NAME : Danilo Lalovic
COUNTRY : Serbia
REGISTRATION NUMBER : 6860

GROUP REF. : D2
PREF. SUBJECT : PS3
QUESTION N° : Q 3.6

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.

Answer to Question 3.6: Based on the implementation of services in EPS IP MPLS network we are providing the following example in order to answer the question.

COMMUNICATIONS OF SCADA SYSTEM OVER IP MPLS NETWORK

The following services are provided through IP MPLS network:

- Operational and administrative IP telephony with video conference
- Business data transmission
- SCADA for the needs of Technical Information Systems
- SCADA for the needs of Dispatch Centers of Electricity Distribution Company
- Video Surveillance
- Control Systems for vehicles access on remote sites.

The following mechanisms for segregation and QoS have been used in the network:

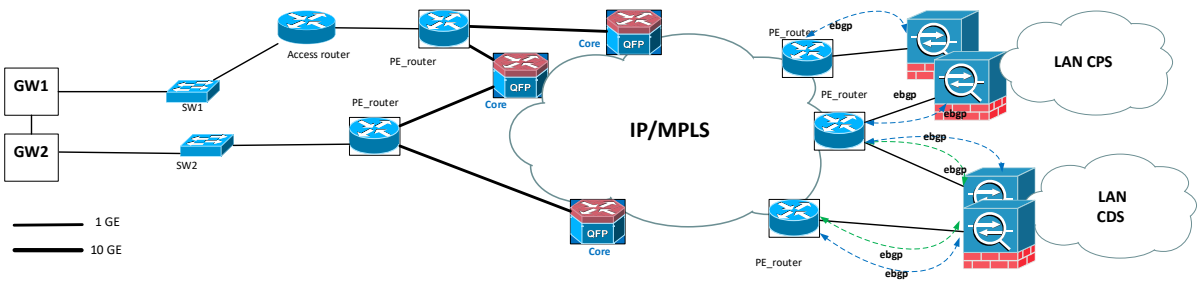
- At the border of IP MPLS network VPN traffic is separated. Each IP packet received has VLAN ID unique for each VPN created for each service.
- Network traffic flows are organized in different classes of services.
- Different routing policies are implemented dependent on class of service.
- DSCP field 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 systems belong to different class of service with lower priority.

The following is an example of SCADA service implementation for Central Dispatching System (CDS) for all Power Plants.

- Realization of service for process data transmission provides communications of remote gateways with SCADA servers at central site utilizing separate VRF SCADA in all Hydro and Thermal Power Plants which are connected to optical network. Traffic flows are organized in different classes of services.

- Hub and spoke model is implemented providing only communications of gateways at remote sites to SCADA servers and work stations at the central facility not allowing communications between the gateways.
- For the security reasons, the principle of connection of gateways within production facilities required establishment of direct physical connection between gateways and access switches within IP MPLS nodes. UTP and optical cables were used requiring, in some instances, deployment of optical approach cables within production facilities , in order to overcome the distance between the gateways and IP MPLS node.
- Logical isolation of SCADA system in respect to corporate and other networks being connected to IP MPLS network is realized through defining separate VRF for process data transport - SCADA communications.
- In order to ensure greater availability and security of central system communication, direct physical connections have been established between two PE routers, one in the central and the other in the remote location, and redundant Firewalls within the CDS system.
- The BGP protocol is used for routing traffic between PE routers and Firewalls.
- For communication between the CDS SCADA environment and the Production Planning System (CPS) , as well as participants from the corporate network, special L3 connections are made between the PE routers and the Firewall, using the same physical links.
- To communicate with these participants from the corporate network, addresses from specific Data traffic address range are used .
- This address range is advertised through L3 connections for Data traffic to communicate with participants from the corporate network, which takes place through VRF Data.
- Depending on the needs, communication with the CDS environment 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 of the PE router and the Firewall and it is separated into different zones on the Firewall

The following figure represents topology of the implemented solution.



Plans for future are to initiate steps together with OT staff to automate the processes in utility. These steps will be in accordance with existing network reference architecture. The following figure is an example of the substation automation reference architecture: