**IEEE 802.1D Protocol – Summarization**

Protocol Operations Multiple Existing Variants New Proposed Changes

**Introduction:**

IEEE 802.1D is an international standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges. The MAC bridges can be used by any type of Local Area Network (IEEE 802) to connect with each other. The advantage of using MAC bridge is that even though each LAN has its own unique MAC, being connected to separate LAN, MAC bridge allows the connection between these devices as if they are connected to a single LAN. The protocols which are in the Network layer or the Logical Link Control layer have access to MAC bridges as MAC bridges are transparent to these protocols. Also, these MAC bridges operate below the MAC service boundary. If there are one or more, MAC bridges it can affect the Quality of Service.

**Bridged Local Area Network:**

There are many advantages of using Bridged Local Area Network. A few of the important ones are listed below:

1. Increase the LANs total performance
2. Increase the number of permissible connection
3. Increase the physical extend
4. Help in maintenance and administrative activities by partitioning the LAN
5. In case of network components failure, this can help in keeping the network service active – providing increased availability

**Support of the MAC Service:**

The MAC Bridges will be configured in such a way that the end points are provided with the redundant paths so that the network communication doesn’t get interrupted even in case of network failure. Thus, supporting network management and improving the availability of the service. An important point to note is that the bridge’s MAC address is never used as destination address field when transmitting between the end stations. Instead the peer end station’s MAC address is used. It is also made sure that all the important aspects of Quality of Services such as service availability, throughput, frame loss etc are very well handled. The filtering service provided by the MAC bridges helps in achieving the Quality of Service such as throughput, priority, transit delay etc.

**Bridge:**

Frames filtering and relay, maintaining the required information to perform the above activities and management of these activities are the main elements of the bridge operation. Bridged Local Area Networks consists of group of separate MACs. The MAC bridge sends the individual MAC between the group of separate MACs. As mentioned above these bridges perform filtering. They do this to reduce the network traffic. A bridge architecture consists of

* MAC relay entity
* Two or more ports
* Higher layer entities which includes Spanning Tree Protocol Entity.

The job of the MAC relay entity is to send the frames between the ports, managing the information needed for filtering, filtering process. The bridge consists of two ports. And each port connects to a single Local Area Network. The spanning tree protocol entity’s job is to compute the network topology.

**Spanning Tree Protocol (STP) [1]:**

STP resides on switches and bridges. This helps in preventing the network loops. STP is used when we need redundant links. These links are helpful during network failures. Whenever there is a network failure, backup links are used. If STP is not installed, then it might result in loop. The rules of operation for STP are as follows: After the identification of root switch, all the switches stick to the following set of rules.

Rule 1: All the ports in the root switch should be in forwarding mode. Each switch then finds the best available path to reach the root. This is done by comparing all the information in BPDUs. The one with the least information is the root port. Now the switches move to Rule 2.

Rule 2: Root port should now be set to forwarding mode. Designated switch is determined during this process which helps in finding the best switch to transfer the data to the root bridge.

Rule 3: The Designated Switch’s port which connects to the Local Area Network should be set to Forwarding mode in case of Single LAN Segment.

Rule 4: All other ports apart from the above-mentioned ports in the switches or bridges should be set to Blocking Mode.

Also, an important thing to note here is that the Spanning Tree runs on all the ports and this cannot be turned off on per-port basis.

**Rapid Spanning Tree Protocol (RSTP):**

Spanning tree algorithm and protocol (STP) is now replaced by Rapid Spanning Tree Protocol (RSTP). The Bridged Local Area Network which contains Local Area Networks which are interconnected by bridges are configured for connectivity using Rapid Spanning Tree Protocol (RSTP). RSTP which works on the Bridged Local Area Network which either has shared LAN or point to point LAN are interconnected with each other using the Bridges. These bridges operate on STP or MSTP or RSTP. RSTP makes sure that it preserves all the quality of MAC services which are mentioned above. Also, the configuration and the complexities of the bridges are limited by implementing the following:

1. The number of LANs and the bridges in the network doesn’t have any influence on the Bridge ports memory requirements.
2. No prior configuration of bridges is required before adding it to the network other than configuring the MAC using the usual process.
3. The protocols timer value has no influence on the time required to configure a point to point LAN’s active topology.

The Bridged Local Area Network consists of the Bridge port and the Port state of these bridge ports are configured by the Rapid Spanning Tree Protocol. It also makes sure that the connectivity provided by the bridges are simple, predictable, symmetric and full. In case of network failure, RSTP makes sure that the temporary loop does not occur in the active topology. Configuration message is transmitted by the each of the bridges. These messages consist of the Spanning Tree Priority Vector. This vector helps in identifying one of the bridge as the Root Bridge. It also helps other bridge to calculate the lowest path cost. One of the port of each bridge is assigned with the Port Role. The Port Roles consist of the state machines. These state machines are useful in setting the state of the Port States. Whenever the LAN or Bride Port or the Bridge fails, the Port role changes. It also changes when it is added to the network or removed from the network. One other use of the RSTP is that it minimizes the frame loss and hence gives way for rapid recovery. Point to Point LANs which has Root Port and the Designated Port can proceed with the transition without worrying about the expiration of the protocol timer. That is, the Root Port can proceed with the transition even without receiving or transmitting the messages and similarly, the Designated Port can proceed with the transition when it receives an agreement from other bridge which is attached to the same LAN. If there is only one Bridge Port in a LAN, then this is configured as the Edge port. This configuration of Edge Port is done automatically by RSTP after confirming that there are no other Bridge Port attached to the LAN. Also, there Edge Ports do not go into loop.

**Multiple Spanning Tree Protocol (MSTP) [4]:**

The connectivity of the VLANs in a Bridged Local Area Network is provided by the Multiple Spanning Tree Protocol. Bridge Protocol Data Units (BPDU) is used by MSTP to communicate between the spanning trees in order to prevent the loops in each Multiple Spanning Tree Protocol and by selecting blocked and active paths in Common and Internal Spanning Tree.

Separate paths are assigned to frames or packets which are sent to different VLANs by MSTP. And this is based on the independent Multiple Spanning Tree Instances (MSTI). Other LANs, Bridges and MST Region which consist of LANs and MST Bridges are connected to a single Common Spanning Tree (CST). For every VLAN, MSTP configures a spanning tree active topology. It is configured in such a way that there is at least one route between any two points without ending up in loops. MST Configuration Identifier is used to advertise the bridge’s configuration to others. CIST is constructed using a priority vector. Additionally, MSTI priority vector is also constructed which has needed information for creating an active topology for any MSTI. Each bridge selects a CIST priority vector for each port. This helps in selecting one bridge as CIST Root. MSTP also encodes additional information to BPDU which holds information regarding the region and configuration.

**Per-VLAN Spanning Tree (PVST) / VLAN Spanning Tree Protocol (VSTP):**

Number of vendors created their own STP for Virtual LAN before the IEEE published one for them. Two main such protocols are PVST and VSTP. PVST was developed by CISCO and VSTP was developed by Juniper Networks. PVST maintains a spanning tree for each VLAN. This uses ISL Trunk and this doesn’t support IEEE 802.1Q (IEEE 802.1Q didn’t support PVST). When IEEE published 802.1Q, they mandated the need for single spanning tree. This specification conflicted with the working of PVST. Hence CISCO improvised it by launching PVST+ which merely changed the destination address to a different L2 multicast address. PVST+ supports IEEE 802.1Q [3]. In case of VSTP, one spanning tree instance which runs RSTP, is assigned to each VLAN. In case of small networks with small number of VLANs, the above-mentioned approach is very effective to optimise the network usage. But in case of large networks which contains many number of VLANs, this can overload switch CPUs. Whereas MSTP takes care of this scenario by not slowing down the network caused by increased number of VLANs. An important thing to note is that VSTP and RSTP can be configured to run on a device concurrently.

**GARP Multicast Registration Protocol (GMRP):**

The MAC bridges and the end stations must register and deregister the group information with the bridges which are of the same Local Area Connection. Also, they would need to spread that information across all the other bridges which supports filtering in BLAN. GMRP provides this facility of registering/deregistering, spreading information across for the MAC bridges and the end stations. The service provided by Generic Attribute Registration Protocol (GARP) is very important for the GMRP to operate successfully. The information used for this purpose is of the following:

* Group Membership Information: Whenever there is this information, it means that there is presence of GMRP participants. These participants belong to a particular group and they have a group MAC address. Whenever this group information is exchanged, the entries in the group membership are updated in the database which contains filtering entries.
* Group Service Requirement: Whenever there is this information, it means that the default group filtering behaviour for the GMRP participants to forward for all the groups or for the unregistered groups.

This process of group membership registration is very important because it makes the bridge to be aware of the groups which are registered with it. Hence it could direct the frame to the correct destined group. Similarly, the process of group service requirement information registration is also very important because it makes the bridges to be aware of the ports which could forward the frame in a direction from which it has received the information and update the group forwarding behaviour accordingly.

**Generic Attribute Registration Protocol (GARP):**

Generic Attribute Registration Protocol permits the GARP application’s participants to register attributes with Bridged Local Area Network’s participants. The attributes mentioned here are very specific to each of the GARP application. A more formal definition of the GARP is as follows. GARP allows its participants to make declarations with the other applicants which would in turn result in these attribute registrations with the other participants of that application. In case if the participants have to withdraw the declaration, then the removal of registration takes place on the other participants of that application. An Application State Machine records the declaration whereas the Registrar state machine records the registration for each participants of the bridge port and the end station.

The GARP architecture is as follows. The end station or the bridge consist of the GARP participants. Each GARP participant consist of GARP application and GARP Information Declaration (GID). The GARP participant exist for every port and GARP Application. GARP Information Propagation (GIP) takes care of carrying the information between the GARP Participants which are located in the same bridge, whereas the protocol exchanges between them are done by LLC service of type -1 which makes use of group MAC address.

**References:**

[1] – Content is referred from CISCO website - <https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/5234-5.html#maintask1>

[2] – Table Source - <https://www.juniper.net/documentation/en_US/junos/topics/concept/spanning-trees-ex-series-vstp-understanding.html>

[3] – Content is referred from CISCO website - <https://learningnetwork.cisco.com/thread/26558>

[4] – Content is referred from HP - <ftp://ftp.hp.com/pub/networking/software/2900-AdvTrafficMgmt-Aug2006-59916197-Chap04.pdf>

**Selecting a Spanning Tree Protocol [2]:**

