Token Bus Protocol Number 3A

Patent Application

GB 2 319 706 A (application no. 9 624 414.0)

Mr Kim Lyon

Contact Details :-

Mr Kim Lyon
Suite 12397
72 New Bond St.
London
W1S 1RR
U.K.

Ph.:- +44-7785-362 319

Web Site :- wrldcomp.com
Token Bus Protocol 3A

Abstract

A retrospective token bus protocol with bandwidth management and hybrid virtual and physical channel based addressing . The bandwidth managment techniques provide for the control of unit and cycle bandwidths . The addressing techniques provide source and destination based channel addressing and broadcast addressing . The protocol provides for a highly efficient , simple and cheap method of implementing communication on a bussed topology and utilises sophisticated communication techniques .

Token Bus Protocol Number 3A Abstract

Token bus protocols provide the low data link overhead of token ring networks with the low cost and high reliability of the bus topology .

The bussed topology consists of a common communication medium over which all units communicate directly with all other units . The bussed topology can exist in a number of forms such as :-

1) a physical medium such as two wires .

2) an optical network where
   i) a number of fibre optic cables are connected to a central hub where they are connected in a bussed manner using optical or opto-electrical means . The connection being wired or-ed .
   ii) a number of fibre optic cables are connected in a multidropped fashion to single or dual open loop fibre optic cables using optical or opto-electrical means . The connection being wired or-ed .

3) a common medium such as a radio or optical medium .

The bussed topology provides high reliability by providing a means for the individual units to connect directly onto a high reliability common communication medium . Thus the reliability of the network , including the individual units , is dependent just on the reliability of the common communication medium and the reliability of the respective individual unit network interface . If one unit network interface fails the rest of the network will continue to operate . This is as opposed to a loop network where messages pass from the source unit to the destination unit through the units placed in between . This results in the reliability of the network being dependent on the reliability of the individual unit network interfaces divided by the number of units . If one unit network interface fails the whole network fails .

Token bus protocols allow messages to be transmitted from multiple units without any unused time being placed in-between messages and without any collisions occurring . This is as opposed to Carrier Sense Multiple Access \ Collision Detection protocols that have unused time due to response times and random retry times and have collisions due to multiple units trying to access the bus simultaneously . These two areas of high data link overhead are eliminated by the use of token passing .

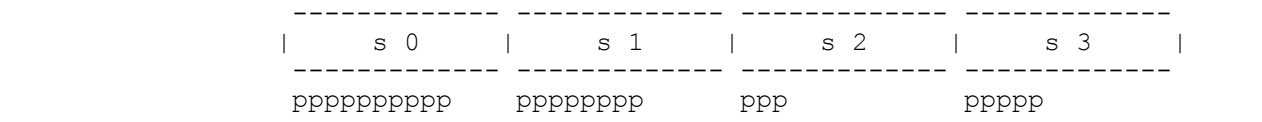
Implementations of token bus protocols usually use prospective token passing where the unit holding the token has to have knowledge (including relationship to itself) of the number (address) of the unit that the token is going to be passed onto . This information may be obtained and stored or gained in response to a presence testing operation .

Retrospective token passing does not require that the unit that is holding the token has knowledge of the unit number (address) of the unit that the token is going to be passed onto . When the unit holding the token completes it's transmission it releases control of the bus and hence the token . The subsequent unit has knowledge of where the token is being held and hence where it is coming from and when it passes into it's time domain it either takes up the token or allows it to pass onto another unit .

Retrospective token bus protocols provide the token bus protocol in a more simple , easily and cheaply implemented and manufactured form than prospective token bus protocols . Retrospective token bus protocols are also faster due to their lower data link overhead .

In many modern day networks bandwidth management is an important factor . This is often not just a matter of designing a network that can accommodate the maximum bandwidth expected but also of ensuring that time critical transmissions are carried in their entirety and within their required time window . Telephone and television traffic are good examples of services requiring this kind of network performance . The solution has often been the slotted network system where the total bandwidth of the network is divided up into smaller equal bandwidths and these slots assigned to the individual services . For computer traffic this often means that there is unused slot space . Further with audio and video compression which results in varying bandwidths and with the time critical aspect requiring that the slot width be assigned corresponding to the maximum required bandwidth there is further unused slot space . As such in order to allow for maximum bandwidth availability the slot width needs to be dynamically variable but with the network operated within a managed bandwidth environment . In this manner the services requiring fixed maximum bandwidth availability will be provided this cycle space but services with no such requirement will wait for available cycle space to transmit their data . Where a time critical service does not use that maximum cycle space made available to it it makes the remaining cycle space available for other services .

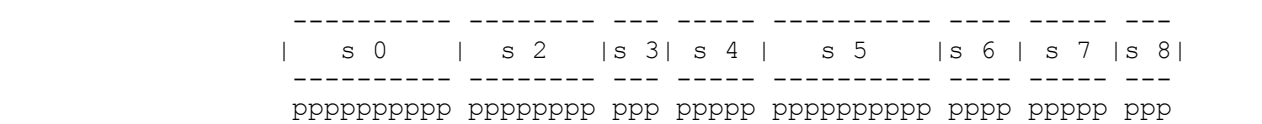
Fixed Slot Widths



-> Data length varies up to slot width .
s = slot . p = active packet area .

Figure 1

Dynamically Varying Slot Widths



-> Slot width equals data length plus data link overhead .
s = slot . p = active packet area .

Figure 2

Consequentially with dynamic bandwidth management more slots can be fitted in per cycle thus ensuring maximum data transfer per unit time . IE. maximum use is made of the total available network bandwidth .

In order to be able to manage the network bandwidth the units transmitting non time critical data will need to be able to clearly determine the packet length . As such the packet length has to be supplied to the unit before the data to be transmitted . This allows the unit to make the necessary decisions with regards to the bandwidth management .

There are 3 techniques that can be used in order to maintain packet synchronisation :-

1) Frame Generation - requires knowledge of the line state and as such is not suitable for units frequently unplugging from and plugging into the line . Synchronisation by blank frames either transmitted regularly or triggered via a separate control line . Fixed line bandwidth relationship to maximum data bandwidth . Low data link control overhead but potentially high data link unused slot space overhead .

2) Enlarged Character Size - eg. 9 bit characters where the 9 th. bit is used to form a unique bit pattern (eg. 9 bits of 1's followed by a 0) as a flag . Data is transmitted as bytes occupying the lower 8 bits . Fixed transmission line bandwidth relationship to actual data bandwidth . High data link control overhead .

3) Zero Insertion - The pattern 01111110 is used as a flag with 0's inserted after 5 1's in order to maintain the uniqueness of the flag . Variable actual data bandwidth relationship to transmission line bandwidth . Low data link overhead .

In the following outline of an implementation of a token bus protocol using the dynamic bandwidth management technique the Zero Insertion technique has been used . Although this technique does not have a fixed relationship between the data bandwidth and the network bandwidth the network bandwidth can be managed by controlling the transmission of non time critical data and averaging over a number of cycles . The advantage of this technique is it's low data link overhead .

This bandwidth management method incorporates two dynamically variable bandwidth management techniques . These techniques allow units to take advantage of the varying availability of the bandwidth thus allowing maximum use of the network and unit bandwidth to occur .

The first technique allows the network's maximum cycle time to be specified . This is undertaken by broadcasting on the network the unit's maximum required cycle length . The network then adjusts to the smallest required cycle length broadcast thus ensuring that the units carrying the time critical services get network access within their required time . Any services that access the network slower will access the network in a staggered format (ie. they will not transmit data during some cycles) . The total cycle length combined with the effective data transfer rate and the individual service required bandwidth determines the total number of services that can use the network . A means is provided to allow individual units to request a holding off of other non time critical traffic in order to create cycle space for it to be able to transmit their pending packets . This ensures that an equal flow of non time critical traffic in ensured .

The second technique allows the individual units to specify their own bandwidth . This provides a means for units to control the rate of flow of data into the units . Thus ensuring that the rate of flow of data into the units is less than the maximum rate of flow of data out of the units into the unit's associated computer system .

Units not transmitting time critical traffic transmit data only when sufficient cycle space (over one or over a number of cycles) is available to transmit the packet .

Conventions

The Following conventions are used :-

1) The most significant bit (the left most bit) shown is shifted out first .

2) All bit patterns are shown in binary except those shown with an H suffix which are shown in hexadecimal .

Glossary

Character - a group of bits of fixed length . Can be electrically present (active) or absent - as time space - (inactive) .

~ - an unspecified transmission .

<,>,^ - indicates what occurs next in time .

Token Bus Protocol Number 3A

The Token Bus Protocol Number 3A known hereafter as the Token Bus Protocol is defined as follows :-

The Token Bus Protocol consists of four types of messages :-

1) Identification and Token Pass Only (data not present) .
2) Bandwidth Request and Token Pass Only (data not present) .
3) Token Pass Only (data not present) .
4) Data Transmission .

The packets are encoded in the following basic format :-

Synchronisation
---

i) All packets are preceded by a flag (01111110) .
ii) The flag is maintained as a unique character by inserting a 0 after 5 consecutive 1's at transmission and by removing any 0's that occur after 5 consecutive 1's at reception of all packet information other than the flag .

Media Access Control

After the flag all packets are preceded by a 4 bit sequence that indicates the function of the packet .

3 2 1 0
---
0 0 Identification with token pass - no data .
0 1 Bandwidth Request with token pass - no data .
1 0 Token Pass - no data .
1 1 Data with token pass .

0 Don't force an active token passing sequence - follow on .
1 Force an active token passing sequence .

Please Note :- If the unit is transmitting an identification packet (includes bandwidth information) and is forcing an active token pass the other units respond with follow on identification packets .

X Sub Function .

Identification

Sub Function
---

3 2 1 0
---
0 0 X 0 Without a valid source address .
0 0 X 1 With a valid source address .

When a unit comes on line the unit has to assign itself a free number (address) . If the network is in passive or active token passing it has to force the other units to identify themselves and to specify their bandwidth requirements . It does this by transmitting an Identification packet without a valid source address and forces the other units to identify themselves by asserting the Force Active Token Passing Cycle bit . During the Identification Cycle it identifies a free number and assigns it to itself . After the cycle has completed it forces a Token Passing Cycle where it identifies it's number to the other units .

Packet Sequence	Bit Size
Function	4 bits
Source Address	6 bits
Channel Bandwidth	11 bits
Unit Bandwidth	11 bits

The channel bandwidth is a multiple of the number of bits that the unit requires per token passing cycle as a maximum channel bandwidth . This effectively specifies the maximum amount of time between the unit's transmissions that is required by the unit . This ensures that the unit has line access in order to transmit time critical traffic .

The unit bandwidth is a multiple of the number of bits that the unit can accommodate per token passing cycle as a maximum unit bandwidth . This ensures that the unit is able to maintain a match between the rate of flow of packets into it from the line and out of it into the attached computer system .

If during normal operation a unit wishes to change it's channel or unit bandwidths it transmits an identification packet but does not force an identification response from other units .

Bandwidth Request

Channel Bandwidth Request

Sub Function

3	2	1	0
0	1	X	0

Packet Sequence	Bit Size
Function	4 bits
Source Address	6 bits
Hold Off Cycle Length	14 bits

The Hold Off Cycle Length specifies the cycle bandwidth in the next cycle requested by the source unit .

Unit Bandwidth Request

Sub Function

3	2	1	0
0	1	X	1

Packet Sequence	Bit Size
Function	4 bits
Destination Address	6 bits
Source Address	6 bits
Hold Off Unit Bandwidth Length	16 bits

The Hold Off Unit Bandwidth Length specifies the unit bandwidth in the next cycle of the destination unit requested by the source unit .

Token Pass Only - No Data

Sub Function
---

3 2 1 0
---
1 0 X 0

Packet Sequence	Bit Size
Function	4 bits
Source Address	6 bits

Data Present Transmission

Addressing

The Token Bus Protocol uses channel based addressing . This allows the addressing to be virtualised . Where a unit is acting as a gateway it substitutes the corresponding outgoing channel address for the incoming channel address as it passes the packet from the receiver to the transmitter . This ensures that the addresses are kept to a minimal length . It also allows for the physical path to be changed without reference to the originating unit thus allowing saturated and broken links to be routed around .

Source Based Destination Channel Addressing

Sub Function
---

3 2 1 0
---
1 0 X 1

Packet Sequence	Bit Size
Function	4 bits
Destination Address	6 bits
Source Address	6 bits
Destination Channel	10 bits
Source Channel	10 bits
Time Criticality	1 bit
Data Length	11 bits
Data	up to 2048 bytes

Source Based Destination Channel Addressing ensures that a group of channels are reserved within the destination unit corresponding to the source unit . As such if a source unit is detected as having gone off line it's channels are not reassigned to another unit .

If the Time Criticality bit is asserted the packet is marked as time critical and is transmitted irrespective of bandwidth considerations being imposed on it .

The data length indicates the length of the subsequent data portion of the packet . If set to 000H the packet length is at the maximum (2048 bytes) .

Error checking of the data is performed by the network layer software or separate hardware . It is not performed by the communications controller as outlined within this specification .

Destination Based Destination Channel Addressing

Sub Function
---

3 2 1 0
---

1 1 X 0

Packet Sequence	Bit Size
Function	4 bits
Destination Address	6 bits
Source Address	6 bits
Destination Channel	10 bits
Source Channel	10 bits
Time Criticality	1 bit
Data Length	11 bits
Data	up to 2048 bytes

Destination Based Destination Channel Addressing allows multiple source transmissions to single destinations to occur .

Broadcast Addressing

Sub Function
---

3 2 1 0
---
1 1 X 1

Packet Sequence	Bit Size
Function	4 bits
Broadcast Address	10 bits
Source Address	6 bits
Time Criticality	1 bit
Data Length	11 bits
Data	up to 2048 bytes

Broadcast Addressing allows single or multiple source transmissions to multiple destinations to occur .

Token Passing

Access to the network is passed onto a subsequent unit at the end of the packet . The token is passed retrospectively . As such the unit holding the token does not know the number (address) of the unit and it's relationship to that unit that it is passing the token on to .

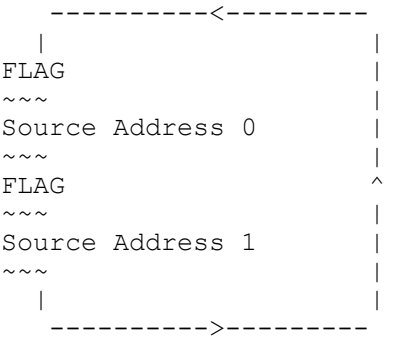
The unit that takes up the token knows the preceding unit's number and hence can access the network when the token is passed into it's numerical and time domain . Further the unit follows where the token has come from and as such in the absence of the preceding unit the unit knows where the token has come from and hence can access the network when the token is passed into it's numerical and time domain .

The token is either passed in an active or passive sequence . The active sequence is where the subsequent unit always takes up the token each cycle . It does this by actively transmitting on the network irrespective of whether it has control information or data to transmit . The passive sequence is where the subsequent unit either takes up the token if it has control information or data to transmit or it allows the token to pass onto a subsequent unit by not transmitting on the network . In both sequences the token is passed into the domain of the subsequent unit after the unit completes transmission .

The Active Token Passing is used to identify all the units on the network when a new unit comes onto the network . It is also used to determine the continued presence of units on the network in order to determine whether unit associated channels are still valid .

The Passive Token Passing is used during normal operation when no all unit identification is required . The Passive Token Passing having significantly less data link overhead than the Active Token Passing and hence effectively being the high speed token passing mode .

Active Token Passing Cycle



inactive character or characters inserted if and as required

Figure 3

The token position is tracked in the active token passing sequence by the use of the source address .

In the above example unit number 1 knows that unit number 0 is the immediately preceding unit numerically and hence in actuality and as such places it's transmission immediately after unit number 0 .

If a consecutive numbered unit is not on the network an inactive character is inserted in between the packet end and the subsequent flag . This becomes a free slot for a subsequent unit to occupy in the token passing sequence .

If a unit is switched on it will monitor the network for a specified time (eg. 65536 characters time) for any activity . If there is no activity it will assign itself the lowest number (eg. 00H) and transmit a " No Data To Be Transferred " message and then monitor again for any activity . If the network is active and passive token passing is occurring it will trigger an Active Token Passing Sequence . If or when active token passing is occurring it will monitor for an inactive character and will assign the number (address) corresponding to that inactive character to itself .

If a unit is disconnected from the network , on the next Active Token Passing Sequence it will be replaced by a number of inactive characters corresponding to the number of units between the previous unit and the subsequent unit for one cycle and then the subsequent unit will place just one inactive character between the previous unit and itself .

IE. if units 0 , 1 and 3 are present on the network and the active token passing mode is being used there will be no inactive characters between units 0 and 1 and there will be one inactive character between units 1 and 3 . If unit 1 is taken off the network there will be initially 2 inactive characters between units 0 and 3 (corresponding to units 1 and 2) and then on the subsequent cycle there will be a single inactive character between units 0 and 3 .

The inactive character is used for the subsequent entering of other units into the token passing sequence .

Passive Token Passing

Passive Token Passing consists of a Token Identification Sequence that consists of a control message , a no data to transfer message or a data to transfer message that is followed by a Token Take Up Period that consists of slots during which subsequent units can take up the token and hence access the network . The Token Identification Sequence and the Token Take Up Period form the Passive Token Passing Cycle during which the token may be taken up by another unit or retrieved by the last unit to transmit . During the Token Take Up Period no transmission occurs by the last unit to transmit . The Token Take Up Slots consist purely of time slices during which any of the subsequent units can take up the token by transmitting the Flag . This being followed by a control message , a no data to transfer message or a data to transfer message and subsequent Passive Token Take Up Cycles until the token is taken up by another unit .

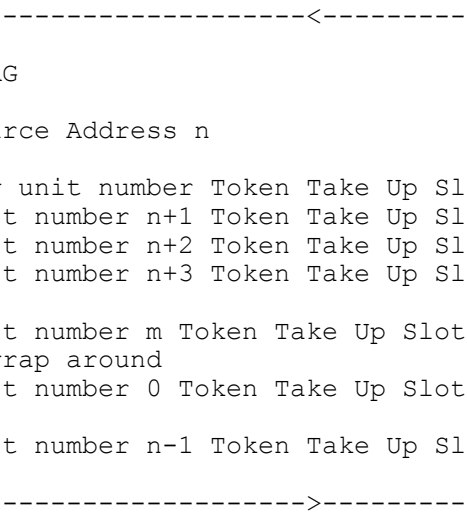


Figure 4

where m and consequently the number of Token Take Up Slots corresponds to the maximum unit number on the network as defined at the last Active Token Passing sequence . This includes the new unit number Token Take Up Slot . n (above) corresponds to the unit sequence position not the physical unit number .

The token position is tracked in the Passive Token Passing Sequence by the use of the source address and the Token Take Up Slot . The Token Take Up Slot is defined by it's unique time position . The Token Take Up Slot has sufficient length to allow the transmission of the unit taking up the token to be identified as the unit having commenced it's transmission . Typically this would be a two bit length to allow a 0 to 1 transition .

If a unit wishes to transmit it commences it's transmission within the Token Take Up Slot corresponding to it's number .

If no other unit transmits the last unit to transmit transmits an Active Token Passing Sequence without or with data being transferred (to identify and hence synchronise the take up slot positions) . This transmission immediately follows the last Token Take Up Slot and effectively corresponds to the unit number n Token Take Up Slot .

Initially Coming onto the Network

If a unit comes onto the network during Passive Token Passing it must first assign itself a free address . To do this it has to inform all other units on the network that it wishes for all units on the network to identify themselves by forcing all units into an active identification and token passing sequence .

If the network is in Active Token Passing this sequence has to be maintained so that all units will identify themselves .

The unit first monitors the network for 1 cycle and determines a position where it can transmit . For both Passive Token Passing and Active Token Passing this will be the first inactive bit . The unit forces all other units to identify themselves and actively token pass . It does this by transmitting a Force Identification and Active Token Passing sequence with an invalid source address (set to 00H) . All other units then respond with a follow on of their Identification and Active Token Passing sequences .

With the network now in active token passing mode the unit uses the first cycle to identify a free unit address (number) . It then assigns this unit address (number) to itself and then actively passes the token during the second cycle (and as required in subsequent cycles) to indicate it's presence on the network .

In Passive Token Passing the placement of the new unit number Token Take Up Slot immediately following the unit Token Identification sequence allows the new unit number token take up slot to be clearly identified without any reference to the number of units on the network . This means that the unit can gain access to the network immediately after one transmission rather than having to wait for at least two transmissions before being able to identify the new unit number Token Take Up Slot . It also places the Token Take Up Slot in the same relative position as an inactive character position within Active Token Passing .

In such a manner the unit coming onto the network can arbitrarily assign itself an address (number) .

Bandwidth Management

There are four bandwidth management controls available :-

1) the Maximum Cycle Length .
2) the Hold Off Cycle Length .
3) the Maximum Unit Bandwidth Length .
4) the Hold Off Unit Bandwidth Length .

Maximum Cycle Length

The Maximum Cycle Length specifies - in multiples of the bit length of the cycle - the maximum cycle length that this unit can accommodate . The network adopts the smallest maximum cycle length transmitted as it's maximum cycle length .

Each unit checks the actual cycle length against the maximum cycle length adopted . The cycle length may be accumulated over a number of cycles . Time critical data is always transmitted . Where non time critical data is present if the difference is greater than a waiting packet length the packet is transmitted . The transmission of a forced maximum cycle length request causes all other units to transmit their maximum cycle length requests and hence the new least cycle length is determined and adopted . The maximum cycle length request will occur when a new unit comes onto the network
- forced by that unit . It will also occur when required
- forced under network management control .

If a unit requests a Maximum Cycle Length of 0 this signifies that it does not require a limited cycle length .

Hold Off Cycle Length

The Hold Off Cycle Length specifies - in multiples of the bit length of the cycle - the amount of cycle space to be created by the other units within the next cycle by the subsequent units transmitting , in accumulation , up to a maximum of the Maximum Cycle Length minus the Hold Off Cycle Length .

Maximum Unit Bandwidth Length

The Maximum Unit Bandwidth Length specifies - in multiples of bytes - the maximum number of bytes that the unit - as specified by it's source address - can accommodate per cycle .

The other units restrict their non time critical direct transmissions to that unit such that they remain within that unit's bandwidth .

If a unit requests a Maximum Unit Bandwidth Length of 0 this signifies that it does not require a limited bandwidth length .

Hold Off Unit Bandwidth Length

The Hold Off Unit Bandwidth Length specifies - in multiples of bytes - the amount of cycle space to be created by the other units within the next cycle by the subsequent units that are transmitting to the destination unit , by transmitting , in accumulation , up to a maximum of the Maximum Unit Bandwidth Length minus the Hold Off Unit Bandwidth Length .

Non Time Critical Traffic

Non time critical data becomes bandwidth limited if a cycle length or unit bandwidth length has been specified .

For a unit transmitting bandwidth limited traffic (all other traffic other than Time Critical Traffic) the unit checks whether room exists in the current cycle or over the last number of cycles to transmit it's data to it's desired destination unit . If there is it transmits the data to that destination unit . If not it either creates cycle space by transmitting a hold off transmission within cycle message or it creates bandwidth space by transmitting a hold off transmission to unit message and waits for space to be created .

Time Critical Traffic

Where a unit has time critical traffic the time critical data is transmitted irrespective of whether there is cycle or unit bandwidth space .

Examples of the Operation of the Token Bus Protocol

The convention used is that the arrow points to what occurs next in time .

Active Token Passing

A Single Unit is Present On the Network

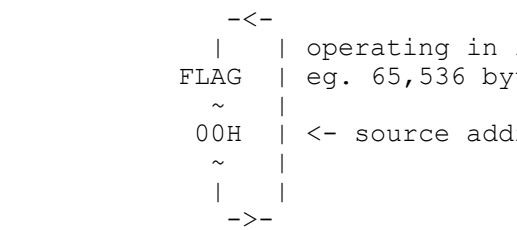


Figure 5

A Second Unit is Plugged into the Network

The second unit hears the first unit during it's inactive time . It assigns itself the next free number -> 1 and places itself into the cycle .

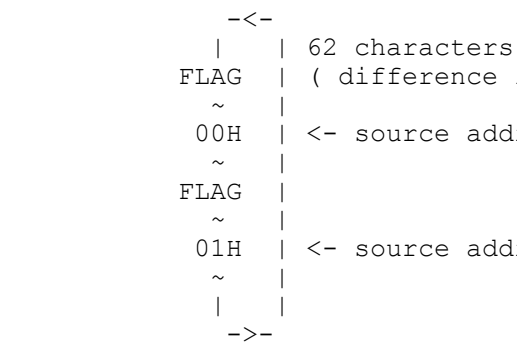


Figure 6

Subsequent Cycles

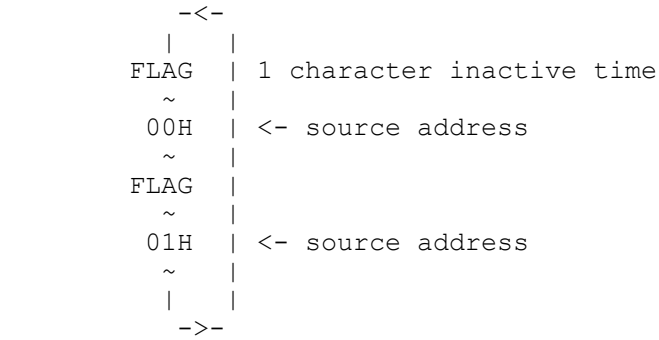


Figure 7

Subsequent Passive Token Passing Sequence

Where no units force Active Token Passing the network goes into Passive Token Passing . Unit number 1 (the last unit to transmit) undertakes the Token Identification Sequence .

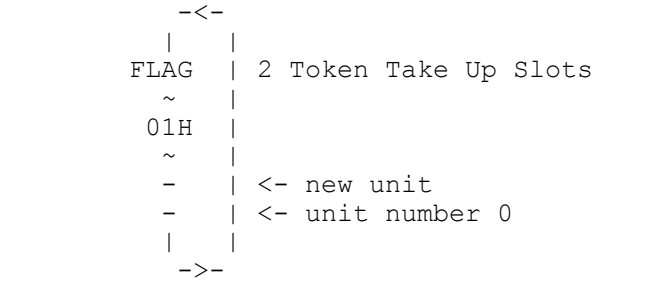


Figure 8

A Third Unit is Plugged into the Network

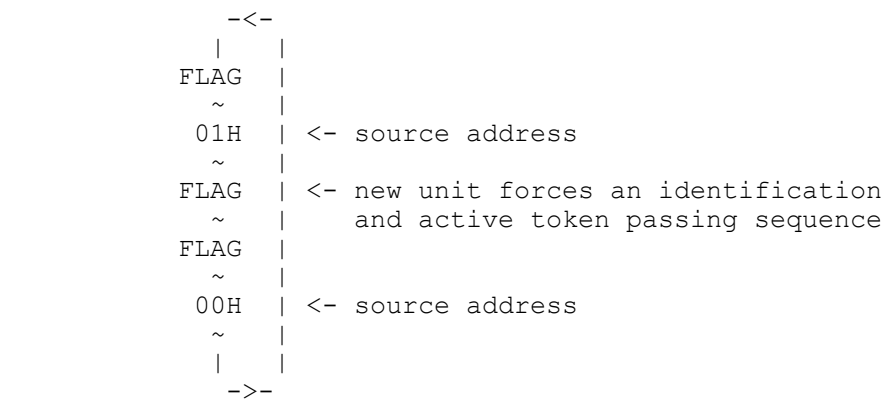


Figure 9

Second Cycle

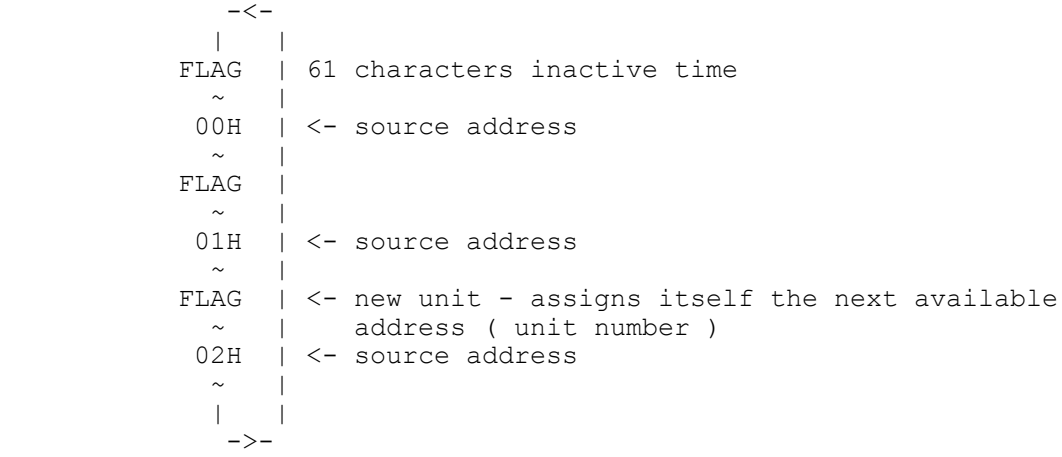


Figure 10

Subsequent Active Token Passing Cycles

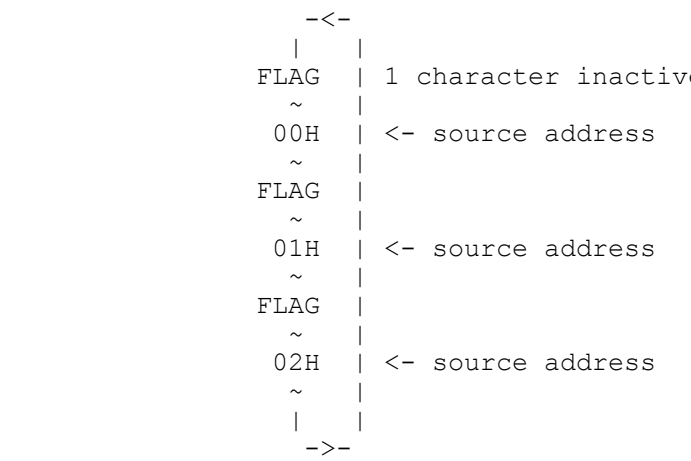


Figure 11

Subsequent Passive Token Passing Cycles

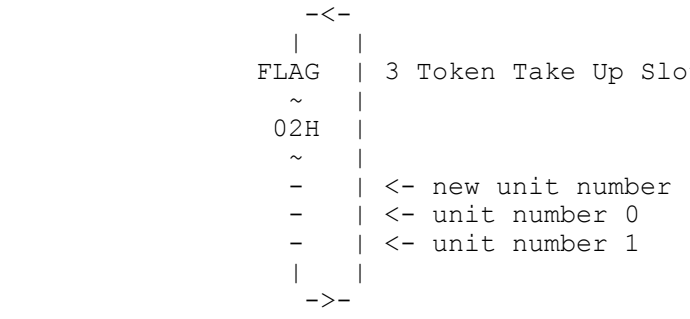


Figure 12

The First Unit is Unplugged from the Network

The Next Active Token Passing Cycle

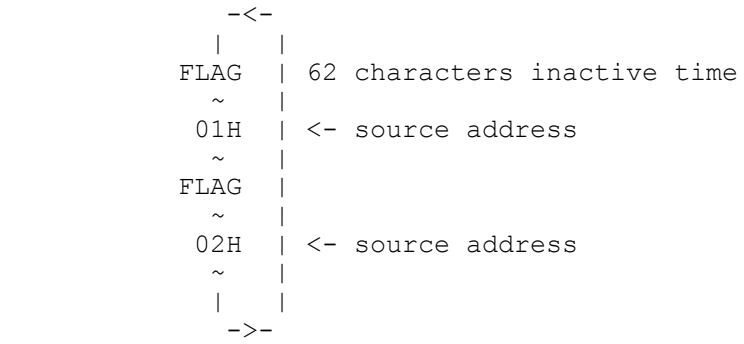


Figure 13

Subsequent Cycles

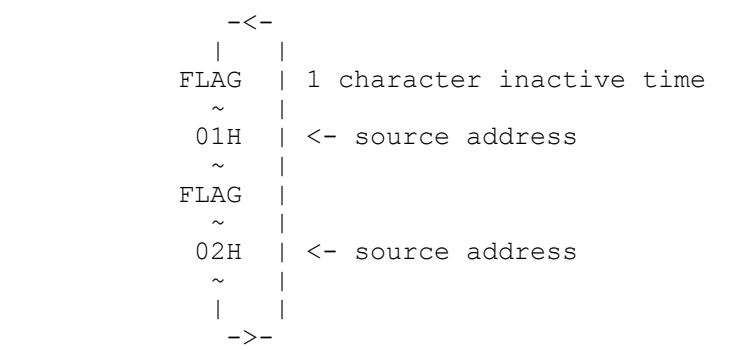


Figure 14

Communication

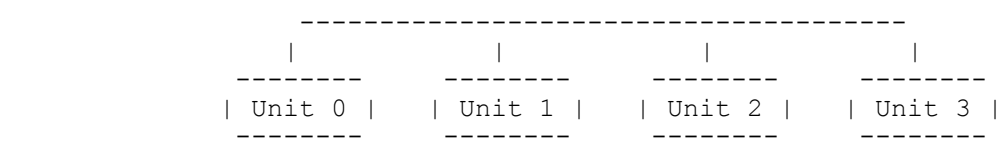


Figure 15

If unit no. 0 wishes to transfer data to unit no. 2 and if it is using channel based addressing it transmits the following sequence :-

FLAG
FUNCTION
DESTINATION UNIT ADDRESS
SOURCE UNIT ADDRESS
DESTINATION CHANNEL ADDRESS
SOURCE CHANNEL ADDRESS
TIME CRITICALITY
DATA LENGTH
DATA

Figure 16

The flag indicates the start of the packet and provides line synchronisation .

The destination address corresponds to the channel address of unit 2 as used by unit 0 . On initiating communication unit 0 will use a broadcast address to link to a unit , process or specific data . A channel providing a virtual link will returned from the unit that has that information .

The source unit address is used to maintain the token passing sequence .

The source address is used to provide a reverse path for the destination unit to communicate with the source unit .

The time criticality specifies whether the packet is to be fitted in within the cycle and unit bandwidth or is to be transmitted regardless of any bandwidth considerations .

The data length indicates the length of the subsequent data portion of the packet .

Usage of Gateways

Because of the use of virtualised channels any unit can act as a gateway without being identified as such on the network .

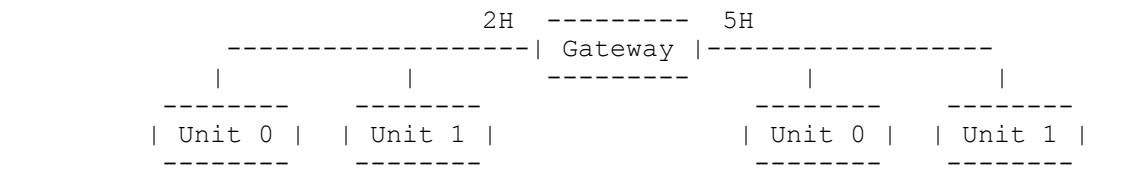


Figure 17

If unit no. 0 in the left hand network wishes to transfer data to unit no. 1 in the right hand network and if it is using channel based addressing it transmits the sequence :-

FLAG	start of packet
~	
02H	destination unit and channel address
00H	source unit and channel address
~	
DATA	data

Figure 18

After passing through the gateway the packet becomes :-

FLAG	start of packet
~	
01H	destination unit and channel address
05H	source unit and channel address
~	
DATA	data

Figure 19

The destination and source address's shown being a representation of the unit and channel addresses .

Operation of The Dynamic Bandwidth Management Method

The Dynamic Management operations are divided into two areas . The first is concerned with ensuring that time critical data is transferred through the network within the time window . The second is concerned with regulating the flow of data into individual units .

Time Critical Traffic

The Time Critical Dynamic Bandwidth Management technique operates on the following basis :-

1) The network can accommodate a maximum bandwidth as determined by the bit rate and the data link protocol .

2) The bandwidth that is available to the individual units is determined by the number of units on the network and the bandwidth required by those units . IE. the maximum bandwidth allocated to individual units is determined by the network installer and network operator and is controlled by the network software and firmware and the data link protocol and the data link protocol logic .

   IE. The network is designed and operated in such a manner that the individual units can transfer their data at their required bandwidth . If the network bandwidth requirement is greater than it's capacity then data transfer is delayed until any short term bottle neck is cleared , the network has to be split up into multiple networks or the network is operated at a faster speed .

3) If an individual unit requires a bandwidth allocation requirement - to transmit time critical data - it transmits a packet that specifies the minimum required cycle length .

4) All units on the network monitor the other units' bandwidth allocation requirement and also transmit their own bandwidth allocation requirement . The network then adjusts it's maximum cycle length to the smallest bandwidth allocation requirement transmitted on the network .

5) Where a unit has time critical data it transmits the packet irrespective of whether or not there is cycle room left .

   The network being designed on a maximum bandwidth requirement or on an average or median bandwidth requirement .

   The resulting design taking into consideration aspects such as the required performance , the end user buffer facilities and associated costs and the resulting access and observational requirements in order to produce a network with the desired bandwidth characteristics .

6) Slower time critical units access the network in a staggered format . As such they transmit on a duty cycle basis and in doing so get their data through on an average corresponding to their required bandwidth .

7) If a unit has non time critical data to transmit it determines whether there is room available in the current cycle or including prior cycles - such as over the last 4 or last 16 cycles - to transmit the packet . If there is room it then transmits the packet . If not it transmits a Channel Bandwidth Request . The other units then transmit up to the maximum bandwidth allocation minus the bandwidth request thus , by holding off non time critical traffic , creating room for the unit's transmission .

In such a manner the Dynamic Bandwidth Management technique ensures that maximum use can be made of the total network bandwidth .

Bandwidth Limited Traffic

The Individual Unit Bandwidth Management technique for data transmission operates on the following basis :-

1) The unit specifies the maximum number of bytes that it can accommodate in any one cycle .

2) All the units monitor the amount of data per cycle or per number of cycles transmitted individually to all units other than themselves .

3) When a unit has data to transmit it checks whether there is sufficient space in the current cycle or over a number of cycles to transmit the data to the specified destination unit .

   i) If there is it transmits the data .

   ii) If not it indicates that it wishes to transmit data to the specified destination by a Unit Bandwidth Request . The other units then transmit up to the maximum bandwidth allocation minus the bandwidth request thus , by holding off non time critical traffic , creating room for the unit's transmission .

In such a manner the flow of the data is managed but all units are given equal access to the network .

The Individual Unit Bandwidth Management technique for data reception operates on the following basis :-

The individual unit monitors the flow of data into and out of it's receive buffer . According to how full the receive buffer is and according to it's receive buffer bandwidth management algorithm and when the receive buffer fills to or past it's associated break points it transmits a new unit bandwidth (by transmitting an Identification message without the Force Active Token Pass bit being asserted) . In such a manner it controls the flow of data into it's receive buffer and matches it to the flow of data out of it's receive buffer . Thus it maximises the transfer of data through the unit whilst minimising the chances of data being lost .

Practical Implementation Considerations

The following section addresses the practical issues of the Token Bus Protocol implementation . As such it shows the specific logical responses of the implemented Token Bus Protocol to varying line conditions and logic states .

Active Token Passing

Condition - The data is corrupted but the flag and header have been received correctly .

Action - The subsequent unit will wait for a total number of characters corresponding to the specified message length for the unit to cease transmission and will then transmit a message .

The destination unit will detect the data corruption by the locally generated error check syndrome disagreeing with the supplied error check syndrome and as such will either correct or reject the message .

Condition - The source address is corrupted .

Example -
```
        00   message intact
        01   message intact
        05   message corrupted
    >   08
```

The subsequent unit maintains a count of the number of units currently on line and notices that the previous message should have come from the previous unit and takes up the token , transmits it's message and then releases the token .

Unit 8 is counting up (retrospective token pass counter) from the previously received source address . The transmission of unit 5's corrupted message triggers off it's own subsequent message transmission .

```
Condition -        00   message intact
                   01   message corrupted
                   05   message corrupted
                >  08
```

Action - the retrospective token pass counter is still effective . The token position is tracked and unit 8 takes over the token .

```
Condition -        00   message intact
                   01   message corrupted
                   02   message corrupted - new unit
                >  05
                >  08
```

Action - the retrospective token pass counter loses synchronisation . Unit 5 and unit 8 will collide and both will detect the collision . Both will cease their transmission and unit 0 will then take over and as a result the token passing sequence will be restored .

Condition - the flag has been received correctly but the message length has been corrupted .

Action - The subsequent unit will wait for a total number of characters corresponding to the maximum message length for the unit to cease transmission and if the line is inactive and if the token passing sequence has not been restored by another unit it will then transmit a message .

Condition - not all units receive a corrupted message .

Action - the maximum message length wait would consist of the actual message followed by inactive characters . The units that have received the message correctly would then count through these inactive characters as if the subsequent units had gone off line . When the first unit had reached it's respective token position it would transmit it's message and the token passing sequence would resume .

The token passing on the next cycle would not be upset when the other units resume transmission . One or more inactive character spaces will be present after the unit whose message was corrupted . The subsequent unit will slot in here and the other units will follow .

Condition - the flag is corrupted .

Action - the subsequent unit still knows that it's turn is coming up . When the message times out it will take over .

A corrupted flag is recognised as an active character in a new message and as such it is ensured that transmission doesn't occur in the middle of a message .

An inactive character consists of all 0's or all 1's and occurs after a packet has completed it's transmission . Any other pattern indicates transitions on the line and hence activity .

Condition - miss-timings and glitches at the start of the character period .

Action - in order to prevent confusion with active characters there will be a window (eg. 2 bits in length) for these to die down before the inactive character sampling occurs .

Passive Token Passing

Condition - The last transmission is received corruptly .

Action - Any subsequent units that wish to access the network wait until the last unit retransmits in order to achieve synchronisation .

Condition - The current token passing unit is disconnected from the network .

Action - After the Token Identification Sequence and the Token Take Up Period and a subsequent period corresponding to the Take Up Slot of the current token passing unit a subsequent Token Take Up Period occurs during which the next subsequent unit takes over the Token Identification Sequence .

Condition - The subsequent unit that wishes to access the network is disconnected from the network .

Action - After the Token Identification Sequence and the Token Take Up Period and a subsequent period corresponding to the Take Up Slot of the current token passing unit a subsequent Token Take Up Period occurs during which the subsequent unit takes over the Token Identification Sequence .

Condition - All other units other than the unit transmitting the token identification sequence go off line .

Action - The unit transmitting the token identification sequence will periodically transmit an active token passing trigger and if this is not responded to it will go to the inactive network state .

Registers

The Token Bus Protocol controller contains a number of registers to manage the operation of the Token Bus Protocol . These include the state register that stores the current state of the unit such as off line \ address assigned \ message started state , Token Bus Protocol parameter registers and message movement management registers along with higher level management registers such as the local enabled general broadcast addresses registers .

Method of Operation of the Token Position Register

Related registers :-

i) The previous unit's address .
ii) The current unit's address .

The Token Position Register will advance at the completion of the message packet to the next unit number . It will also advance at the reception of any subsequent consecutive inactive characters or Token Take Up Slots to subsequent unit numbers . When a message has been received intact it will use the source address contained in the message to determine the next unit number . It requires a qualifying register to store the source address and to allow the necessary decisions to be set up and handled . When the Token Position Register is equal to the Current Unit Address Register the current unit is queued in for transmission . It either transmits a message or allows the token to pass onto a subsequent unit .

Method of Operation of the Number of Units on Network Register
---

The Number of Units on Network Register will be set up on each complete intact cycle . It purpose being purely by noticing any change in the number of units on the network allowing the network directory held by the associated processor to be updated . A comparison is made with the number of units detected on a previous active token passing cycle and if any difference occurs the associated processor is suitably informed .

Claims
---

1) A token bus protocol that uses

i) a bussed network topology which , by definition , consists of a single communication medium onto which all the network units are connected ;

and

ii) a retrospective token passing method where each unit monitors the prior transmission sequence and uses this to identify the transmission of the previous unit and to identify the number (address) of the previous unit and uses this to determine the starting position of it's transmission ;

The Retrospective Token Passing being where knowledge is maintained as to where the token is coming from , in the logical token passing cycle , but no knowledge is maintained as to where the token is going to ;

and

iii) a retrospective token passing method where the unit that holds the token , by definition , has sole access to the network bus ;

The unit releases it's sole access to the network bus by completing it's transmission and in this manner allows the next unit , in the logical token passing cycle , to access the network ;

The next unit is not defined as having a specific number or as having a consecutive number but as being the next numerically numbered unit currently connected to the network bus ;

The numbers being organised in a wrapped around fashion ;

and

iv) a retrospective token passing method where the unit’s transmission occurs immediately after it's previous unit has finished transmission and with or without an inactive period of time inserted between the previous unit's transmission and the unit's transmission ;

The length of any period of time between the previous unit’s transmission and the unit’s transmission being dependent on the difference in the number (address) of the current unit with reference to the previous unit ;

and

v) Active Token Passing where each unit takes up the token , transmits a message and then releases the token thus allowing it to be taken up by a subsequent unit ;

The releasing of the token being accomplished by the completion of the message transmission ;

and

vi) Passive Token Passing where the last unit to transmit follows the Token Identification Sequence with a Token Take Up Period consisting of Token Take Up Slots ;

The Token Take Up Period being a period where the last unit to transmit does not undertake any transmission ;

The Token Take Up Slots being portions of time of equal length contained within the Token Take Up Period ;

Each unit has a corresponding Token Take Up Slot during which it can take up the token and hence access the network ;

The action of the unit taking up the token being the unit undertaking transmission ;

The action of the unit allowing the token to pass onto a subsequent unit being the unit not undertaking transmission during it's corresponding Token Take Up Slot time window ;

and

vi) a) Dynamic Bandwidth Control where units requiring the successful transmission of time critical data transmit their required maximum cycle length ;

The other units on the network adjust the maximum cycle time to the length corresponding to the smallest cycle length request transmitted on the network ;

Units with time critical data always transmit that data when it is present to transmit ;

Units with non time critical data only transmit that data where there is sufficient room remaining after the last cycle or cycle group ;

Units with non time critical data can transmit a hold off message to create space within the subsequent cycle ;

b) Dynamic Bandwidth Control where units can manage the rate of flow of data into their receivers by the units transmitting their maximum bandwidth ;

Units with time critical data always transmit that data when it is present to transmit ;

Units with non time critical data only transmit that data where there is sufficient room remaining after the last cycle or cycle group ;

Units with non time critical data can transmit a hold off message to create space within the subsequent cycle .

2) A token bus protocol as defined in claim 1 that provides for Arbitrary Unit Number (Address) Assignment ;

The Arbitrary Unit Number (Address) Assignment , by definition , being that the unit does not require a predefined number (address) but assigns itself an available number (address) on connection to the network bus ;

The arbitrary unit number (address) assignment being accomplished by the use of the retrospective token passing in conjunction with the inactive characters such that the unit coming onto the network assigns the number (address) corresponding to the source address plus 1 of the first received message that is immediately followed by an inactive character ; This being the first available address .

3) A token bus protocol as defined in claim 1 that provides for the use of Source Based Channel Addresses ;

   The Source Based Channel Address being , by definition , an address in which the source unit number (address) forms part of the channel address ;

   The channel address being a virtual channel address within the destination unit .

4) A token bus protocol as defined in claim 1 that provides for the use of Destination Based Channel Addresses ;

   The Destination Based Channel Address being , by definition , an address in which the destination unit number (address) forms part of the channel address ;

   The channel address being a virtual channel address within the destination unit .

5) A token bus protocol as defined in claim 1 that provides for the use of General Broadcast Addresses ;

   The General Broadcast Address being , by definition , an virtual address that has single or multiple sources and single or multiple destinations .