8. Principles of bridge operation

<<In areas of change this draft often provides more text than strictly necessary. This is partly to satisfy references but more often to provide context necessary to understand the changes and to clarify what base text is being used: currently (as of 13AUG2008) 802.1Q Edition 0.1 2006 plus 802.1ag-2007, P802.1ah D4.2, P802.1ajD2.2, 802.1ak-2007, P802.1ayD4.0. The editor suggests that the text be reduced to its logical minimum just prior to WG recirculation ballot, i.e. to: changes to bullet items and paragraphs with changes in them, new clauses, and text that may not have changed but was the subject of a comment on the prior ballot. The most extensive areas of change required by this draft are those where the existing base text contained a bug or was ambiguous or vague on technical points or distinctions that have to be very clear for shortest path bridging.>>

Change the text immediately following this heading (8) as indicated:

This clause

a) Explains the principal elements of the operation of VLAN-aware Bridges, and the operation of VLAN-aware ~~b~~Bridge components within systems, and lists the supporting functions.
b) Establishes a ~~B~~bridge architecture that governs the provision of these functions.
c) Provides a model of ~~B~~bridge operation in terms of processes and entities that support the functions.
d) Details the addressing requirements in a bridged network ~~Bridged Local Area Network~~.
e) Specifies the addressing of ~~E~~entities in a ~~B~~bridge.

NOTE—The provisions of this clause subsume the provisions of IEEE Std 802.1D, Clause 7.

8.1 Bridge operation

This amendment does not change the text immediately following this heading (8.1).

Change clauses 8.1.1–8.1.3 as follows, retaining Figure 8-1 unchanged:

8.1.1 Relay

A MAC Bridge or VLAN-aware Bridge relays individual MAC user data frames between the separate MACs of the ~~bridged~~ individual LANs connected to its Ports. The functions that support relaying of frames and maintain the Quality of Service are

a) Frame reception (8.5).
b) Discard on received frame in error (6.5.2).
c) Discard of frames that do not carry user data (6.7).
d) Priority and drop eligibility decoding from a VLAN TAG, if present, and regeneration of priority, if required (6.9).
e) ~~Classification of each received frame to a particular VLAN~~ Assignment of a VLAN Identifier to each received frame (6.9).
f) Frame discard to enforce a loop-free active topology for each frame (8.6.1).
g) Frame discard to support management control over the active topology of each VLAN (8.6.2).
~~g) Frame discard to suppress loops in the physical active topology of the network (8.6.1).~~
h) Frame discard following the application of filtering information (8.6.3).
i) Metering of frames, potentially marking as drop eligible or discarding frames exceeding bandwidth limits (8.6.5).
j) Forwarding of received frames to other Bridge Ports (8.6.4).
k) Selection of traffic class and queuing of frames by traffic class (8.6.6).
l) Frame discard to ensure that a maximum bridge transit delay is not exceeded (6.5.6, 8.6.7).
m) Selection of queued frames for transmission (8.6.8).
n) Mapping of service data units and Frame Check Sequence recalculation, if required (6.5.7).

Copyright © 08 IEEE. All rights reserved.

This is an unapproved IEEE Standards Draft, subject to change.

o) Frame discard if the service data unit cannot be mapped correctly (9.6).
p) Frame discard on transmittable service data unit size exceeded (6.5.8).
q) Selection of outbound access priority (6.5.9).
r) Frame transmission (8.5).

Figure 8-1 gives an example of the physical topology of a Bridged Local Area Network.

8.1.2 Filtering and relaying information

A Bridge maintains filtering and relaying information for the following purposes:

a) Duplicate frame prevention: to maintain a loop-free active topology for ~~each VLAN~~ every frame;
b) Traffic segregation: to separate communication by different sets of network users;
c) Traffic reduction: to confine frames to the path(s) between their source and destination(s);
d) Traffic expediting: to classify frames in order to expedite time critical traffic;
e) Frame format conversion: to tag or untag as appropriate for the destination LAN and stations.

8.1.3 Duplicate frame prevention

A Bridge filters frames, i.e., does not relay frames received by a Bridge Port to other Ports on that Bridge, in order to prevent the duplication of frames (6.5.4). The functions that support the use and maintenance of information for this purpose are

a) Configuration and calculation of one or more spanning tree active topologies.
b) In MST Bridges: explicit configuration to assign ~~of the relationship between~~ VIDs ~~and spanning trees~~ to MSTIs (8.9).
c) In SPT Bridges: explicit or default selection of shortest path or CIST support for specified VLANs; and automatic assignment of VIDs to SPTs for shortest path VLANs.

This amendment does not change clauses 8.1.4–8.1.7.

8.1.4 Traffic segregation

8.1.5 Traffic reduction

8.1.6 Traffic expediting

8.1.7 Conversion of frame formats

Change clause 8.2 as follows:

8.2 Bridge architecture

Change the third and fourth paragraphs of clause 8.2 and the accompanying notes as follows:

Each Bridge Port also functions as an end station and shall provide ~~providing one or more instances of~~ the MAC Service to an LLC Entity that operates LLC Type 1 procedures to support protocol identification, multiplexing, and demultiplexing, for PDU transmission and reception by the Spanning Tree Protocol Entity and other higher layer entities. Other types of LLC procedures can also be supported for use by other protocols. The Bridge Port provides additional MAC service access points if those are explicitly required by the specifications of the attached higher layer entities. Each instance of the MAC Service is provided to a

Copyright © 08 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

distinct LLC Entity that supports protocol identification, multiplexing, and demultiplexing, for PDU transmission and reception by one or more higher layer entities.

~~NOTE 1—In most cases each Port provides a single instance of the MAC Service, to an LLC Entity that supports all the Higher Layer Entities that require a point of attachment to the Port. Further instances are only provided when the specifications of the Higher Layer Entities require the use of different instances of the MAC service or of different source addresses.~~

~~An LLC Entity for each Bridge Port shall use an instance of the MAC Service provided for that Port to support the operation of LLC Type 1 procedures in order to support the operation of the Spanning Tree Protocol Entity. Bridge Ports may support other types of LLC procedures for use by other protocols, such as protocols providing Bridge Management (8.12).~~

NOTE ~~2~~—For simplicity of specification this standard refers to a single LLC Entity that can provide both the procedures specified by IEEE Std 802.2 and Ethernet Type protocol discrimination in the cases where the media access method for the attached LAN supports the latter.

8.3 Model of operation

Change clause 8.3 bullet c)1) as follows:

1) Enforces~~ a~~ loop free active topolog~~y~~ies for all frames~~ for all VLANs~~ (8.1.3, 8.4, 8.6.1);

Change the penultimate paragraph of 8.3 and the following note as follows:

Higher Layer Entities that require only one point of attachment for the ~~B~~bridge as a whole may attach to an LLC Entity that uses an instance of the MAC Service provided by a Management Port. A Management Port does not use an instance of the ISS to attach to a network, but uses the Bridge Port Transmit and Receive Process and the MAC Relay Entity to provide connectivity to other Bridge Ports and the attached LANs.

NOTE—Management port functionality may also be provided by an end station connected to an IEEE 802 LAN that is wholly contained within the system that incorporates the ~~B~~bridge. The absence of external connectivity to the LAN ensures that the management port is always forwarding ~~access to the management port through the bridge's relay functionality can be assured at all times~~.

Figure 8-2 illustrates the reception and transmission by an ~~E~~entity attached to a Management Port.

Replace clause 8.4 with the following:

<These changes are based on text that the editor has contributed in support of a ballot comment on P802.1ayD4.0, and will be updated depending on the adoption (or not) of that comment. The appropriate editing instruction is therefore 'Replace' as given above, even though changes against a hypothetical base are shown. The ballot comment referred to followed review of the degree to which 1ay changes/extends/redefines the concepts of 'active topology' and Port State. 1ayD4.0's continued use and partial redefinition of Port State doesn't appear to make sense in the long run, particular as SPBB also needs to redefine it.>

8.4 ~~Port states and the active topology~~Active topologies, learning, and forwarding

An *active topology* is the connectivity provided, for frames with a specified set of VID, destination address, and source address values, by interconnecting the LANs and bridges in a bridged network with *forwarding* Bridge Ports.

The distributed spanning tree algorithms and protocols, i.e. the Rapid Spanning Tree Protocol (RSTP, IEEE Std 802.1D Clause 17), ~~and~~ the Multiple Spanning Tree Protocol (MSTP, Clause 13), and IS-IS with Shortest Path Bridging extensions and Tree Agreement Protocol (ISIS-SPB, Clause 29) construct one or

Copyright © 08 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

more active topologies, each simply and fully connected for frames belonging to a given VLAN and transmitted from any end station to any other. The *forwarding* and *learning* performed by each Bridge Port for each spanning tree is dynamically managed by RSTP, or MSTP, or ISIS-SPB to prevent temporary loops and reduce excessive traffic in the network while minimizing denial of service following any change in the *physical topology* of the network.

Provider Backbone Bridge Traffic Engineering enables construction of active topologies by the external agent that is responsible for setting up provisioned Ethernet Switched Paths (ESPs).

Any port that is not enabled, i.e., has MAC_Operational (6.6.2) False or has been excluded from the active topology by management setting of the Administrative Bridge Port State to Disabled, has both forwarding and learning disabled for all spanning trees and ESPs.

If the Bridge Port is enabled, PBB-TE disables learning and enables forwarding for all frames allocated to each ESP-VID. An external agent manages the Filtering Database to control the forwarding of frames with particular values of ESP-VID and destination MAC address.

The term Port State summarizes per tree combinations of *forwarding* and *learning*, and any additional per tree variables, used by a given spanning tree protocol to enforce the active toplogies it has calculated, and is used by RSTP and MSTP as follows. Any Port that has *learning* enabled but *forwarding* disabled has the Port State Learning, and a Port that both learns and forwards frames has the Port State Forwarding. However the RSTP and MSTP state machines (IEEE Std 802.1D-2004, Clause 17 and Clause 13 of this standard) do not control the Port State directly but use independent *forwarding* and *learning* variables for each tree.

ISIS-SPB controls both *forwarding* and *learning* variables for each spanning tree and Bridge Port directly when used to support Shortest Path Bridging (SPB, Clause 27), but disables *learning* when supporting Shortest Path Backbone Bridging (SPBB, Clause 28).

RSTP constructs a single spanning tree, the Common Spanning Tree (CST), and maintains a single Port State for each Bridge Port. SST Bridges allocate all frames to that single spanning tree irrespective of their VLAN classification or source and destination MAC addresses.

MSTP constructs multiple spanning trees, the Common and Internal Spanning Tree (CIST) and additional Multiple Spanning Tree Instances (MSTIs), and maintains a Port State for each spanning tree for each Port. An MST Bridge allocates all frames classified as belonging to a given VLAN to the CIST or to one of the MSTIs using the MST Configuration Table. An MISTID of 0 identifies the CIST. A reserved MSTID value (TE-MSTID) is used to identify VIDs for use by PBB-TE with ESPs. Further MSTID values are used to identify SPT sets for use with ISIS-SPB. A single VID is used to identify frames assigned to any given VLAN that is supported by the CIST or an MSTI. That VID is used by the Forwarding Process (Clause 8.6) to identify the spanning tree for the relayed frame, and thus identifies the applicable Port State.

ISS-SPB constructs symmetric (3.16) shortest path spanning trees (SPTs) rooted at each bridge within an SPT Region, and maintains independent *forwarding* and *learning* variables for each spanning tree for each Port. Each frame classified as belonging to a VLAN supported by shortest path bridging, is allocated to an SPT rooted at the bridge that first relays the frame into the Region, If a C-VLAN or S-VLAN is supported by Shortest Path Bridging (SPB, Clause 27) the frame is assigned a Shortest Path VLAN Identifier (SPVID) that is used by the Forwarding Process (Clause 8.6) to identify both the VLAN and the SPT, and thus identifies the applicable *learning* and *forwarding* values. If a B-VLAN is supported by Shortest Path Backbone Bridging (SPBB, Clause 28) the frame is assigned a B-VID value that identifies the frame as subject to SPBB and identifies the B-VLAN and the SPT Set (3.10). The SPT is identified (from amongst those in that set) by the source address of the frame. If ISS-SPB sets *forwarding* True for that SPT, a Dynamic Filtering Entry for that B-VID, source address tuple is included in the Filtering Database so that it passes the active topology enforcement check (see Clause 8.6.1). If a B-VLAN is supported by SPBB, *learning* is disabled for all frames for that B-VLAN.

Copyright © 08 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

Figure 8-5 illustrates the operation of the Spanning Tree Protocol Entity, which operates the Spanning Tree algorithm and its related protocols, and its modification of Port state information as part of determining the active topology of the network.

Figure 8-3 illustrates the Forwarding Process's use of the Port State: first, for a Port receiving a frame, to determine whether the received frame is to be relayed through any other Ports; and second, for another Port in order to determine whether the relayed frame is to be forwarded through that particular Port.

Figure 8-4 illustrates the use of the Port state information for a Port receiving a frame, in order to determine whether the station location information is to be incorporated in the Filtering Database.

8.5 Bridge Port Transmit and Receive

This amendment makes no changes to clause Clause 8.5.

8.6 The Forwarding Process

This amendment does not change the text immediately following this heading (8.1).

<However the text has been retained in order to keep Figure 8-4 for the time being, since this requires a minor change (arrow from Filtering Database to Active Topology Enforcement) to allow loop mitigation (rather than loop prevention) for B-VLAN unicast frames supported by SPBB.>

Each frame submitted to the MAC Relay Entity shall be forwarded subject to the constituent functions of the Forwarding Process (Figure 8-1). Each function is described in terms of the action taken for a given frame received on a given Port (termed "the reception Port"). The frame can be forwarded for transmission on some Ports (termed "transmission Ports") and discarded without being transmitted at the other Ports.

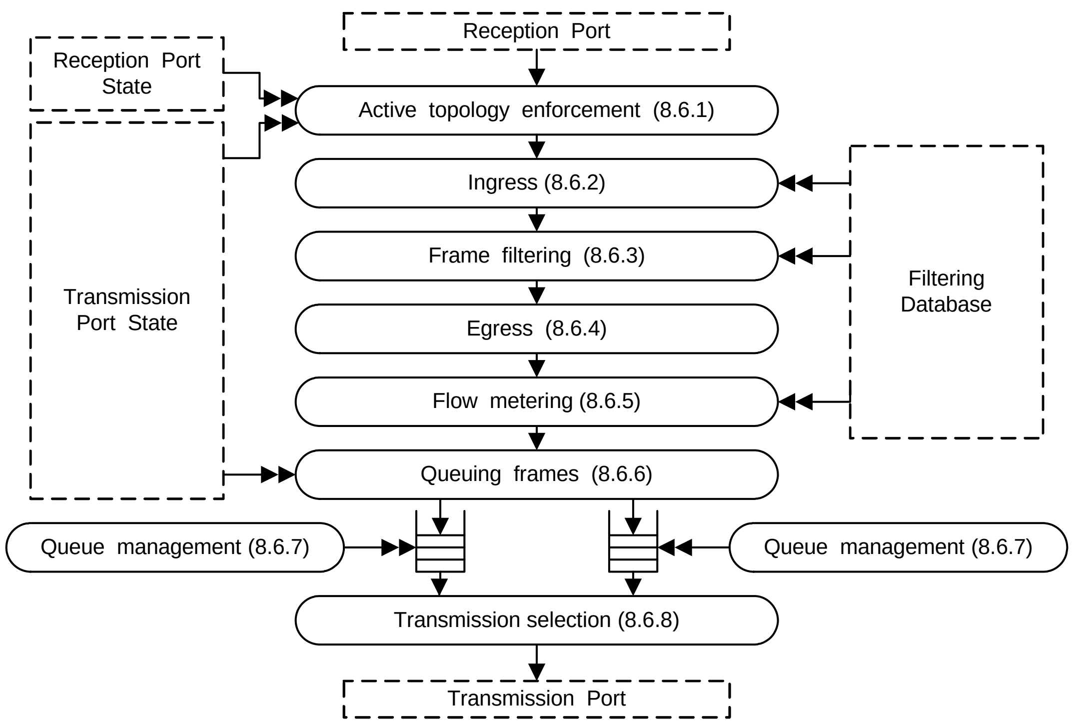

Figure 8-1—Forwarding Process functions

Copyright © 08 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

NOTE 1—IEEE Std 802.1Q-2003 Edition included frame formatting and FCS recalculation functions within the Forwarding Process. This revision of the standard places those functions below the EISS interface, to allow the specification of additional methods for Bridge Port support of the EISS.

NOTE 2—The Forwarding Process models the Bridge relay function, and does not take into consideration what may occur once frames are passed to the Bridge Port for transmission. Conformant implementations of some media access methods can vary the transmission order in apparent violation of the transmission selection rules when observing frames on the medium. Historic examples include the handling of access_priority in Token-Passing Bus MACs, and the effect of different values for Token Holding Time in FDDI LANs. It may not be possible to test conformance to this standard for some implementations simply by relating observed LAN traffic to the functionality of the forwarding process; tests also have to allow for the (conformant) behavior of the MAC.

Figure 8-3 illustrates the operation of the Forwarding Process in a single instance of frame relay between the Ports of a Bridge with two Ports.

8.6.1 Active topology enforcement

<Using P802.1ay D4.0 as the base text for 8.6.1 has proved problematic. The text here is based on 802.1Q and tries to cover the technical changes made in P802.1ay D4.0 (a comment will be/has been made on P802.1ay D4.0 in an attempt to restore alignment).

~~The Forwarding Process allocates each received frame to a spanning tree.~~ To prevent data loops and unwanted learning of source MAC addresses, the Forwarding Process applies the values of the *learning* and *forwarding* controls (Clause 8.4) to each received frame. If *learning* is True for the receiving Port and ingress filtering (Clause 8.6.2) would not cause the received frame to be discarded, ~~If the reception Port State for that spanning tree is Forwarding or Learning,~~ the frame's source address and VID are submitted to the Learning Process. If *forwarding* is True for the receiving Port, ~~If the reception Port State is Forwarding,~~ each Bridge Port, other than that receiving Port, with *forwarding* True ~~with a Port State of Forwarding for that tree~~ is identified as a potential transmission Port.

An SST Bridge ~~allocates all frames to a single spanning tree~~ supports a single active topology, the Common Spanning Tree (CST). For each Bridge Port, RSTP determines a single value for *forwarding* and a single value for *learning* (Clause 8.4) for all frames.

~~An MST Bridge allocates all frames with a given VID to the CIST or to a Multiple Spanning Tree Instance (MSTI). The allocation can be controlled by configuration of the MST Configuration Table (8.9.1) maintained by the Forwarding Process, subject to constraints (if any) imposed by the allocation of VIDs to FIDs (8.8.7). VIDs allocated to different spanning trees shall also be allocated to different FIDs. VIDs allocated to a given spanning tree may share the same FID.~~

Bridges with MST, PBB-TE, or SPB capabilities, use the VID of the received frame to determine *forwarding* and *learning* for that frame for each Bridge Port that is enabled, i.e. has MAC_Operational True and an Administrative Bridge Port State of Enabled, as follows.

If the bridge supports PBB-TE, and the VID is an ESP-VID, then *forwarding* is True and *learning* False.

NOTE 1—Effective control over the active topology of each ESP is provided by an external agent that configures static filtering entries in the Filtering Database (Clause 8.8.1, 25.10.1).

If the bridge uses MSTP to configure the CIST, and the VID identifies a VLAN assigned to the CIST, *forwarding* and *learning* are as determined by MSTP (Clause 13) for the CIST.

If the bridge uses MSTP to configure MSTIs, and the VID identifies a VLAN assigned to an MSTI calculated by MSTP, *forwarding* and *learning* are as determined by MSTP for that MSTI.

Copyright © 08 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

If the bridge uses ISIS-SPB to configure the CIST, and the VID identifies a VLAN assigned to the CIST, *forwarding* and *learning* take the value of *forwarding* determined by ISIS-SPB (Clause 29) for the CIST.

If the bridge uses ISIS-SPB, and the VID is reserved for use by SPB or SPBB as an SPVID and is not currently used, *forwarding* and *learning* shall be False.

If the bridge uses ISIS-SPB, and the VID identifies a C-VLAN or S-VLAN assigned to an SPT, both *forwarding* and *learning* take the value of *forwarding* determined by ISIS-SPB for the SPT.

If the bridge uses ISIS-SPB and the VID identifies a B-VLAN assigned to an SPT (i.e. use of SPBB), then *learning* is False for all Bridge Ports, *forwarding* is True for the reception Port if and only if a Dynamic Filtering Entry for the frame's source address and VID exists and specifies Forward for that Port, and forwarding is True for all other Bridge Ports.

NOTE 2—Effective control over the egress component of an SPBB SPT is provided by EISS-SPB configuration of (a) a Dynamic Filtering Entry for the SPT's B-VID and Root MAC Address (for unicast frames); and (b) MAC Address Registration Entries for the SPT's B-VID for "All Unregistered Group Addresses" and SPT specific Group MAC Addresses (for multicast frames).

All bridges other than SST Bridges implement the MST Configuration Table (Clause 8.9.1). Bridges with SPB capabilities also implement the SPT Configuration Table (Clause 8.9.4) and the SPT Set List (Clause 8.9.5). The use of VIDs to determine learning and forwarding, as required by this clause shall be consistent with those tables and lists as follows. All VIDs allocated by the MST Configuration Table to the CIST-MSTID (0x000) are assigned to the CIST, all VIDs allocated to MSTID 0xFFF are reserved for use by ISIS-SPB but are not currently in use, all VIDs allocated to the TE-MSTID (0xFFE) are ESP-VIDs, and all VIDs allocated to other values of MSTID are assigned to the MSTI identified by that MSTID. If a VID assigned to an MSTI has an SPT Configuration Table entry whose Base VID is not that of the VID itself, that VID is an SPVID.

<<The above text does not yet satisfactorily distinguish between SPB and SPBB support of VLANs. Just as it is possible to support both S-VLANs and B-VLANs in a backbone network, this standard should allow SPB and SPBB to coexist within the same bridged network—in other words categorization of the entire bridged network is not an adequate way of making the needed distinction. This issue is not especially difficult, an elegant way of making the distinction i.e. one that adds the minimum of additional management objects, needs to be specified.>>

Change the heading of clauses Clause 8.6.2 as follows:

8.6.2 Ingress filtering

This amendment makes no changes to clauses Clause 8.6.3 through Clause 8.6.8

8.6.3 Frame filtering

8.6.4 Egress

8.6.5 Flow classification and metering

8.6.6 Queuing frames

8.6.7 Queue management

Change bullet (c) of clause Clause 8.6.7 as follows.

Copyright © 08 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

c) If the ~~associated~~ transmission Port is no longer *forwarding* for that frame (Clause 8.4, Clause 8.6.1) ~~leaves the Forwarding state~~.

8.6.8 Transmission selection

8.7 The Learning Process

Change the initial paragraph of clause Clause 8.7, creating two paragraphs as follows.

The Learning Process receives the source MAC Addresses and VIDs of received frames from the Forwarding Process, subject to active topology enforcement (Clause 8.6.1) and ~~following~~ the application of ~~the~~ ingress ~~rules~~ filtering (8.6.2). The Learning Process is not invoked (see Clause 8.6.1) for frames whose VID is an ESP-VID or identifies a B-VLAN supported by SPBB.

When invoked, the Learning Process ~~It~~ shall create or update a Dynamic Filtering Entry (8.8.3) that specifies the reception Port for the frame's source address and VID, if and only if the source address is an Individual Address, i.e., is not a Group Address, the resulting number of entries would not exceed the capacity of the Filtering Database, and the filtering utility criteria for the receiving Bridge Port are met, as specified below.

This amendment makes no changes to clauses Clause 8.7.1 through Clause 8.7.2

8.7.1 Default filtering utility criteria

8.7.2 Enhanced filtering utility criteria

8.8 The Filtering Database

Change the initial text of clause Clause 8.8 as follows.

The Filtering Database supports frame filtering (Clause 8.6.3) queries by the Forwarding Process ~~as~~ to determine whether received frames ~~received by the Forwarding Process~~, with given values of destination MAC Address ~~parameter~~ and VID, are to be forwarded through a given potential transmission Port (8.6.2, 8.6.3, 8.6.4). It can also be used, by SPBB (8.6.1), to determine whether received frames with given values of source MAC Address and VID, are to be forwarded from a given reception Port. The Filtering Database contains filtering information in the form of filtering entries that are either

Change bullet e) of clause Clause 8.8 as follows.

e) Forwarding of frames with particular VIDs;

Change bullet h) and i) of clause Clause 8.8 as follows.

h) Each Dynamic Filtering Entr~~ies~~y ~~are used to~~ specif~~y~~ies the Port~~s~~ through ~~on~~ which a frame with a given individual source MAC Address~~es~~ and VID has or can be received ~~have been learned for a given VLAN ....~~. ~~They~~ Dynamic Filtering Entries can be ~~are~~ created and updated by the Learning Process (8.7) or by ISIS-SPB (for B-VLANs supported by SPBB). Entries that are updated by the Learning Process~~, and~~ are subject to ageing and removal by the Filtering Database.

NOTE—When ISIS-SPB is supporting B-VLANs (for SPBB) it has to create the Dynamic Filtering Entries used to locate stations, since *learning* is not used. However initial creation of these entries does no harm for SPB when *learning* is used, and can reduce flooding of frames to unknown destinations.

i) MAC Address Registration Entries support the registration of group MAC Addresses. They are created, updated, and removed by the MMRP protocol in support of Extended Filtering Services (8.8.4, Clause 10), ~~subject to the state of the Restricted_MAC_Address_Registration management control (10.12.2.3)~~ and by EISS-SPB. If ~~the value of this~~ of the

Copyright © 08 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

Restricted_MAC_Address_Registration management control (10.12.2.3) is TRUE, then the creation of a MAC Address Registration Entry is not permitted unless a Static Filtering Entry exists that permits dynamic registration for the Group concerned.

Consider ISIS-SPB support of (S,G) for VLAN Registration, and possible modification of bullet (j) of clause Clause 8.8.

j) Dynamic VLAN Registration Entries are used to specify the Ports on which VLAN membership has been dynamically registered. They are created, updated, and removed by the MVRP protocol, in support of automatic VLAN membership configuration (Clause 11), subject to the state of the Restricted_VLAN_Registration management control (11.2.3.2.3). If the value of this control is TRUE, then the creation of a Dynamic VLAN Registration Entry is not permitted unless a Static VLAN Registration Entry exists that permits dynamic registration for the VLAN concerned.

Change the paragraph beginning "The Filtering Database shall support the creation" and add a following paragraph as follows:

The Filtering Database shall support the creation, updating and removal of Dynamic Filtering Entries by the Learning Process (8.7). In Bridges that support Extended Filtering Services, the Filtering Database shall support the creation, updating, and removal of MAC Address Registration Entries by MMRP (Clause 10 of IEEE Std 802.1D). In bridges that support SPB or SPBB, Dynamic Filtering Entries are populated by ISIS-SPB (Clause 29).

Shortest Path Bridging (SPB, Clause 28) allocates SPVIDs dynamically to support shortest path bridging of frames assigned to one or more VLANs, each identified by a Base VID (3.1). A Static Filtering Entry should not be created for an SPVID, irrespective of whether that SPVID is currently used or not, and SPVIDs should not be used in registration protocols that create MAC Address Registration Entries or Dynamic VLAN Registration Entries. In an SPT Bridge, configuration or registration of a filtering database entry with the Base VID of a VLAN supported by SPB shall cause the bridge to filter frames as if that entry was also present for every one of the SPVIDs for that Base VID.

Change the paragraph beginning "Figure 8-4 illustrates" and delete the following note, as follows:

Figure 8-4 illustrates the creation or update of a dynamic entry in the Filtering Database by the Learning Process. The entries in the Filtering Database allow MAC Address information to be learned independently for each VLAN or set of VLANs, by relating a MAC Address to the VLAN or set of VLANs on which that address was learned. ~~This has the effect of creating independent Filtering Databases for each VLAN or set of VLANs that is present in the network.~~

~~NOTE 2—This standard specifies a single Filtering Database that contains all Filtering Database entries; however, the inclusion of VIDs and FIDs in the filtering entries effectively provides distinct IEEE Std 802.1D-style Filtering Databases per VLAN or set of VLANs.~~

This amendment makes no changes to clauses Clause 8.8.1 and Clause 8.8.2

8.8.1 Static Filtering Entries

8.8.2 Static VLAN Registration Entries

8.8.3 Dynamic Filtering Entries

Add the following paragraph after the paragraph beginning "Dynamic Filtering Entries are created and updated by the Learning Process .."

Copyright © 08 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

Dynamic Filtering Entries can also be created and updated by ISIS-SPB (Clause 29). ISIS-SPB refreshes these entries, so they are not aged out by the normal operation of the filtering database. These entries are used by SPBB (Clause 28) to support both unicast loop mitigation (6.5.4.1) and multicast loop prevention (6.5.4.2) for active topology enforcement (Clause 8.6.1), as well as to locate end stations. These entries are also configured for SPB, so that end station functions associated with a bridge are located rapidly after any topology change.

8.8.4 MAC Address Registration Entries

Change the paragraph beginning "MAC Address Registration Entries are created .." as follows:

MAC Address Registration Entries are created, modified and deleted by the operation of MMRP (Clause 10 of IEEE Std 802.1D, as modified by Clause 10 of this standard) or by ISIS-SPB. No more than one MAC Address Registration Entry shall be created in the Filtering Database for a given combination of MAC Address specification and VID.

Change the paragraph beginning "The creation of MAC Address Registration Entries is subject .." as follows:

The creation of MAC Address Registration Entries by MMRP is subject to the Restricted_Group_Registration management control (10.3.2.3 of IEEE Std 802.1D). If the value of this control is TRUE, a dynamic entry for a given Group may only be created if a Static Filtering Entry already exists for that Group, in which the Registrar Administrative Control value is Normal Registration.

This amendment makes no changes to clauses Clause 8.8.5 and Clause 8.8.6

8.8.5 Dynamic VLAN Registration Entries.

8.8.6 Default Group filtering behavior

8.8.7 Allocation of VIDs to FIDs

Change the initial paragraphs of clause Clause 8.8.7 as follows:

~~The allocation of VIDs to FIDs within a Bridge determines how learned individual MAC Address information is used in forwarding/filtering decisions within a Bridge; whether such learned information is confined to individual VLANs, shared among all VLANs, or confined to specific sets of VLANs.~~

The ~~allocation of VIDs to FIDs is determined on the basis of~~

~~a) The set of VLAN Learning Constraints that have been configured into the Bridge (by means of the management operations defined in Clause 12);~~

~~b) Any fixed mappings of VIDs to FIDs that may have been configured into the Bridge (by means of the management operations defined in Clause 12);~~

~~c) The *set of active VLANs* (i.e., those VLANs on whose behalf the Bridge may be called upon to forward frames). A VLAN is active if either of the following is true:~~

~~1) The VLAN's member set (8.8.9) contains one Port that is in a forwarding state, and at least one other Port of the Bridge is both in a forwarding state and has Ingress Filtering (8.6.2) disabled;~~

~~2) The VLAN's member set contains two or more Ports that are in a forwarding state.~~

~~d) The capabilities of the Bridge with respect to the number of FIDs that it can support, and the number of VIDs that can be allocated to each FID.~~

Copyright © 08 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

~~A Bridge shall support a minimum of one FID, and may support up to 4094 FIDs. For the purposes of the management operations, FIDs are numbered from 1 through N, where N is the maximum number of FIDs supported by the implementation.~~

~~A Bridge shall support the ability to allocate at least one VID to each FID, and may support the ability to allocate more than one VID to each FID.~~

~~The number of VLAN Learning Constraints supported by a Bridge is an implementation option.~~

~~NOTE—In an SVL/IVL Bridge (3.60), a number of FIDs are supported, and one or more VID can be mapped to each FID. In an SVL Bridge (3.59), a single FID is supported, and all VIDs are mapped to that FID. In an IVL Bridge (3.27), a number of FIDs are supported, and only one VID can be mapped to each FID.~~

~~An MST Bridge shall support the ability to allocate at least one FID to each spanning tree, and may support the ability to allocate more than one FID to each spanning tree.~~

~~NOTE—In other words, the number of FIDs supported by the Bridge must be greater than or equal to the number of spanning trees supported by the Bridge.~~

~~An MST Bridge shall ensure that the maximum supported numbers of FIDs and VLANs can be associated unambiguously. This requires either 1) a number of fixed VID to FID allocations at least equal to the maximum number of VLANs supported; or 2) one I Constraint entry per FID supported and one S Constraint entry per MSTI supported, or both. (8.8.7.1).~~

The allocation of VIDs to FIDs within a VLAN-aware Bridge determines how learned individual MAC Address information is used in forwarding and filtering decisions. If two VIDs are allocated to the same FID learned information is shared: an individual MAC address learned following receipt of a frame affects the forwarding or filtering of a subsequent frame with the same address as its destination address if either of the two VIDs have been assigned to each of the two frames. If two VIDs are allocated to different FIDs learned information is independent: learning of MAC addresses for frames that have one of the VIDs assigned does not affect forwarding or filtering of frames with the other VID. Independent VLAN Learning can allow two separate stations to use the same MAC address, provided they use different VLANs, and also allows frames transmitted by a single station to be assigned to independent active topologies. Shared VLAN Learning allows support of a single VLAN by multiple VIDs, enabling further control over the filtering of frames for that VLAN, and allowing shortest path bridging to support the VLAN with a set of symmetric trees while still using learning. Further considerations for the use of Independent and or Shared VLAN Learning are described in Annex B (informative).

A VLAN-aware Bridge shall support either Shared or Independent VLAN Learning, and may support both. If Independent VLAN Learning is not supported the bridge shall support a single FID. If Independent VLAN Learning is supported, the number of FIDs shall be the same as the maximum number of VLANs supported by the implementation. For the purposes of the management operations, FIDs are numbered from 1 through N, where N is the maximum number of FIDs supported by the implementation. A bridge that supports both Shared and Independent VLAN Learning shall be capable of allocating any VID to any FID, through configuration of the VID to FID allocation table. Following any set of management operations designed to change the allocation of VIDs to FIDs, whether initiated by an administrative request or as a consequence of other aspects of the bridge's operation, the value of any FID that is in use should be the same as that of one of the VIDs allocated to that FID.

Delete the clause heading "Clause 8.8.7.1 Fixed and dynamic VID to FID allocations", adding the text of that clause after the text of Clause 8.8.7, with the following changes:

Copyright © 08 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

~~8.8.7.1 Fixed and dynamic VID to FID allocations~~

~~A Bridge may support the ability to define fixed allocations of specific VIDs to specific FIDs, via an~~ The VID to FID allocation table ~~that~~ may be read and modified by means of the management operations defined in Clause 12. For each VID supported by the implementation, the allocation table indicates one of the following:

a) The VID is currently not allocated to any FID; or
b) A fixed allocation has been defined (via management), allocating this VID to a specific FID; or
c) A dynamic allocation has been defined ~~(as a result of applying the VLAN Learning Constraints)~~, allocating this VID to a specific FID.

~~For any VID that has no fixed allocation defined, the Bridge can dynamically allocate that VID to an appropriate FID, in accordance with the current set of VLAN Learning Constraints.~~

An SPT Bridge can dynamically allocate VIDs, that have been reserved for use as SPVIDs, to FIDs.

An MST Bridge shall support Independent VLAN Learning and may support Shared VLAN Learning. An SPT Bridge shall support both Independent and Shared VLAN Learning. An MST or SPT Bridge shall be capable of allocating any FID to any MSTID through configuration of the FID to MSTID Allocation Table (12.12.2).

Delete clauses Clause 8.8.7.2 and Clause 8.8.7.3.

~~8.8.7.2 VLAN Learning Constraints~~

~~8.8.7.3 VLAN Learning Constraint inconsistencies and violations~~

8.8.8 Querying the Filtering Database

Retain the existing Tables 8-5 and 8-6 referenced by clause Clause 8.8.8 unchanged, but change the text of the clause as follows:

~~If a frame is classified into a VLAN containing a given outbound Port in its member set (8.8.9), forwarding or filtering through that Port is determined by the control elements of filtering entries for the frame's destination MAC Address and for VLANs with the same VID or Filtering Identifier (FID, 8.8.7) as the frame's VLAN.~~

If the VID assigned to a relayed frame identifies a VLAN with a given outbound Port in its member set (8.8.9), the Filtering Database entries that are applicable to the frame's destination MAC Address and VID determine whether the frame is filtered or forwarded through that Port. More than one entry can apply to a given frame. This clause (Clause 8.8.8) specifies the effect of combining applicable entries, and of the absence of certain types of entries (not all possible entries are necessarily present). For an overview of the different types of entries see the introductory text of clause Clause 8.8.

~~Each entry in the Filtering Database for a MAC Address comprises~~

~~a) A MAC Address specification;~~
~~b) A VID or, in the case of Dynamic Filtering Entries, an FID;~~
~~c) A Port Map, with a control element for each outbound Port.~~

~~For Dynamic Filtering Entries, the FID that corresponds to a given VID is determined as specified in 8.8.7.~~

Copyright © 08 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

For a given VID, a given individual MAC Address specification can be included in the Filtering Database in a Static Filtering Entry, a Dynamic Filtering Entry, both or neither. Table 8-5 combines Static Filtering Entry and Dynamic Filtering Entry information for an individual MAC Address to specify forwarding, or filtering, of a frame with that destination MAC Address and VID through an outbound Port.

NOTE 1—The use of FID in this table for Static Filtering Entries, and the text in parentheses in the headings, reflects the fact that, where more than one VID maps to a given FID, there may be more than one Static Filtering Entry that affects the forwarding decision for a given individual MAC Address. The effect of all Static Filtering Entries for that address, and for VIDs that correspond to that FID, is combined, such that, for a given outbound Port:
— IF <any static entry for any VIDs that map to that FID specifies Forwarding> THEN <result = Forwarding>
— ELSE IF <any static entry for any VIDs that map to that FID specifies Filtering> THEN <result = Filtering>
— ELSE <result = Use Dynamic Filtering Information>

The Filtering Database entries applicable to a frame whose destination MAC Address is a specific individual MAC Address are the Dynamic Filtering Entry (if present) with that MAC Address and the FID to which the frame's VID is allocated (8.8.7), and all Static Filtering Entries (if any) with that MAC Address and a VID that is also allocated to that FID. An entry with a wildcard VID applies only if there is no applicable Static Filtering Entry for a specific VID. Table 8-5specifies the result of combining this informationfor an individual MAC address and a given outbound Port, and can be summarized as follows:

— IF any static entry for a VID allocated to the FID specifies Forward THEN Forward;
— ELSE IF any static entry for a VID allocated to the FID specifies Filter THEN Filter;
— ELSE IF a static entry for the wildcard VID specifies Forward THEN Forward;
— ELSE IF a static entry for the wildcard VID specifies Filter THEN Filter;
— ELSE IF dyamic (learnt filtering information) entry for the FID specifies Filter THEN Filter;
— ELSE Forward.

Table 8-6 specifies the result, Registered or Not Registered, of combining a Static Filtering Entry and a MAC Address Registration Entry for the "All Group Addresses" address specification, and for the "All Unregistered Group Addresses" address specification for an outbound Port. Table 8-7 combines Static Filtering Entry and MAC Address Registration Entry information for a specific group MAC Address with the Table 8-6 results for All Group Addresses and All Unregistered Group Addresses to specify forwarding, or filtering, of a frame with that destination group MAC Address through an outbound Port.

The Filtering Database entries applicable (if present) to a frame whose destination MAC Address is a specific group MAC Address are the Static Filtering Entries and MAC Address Registration Entries (for the frame's VID and for the wildcard VID) whose address specification is that group MAC address or "All Group Addresses" or "All Unregistered Group Addresses". A Static Filtering Entry for a wildcard VID applies only if there is no applicable Static Filtering Entry for a specific VID, MAC Address Registration Entries do not use wildcard VIDs. Table 8-6 specifies the results, Registered or Not Registered for a given outbound Port, of combining the entries for the "All Group Addresses" and for combining the entries for "All Unregistered Group Addresses". Table 8-7 combines these results with the entries for the specific group MAC Address. The result of Table 8-6 for "All Group Addresses" can be summarized as follows:

— IF a static entry for "All Group Addresses" and the frame's Base VID specifies Forward (Registration Fixed) THEN "All Group Addresses" is Registered;
— ELSE IF a static entry for "All Group Addresses" and the frame's Base VID specifies Filter (Registration Forbidden) THEN "All Group Addresses" is Not Registered;
— ELSE IF a static entry for "All Group Addresses" and the wildcard VID specifies Forward (Registered) THEN "All Group Addresses" is Registered;
— ELSE IF a static entry for "All Group Addresses" and the wildcard VID specifies Filter (Registration Forbidden) THEN "All Group Addresses" is Not Registered;

Copyright © 08 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

- ELSE IF a dynamic (MAC Address Registration) entry for "All Group Addresses" and the frame's Base VID specifies Forward (Registered) THEN "All Group Addresses" is Registered;
- ELSE "All Group Addresses" is NOT Registered

NOTE—The result for "All Unregistered Group Addresses" is given by substituting that address specification for "All Group Address" throughout the summary.

The result of Table 8-7 can be summarized as follows:

- IF a static entry for the specific group address and the frame's Base VID specifies Forward THEN Forward;
- ELSE IF a static entry for the specific group address and the frame's Base VID specifies Filter THEN Filter;
- ELSE IF a static entry for the specific group address and the wildcard VID specifies Forward THEN Forward;
- ELSE IF a static entry for the specific group address and the wildcard VID specifies Filter THEN Filter;
- ELSE IF the Table 8-6 result for "All Group Addresses" is Registered THEN Forward;
- ELSE IF the Table 8-6 result for "All Unregistered Group Addresses" is Registered THEN Forward;
- ELSE IF a dynamic (MAC Address Registration) entry for the specific group address and the frame's Base VID specifies Forward THEN Forward;
- ELSE Filter.

~~Where a given VID is allocated to the same FID as one or more other VIDs, it is an implementation option as to whether~~

a) ~~The results shown in Table 8-7 directly determine the forwarding/filtering decision for a given VID and group MAC Address (i.e., the operation of the Bridge with respect to group MAC Addresses ignores the allocation of VIDs to FIDs); or~~
b) ~~The results for a given MAC Address and VID are combined with the corresponding results for that MAC Address for each other VID that is allocated to the same FID, so that if the Table 8-7 result is Forward in any one VLAN that shares that FID, then frames for that group MAC Address will be forwarded for all VLANs that share that FID (i.e., the operation of the Bridge with respect to group MAC Addresses takes account of the allocation of VIDs to FIDs).~~

~~NOTE 2—In case d), the implementation effectively operates a single FDB per VLAN for group MAC Addresses. In case e), the implementation combines static and registered information for group MAC Addresses in accordance with the VID to FID allocations currently in force, in much the same manner as for individual MAC Addresses.~~

When forwarding or filtering a frame with a destination group MAC Address, a VLAN-aware Bridge may:

a) Ignore the allocation of VIDs to FID, and use Table 8-7 directly for the frame's Base VID; or
b) Take the same decision for all VIDs allocated to any given FID, forwarding if Table 8-7 specifies Forward for any VID allocated to the same FID as the frame's Base VID, and filtering otherwise.

Copyright © 08 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

Change Table 8-7 as follows:

Table 8-7—Forwarding or Filtering for specific group MAC Addresses

		Static Filtering Entry Control Element for this group MAC Address, VID and outbound Port specifies:				
		Registration Fixed (Forward)	**Registration Forbidden (Filter)**	**Use MAC Address Registration Information, or no Static Filtering Entry present. MAC Address Registration Entry Control Element for this group MAC Address, VID and outbound Port specifies:**		
				Registered (Forward)	**Not Registered (Filter)**	**No Group Registration Entry present**
All Group Addresses control elements for this VID and Port specify (Table 8-6): Not Registered	**All Unregistered Group Addresses control elements for this VID and Port specify (Table 8-6):** Not Registered	Forward	Filter	Forward	Filter (Filter Unregistered Groups)	Filter (Filter Unregistered Groups)
All Group Addresses control elements for this VID and Port specify (Table 8-6): Not Registered	**All Unregistered Group Addresses control elements for this VID and Port specify (Table 8-6):** Registered	Forward	Filter	Forward	~~Filter~~ Forward (Forward Unregistered Groups)	Forward (Forward Unregistered Groups)
All Group Addresses control elements for this VID and Port specify (Table 8-6): Registered		Forward	Filter	Forward (Forward All Groups)	Forward (Forward All Groups)	Forward (Forward All Groups)

<<The corrected entry was clearly a bug. A MAC Address Registration Entry of Not Registered can be created due to a registration on another port, and the removal of a MAC Address Registration Entry that has Not Registered on all ports is implementation dependent.>>

This amendment makes no changes to clauses Clause 8.8.9 and Clause 8.8.10

8.8.9 Determination of the member set for a VLAN

8.8.10 Permanent Database

Change clauses Clause 8.9 as follows:

8.9 MST, SPT, and ESP configuration information

In order to support multiple spanning trees and shortest path bridging, all the bridges in an MST or SPT Region have ~~an MST Bridge has~~ to be configured with compatible ~~an unambiguous~~ assignments of VIDs to spanning trees. ~~This is achieved by:~~

Copyright © 08 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

~~a) Ensuring that the allocation of VIDs to FIDs (8.8.7) is unambiguous; and~~

~~b) Ensuring that each FID supported by the Bridge is allocated to exactly one Spanning Tree.~~

~~The first of these requirements is met by configuring a set of VLAN learning constraints and/or fixed VID to FID mappings that are self-consistent, and which define an I Constraint, an S Constraint, or a fixed VID to FID allocation for all VIDs supported by the Bridge.~~

~~The second requirement is met by means of the FID to MSTI Allocation Table (8.9.3).~~

In MST Bridges the ~~The~~ combination of the VID to FID allocations(8.8.7) and the FID to MSTID Allocation Table (8.9.3) ~~allocations~~ defines a mapping of VIDs to ~~spanning trees~~ MSTIDs, represented by the MST Configuration Table (8.9.1).

A ~~B~~bridge supporting PBB-TE can assign specific VID values to provisioned ESPs but can also support any of the spanning tree protocols. This is achieved by allocating the VIDs associated with the PBB-TE ESPs to a special MSTID, the TE-MSTID.

An SPT Bridge can allocate any given VLAN to the CIST, or to one of a number of MSTIs, as well as supporting shortest path bridging for other VLANs within an SPT Region. The assignment of VLANs and VIDs to MSTIs is subject to exactly the same considerations and constraints as for MST Bridges. In addition to the Base VID used to identify frames for the VLAN when transmitted on the CST outside the region, each shortest path VLAN is supported by a number of shortest path VIDs (SPVIDs), one for each SPT Bridge within the region. SPVIDs are dynamically allocated to identify a shortest path VLAN (as identified by the Base VID) and the SPT (rooted at a particular SPT Bridge) as required.

Dynamic SPVID allocation is supported by SPB and SPBB protocols and allows the addition of bridges to existing SPT Regions without disruptive configuration changes, as well as allowing supporting autoconfiguration of shortest path bridging in simple networks where all user data is assigned to a VLAN identified by the default PVID of 1 (<Table 9-2>). However, prior to SPVID allocation, all bridges in an SPT Region have to agree which VLANs are to be shortest path bridged, and which SPT Set is to be used for each of those VLANs. By default all VLANs whose Base VID is allocated to MSTID 1, will be shortest path bridged using the SPT Primary Set. The SPT configuration information can also identify specific SPT Sets, by specifying that frames for a VLAN with a Base VID that has been associated with a specific MSTID be supported by that set instead of by the MSTI.

An SPT Bridge allows a configuration choice of the protocol used to support MSTIs. That choice includes MSTP as specified in clause 13. If no protocol is chosen the MSTIs will not be constructed but the MSTID can still be used to select SPT Sets.

NOTE—The use of MSTIDs to support allocation of Base VIDs to SPT Sets allows the per VLAN components of the necessary information to be conveyed in the MST Configuration Digest, thus avoiding any need for a separate digest.

8.9.1 MST Configuration Table

The MSTI Configuration Table specifies an MSTID for each possible VID.

In an MST Bridge ~~defines, for each VID, the~~ each MSTID identifies ~~of~~ the MSTI ~~spanning tree instance~~ to which the VID is allocated, and an MSTID of zero identifies the CIST.

In a Bridge that supports PBB-TE an MSTID of 0xFFE, the TE-MSTID, identifies VIDs that can be used by ESPs.

Copyright © 08 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

In an SPT Bridge, MSTIDs that do not appear in the SPT Set List (8.9.5) also identify an MSTI to which the VID is allocated or the CIST. MSTIDs that do appear in the SPT Set List identify the SPT Set for the VID. An MSTID of hex FFF identifies VIDs that can be used as SPVIDs for any SPT Set.

The MST Configuration Table cannot be configured directly; configuration of the table occurs as a consequence of configuring the relationships between VIDs and FIDs (8.8.7), and between FIDs and MSTIDs ~~spanning trees~~ (8.9.3).

8.9.2 MST configuration identification

For two or more MST Bridges to be members of the same MST Region (3.32), it is necessary for those Bridges to be directly connected together (i.e., interconnected only by means of LANs, without intervening Bridges that are not members of the region), and for them to support the same MST Region configuration. Two MST Region configurations are considered to be the same if the correspondence between VIDs and spanning trees is identical in both configurations and they use the same information to identify the configuration, including the same Configuration Name.

NOTE 1—If two adjacent MST Bridges consider themselves to be in the same MST Region despite having different mappings of VIDs to spanning trees, then the possibility exists of undetectable loops arising within the MST Region.

In order to ensure that adjacent MST Bridges are able to determine whether they are part of the same MST Region, the MST BPDU supports the communication of an MST Configuration Identifier (13.7).

NOTE 2—As the MST Configuration Identifier is smaller than the mapping information that it summarizes, there is a small but finite possibility that two MST Bridges will assume that they have the same MST Region Configuration when this is not actually the case. However, given the size of the identifier, this standard assumes that this possibility is sufficiently small that it can safely be ignored. Appropriate use of the Configuration Name and Revision Level portions of the identifier can remove the possibility of an accidental match between MST Configuration Identifiers that are derived from different configurations within a single administrative domain (see 13.7).

8.9.3 FID to MSTID Allocation Table

The FID to MSTID Allocation Table defines, for all FIDs that the Bridge supports, the MSTID ~~of the spanning tree instance~~ to which the FID is allocated. An MSTID of zero is used to identify the CIST.

NOTE—MSTIDs that are present in the MSTI List (12.12) identify spanning tree instances supported by MSTP. MSTIDs that are in the SPT Set List (8.9.5) identify (indirectly) VLANs that are supported by shortest path bridging.

~~NOTE—The management operations defined in Clause 12.12 make use of the concept of an MSTI List to instantiate/de-instantiate MST instances, and will only permit the allocation of FIDs to MSTIDs that are present in the MSTI List.~~

8.9.4 SPT Configuration Table

The SPT Configuration Table specifies the following for each VID:

a) A Base VID.

If the VID is not an SPVID, the Base VID is the VID itself. If the VID is an SPVID and is not currently used the Base VID is hex FFF. Otherwise, if the VID is a SPVID and has been allocated to support a specific VLAN, the Base VID is the Base VID for that VLAN and the following is also specified:

b) The Root Identifier for the SPT that uses the SPVID

Copyright © 08 IEEE. All rights reserved.

This is an unapproved IEEE Standards Draft, subject to change.

8.9.5 SPT Set List

The SPT Set List is a list of {MSTID, SPT Set identifier} tuples. VLANs whose Base VID appears in the MST Configuration Table with an MSTID that is included in this list are supported by shortest path bridging. SPT Set identifiers are small integers: the SPT Primary Set identifier is 1. By default, the list comprises a single entry for MSTID 1 and SPT Set 1. Addition of a tuple with an MSTID of zero, to specify that VLANs that would otherwise be allocated to the CIST will be shortest path bridged, shall not be permitted. If the MSTI Enabled flag is false the MSTI is not constructed for this MSTID, and VLANs allocated to this MSTID will be supported by the CIST if there are insufficient SPVIDs to do SPB.

NOTE—It is anticipated that SPB and SPBB protocols will support no more than two SPT Sets. If there are more entries in the SPT Set List than supported SPT Sets the additional MSTID values are taken as also identifying the SPT Primary Set.

8.9.6 SPT configuration identification

For two or more SPT Bridges to be members of the same SPT Region (3.32), it is necessary for those Bridges to be directly connected together (i.e., interconnected only by means of LANs, without intervening Bridges that are not members of the region), and for them to support the same SPT Region configuration. This requirement is identical to that for MST Regions: a given SPT Region can support selected MSTIs as well as shortest path trees, and the configuration of the SPT Region that a particular SPT Bridge can participate in is identified by an SPT Configuration Identifier that is a compatible extension of the MST Configuration Identifier (8.9.2,13.7). The part of the SPT Configuration Identifier that identifies the MST Configuration and signals that the configuration is further extended to provide for shortest path bridging, can be communicated in MST BPDUs if necessary.

Two SPT Region configurations are considered to be the same if their MST Region configurations are the same, they reserve the same VIDs to support shortest path bridging, they agree on the VLANs that are to be shortest path bridged and on which SPT Set is to be used for each of these, and they use the same SPB(27) and SPBB (28) protocols.

8.10 Spanning Tree Protocol Entity

Add the following paragraph at the end of clause Clause 8.10 as follows.

The ISIS-SPB Entity comprises an instance of IS-IS with shortest path bridging extensions as specified in Clause 29. The ISIS-SPB Entity is described, for the purposes of management, as distinct from the Spanning Tree Protocol Entity. However, ISIS-SPB and Spanning Tree Protocol Entities that calculate active topologies for the same Bridge Port use the ISS service access point (see Clause 8.5), the same individual MAC address, and the same group MAC Address (for frames transmitted and received using a group destination MAC address). The ISIS-SPB Entity uses the state machines and state machine variables supported by the Spanning Tree Protocol Entity to determine the extent of the SPT Region, and to communicate the TAP Digest in BPDUs.

This amendment makes no changes to clauses Clause 8.11 and Clause 8.12

Copyright © 08 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

8.11 MRP Entities

8.12 Bridge Management Entity

8.13 Addressing

Change the initial paragraph of clause Clause 8.13 as follows:

All MAC Entities communicating across a ~~Bridged Local Area Network~~ bridged network use 48-bit addresses. These can be Universally Administered Addresses or a combination of Universally Administered and Locally Administered Addresses.

This amendment makes no changes to clauses Clause 8.13.1 through Clause 8.13.2.

8.13.1 End stations

8.13.2 Bridge Ports

8.13.3 Use of LLC by Spanning Tree Protocol Entities

Change the first paragraph of clause Clause 8.13.3 as follows.

Spanning Tree Protocol Entities uses the DL_UNITDATA.request and DL_UNITDATA.indication primitives (ISO/IEC 8802-2) provided by individual LLC Entities associated with each Bridge Port to transmit and receive ~~frames~~ BPDUs (Clause 14). The source_address and destination_address parameters of the DL_UNITDATA.request shall both denote the standard LLC address assigned to the Bridge Spanning Tree Protocol (Table 8-6). Each DL_UNITDATA request primitive gives rise to the transmission of an LLC UI command PDU, which conveys the BPDU or MRP PDU in its information field.

Add the following paragraph at the end of clause Clause 8.13.3 as follows.

A Spanning Tree Protocol Entity that supports ISIS-SPB uses the EtherTypes allocated for IS-IS and ES-IS, as specified for the relevant protocols, to identify their use of the frames it transmits (see Clause 29).

This amendment makes no changes to clauses Clause 8.13.4.

8.13.4 Reserved MAC Addresses

8.13.5 Group MAC Addresses for spanning tree protocols

Add the following paragraph at the end of clause Clause 8.13.5 as follows.

The same Group Address is used by a given Spanning Tree Protocol Entity to transmit BPDUs (Clause 14) and all other frames transmitted to support ISIS-SPB operation (Clause 29).

This amendment makes no changes to clauses Clause 8.13.6 through Clause 8.13.8.

Copyright © 08 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

8.13.6 Group MAC Addresses for MRP Applications

8.13.7 Bridge Management Entities

8.13.8 Unique identification of a Bridge

8.13.9 Points of attachment and connectivity for Higher Layer Entities

Change the first paragraph of clause Clause 8.13.9 as follows.

The Higher Layer Entities in a ~~B~~bridge, such as the Spanning Tree Protocol Entity (8.10), MRP Entities (8.11), the ISIS-SPB Entity (8.10, Clause 29), and Bridge Management (8.12), are modeled as attaching directly to one or more individual LANs connected by the Bridge's Ports, in the same way that any distinct end station is attached to the network. While these entities and the relay function of the ~~B~~bridge use the same individual MAC entities to transmit and receive frames, the addressing and connectivity to and from these entities is the same as if they were attached as separate end stations "outside" the Port or Ports where they are actually attached. Figure 8-5 is functionally equivalent to Figure 8-2, but illustrates this logical separation between the points of attachment used by the Higher Layer Entities and those used by the MAC Relay Entity.

Change the tenth and eleventh paragraphs of clause Clause 8.13.9 as follows.

~~The connectivity provided to Higher Layer Entities and to the LANs that compose a Bridged Local Area Network can be further controlled by a Bridge Port operating as a network access port (IEEE Std 802.1X). The operation of Port-based access control has the effect of creating two distinct points of access to the LAN. One, the Uncontrolled Port, allows transmission and reception of frames to and from the attached LAN regardless of the authorization state; the other, the Controlled Port, only allows transmission following authorization. If the port is not authorized, the Spanning Tree Protocol Entity, which uses the Controlled Port (as does the MAC Relay Entity) will be unable to exchange BPDUs with other Bridges attached to LAN A, and will set the Bridge Port State to Discarding.~~
Port-based network access control (IEEE Std 802.1X) and MAC Security (IEEE Std 802.1AE) can be used to provide a further level of control over the connectivity provided by a Bridge Port to the MAC Relay Entity and the Higher Layer Entities within a bridge. Port-based network access control creates two distinct service access points for the LAN: the *Controlled Port* and the *Uncontrolled Port*. MAC_Operational is TRUE for the Controlled Port only when criteria for authentication, authorization, and secure connectivity have been satisfied; while MAC_Operational for the Uncontrolled Port is the same as that for direct access to the LAN. Both the Spanning Tree Protocol Entity and the MAC Relay Entity attach to the Controlled Port, thus ensuring that the connectivity seen by each of those entities is the same. If MAC_Operational for the Controlled Port is FALSE, the Spanning Tree Protocol Entity will ensure that both forwarding and learning (Clause 8.4) will be FALSE for that Port (i.e. the Port State will be Discarding). The Uncontrolled Port supports the operation of protocol entities such as the PAE specified by IEEE Std 802.1X, that participate in the authentication exchanges necessary before Controlled Port connectivity is permitted or that distribute other unsecured information.

~~NOTE—If the Spanning Tree Protocol Entity was not aware of the Unauthorized state of the Port, and believed that it was transmitting and receiving BPDUs it might assign a Bridge Port State of Forwarding. Following authorization a temporary loop in network connectivity might then be created.~~

Figure 8-16 illustrates the connectivity provided to Higher Layer Entities if the MAC entity is physically capable of transmitting and receiving frames~~, i.e., MAC_Operational is TRUE~~, but MAC_Operational is FALSE for the Controlled Port ~~AuthControlledPortStatus is Unauthorized~~. Higher Layer Entity A and the PAE ~~(the port access entity that operates the authorization protocol)~~ are connected to ~~the~~ an Uncontrolled Port and can transmit and receive frames using the MAC entity associated with the Port for LAN A, which Higher Layer Entity B cannot. None of the three entities can transmit or receive to or from LAN B.

Copyright © 08 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

Change Figure 8-16 as follows, also removing the arrows from the deleted text.

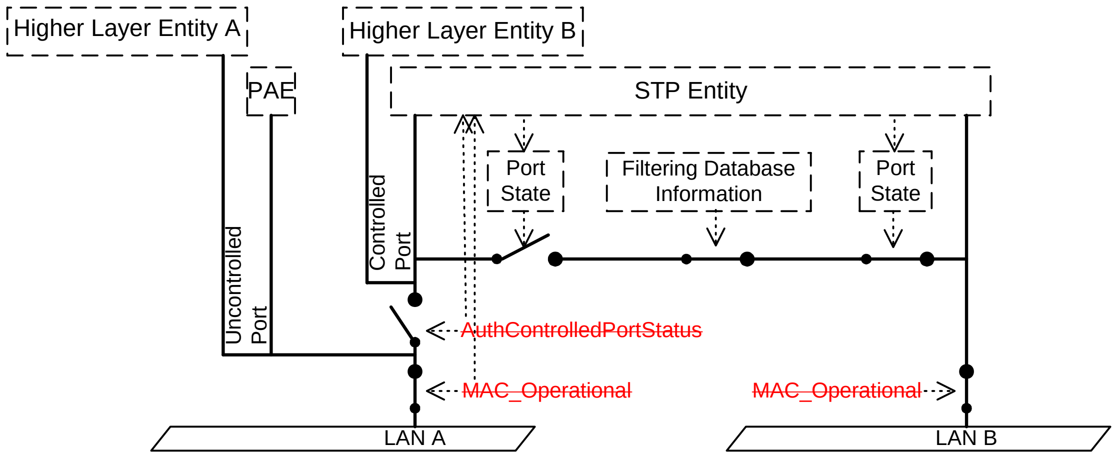

Figure 8-16—~~Effect of authorization~~ Controlled and Uncontrolled Port connectivity

This amendment makes no changes to clause Clause 8.13.10 and Clause 8.13.11.

8.13.10 VLAN attachment and connectivity for Higher Layer Entities

8.13.11 Connectivity Fault Management Entities

Copyright © 08 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.