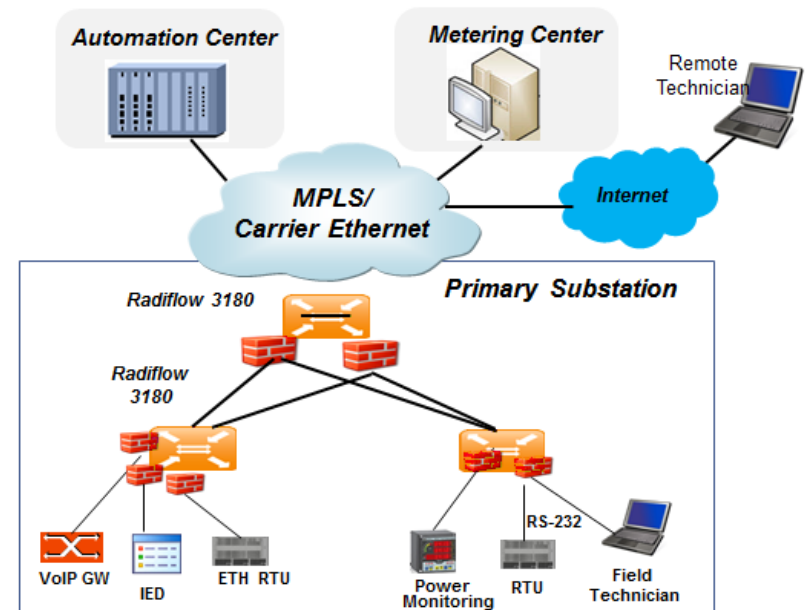
- Segmentation of the network
 - L2 vlan services.
 - L3 routing services
- Resiliency
 - G.8032 Fast recovery protocol
- SCADA protocol support
 - IEC 101/104
 - DNP3
 - MODBUS TCP
- In depth packet inspection Firewall on the Ethernet and Serial

LAN Substation Services & Security

- Legacy equipment migration to IP
 - Serial tunneling
 - Terminal server
 - Protocol gateway
 - Special modes to handle propriety protocols
 - Handling sensitivity to network latency
 - Serial RS 232 RS 485 ports

LAN Substation Services & Security

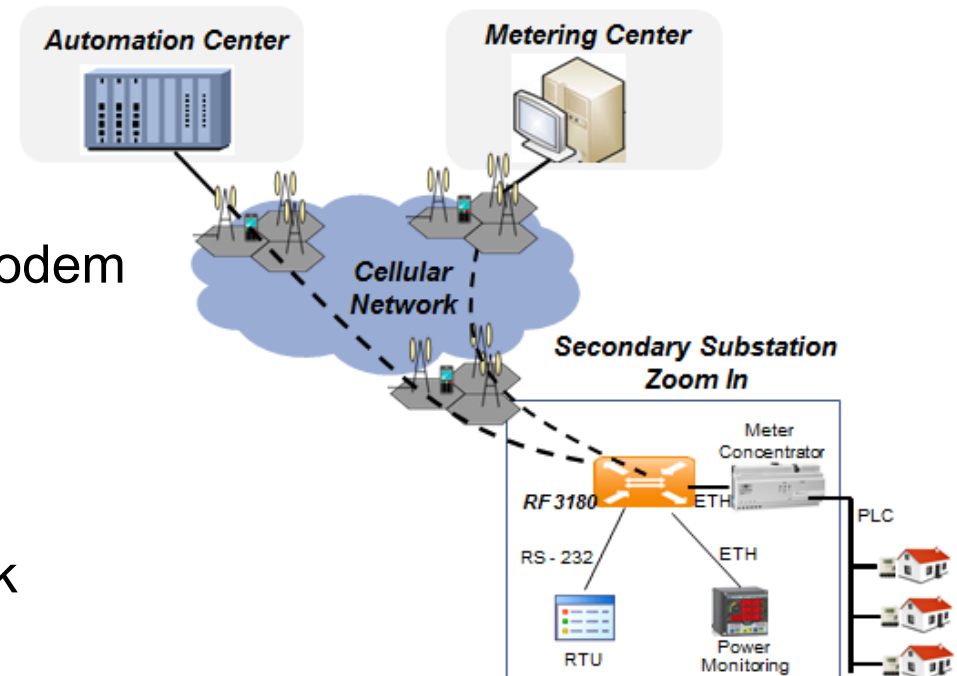
- Security
 - 802.1x
 - ACLs
 - Port based firewall
 - Service based policy
 - Port limit and shutdown
 - Port based Mac limit
- Physical security
 - Managing IP cameras using POE
 - Servicing Discrete channels of control /alarms /security /safety
- Logs ,alarms and notifications to northbound centralized management



WAN – Secure Networking of remote sites

The WAN connects the utility segments, including substations, Distributed energy resources (DER) and the control center and datacenter networks for utility operations.

- Physical requirement
 - Secure FO link
 - Backup option using cellular modem
- Traffic servicing QOS
 - prioritizing of traffic
 - Rate limit to protect the network
- NAT



WAN - Secure Networking of remote sites

- Segmentation of the network
 - L2 VPN : L2 services.
 - L3 VPN : L3 services
- Resiliency
 - Protection using layer 2 or 3 capacities
 - OSPF
 - xSTP
- Time synchronization services
 - 1588
 - NTP

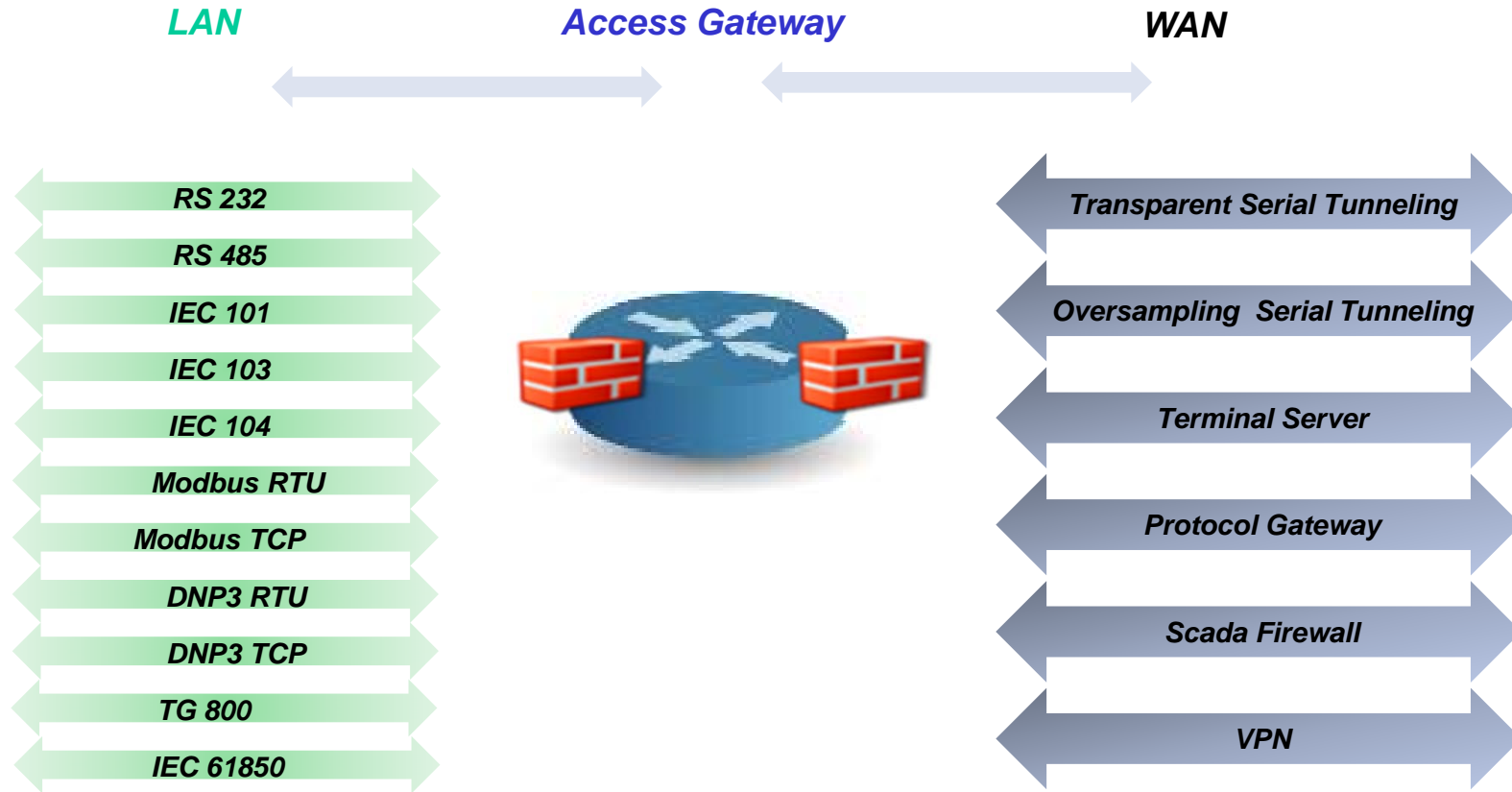
WAN - Networking of remote sites

- Security
 - Connect to Radius server , authentication / accounting
 - IPSec
 - User policy for traffic type
 - IKE, AES or 3DES encryptions
 - Dynamic key exchange
 - Secure remote access – reverse SSH tunnel
 - L2- L4 ACLs
- Reliable maintenance to the network switch /router connecting the remote site to the wan backbone
 - SFTP
 - SNMP
 - SSH

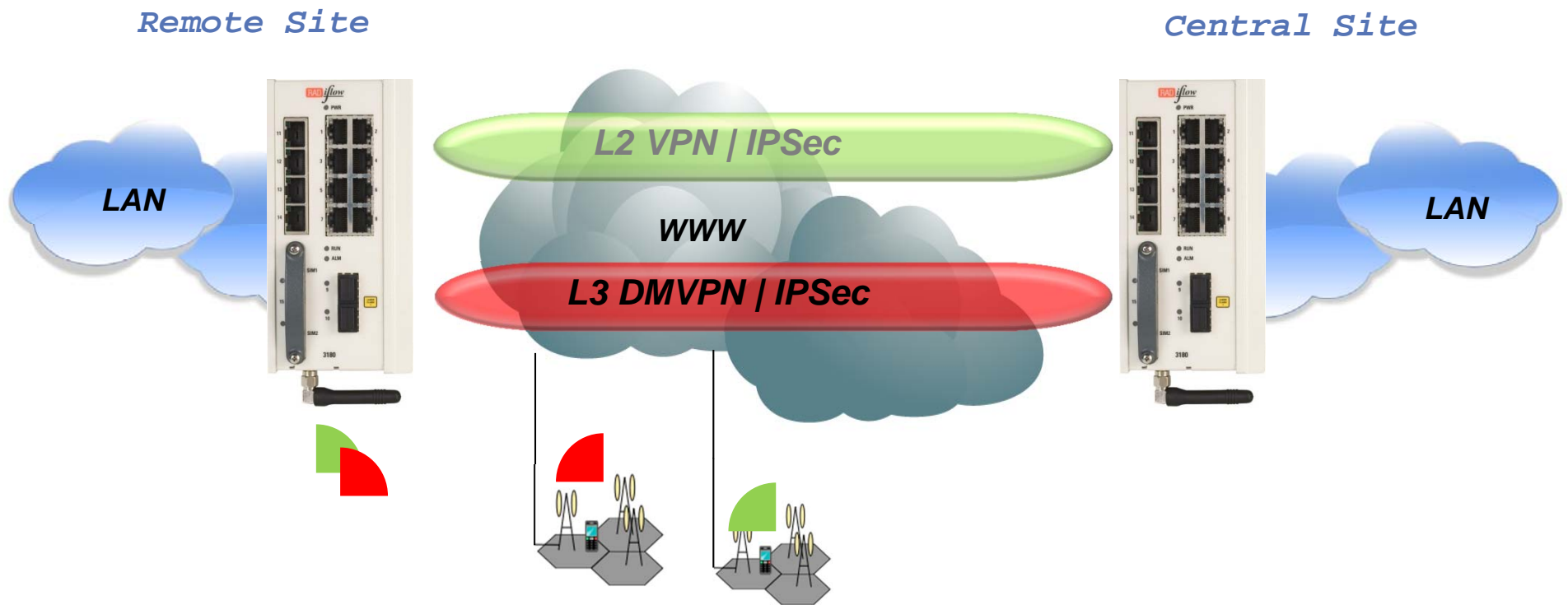
WAN - Secure Networking of remote sites

- SCADA protocol support
 - IEC 104
 - DNP3
 - MODBUS
- Firewall on the WAN port

LAN /WAN Services at a substation



WAN Services



L2 VPN

- GRE tunnel, layer 3 service, allowing L2 connectivity to end points



L3 VPN

- mGRE tunnels, layer 3 service, allowing L3 connectivity to end points



VPN

- The RADiFlow switches support such a VPN (Virtual Private Network) connection using GRE tunnels (RFC2 2784) over an IPSec encrypted link. The IPSec tunnel can use 3DES or AES encryption according to the user configuration.
- **Modes supported**
- With the RADiflow switches both L2 and L3 VPNs are supported.
- Both modes are based on GRE tunneling.
- Operational Modes:
 - L2 GRE VPN
 - L3 mGRE DM-VPN .route based
 - IPSec VPN. route based

IPSec

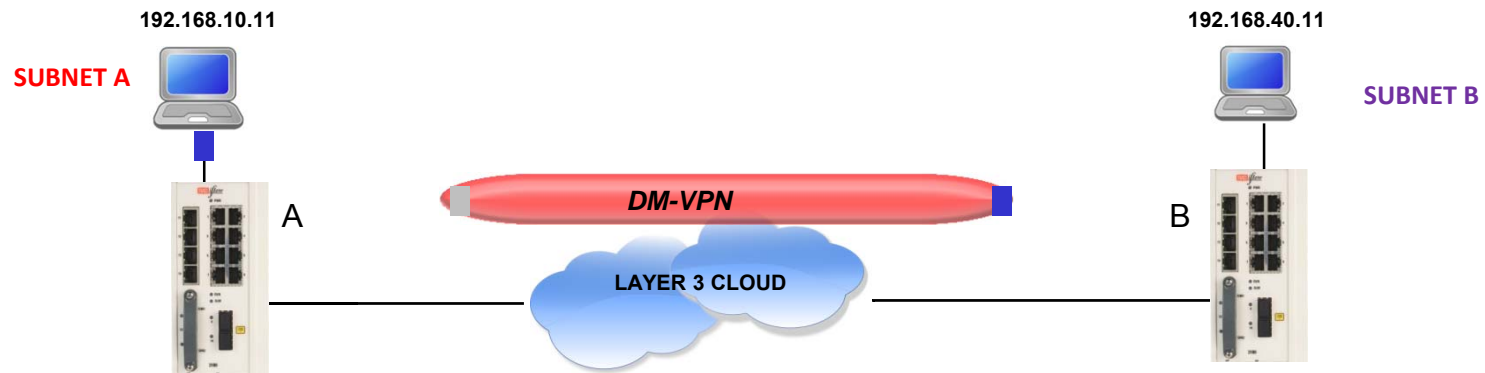
- Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and/or encrypting each IP packet of a communication session.

- **Applications**

IPSec should be configured when a VPN is used :

- DM-VPN : IPSec is mandatory.
- IPSec-VPN : IPSec is mandatory.
- L2-VPN :IPSec Mandatory when the VPN is established over the public network and /or when security is required.

L3 DM-VPN Concept



L2 VPN without IPSec

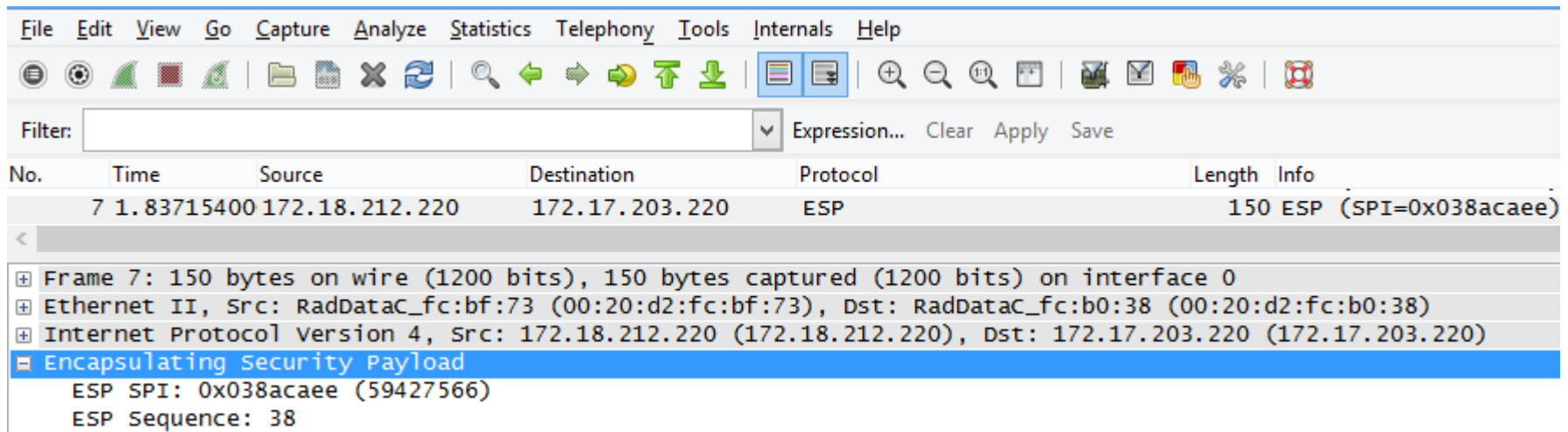
The screenshot shows the Wireshark interface with a packet capture of an ICMP Echo request. The packet list pane shows a single packet (No. 975) at time 43.8515280, source 192.168.0.101, and destination 192.168.0.102. The packet details pane is expanded to show the Generic Routing Encapsulation (GRE) header and the encapsulated ICMP Echo request.

No.	Time	Source	Destination	Protocol	Length	Info
975	43.8515280	192.168.0.101	192.168.0.102	ICMP	116	Echo (ping) request

Frame 975: 116 bytes on wire (928 bits), 116 bytes captured (928 bits) on interface 0

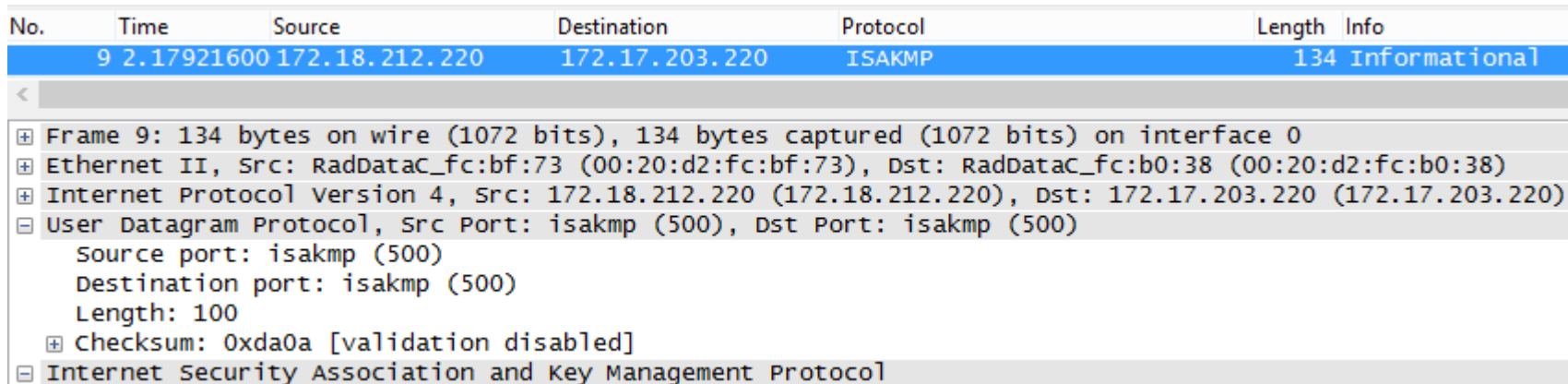
- Ethernet II, Src: RadDataC_fc:b0:38 (00:20:d2:fc:b0:38), Dst: RadDataC_fc:bf:73 (00:20:d2:fc:bf:73)
- Internet Protocol Version 4, Src: 172.17.203.220 (172.17.203.220), Dst: 172.18.212.220 (172.18.212.220)
- Generic Routing Encapsulation (Transparent Ethernet bridging)
 - Flags and Version: 0x0000
 - Protocol Type: Transparent Ethernet bridging (0x6558)
 - Ethernet II, Src: RadDataC_fc:b0:20 (00:20:d2:fc:b0:20), Dst: RadDataC_fc:bf:68 (00:20:d2:fc:bf:68)
 - 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 10
 - Internet Protocol Version 4, Src: 192.168.0.101 (192.168.0.101), Dst: 192.168.0.102 (192.168.0.102)
 - Internet Control Message Protocol
 - Type: 8 (Echo (ping) request)
 - Code: 0
 - Checksum: 0x9da4 [correct]
 - Identifier (BE): 0 (0x0000)
 - Identifier (LE): 0 (0x0000)
 - Sequence number (BE): 1 (0x0001)
 - Sequence number (LE): 256 (0x0100)
 - [\[Response frame: 976\]](#)
 - Data (32 bytes)

L2 VPN with IPSec



Wireshark interface showing a capture of an Encapsulating Security Payload (ESP) packet. The packet list shows a single entry for frame 7, which is 150 bytes long and of type ESP. The packet details pane shows the following structure:

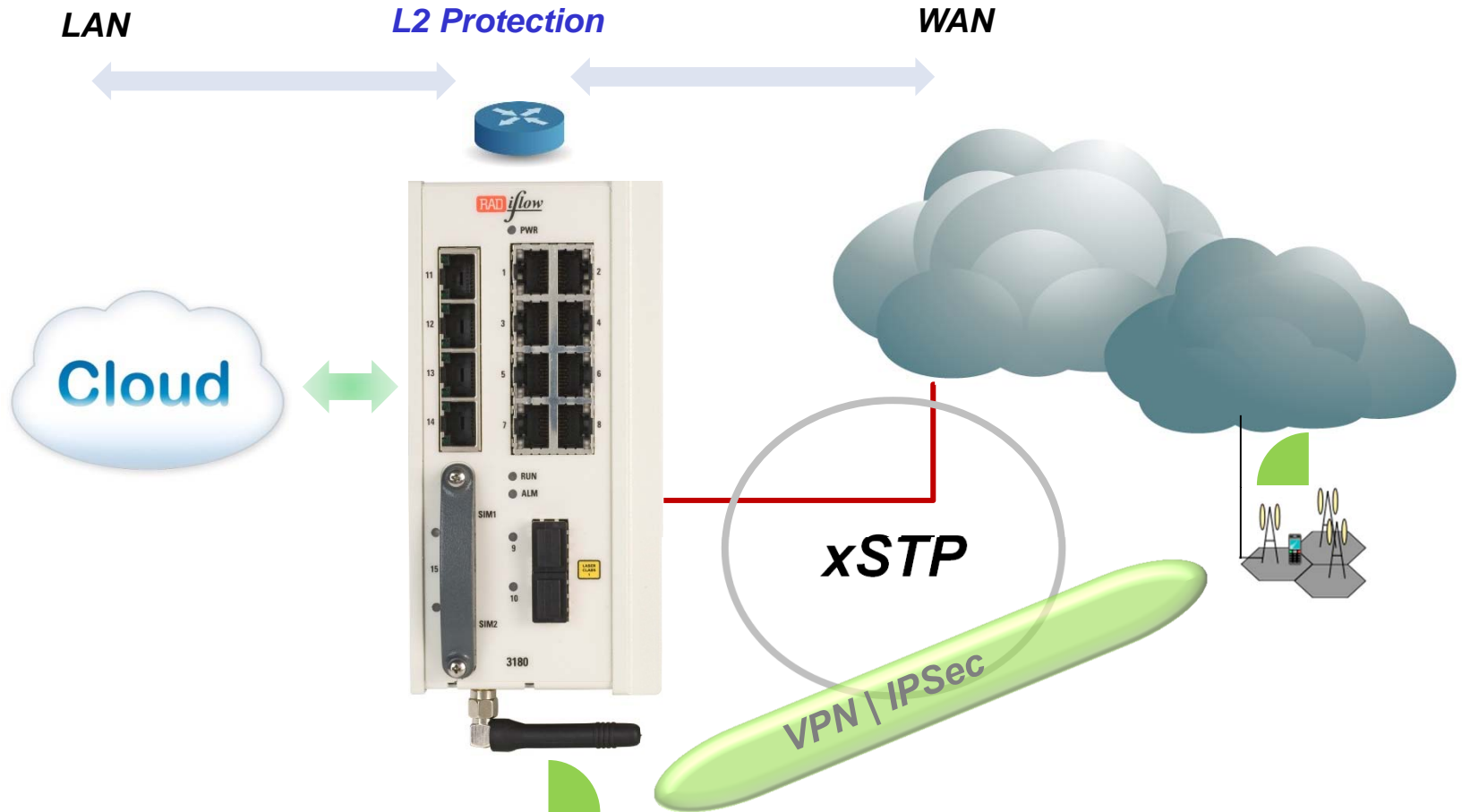
- Frame 7: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on interface 0
- Ethernet II, Src: RadDataC_fc:bf:73 (00:20:d2:fc:bf:73), Dst: RadDataC_fc:b0:38 (00:20:d2:fc:b0:38)
- Internet Protocol Version 4, Src: 172.18.212.220 (172.18.212.220), Dst: 172.17.203.220 (172.17.203.220)
- Encapsulating Security Payload
 - ESP SPI: 0x038acae (59427566)
 - ESP Sequence: 38



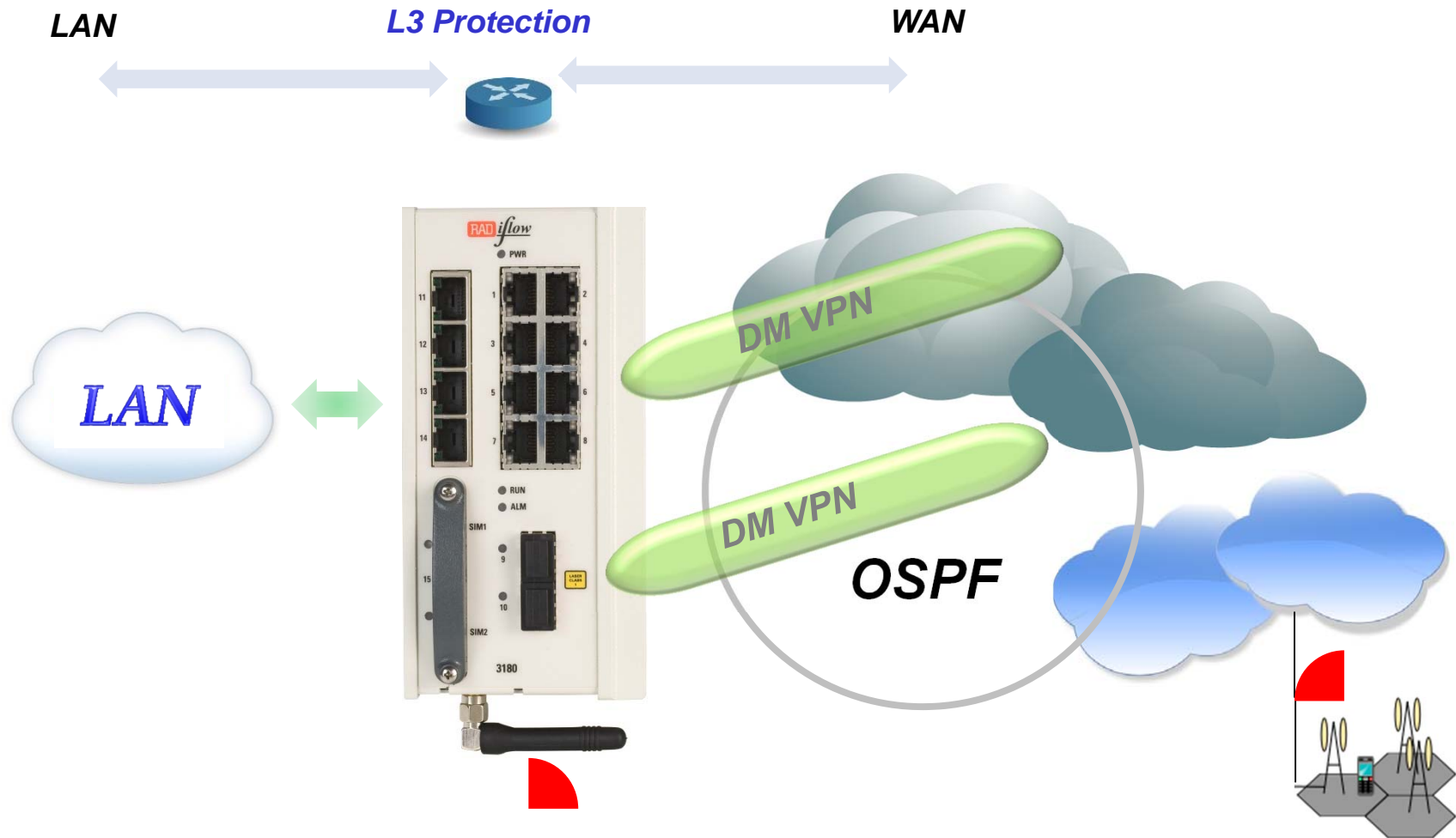
Wireshark interface showing a capture of an Internet Security Association and Key Management Protocol (ISAKMP) packet. The packet list shows a single entry for frame 9, which is 134 bytes long and of type ISAKMP. The packet details pane shows the following structure:

- Frame 9: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface 0
- Ethernet II, Src: RadDataC_fc:bf:73 (00:20:d2:fc:bf:73), Dst: RadDataC_fc:b0:38 (00:20:d2:fc:b0:38)
- Internet Protocol Version 4, Src: 172.18.212.220 (172.18.212.220), Dst: 172.17.203.220 (172.17.203.220)
- User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
 - Source port: isakmp (500)
 - Destination port: isakmp (500)
 - Length: 100
 - Checksum: 0xda0a [validation disabled]
- Internet Security Association and Key Management Protocol

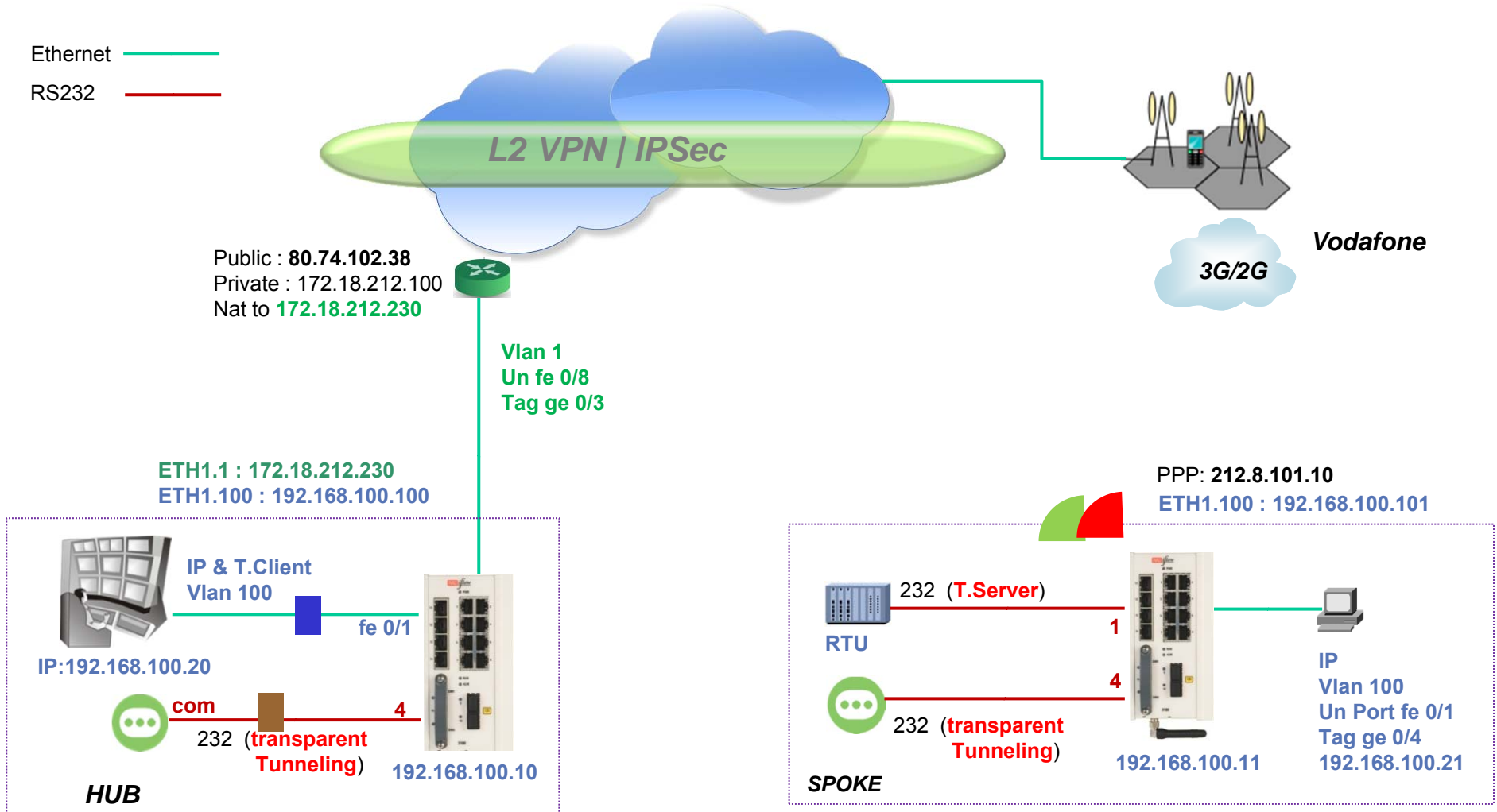
WAN Services



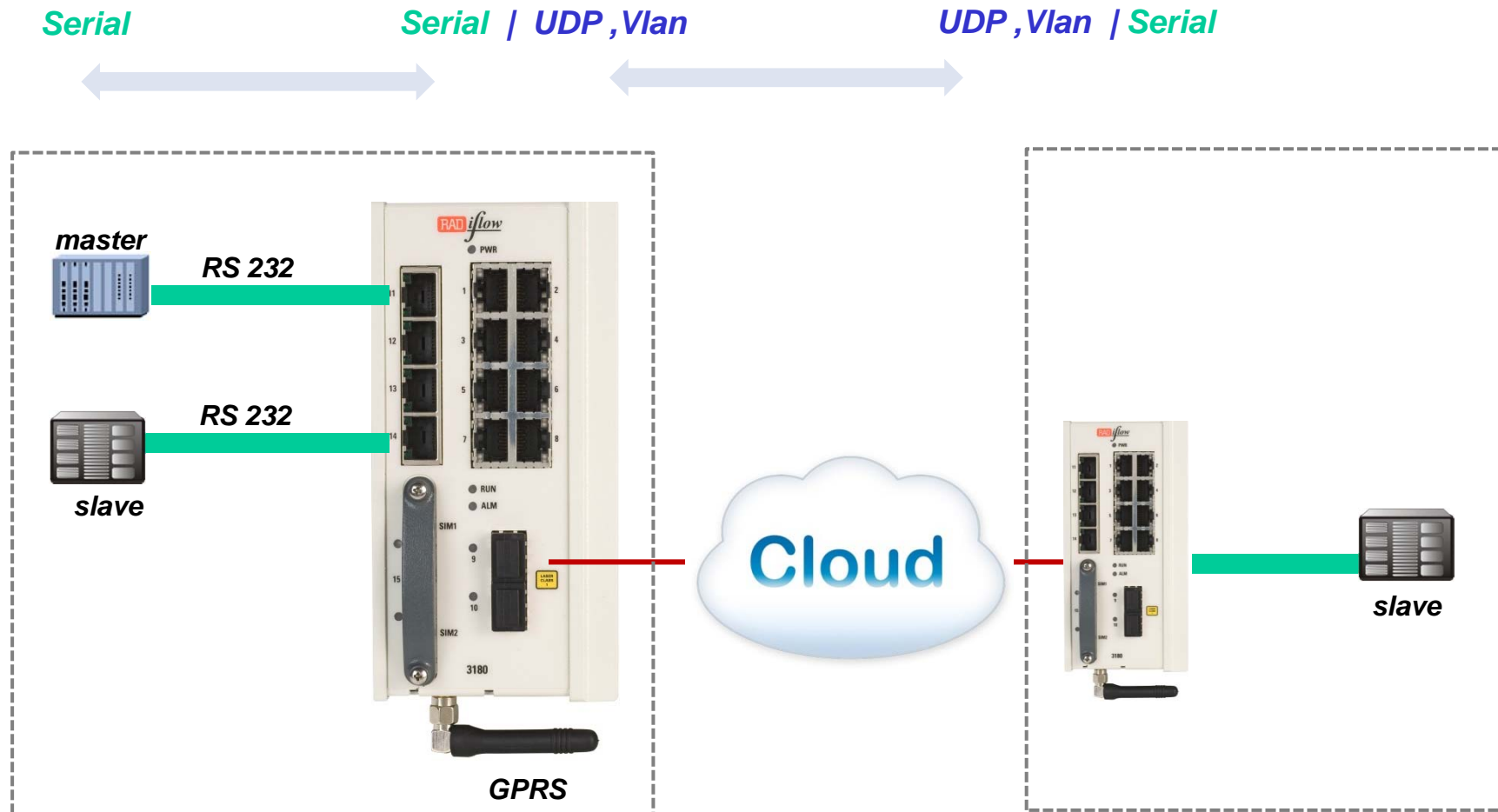
WAN Services



GPRS/UMTS : Example L2 VPN Setup

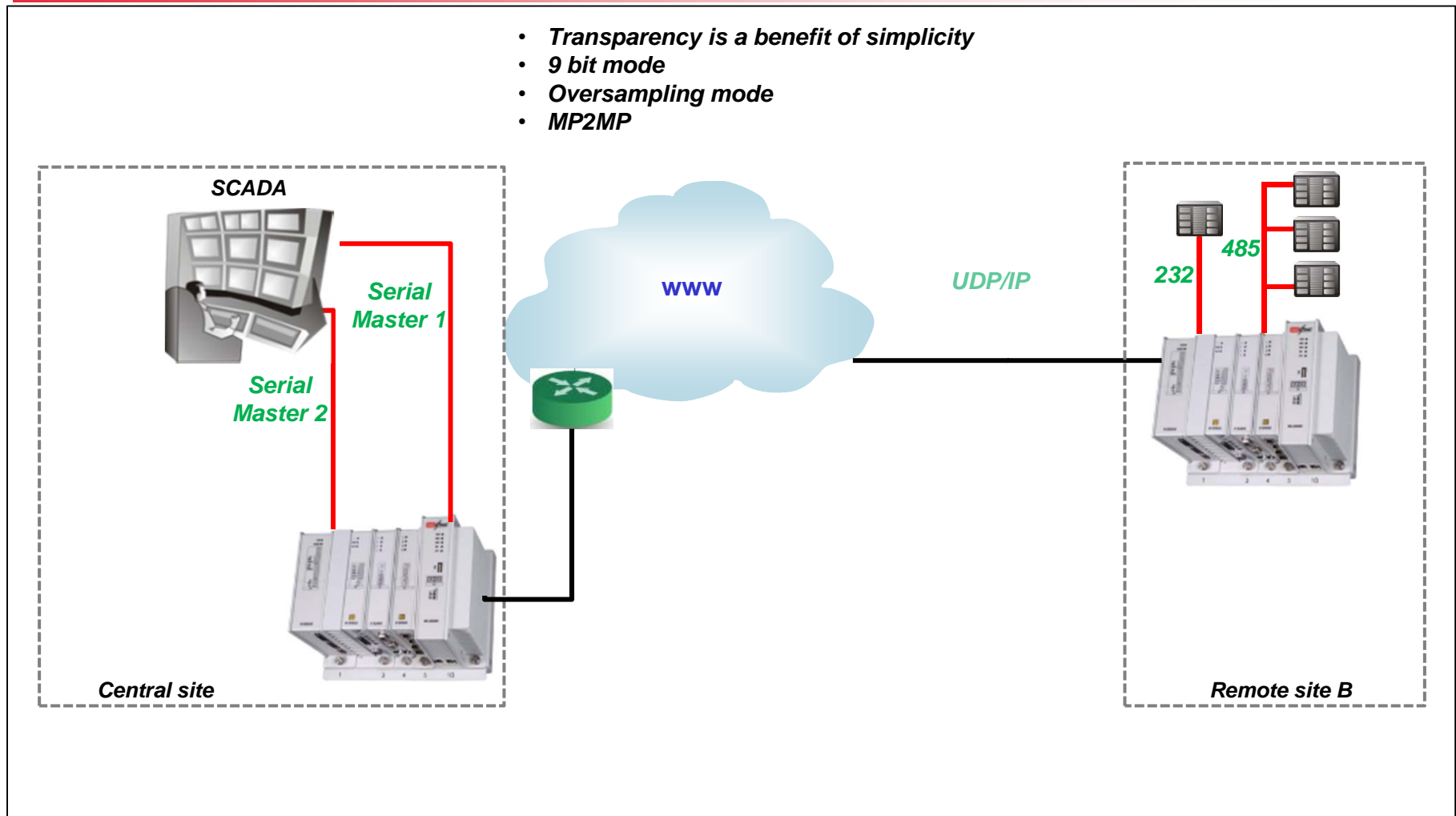


Transparent Serial Tunneling

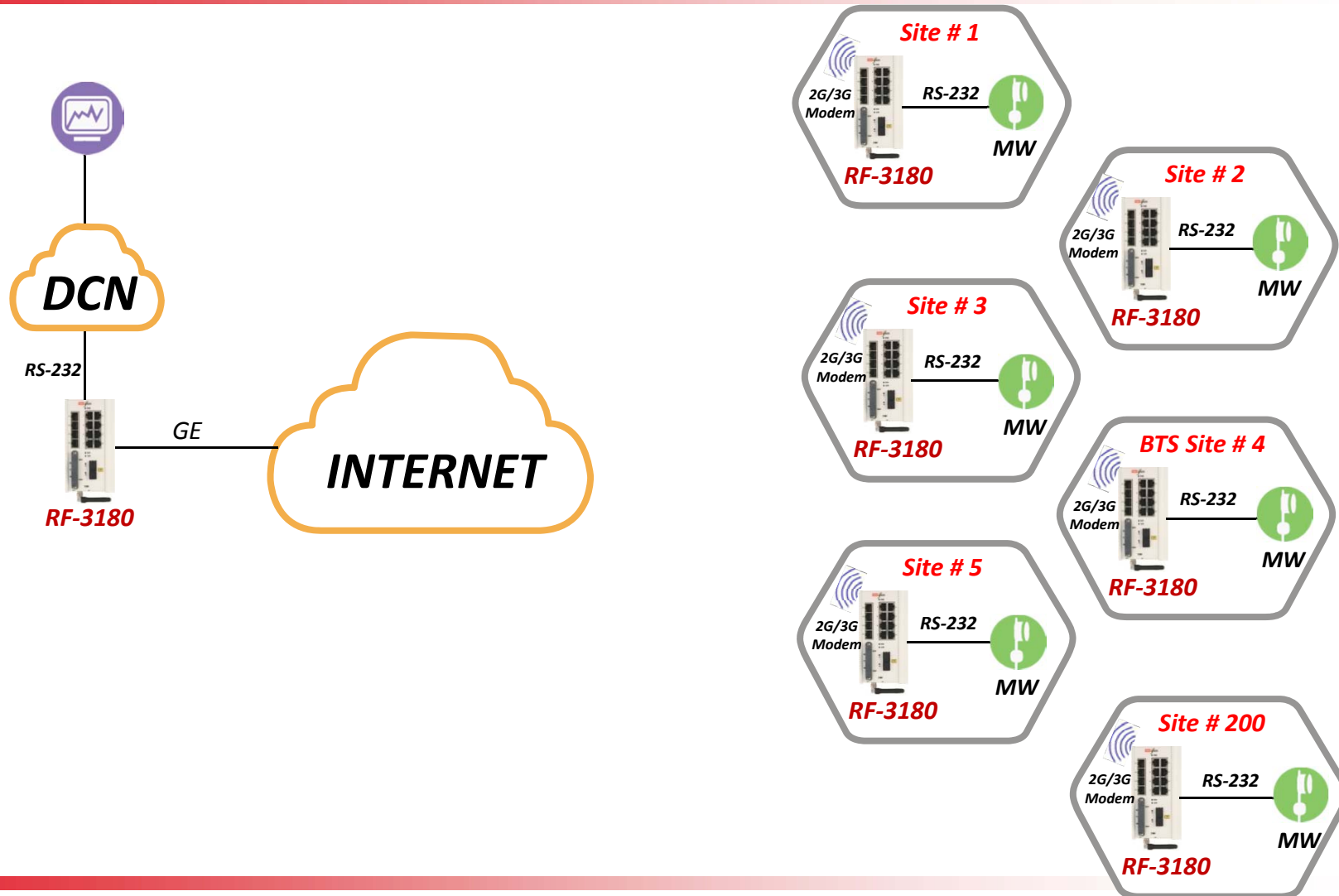


Transparent Serial Tunneling

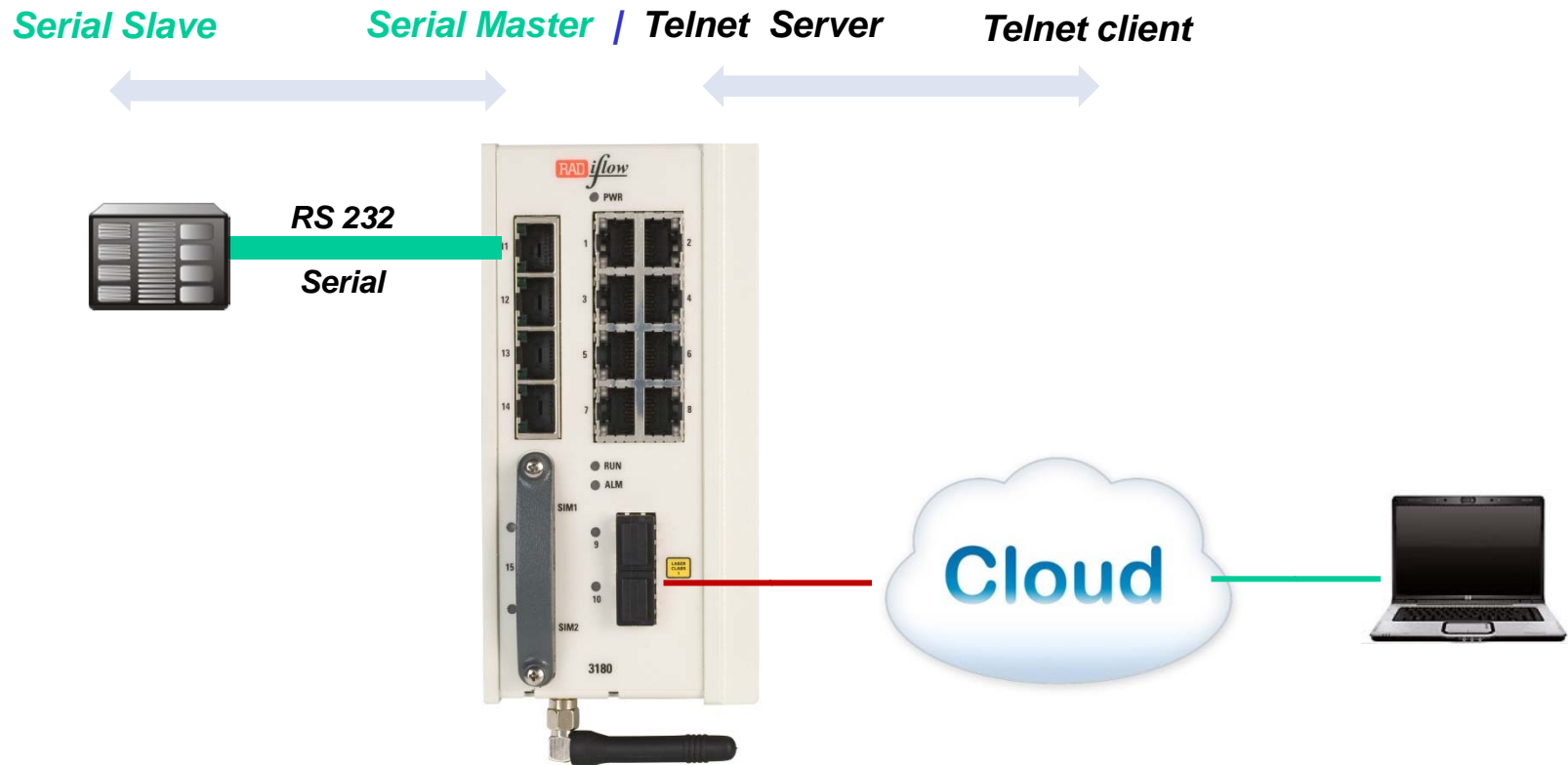
- *Transparency is a benefit of simplicity*
- *9 bit mode*
- *Oversampling mode*
- *MP2MP*



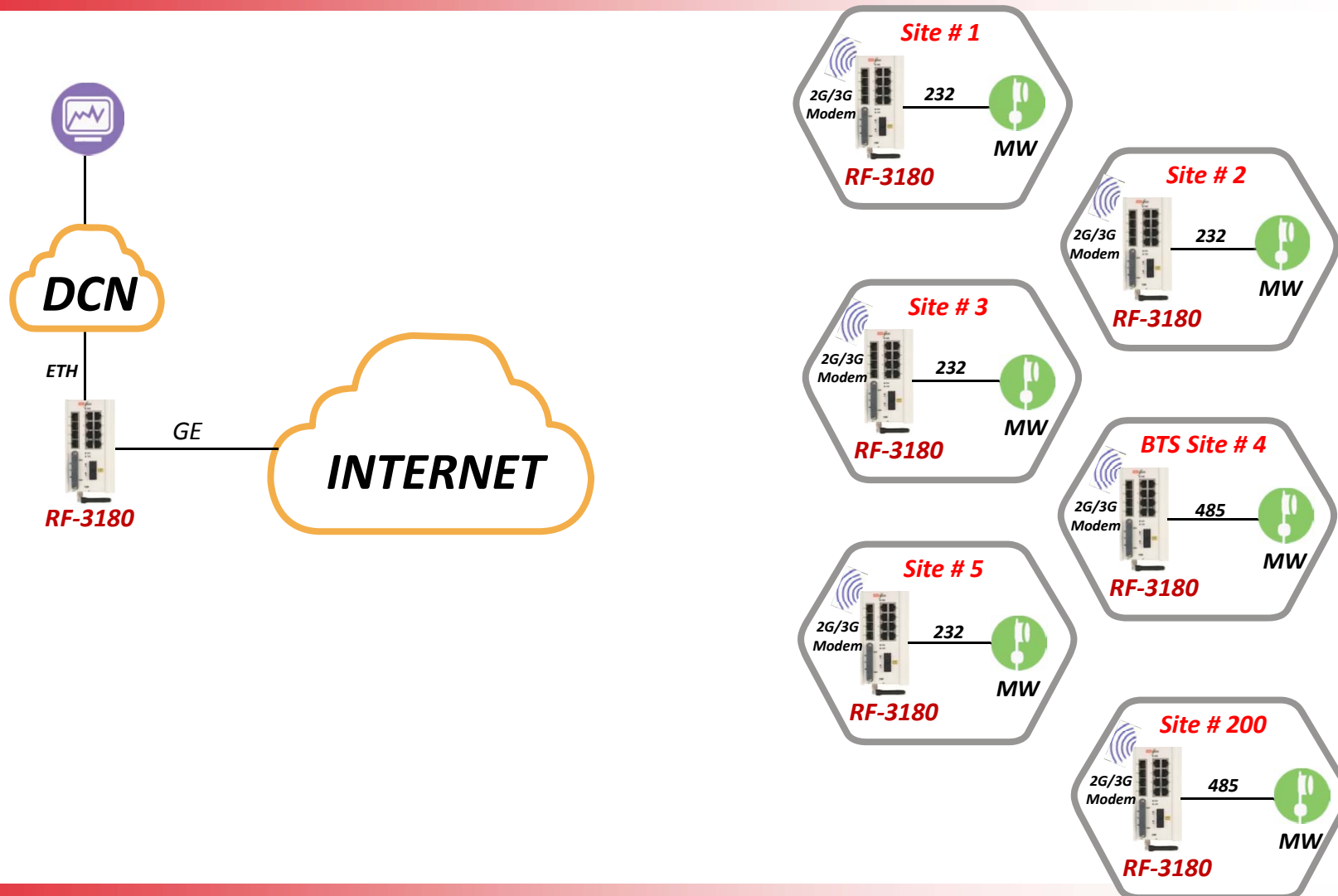
Transparent Serial Tunneling



Terminal Server

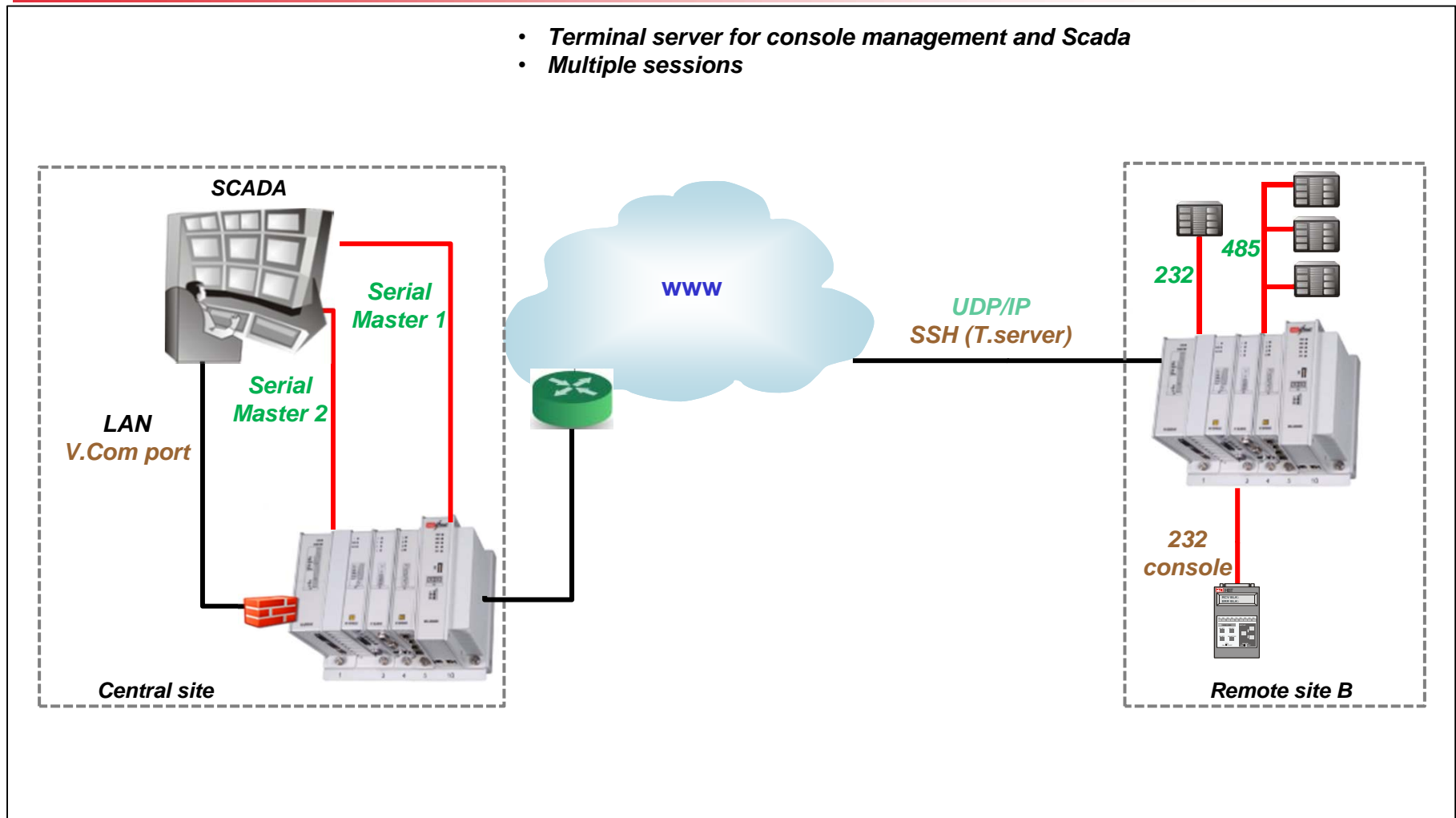


Terminal Server



Terminal Server

- Terminal server for console management and Scada
- Multiple sessions



Protocol Gateway

IEC 101 Slave *IEC 101 Master | IEC 104 Server* *IEC 104 client*



RTU

RS 232
IEC 101



IEC 104

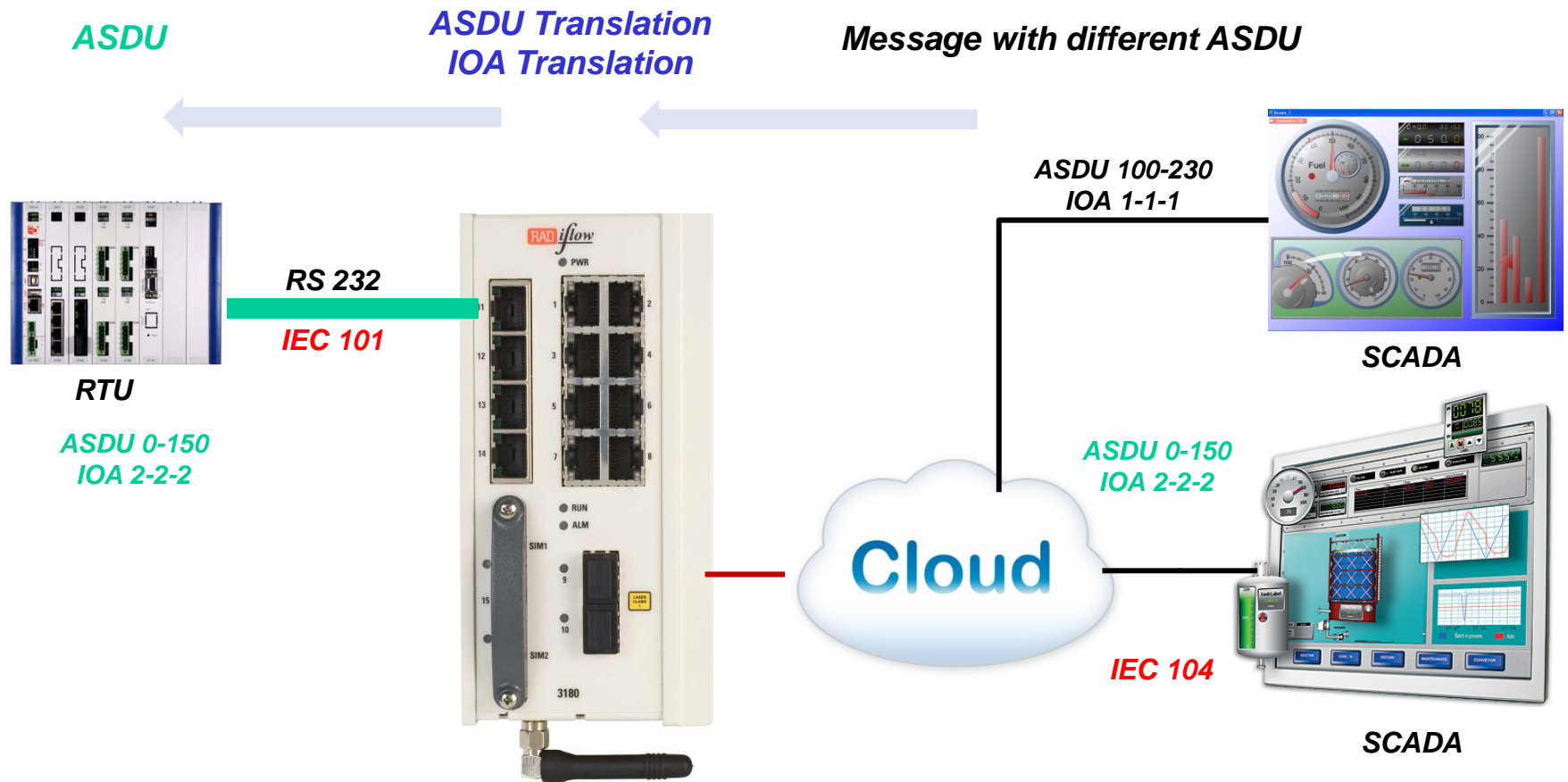


SCADA

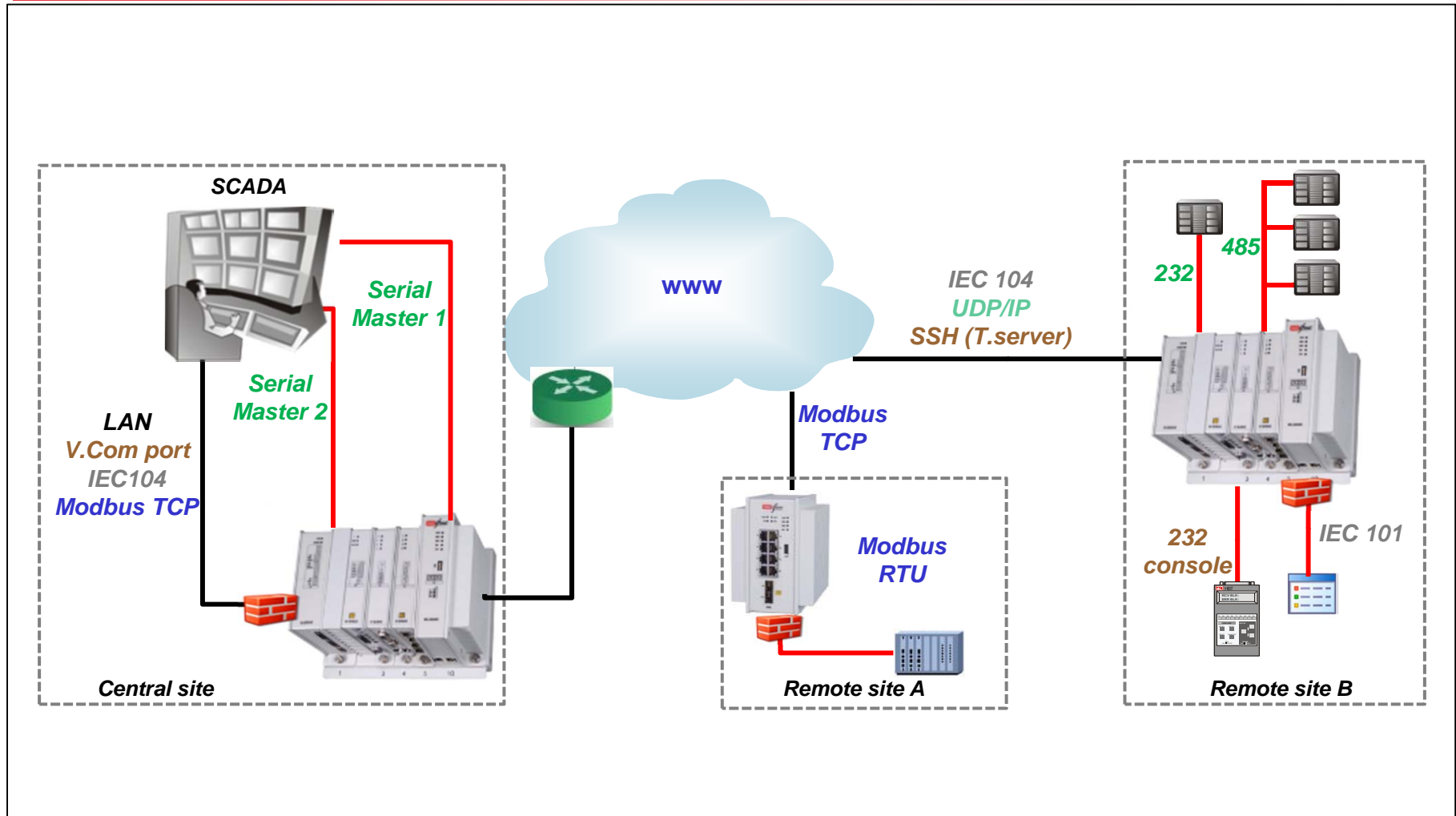
101 properties are configurable :

- **LA**
- **CA**
- **Address Length**
- **Single Char**
- **Direction bit**
- **Balanced**
- **Unbalanced**
- ..
- ..

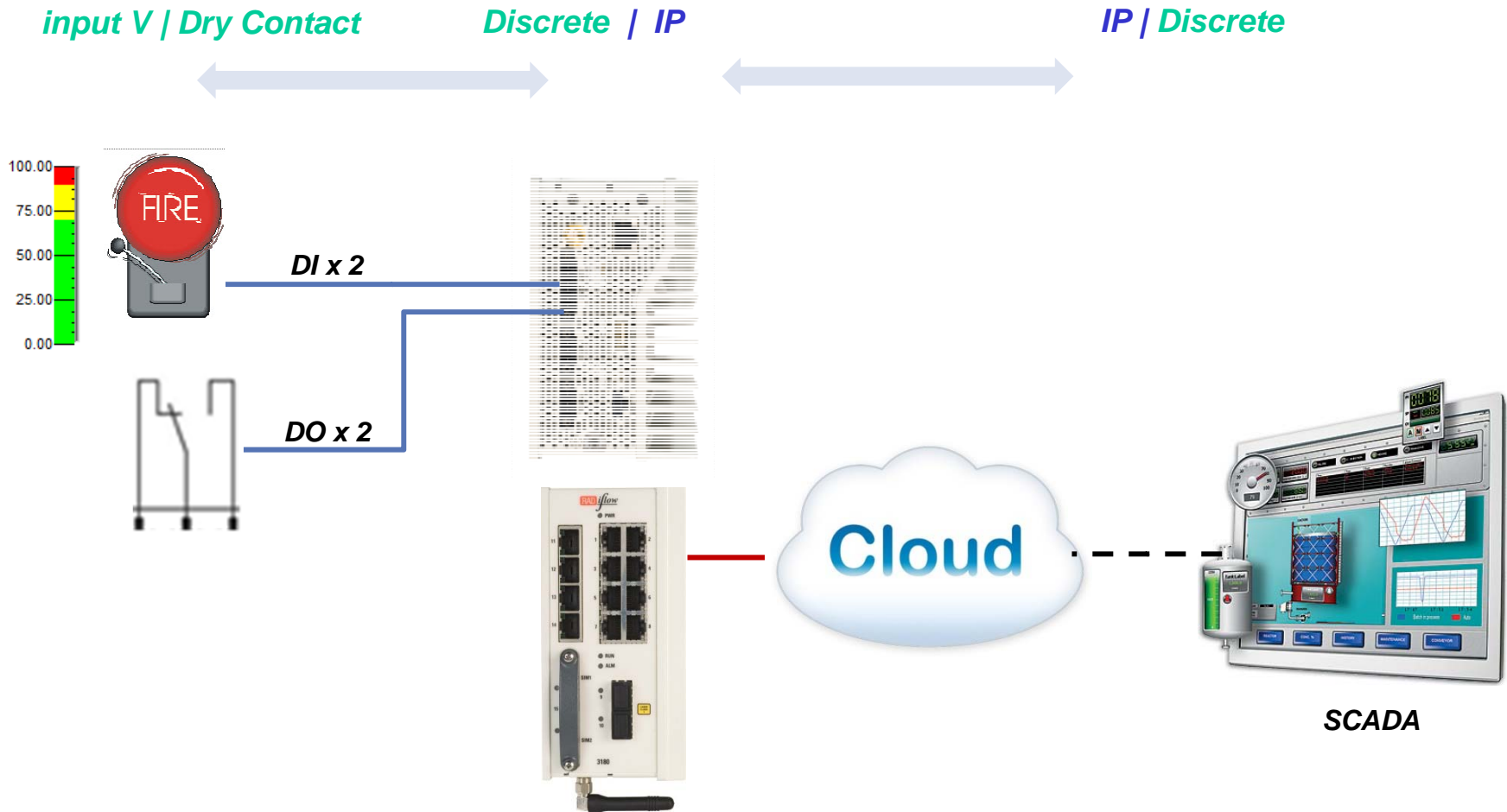
Protocol Gateway



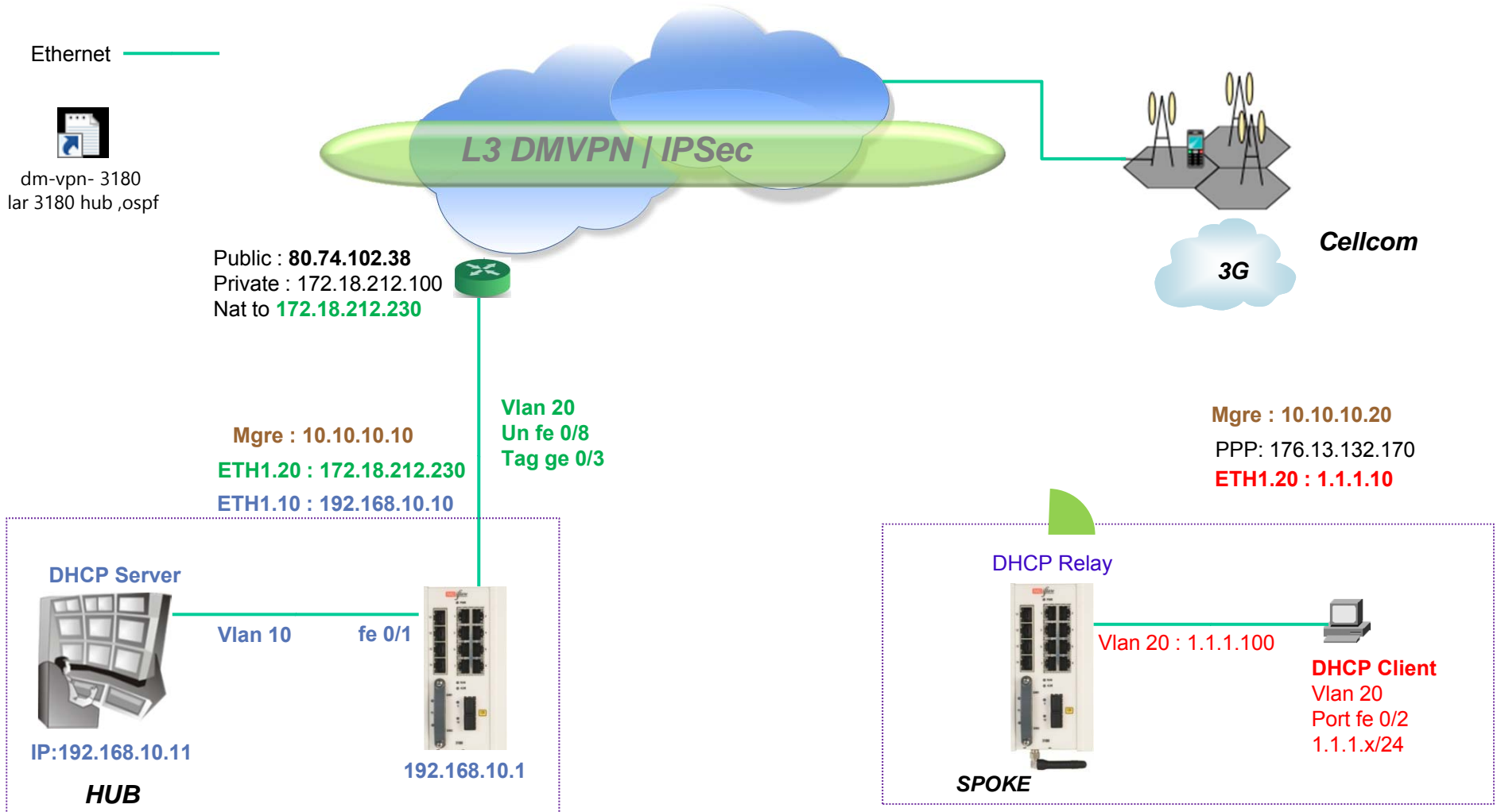
Protocol Gateway



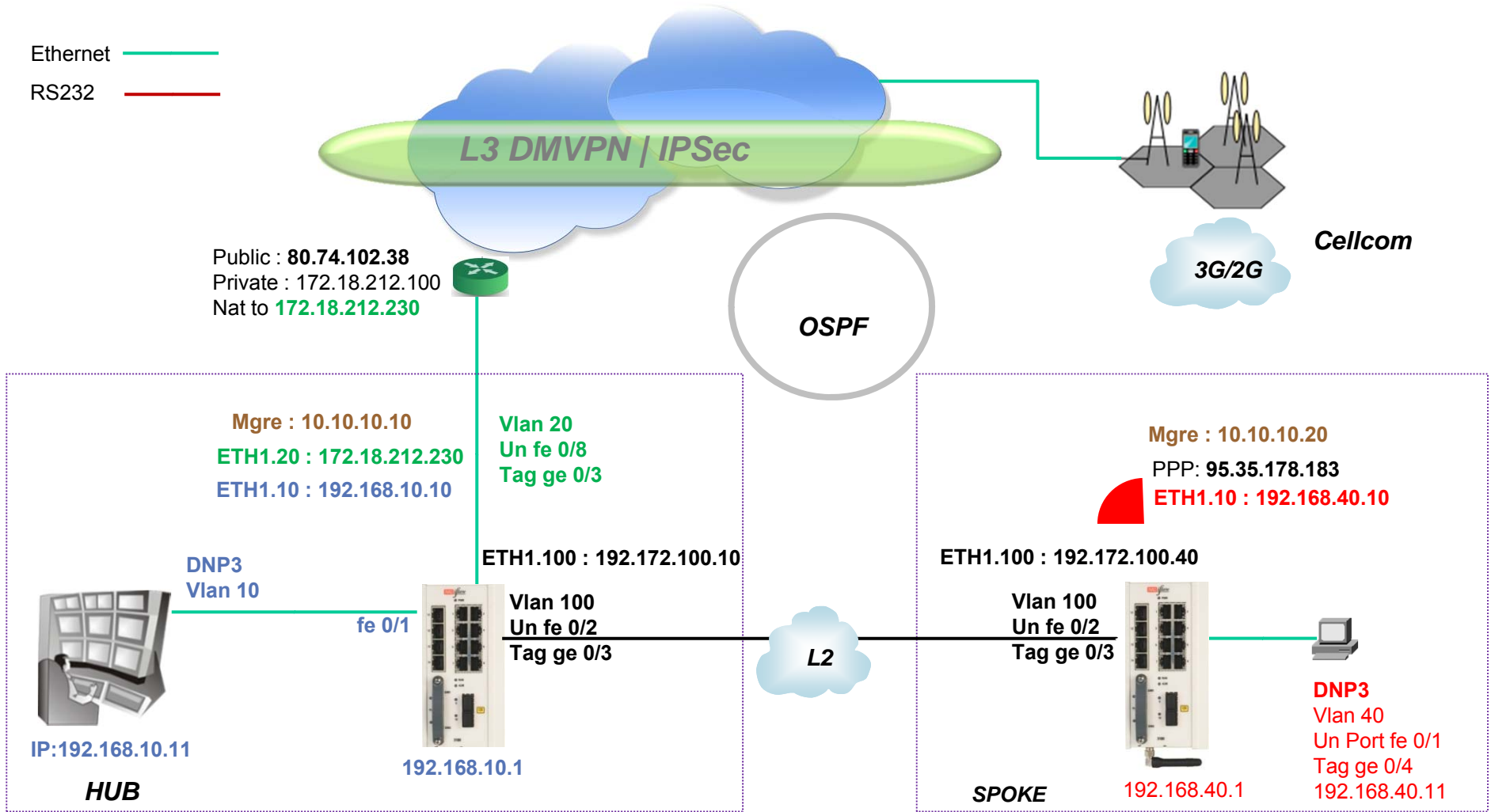
Discrete IO



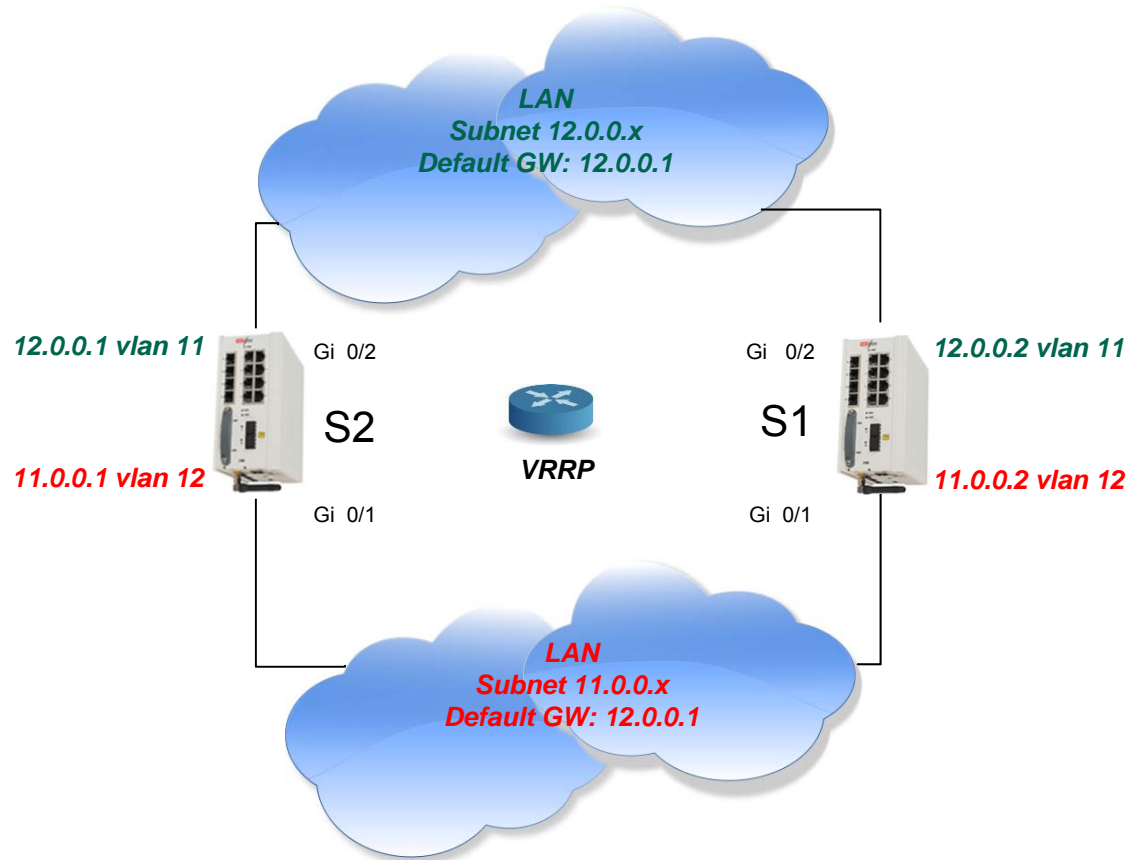
Cellular L3 DMVPN with DHCP Relay



L3 DMVPN , OSPF protection to LAN



VRRP Example



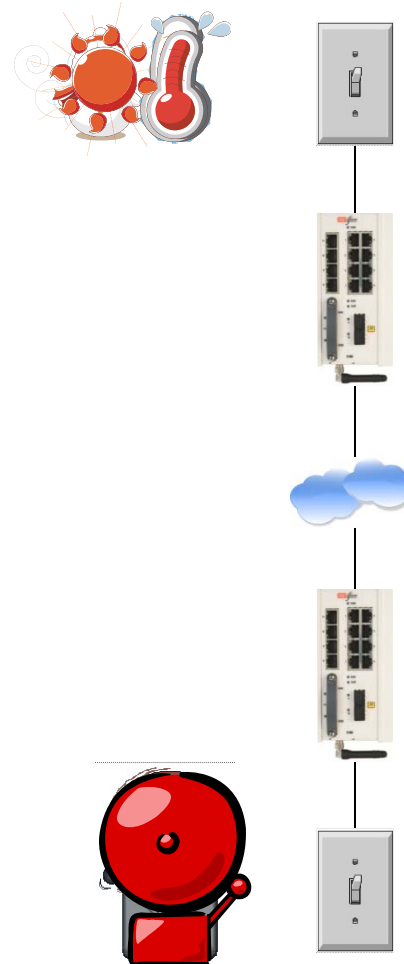
VRRP 2x3180 S1.txt (Command Line)



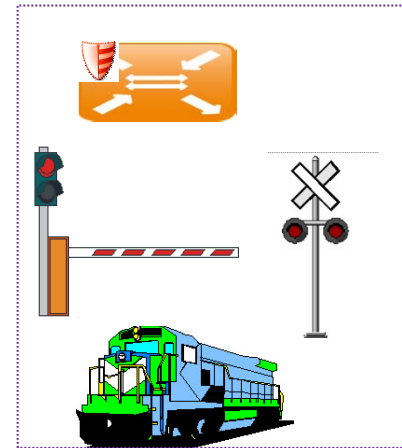
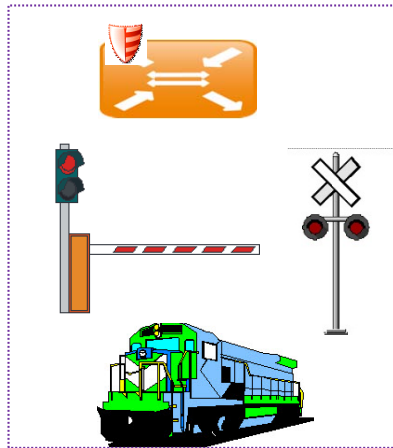
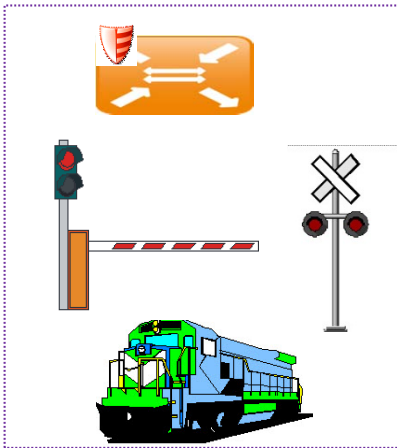
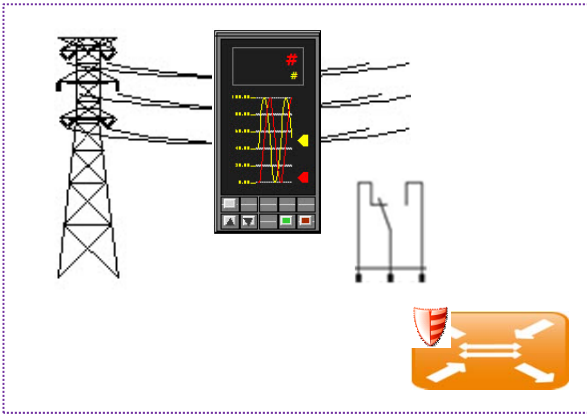
VRRP 2x3180 S2.txt (Command Line)

Discrete IO*

- Digital Input and Outputs are of common use to indicate status of a sensor reading ,security alarm ,safety notice and more.
- Areas of applications are endless.
- The digital status of discrete input at site A will be monitored and mirrored as relay switching output at site B.
- The traffic can be protected using IPsec to make sure the command originated from a valid source.

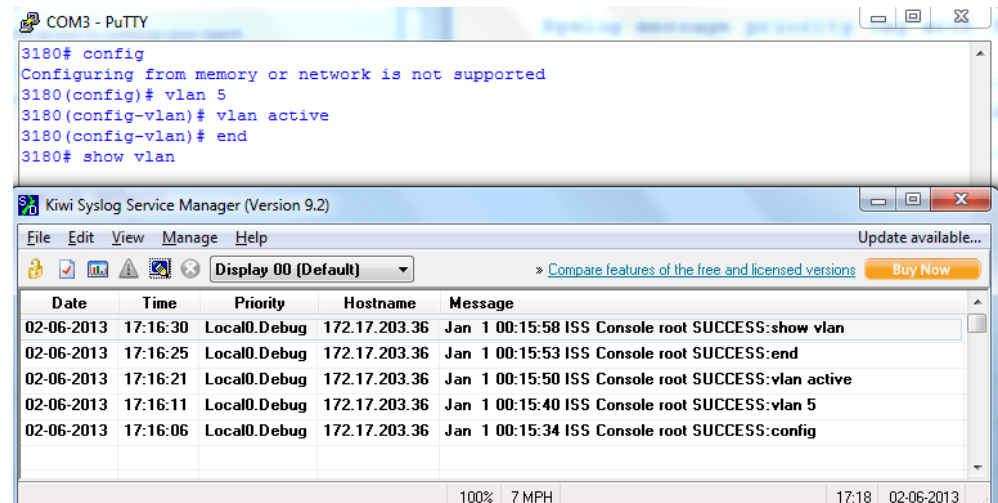


Discrete IO – Transportation



Monitoring and Diagnostics

- Leds
 - Serial ,Ethernet ,Power ,Cellular
- Counters
 - Serial ports , Ethernet ports ,Tunnels
- RMON statistics
- Port Mirroring
- Relay Alarm notifications
- SNMP traps
- Syslog



The screenshot shows two windows. The top window is a PuTTY terminal titled 'COM3 - PuTTY' showing the following commands and output:

```
3180# config
Configuring from memory or network is not supported
3180(config)# vlan 5
3180(config-vlan)# vlan active
3180(config-vlan)# end
3180# show vlan
```

The bottom window is 'Kiwi Syslog Service Manager (Version 9.2)'. It displays a table of syslog messages:

Date	Time	Priority	Hostname	Message
02-06-2013	17:16:30	Local0.Debug	172.17.203.36	Jan 1 00:15:58 ISS Console root SUCCESS:show vlan
02-06-2013	17:16:25	Local0.Debug	172.17.203.36	Jan 1 00:15:53 ISS Console root SUCCESS:end
02-06-2013	17:16:21	Local0.Debug	172.17.203.36	Jan 1 00:15:50 ISS Console root SUCCESS:vlan active
02-06-2013	17:16:11	Local0.Debug	172.17.203.36	Jan 1 00:15:40 ISS Console root SUCCESS:vlan 5
02-06-2013	17:16:06	Local0.Debug	172.17.203.36	Jan 1 00:15:34 ISS Console root SUCCESS:config

Monitoring and Diagnostics

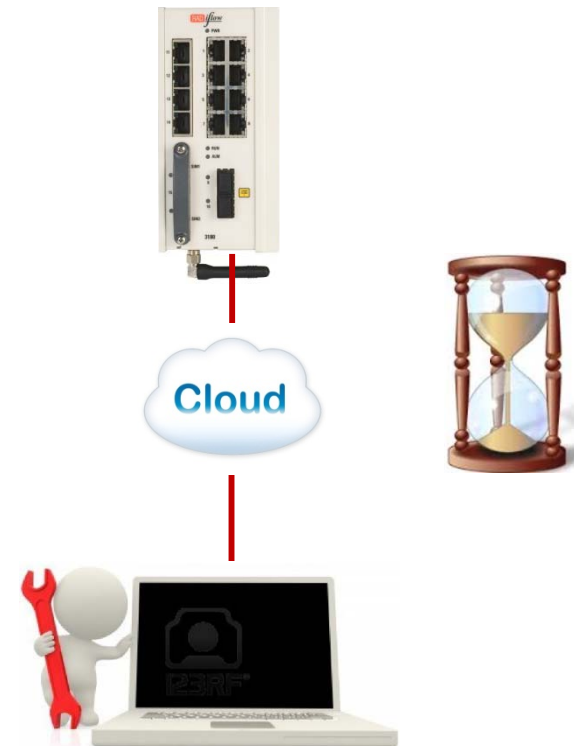
- Time conditioned system reload
- Cellular modem state conditions reload
- Tracking of IEC 101 state
- Tracking of SIM card state
- Logs export ,ad-hoc and time conditioned
- Serial control process reload upon failure
- Capture of Ethernet service traffic
- Debug Logging
- DDM (digital diagnostics monitoring)

Time conditioned system reload

- Set a time conditioned system reload to recover remote session
- Uncommitted changes are not preserved

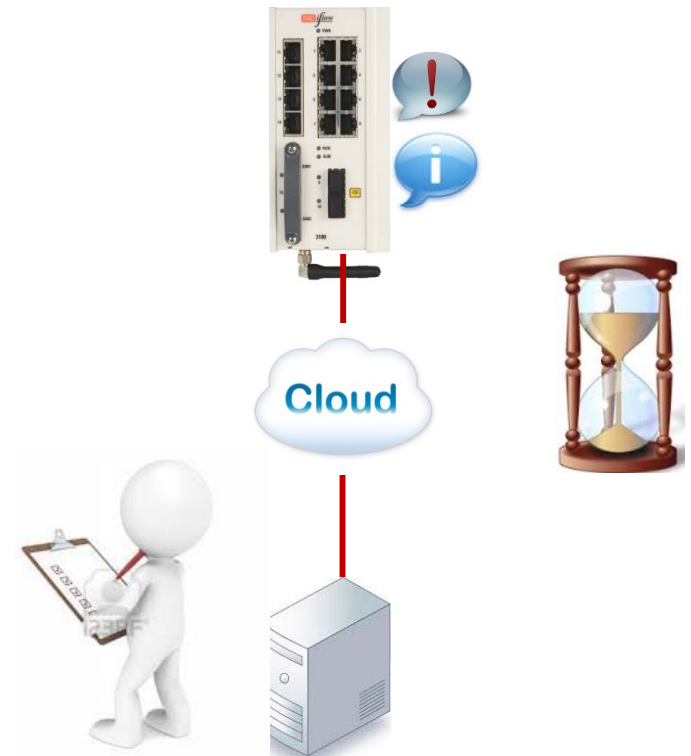
+ Application connect

- reload schedule date-and-time YYYY-MM-DD,HH:MM:SS
- reload schedule every <180 - 604800 seconds >
- reload schedule time HH:MM:SS
- reload schedule in <0 - 604800 seconds >
- reload cancel
- reload show



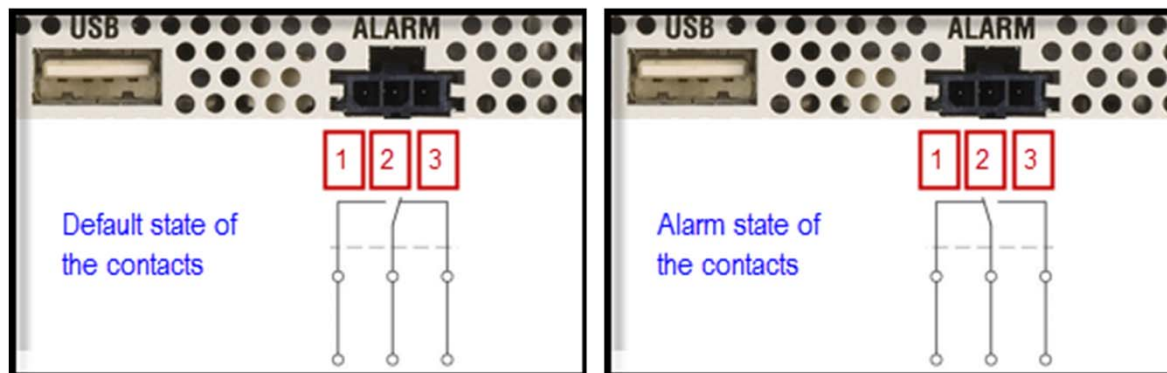
Logs export ,ad-hoc and time conditioned

```
+ Root
- logs-export    [flash: <file_name> |
                 sftp://user:password@aa.bb.cc.dd/<file_name> |
                 tftp://aa.bb.cc.dd/<file_name> ]
+ application connect
+ schedule
  - add task-name copy-logs [day |hour |minute |month |year]
  - remove task-name copy-logs
- show
```



Alarm Relay – “Alarm” Interface

- The system has a dedicated relay output to reflect specific alarms.
- The relay is a 3 pole interface holding a Normally Closed (NC) state between terminals 2 and 3 ,and a Normally Open state between terminals 2 and 1.



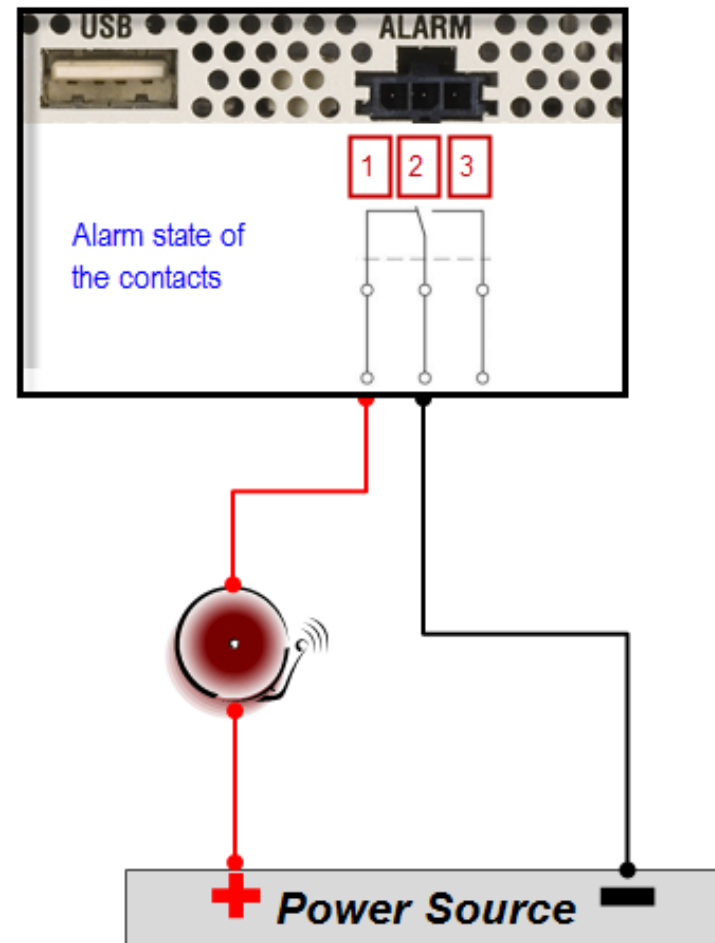
Alarm Relay – Supported Alarms

- SFP port state
 - A state of port down
- L2 VPN state
 - The state of a layer 2 VPN is monitored by the IPsec SA.
- Temperature threshold
 - Alarm set if exceeds 76oC. Alarm clear when lower than 72oC.
- CPU threshold
 - Alarm set if exceed 95% for more than 60 sec. Alarm clears when lower than 90% for more than 60 sec.
- System up/down
 - Alarm set while system is in BOOT phase.

Capture of Ethernet service traffic

- The system supports sniffing and capturing of Ethernet traffic for selected service IP interfaces. This capability is important in order to diagnose network traffic of a service for debugging.
- The capturing is available for traffic passing via the application ports gigabitethernet 0/3-4.
- The capture command is implemented on the IP interfaces eth1.<vlan id> or eth2 where :
 - eth1.<vlan id> : ACE IP interface configured by the user. Port gigabitethernet 0/3 is a tagged member at vlan x.
 - eth2 : ACE IP interface set internally by the system. Port gigabitethernet 0/4 is a tagged member at the service vlan.

Alarm Relay – “Alarm” Interface



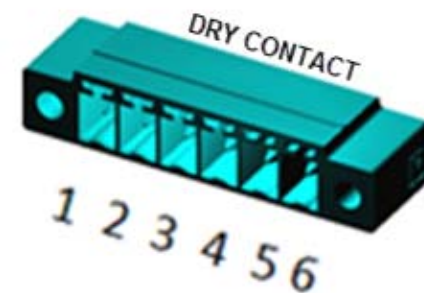
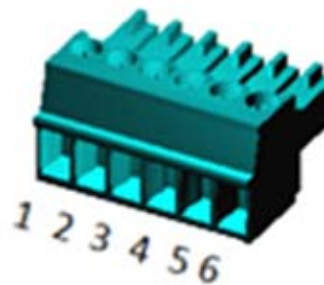
Contact switching capabilities

- Max DC voltage : 220v
- Max current : 1A
- Max power : 30w

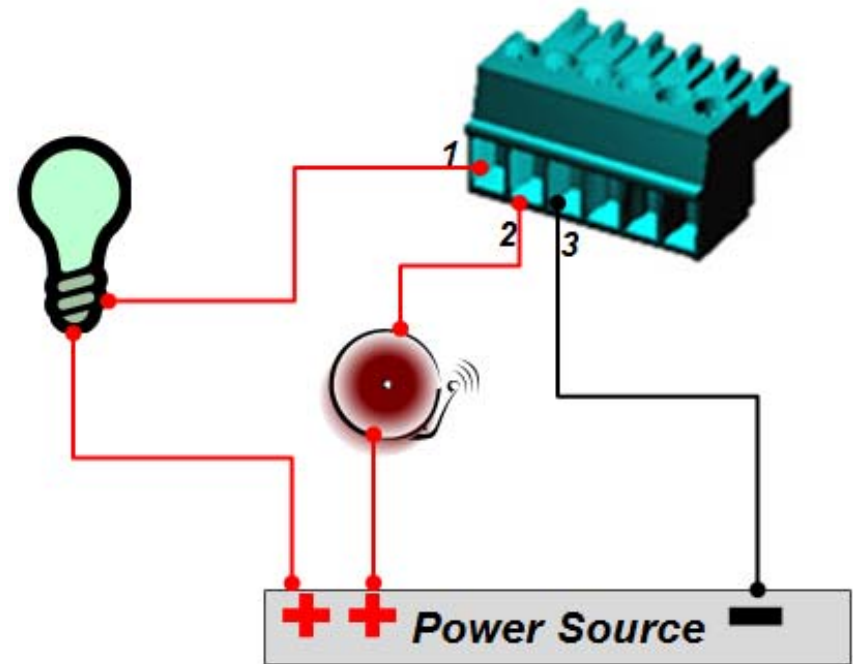
Alarm Relay – “Dry Contact” Interface

- The system can as well use the dry output contacts to reflect output alarms.
- The dry contact interface holds two N/O contacts

1. Digital Output 1
2. Digital Output 2
3. Digital Output Common
4. Not Applicable
5. Not Applicable
6. Not Applicable



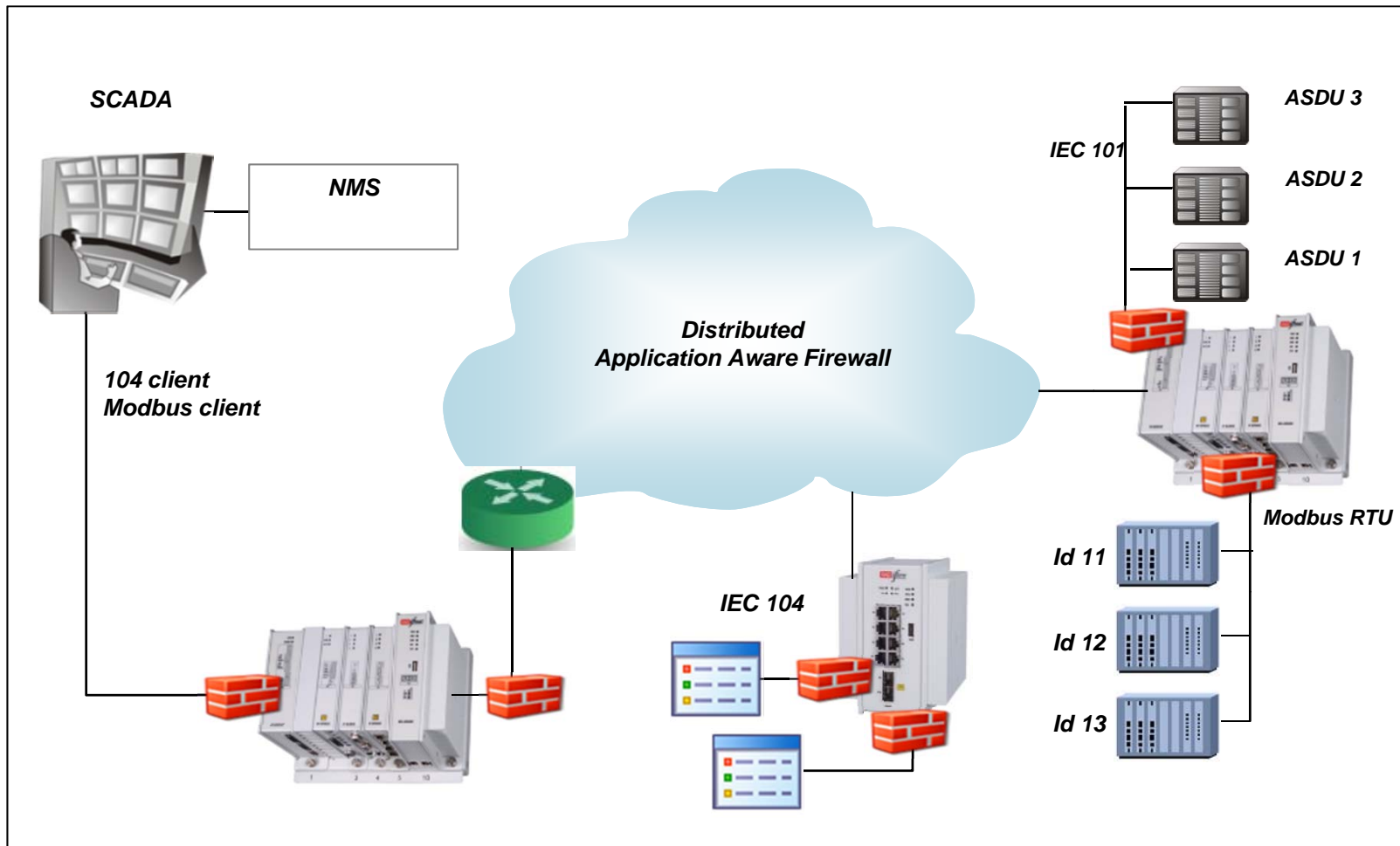
Alarm Relay – “Dry Contact” Interface



Contact switching capabilities

- Max AC voltage : 250v ,37.5 VA.
- Max DC voltage : 220v ,30 W.

Distributed firewall

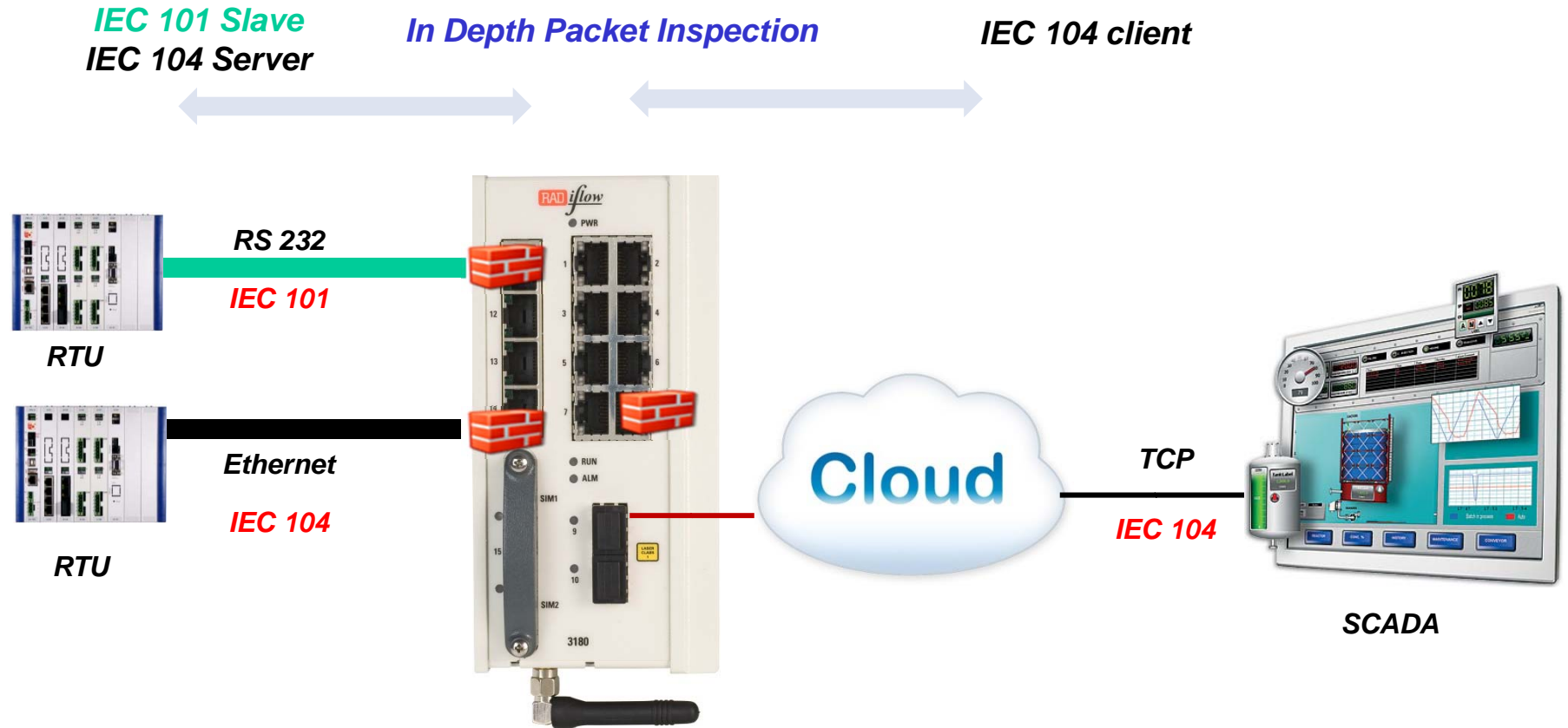


Security – application aware Firewall

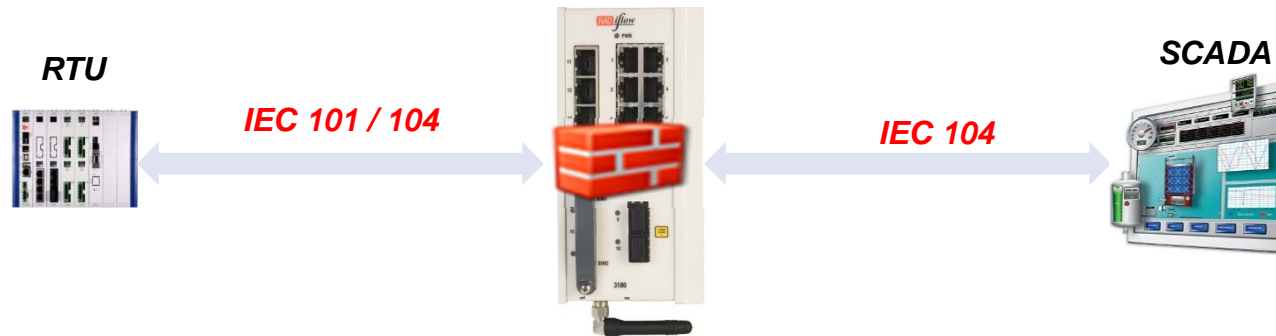
The screenshot displays the iSIM 0.0.7.7 interface. On the left, a 'Logical Network' tree shows a 'Factory' containing a 'CLI Sample' and several 'Switch' and 'IO' components. The main workspace shows a network diagram with PLC-A connected to Switch-AA, which is connected to Switch-BB, which is connected to Switch-CC. Below the diagram is a 'Status' window with a 'Security Log' tab. The log contains the following entries:

ID	Dup	Time	Severity	Serv Grp	Source	Destination	Protocol	Message
26		09/11/10 11:13:54	Error	3585	PLC-A:502	IO-B:3201	TCP	Rule violation: out of allowed address range (
27		09/11/10 11:13:55	Error	3585	IO-B:3201	IO-B:3201	TCP	Rule violation: out of allowed address range (
28		09/11/10 11:13:55	Warning	3585	PLC-A:502	IO-B:3201	TCP	Modbus validity: illegal data length (20)
29		09/11/10 11:13:56	Alert	3585	IO-A:502	IO-B:3201	TCP	Flow is not allowed
30		09/11/10 11:13:56	Alert	3585	IO-B:3201	IO-B:3201	TCP	Flow is not allowed
31		09/11/10 11:13:56	Warning	3585	PLC-A:502	IO-B:3201	TCP	Modbus validity: illegal data length (20)
32	1	09/11/10 11:13:56	Alert	3585	IO-B:3201	IO-B:3201	TCP	Flow is not allowed
33		09/11/10 11:13:56	Warning	3585	IO-B:3201	PLC-A:502	TCP	Modbus validity: illegal data length (20)
34	1	09/11/10 11:13:56	Error	3585	IO-A:502	IO-B:3201	TCP	Flow is not allowed
35		09/11/10 11:13:56	Warning	3585	PLC-A:502	IO-B:3201	TCP	Modbus validity: illegal data length (20)
36		09/11/10 11:15:09	Alert	3585	IO-A:502	IO-B:3201	TCP	Flow is not allowed
37		09/11/10 11:15:09	Info	3585	IO-B:3201	IO-B:3201	TCP	Packet not expected while in time wait state

Distributed Firewall



Firewall IPS inspection flow



IP

- Packet originated from and designated to a service member (source/destination IP)

Port

- Packet holds a service permissible TCP/UDP port number (examples - IEC 104 :2404 ; Modbus : TCP 502 ;SNMP :UDP161)

addresses

- Validation according to protocol specific device addresses (Originator address ;Link address ;ASDU ;IO objects)

payload

- In-depth packet payload inspection to comply with the “firewall rules” file.
- Firewall rules are configured uniquely between each pair of service members

login

- Visual alerts and logging of firewall violations

Firewall Protocols

- DNP3
- Modbus
- IEC 101
- IEC 104
- 61850 * (Q2)

Firewall Modes of Operation

- Protect– protective mode.
 - Traffic is inspected and allowed/ blocked.
 - Violations are logged and presented visually
 - Traps are sent to northbound management system
 - Email notifications
- Simulation
 - Traffic is inspected but not blocked
 - Violations are logged and presented visually
- Learning mode
 - Traffic is learned and a tentative firewall rules is created

Security Measures Supported

- Interfaces
 - FO ports : resiliency to tapping
 - Serial ports and services : less susceptible to sniffing
 - USB : file authentication to a designated node
- File transfer
 - SFTP
 - USB
 - Over a secure VPN
- Authentication
 - Local
 - Centralized

Security Measures Supported

- Management
 - SSH v2
 - Telnet can be blocked
 - Over a secure VPN
 - SNMP v3
- Networking of remote sites
 - Secure remote access – reverse SSH tunnel
 - L2 VPN : L2 services.
 - L3 VPN : robust L3 protection and redundancy
 - IPSec
 - User policy for traffic type
 - IKE, AES or 3DES encryptions
 - Dynamic key exchange
 - NAT traversal

Security Measures Supported

- 802.1x port based
- ACLs
- Vlans
- Port limit and Port shutdown
- Firewall
 - Distributed , application aware
 - Over serial and Ethernet
 - Learning mode
 - Simulation mode