Paris Session 2022

SCADA over IP/MPLS

D2

PS3+ question 3.6: At the remote site level, for example at the substations, where multiple services exist, discuss the techniques used to segment, isolate and apply service differentiation in a multi-service packet-switched network. A challenging example is the case of protection relays – discuss the approaches that can be used in designing a packet-switched network to securely segregate the two services (SCADA and relay management), both of which are applicable to protection relays – you may choose to submit your contribution to include this challenging example, or you may choose to contribute other example cases if desired.

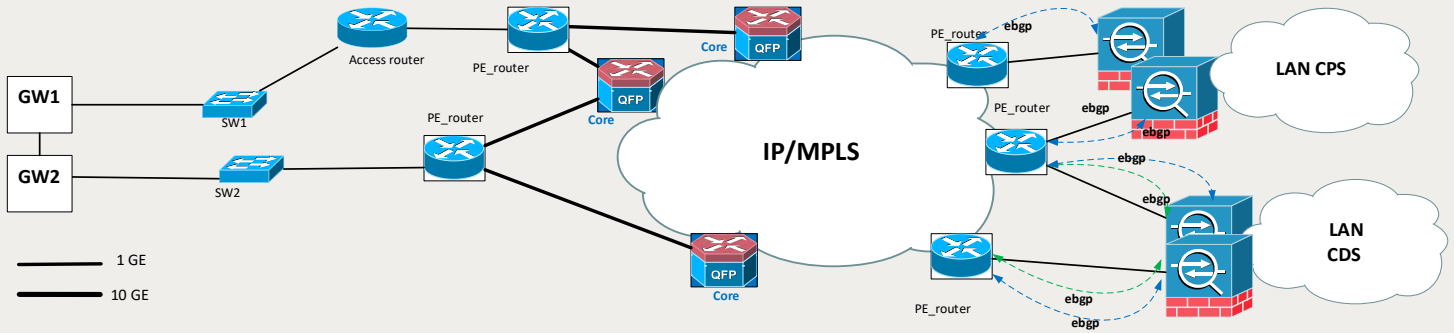
Danilo Lalovic, Serbia

SCADA over IP/MPLS network

The following mechanisms for segregation and QoS are implemented in the network:

- Network traffic flows are organized in different classes of services.
- Different routing policies are implemented dependent on class of service.
- DSCP field in IP packet is set based on the rule from which VLAN the packet was received at the access router or PE router.
- Routing policy is implemented dependent on class of service the packet belongs to and DSCP filed is further mapped into EXP field of MPLS label, based on which class of service is determined in the core network and further forwarding is carried out.
- Voice traffic uses class of service for real time with highest priority (*Expedited Forwarding)*. SCADA traffic belongs to Critical service class. Video surveillance and Control system belong to different class of service with lower priority.

SCADA over IP/MPLS network



The following approaches are used In order to provide security of SCADA communications:

- Logical isolation of SCADA system (CDS) in respect to corporate and other networks being connected to IP MPLS network is realized through separate VRF for SCADA communications.
- In order to ensure greater security of central system communication, direct physical connections have been established between two PE routers and redundant Firewalls within the SCADA system.
- For communication between the SCADA environment and the Production Planning System (CPS), which is in Corporate Network, dedicated L3 connections are made between the PE routers and the Firewall.
- Communication with the SCADA system will take place through separate L3 connections for SCADA and Data traffic, which are mapped into different VRFs , securely segregating in this way SCADA and Data services.
- Complete SCADA and Data traffic is uniquely passed through redundant physical connections between PE router and the Firewall and it Is separated into different zones on the Firewall.

Thank you for your attention !