Envelope-to: tony@jeffree.co.uk
Received: from [161.71.169.13] (helo=columba.eur.3com.com)
by mserv1c.u-net.net with esmtp (Exim 2.10 #34)
id 11WQMk-0006QA-00
for tony@jeffree.co.uk; Wed, 29 Sep 1999 20:30:18 +0000
Received: from toucana.eur.3com.com (eurelay.eur.3com.com
[140.204.220.50])
by columba.eur.3com.com (8.9.3/8.9.3) with ESMTP id VAA25836
for <tony@jeffree.co.uk>; Wed, 29 Sep 1999 21:28:07 +0100 (BST)
Received: from notesmta.eur.3com.com (eurmta1.EUR.3Com.COM
[140.204.220.206])
by toucana.eur.3com.com (8.9.3/8.9.3) with SMTP id VAA16867
for <tony@jeffree.co.uk>; Wed, 29 Sep 1999 21:26:44 +0100 (BST)
Received: by notesmta.eur.3com.com(Lotus SMTP MTA v4.6.3 (733.2 10-16-
1998)) id 802567FB.007185B4 ; Wed, 29 Sep 1999 21:39:57 +0100
X-Lotus-FromDomain: 3COM
From: "Les Bell" <Les_Bell@eur.3com.com>
To: tony@jeffree.co.uk
Message-ID: <802567FB.00718338.00@notesmta.eur.3com.com>
Date: Wed, 29 Sep 1999 21:31:50 +0100
Subject: 802.1 Meeting Minutes, York
Mime-Version: 1.0
Content-type: text/plain; charset=iso-8859-1
Content-Disposition: inline

# 1 802.1x - Port Based Network Access Control

There was a discussion about the nature of a point-to-point connection. There is a view that this may be a ?logical? point-to-point link, not necessarily just a physical point-to-point connection. The document should bear this in mind throughout.

There is an IP ?connection? between the switch and the authentication server, Section 3.2 needs to be modified to reflect this.

Section 3.3 Peer - a better term for ?peer? would be ?supplicant?. ... at one end of a point-to-point link...

Norm Finn and others, wanted to have 802.1x defined as a separate document, not just a set of changes to 802.1D. This is because this can apply to more than just 802.1D Bridges. The careful use of the ?logical point-to-point link? definition would allow this. Mick Seaman expressed that he would prefer to limit the scope to 802.1D for now, as we have no say over the other applications, such as 802.11 or to a ?smart repeater?. There is no current definition of how 802.1D applies to 802.11 networks, so this would have to be resolved first. Summary ? stick to ?LAN Segment? for now, but don?t forget 802.11.

Norm asked if we need to describe the discarding of frames, due to the denial of service on un-authenticated ports. In Section 6.3. This is analogous to the discarding of frames on ports that are not yet a member of an 802.3ad Aggregate Link, which we do not describe. As a definition of a ?piece of equipment?, the original intent of 802.1D, the description of this behaviour is appropriate, but as a description of a ?protocol? it is not.

There is a ?goal? here that it should be possible to take any device, not a 802.1D Bridge, and apply 802.1x to that device. It should not be necessary to modify 802.1x to allow this.

Section 7.4 - The authentication state should be no different from the port being physically enabled/disabled.

Interaction with 802.3ad is an issue, it is undesirable to allow un-authenticated ports to aggregate with authenticated ports, but the Bridge does not see the Aggregate Link until aggregation is completed. The Bridge can overcome this problem by forcing all ports to be ?Individual? until they are authenticated.

The wording of 7.4 needs to reflect that frames may be discarded because of influences beyond control of 802.1D, such as 802.3ad or 802.1x.

The idea of allowing management (e.g. SNMP) through an un-authenticated switch is not popular. But there is some sympathy with the view that we need to prevent cutting off management altogether. This seems to be at the discretion of the Bridge implementor.

GARP does not break if it takes no notice of the disabled state, however, it is cleaner if it does.

Taking the view that 802.1x frame discard occurs before the forwarding process, section 7.7, Forwarding Process, is NOT affected, so the suggested text may be removed from 802.1x Draft.

Section 7.12 - There needs to be a description of how to get the Bridge authenticated itself, or whether it needs to be authenticated. Either the Bridge is a ?supplicant? on all ports, until one of them is authenticated; or one port is ?always authenticated?, being the connection used to reach the Authentication Server. Once the switch has this authenticated path, it may then become an authenticator to its other ports. At least one Bridge has to be the ?all powerful? core of the network, which has direct access to the Authentication Server.

Section 7.12.3 - It is assumed that a filtered Bridge Multicast address will be allocated for EAPOE. There is a potential for malicious interference if a unicast address is used, but this was not detailed. The text should ensure unicast is not used.

Clause 7.12.3 h) We probably want to allow other options, including RADIUS. We do not want to exclude other authentication server options. There is a possible need to define a RADIUS Profile to ensure inter-operability.

Section 8 needs to distinguish between STAP disabled/enabled and Authentication disabled/enabled. This could be just modelled on the ifStatus up/down states for the physical port state, which has administrative

and operational states of the port. Spanning Tree enabled/disabled simply reflects the up/down-ness. We need to fix this in 802.1t

Section 12 GARP - This is now clear ? part of the bridge, therefore subject to disabling.

Section 14 - Bridge Management. If we separate X, we need a concept of a separate 802.1X Management stack.

Likely to need:

- Authentication on/off.
- Counters for protocol exchanges?
- ??

Section 15 - We do need to define an SNMP MIB as part of this activity.

Section 18 - Change section title to ?Port Access Control?.

Section 18.1 - This needs to talk about the port being isolated from whatever sits above the port, in more general terms. It could usefully include annex material that describes the application of this in a Bridge, plus other examples, such as server, router, etc.

May need to refer to 'a system' as the container in which ports may be found.

Section 18.3.1 - Need to put the ?Y? diagram in here, so the Note about DHCP becomes unnecessary.

Section 18.3.2 - This does not belong here.

Section 18.3.3 - Discuss the mechanisms that contribute to opening the switch:

- Sever tells you it is unauthorized
- Management control

- Port not operational
- Explicit logoff
- Lose connection to the server & time out
- Retransmission timer expires

Section 18.4.5 - We need an explicit Logoff message.

There is concern about the state of the EAP in RADIUS specification. This is believed to be an IETF Draft, so 802.1x cannot refer it to. We need to check this and take appropriate action.

Section 18.4.6 - There was discussion about the IDLE_TIMEOUT, whether the suggested default value of 3600 seconds is reasonable or not. Everyone agreed that this should be user configurable, but no suggestions were made for a different default value.

Section 18.4.8 - This needs to clarify which EAP messages get relayed on (everything except EAP Start/Stop) Describe the realy function half, plus references to the EAP/RADIUS definition.

Section 18.4.9 - Eliminate the use of unicast (always use multicast address).

Do we need to use a 802.5 FA? Is this an issue? Ask 802.5.

Section 8.4.10 - Clean up the state machine descriptions re action/event definitions, etc. Do a state table.

Section 18.6.2 - The encapsulation format defined differs from the original papers, in that it collapses the description of the packet to a single level of encapsulation. The frame definition is actually unchanged in the definition of the fields transmitted.

Section 18.6.3 - EAPOE frames would never need to be source-routed in Token-Ring networks. State that it is an LLC frame.

Section 18.6.4 - Need to liase with Bernard Abobo (?) regarding the allocation of a new EAP message code to be used for Start/Stop messages. Paul Congdon volunteered to do this.

There were no issues discussed on the Annexes to the current 802.1x Draft.

Does 802.1X need to be a separate document? Or is it 802.1x, an addendum to 802.1D? There are some changes that are required for 802.1D, even if 802.1X is a separate document. These changes could be incorporated into 802.1t. The consensus seemed to be in favour of a separate document. This will require a change to the PAR, which should be done as soon as possible.

## 2 802.1w - Rapid Reconfiguration of Spanning Tree

Mick Seaman is working on producing a new draft for 802.1w, this is not completed yet. It is based on an implementation in progress. He gave a presentation on this work. Details are in Mick?s document, which should be made available separately on the 802.1 FTP site in a few days.

There are new state machines, re-defining the behaviour in the exiting states. The protocol has been simplified and defined in terms of ports, rather than Bridges. Hello Timers are driven independently for each port, rather than from the Root port. A detailed run-through of the state machine was made for a root port. Other implications to other areas of the protocol were also presented.

## 3 802.1t - .1D Maintenance

Most changes are the result of moving items from other documents into this draft, as agreed at the last meeting.

The table 12-7 is incorrect for the rLeaveIn event in state VO, saying this transitions to LO state. The example code and Table 12-3 both say this stays in state VO. Table 12-7 is to fixed to agree with the others.

Annex Z - Itemes a) through d) are not required. Rather than change the figures, need a global statement on LLC Entities explaining that it also includes Ethernet.

Need to fix the some errors in the GARP/GMRP source code. Mick will take a look at these.

There needs to be a comment on what the initial state should be for the state machines. The intention is that it does not matter, as they should learn the current situation and transition to the correct state very quickly.

## 4 802.1u - .1Q Maintenance

No issues were raised regarding 802.1u Draft 2.0.

## 5 802.1w - Rapid Reconfiguration of Spanning Tree (revisited)

Mick Seaman distributed paper copies of the three state diagrams presented at yesterday?s meeting. He explained the states and transitions between them for each of the state diagrams.

[Need to include Figure 17-1, 17-2 and 17-3 here.]

The first, Figure 17-1 - Port Role Transitions, is the only Bridge-centric state machine. There are no exit transitions marked for states A and B, these should occur when the port is enabled, in any role, always transitioning back to state PT.

Figure 17-2, Designated Port Transitions and Figure 17-3, Root Port Transitions, no issues were raised on these yet.

Mick believes the reconfiguration time of the network as a result of these changes becomes the processor scheduling and transmission time at each node from the root to the edge of the network. There should be a limit on the rate of BPDUs transmitted, similar to what has been defined for

802.3ad, a limit of 3 BPDUs per second (or two seconds) is suggested. Multiple Spanning Trees should not share the same BPDUs.

Migration issues. It seems necessary to use a new version number in the BPDUs, as the version 1 BPDUs cannot be changed. It is suggested that a port should send old and new BPDUs on a point-to-point link, until it sees a new BPDU returned, in which case it stops sending old BPDUs. Old Bridges should not see the new BPDUs at all, but should filter them.