

SURPASS hiD 6630/6650/6670

Advanced Ethernet Package



Advanced Ethernet Package

SURPASS hiD 6630/6650/6670

Authored by: Sales Engineering

Advanced Ethernet Package v1.10.doc	Date: 06.07.2006
Copyright © Siemens COM FN A SB	Version: 1.10
	Page 1 of 16

Confidential

TABLE OF CONTENTS:

1	GLOSSARY	3
2	INTRODUCTION	4
3	VLAN MANIPULATION	4
3.1	INGRESS VLAN MANIPULATION FUNCTIONS	4
3.1.1	VLAN Tagging	4
3.1.2	VLAN Double Tagging.....	5
3.1.3	VLAN Translation.....	6
3.1.4	VLAN Swapping	6
3.1.5	Ingress VLAN manipulation summary.....	6
3.2	EGRESS VLAN MANIPULATION FUNCTIONS	7
3.2.1	VLAN Stripping.....	7
3.2.2	VLAN Double Stripping	8
3.2.3	VLAN Translation.....	8
3.2.4	VLAN Swapping	8
3.2.5	Egress VLAN manipulation summary.....	8
3.3	SERVICE EXAMPLES	9
3.3.1	Wholesale Internet service.....	9
3.3.2	Simplifying DSLAM provisioning	10
4	VLAN CROSS-CONNECT	ERROR! BOOKMARK NOT DEFINED.
4.1	S-VLAN CROSS-CONNECT.....	11
4.2	S+C VLAN CROSS-CONNECT	12
4.3	VLAN CROSS-CONNECT RESILIENCY.....	13
4.4	PROVISIONING	15
5	SUMMARY	15

1 Glossary

C-VLAN – Customer VLAN. VLAN used in the customer premises

S-VLAN – Service Provider VLAN. VLAN used in the service provider domain

VLAN Assignment Mode

- Port based (PVID) – VLAN according to incoming port
- IP subnet based – VLAN according to IP Source Address or IP SA subnet (for IP packets)
- VLAN based – VLAN according to incoming VLAN

VLAN Operations

- Look up – Search outer VLAN tag
- Swap – Swap between inner and outer VLANs
- Add – Add (stack) new VLAN tag (inner/outer)
- Strip – Remove VLAN tag/s (inner/outer/double)
- Translate – Translate outer VLAN

Null – No operation

2 Introduction

Metro Ethernet networks are becoming increasingly popular with carriers who want simple, cost effective and multiple service platforms.

However, as networks grow and new services are introduced, some of the underlying weaknesses of Ethernet are being exposed and service providers are having to deal with them.

Some of the challenges facing these carriers are the following:

- Scalability: Quantity of VLANs and MAC addresses
- End-to-End QoS: Providing guaranteed end-to-end service
- Security: Preventing MAC address spoofing
- Flexibility: Support different network configurations and service capabilities

Siemens' Advanced Ethernet Package which includes VLAN Manipulation and VLAN Cross-connect solves these problems by adding additional functionality to the standard Ethernet portfolio.

This document describes the VLAN Manipulation and VLAN Cross-connect functions and shows how the SURPASS hiD 6650/6670 Carrier Ethernet Switch family provides answers to all the challenges mentioned above.

3 VLAN Manipulation

VLAN manipulation provides improved flexibility and scalability for customers. It allows the SURPASS hiD 6650/6670 to meet any customer configuration requirements.

VLAN Manipulation is provided on both the ingress and egress ports and supports the following functionality:

- VLAN Tagging/Stripping
- VLAN Double tagging/stripping
- VLAN Translation
- VLAN Swapping

3.1 Ingress VLAN Manipulation functions

3.1.1 VLAN Tagging

VLAN Tagging can be performed on untagged or tagged frames. A VLAN tag can be added to the packet. The tagging decision can be per port, per VLAN (for tagged packets) or per IP Source Address.

3.1.1.1 VLAN Tagging per port

If the tagging is per port, then all packets received from that port will be tagged with a specific VLAN tag. Untagged traffic will be tagged with a C-VLAN tag, and tagged traffic will be stacked with a second VLAN (Q-in-Q) - with an S-VLAN tag. This is useful when tagging a specific customer's traffic which is tagged with customer C-VLANs and the outer S-VLAN tag represents the customer.

3.1.1.2 VLAN Tagging per VLAN or per IP Source

If the tagging is per VLAN or per IP source, then selective tagging can be performed and only packets that meet the criteria will be tagged. This means that, for instance, untagged packets will be tagged with one C-VLAN tag, packets with C-VLAN ID 10-20 will be stacked with an S-VLAN tag, packets with C-VLAN ID 30-40 will be stacked with a different S-VLAN tag, and other C-VLAN IDs will not be tagged at all.

This flexibility allows traffic separation for different service types or to access different destinations. For instance, a business customer can use inner tags to indicate different services. By stacking by VLAN, the different services can be separated allowing the traffic flow to access multiple servers.

The table below shows the VLAN stacking possibilities:

Incoming packets	Tag on Ingress	Don't Tag on Ingress
Untagged	Single Tag	Not Relevant
Tagged	Double Tag (Q-in-Q)	Single Tag

As stated above, since customer traffic can be tagged, the SURPASS hiD 6650/6670 can add a second S-VLAN tag to the packet and thus perform a Q-in-Q operation. The default Ethertype value for Q-in-Q is 8100. However the SURPASS hiD 6650/6670 is flexible and the Ethertype value can be changed to support interworking with other equipment that does not support this standard value.

3.1.1.3 802.1p bits manipulation capabilities

When performing Q-in-Q, the question arises as to what to do regarding the customer's 802.1p priority bits information. There are a number of possibilities which allow complete flexibility:

- Copy the 802.1p value from the existing C-VLAN tag to the outer S-VLAN tag
- Override the 802.1p value as part of the classification/policing.

If the VLAN stacking is performed on a port basis (and not on a VLAN basis), the 802.1p bits can be manipulated as follows:

- Use a default PVID 802.1p value (for untagged packets)
- Copy the 802.1p value from the existing C-VLAN tag to the outer S-VLAN tag
- Override the 802.1p value as part of the classification/policing.

3.1.2 VLAN Double Tagging

If packets arrive at an ingress port untagged, they can be double tagged by the SURPASS hiD 6650/6670. Thus 2 tags are added to the untagged traffic.

The 802.1p bits can be manipulated as follows:

- Use a default PVID 802.1p value
- Override the 802.1p value as part of the classification/policing.

2 tags can also be added to an already tagged packet giving a total of 3 VLAN tags. This preserves the customer VLAN tag whilst adding on 2 service tags. This procedure is the same as single tagging and can be per port or per VLAN. The 802.1p bits are either copied from the customer tag, or overwritten during the classification/policing procedures.

3.1.3 VLAN Translation

Often a service provider is not interested in the customer's C-VLAN tag or would like to maintain or control its own VLAN scheme. Instead of double tagging the packet, the C-VLAN can be translated into an S-VLAN. This can be performed per VLAN. Thus each C-VLAN can be mapped and translated into another value which the provider specifies (S-VLAN). So a business customer might tag his internet traffic with a C-VLAN. The service provider can override this information and map it into the service provider's S-VLAN

VLAN translation can be combined with VLAN stacking. Thus the C-VLAN can be translated to a specific value defined by the service provider, and then a second tag can be added (Q-in-Q). The second tag is added as the outer VLAN tag.

If a double tagged packet arrives from the customer, both the inner and outer tags can be translated.

3.1.4 VLAN Swapping

VLAN swapping allows the inner and outer tags to be swapped so that the inner tag becomes the outer tag, and vice versa. This is useful when a customer sends a double tagged packet where the inner tag represents the service, or if a single tagged packet is received and double tagging is performed, but the inner tag represents the service. VLAN swapping can be performed together with VLAN translation. For instance, if a double tagged packet arrives, the S-VLAN tag (outer tag) can be translated, and be swapped into the inner VLAN. The C-VLAN (which is now the outer VLAN tag) can now be translated as well. During VLAN swapping, the inner tag, outer tag or both inner and outer tags can be translated.

3.1.5 Ingress VLAN manipulation summary

Table 1 summarizes the functionality described in this section.

No.	Manipulation	Incoming Format	Inner tag Look up	Outgoing Format
1	Port based Stacking	OUTER = X ETH	No	OUTER = S-PVID INNER = X ETH
2	VLAN based Stacking	OUTER = X ETH	No	OUTER = Y INNER = X ETH
3	Translate inner tag	OUTER = X INNER = Y1 ETH	Yes	OUTER = X INNER = Y2 ETH
4	Translate outer tag	OUTER = X1 ETH	No	OUTER = X2 ETH
5	Translate outer & inner tag	OUTER = X1 INNER = Y1 ETH	Yes	OUTER = X2 INNER = Y2 ETH
6	Translate and stack	OUTER = X1 ETH	No	OUTER = Y INNER = X2 ETH
7	Swap outer & inner tag locations	OUTER = X INNER = Y ETH	No	OUTER = Y INNER = X ETH
8	Translate outer and swap outer and inner tag locations	OUTER = X1 INNER = Y ETH	No	OUTER = Y INNER = X2 ETH
9	Translate inner and swap outer and inner tag locations	OUTER = X INNER = Y1 ETH	Yes	OUTER = Y2 INNER = X ETH
10	Port based double stacking	OUTER = X ETH	No	OUTER1 = Y1 OUTER2 = Y2 INNER = X ETH
11	VLAN based double stacking	OUTER = X ETH	No	OUTER1 = Y1 OUTER2 = Y2 INNER = X ETH
12	Translate inner and outer tag and swap tag locations	OUTER = X1 INNER = Y1 ETH	Yes	OUTER = Y2 INNER = X2 ETH

Table 1 Ingress VLAN Manipulation Functions

3.2 Egress VLAN Manipulation functions

3.2.1 VLAN Stripping

In the same way as VLANs can be tagged on the ingress port, the VLAN tag can be stripped again at the egress port. The stripping can be performed either per port, or per VLAN.

If a double tagged packet arrives, the outer tag is stripped and the packet is transmitted with only the inner tag (C-VLAN).

3.2.2 VLAN Double Stripping

If a double tagged packet arrives, both tags can be stripped so that the packet is transmitted untagged from the egress port.

3.2.3 VLAN Translation

VLAN translation is performed in the same way as for ingress ports. VLAN translation and stripping can be performed simultaneously so that the outer VLAN is stripped, and the inner VLAN tag is translated, or the inner VLAN is stripped and the outer VLAN is translated.

3.2.4 VLAN Swapping

VLAN swapping is performed in the same way as for ingress ports. Please see section 3.1.4 for more details.

3.2.5 Egress VLAN manipulation summary

Table 2 summarizes the functionality described in this section.

No.	Manipulation	Incoming Format	Inner tag Look up	Outgoing Format						
1	Outer tag Stripping	<table border="1"> <tr><td>OUTER = Y</td></tr> <tr><td>INNER = X</td></tr> <tr><td>ETH</td></tr> </table>	OUTER = Y	INNER = X	ETH	No	<table border="1"> <tr><td>INNER = X</td></tr> <tr><td>ETH</td></tr> </table>	INNER = X	ETH	
OUTER = Y										
INNER = X										
ETH										
INNER = X										
ETH										
2	Translate inner tag	<table border="1"> <tr><td>OUTER = X</td></tr> <tr><td>INNER = Y1</td></tr> <tr><td>ETH</td></tr> </table>	OUTER = X	INNER = Y1	ETH	Yes	<table border="1"> <tr><td>OUTER = X</td></tr> <tr><td>INNER = Y2</td></tr> <tr><td>ETH</td></tr> </table>	OUTER = X	INNER = Y2	ETH
OUTER = X										
INNER = Y1										
ETH										
OUTER = X										
INNER = Y2										
ETH										
3	Translate outer tag	<table border="1"> <tr><td>OUTER = X1</td></tr> <tr><td>ETH</td></tr> </table>	OUTER = X1	ETH	No	<table border="1"> <tr><td>OUTER = X2</td></tr> <tr><td>ETH</td></tr> </table>	OUTER = X2	ETH		
OUTER = X1										
ETH										
OUTER = X2										
ETH										
4	Translate outer & inner tag	<table border="1"> <tr><td>OUTER = X1</td></tr> <tr><td>INNER = Y1</td></tr> <tr><td>ETH</td></tr> </table>	OUTER = X1	INNER = Y1	ETH	Yes	<table border="1"> <tr><td>OUTER = X2</td></tr> <tr><td>INNER = Y2</td></tr> <tr><td>ETH</td></tr> </table>	OUTER = X2	INNER = Y2	ETH
OUTER = X1										
INNER = Y1										
ETH										
OUTER = X2										
INNER = Y2										
ETH										
5	Strip and translate	<table border="1"> <tr><td>OUTER = Y</td></tr> <tr><td>INNER = X1</td></tr> <tr><td>ETH</td></tr> </table>	OUTER = Y	INNER = X1	ETH	No	<table border="1"> <tr><td>OUTER = X2</td></tr> <tr><td>ETH</td></tr> </table>	OUTER = X2	ETH	
OUTER = Y										
INNER = X1										
ETH										
OUTER = X2										
ETH										
6	Swap outer & inner tag locations	<table border="1"> <tr><td>OUTER = X</td></tr> <tr><td>INNER = Y</td></tr> <tr><td>ETH</td></tr> </table>	OUTER = X	INNER = Y	ETH	No	<table border="1"> <tr><td>OUTER = Y</td></tr> <tr><td>INNER = X</td></tr> <tr><td>ETH</td></tr> </table>	OUTER = Y	INNER = X	ETH
OUTER = X										
INNER = Y										
ETH										
OUTER = Y										
INNER = X										
ETH										
7	Translate Inner and swap outer and inner tag locations	<table border="1"> <tr><td>OUTER = X</td></tr> <tr><td>INNER = Y1</td></tr> <tr><td>ETH</td></tr> </table>	OUTER = X	INNER = Y1	ETH	Yes	<table border="1"> <tr><td>OUTER = Y2</td></tr> <tr><td>INNER = X</td></tr> <tr><td>ETH</td></tr> </table>	OUTER = Y2	INNER = X	ETH
OUTER = X										
INNER = Y1										
ETH										
OUTER = Y2										
INNER = X										
ETH										
8	Translate outer and swap outer and inner tag locations	<table border="1"> <tr><td>OUTER = X1</td></tr> <tr><td>INNER = Y</td></tr> <tr><td>ETH</td></tr> </table>	OUTER = X1	INNER = Y	ETH	No	<table border="1"> <tr><td>OUTER = Y</td></tr> <tr><td>INNER = X2</td></tr> <tr><td>ETH</td></tr> </table>	OUTER = Y	INNER = X2	ETH
OUTER = X1										
INNER = Y										
ETH										
OUTER = Y										
INNER = X2										
ETH										
9	Double tag stripping	<table border="1"> <tr><td>OUTER1 = X1</td></tr> <tr><td>OUTER2 = X2</td></tr> <tr><td>INNER = Y</td></tr> <tr><td>ETH</td></tr> </table>	OUTER1 = X1	OUTER2 = X2	INNER = Y	ETH	No	<table border="1"> <tr><td>OUTER = X</td></tr> <tr><td>ETH</td></tr> </table>	OUTER = X	ETH
OUTER1 = X1										
OUTER2 = X2										
INNER = Y										
ETH										
OUTER = X										
ETH										
10	Translate inner and outer tag and swap tag locations	<table border="1"> <tr><td>OUTER = X1</td></tr> <tr><td>INNER = Y1</td></tr> <tr><td>ETH</td></tr> </table>	OUTER = X1	INNER = Y1	ETH	Yes	<table border="1"> <tr><td>OUTER = Y2</td></tr> <tr><td>INNER = X2</td></tr> <tr><td>ETH</td></tr> </table>	OUTER = Y2	INNER = X2	ETH
OUTER = X1										
INNER = Y1										
ETH										
OUTER = Y2										
INNER = X2										
ETH										

Table 2 Egress VLAN Manipulation Functions

3.3 Service Examples

Different service providers plan to have different network architectures, varying services and alternative VLAN provisioning schemes.

In order to efficiently and flexibly provide these services, VLAN manipulation is required. This section shows a few examples of how VLAN Manipulation functions can be used to provide solutions for certain services and scenarios.

3.3.1 Wholesale Internet service

In this example, a service provider might provide wholesale Internet services to 3rd party providers. In this case, the service provider does not have control over the wholesale

VLANs. The wholesale provider might provision the C-VLAN as representing the ISP, and the S-VLAN as representing the DSLAM.

Since the switching of the traffic should be per ISP, VLAN manipulation could be used to swap the S and C VLAN tags so that the C-VLAN tag representing the ISP, now becomes the outer tag and switching can be performed according to that tag. This example is shown in Figure 3-1.

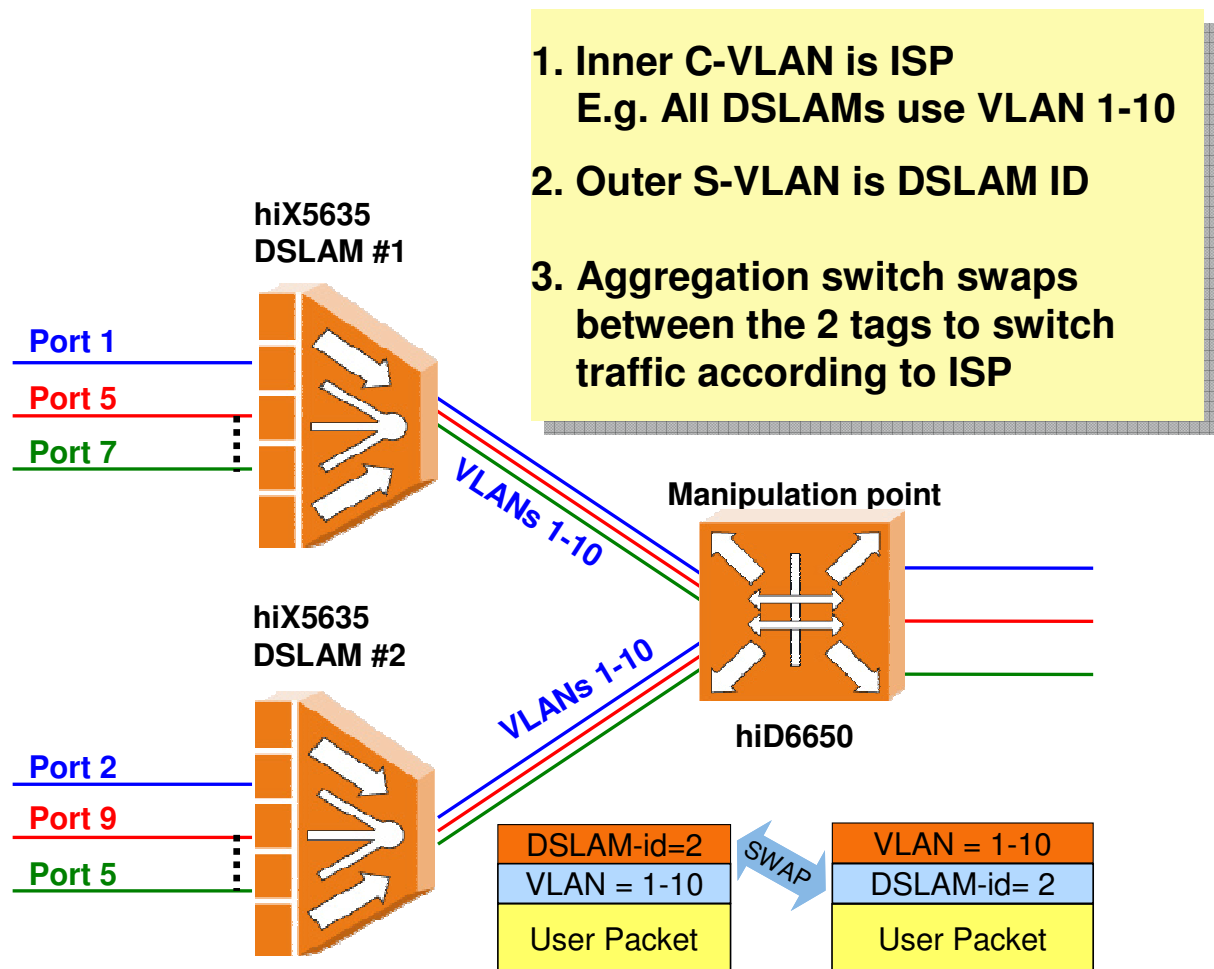


Figure 3-1 Example of Wholesale Service

In addition, in order to prevent any clash of VLAN tags with other wholesale providers, VLAN IDs could be translated so that the VLAN ID is a known acceptable value.

3.3.2 Simplifying DSLAM provisioning

By utilizing the advantages of VLAN Manipulation, DSLAM provisioning can become much simpler. Each DSLAM can be configured with a standard and fixed VLAN configuration and then these VLANs can be manipulated when they reach the aggregation switch.

This also allows simple DSLAMs to be installed and to rely on the aggregation switch to provide the major functionality.

4 VLAN Cross-connect

VLAN Cross-connect is a complementary technology to Ethernet bridging, which relies on MAC Learning, and therefore solves many of the limitations and security risks associated with MAC Learning.

There are 2 major scalability issues when using Ethernet technology – The number of VLANs and the number of MAC addresses.

The security risks with MAC addresses involve customers using MAC spoofing to try to disrupt service, hack into unauthorized services/sites, or bypass billing mechanisms.

Although the hiD 6650/6670 has mechanisms which solve all these issues, VLAN Cross-connect provides an additional level of scalability and security which can be used.

VLAN Cross-connect, in effect, changes the Layer 2 domain from a connectionless domain to a connection-oriented domain. It is mainly required for point-to-point connections and therefore is often used in conjunction with MAC learning to support point-to-point, point-to-multipoint and Multicast services across the same platform.

VLAN Cross-connect removes the need for MAC learning and therefore removes a major bottleneck from the network.

It is also completely inter-operable with other equipment that does not support VLAN Cross-connect since it uses standard Ethernet packets and standard VLANs and thus can seamlessly connect up to 3rd party equipment without that equipment being aware that VLAN Cross-connect is enabled.

An example of service split between VLAN Cross-connect and Bridging is shown in Figure 4-1.

Service	Method
High Speed Internet Service	VLAN Cross-Connect
Business VPN PtP (E-Line)	VLAN Cross-Connect
Voice Services	VLAN Cross-Connect
Video on Demand	VLAN Cross-Connect
Wholesale Services	VLAN Cross-Connect
IPTV	Bridging
Business VPN MPtMP (E-LAN)	Bridging
Network Element Management	Bridging

Figure 4-1 Service Implementation

2 options for VLAN Cross-connect are supported:

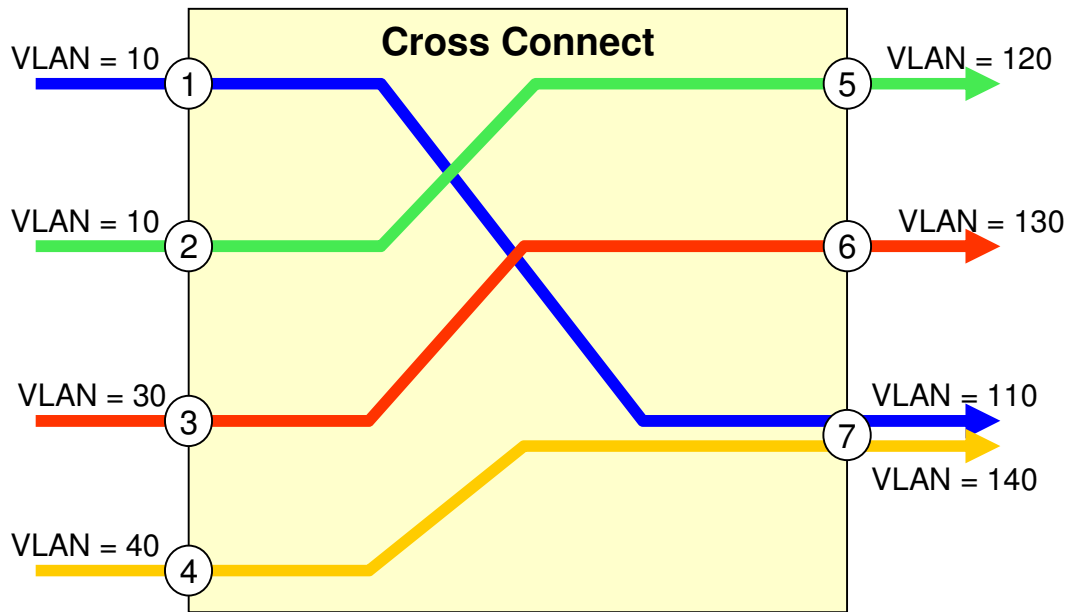
- S-VLAN Cross-connect where the Cross-connect is performed exclusively according to the outer S-VLAN
- S+C VLAN Cross-connect where the Cross-connect is performed according to the inner and outer VLAN (Similar to VP and VC in ATM).

In addition, Siemens VLAN Cross-connect solution also provides a standard-based solution for resiliency which gives it an additional advantage over other vendors' solutions.

4.1 S-VLAN Cross-connect

S-VLAN Cross-connect allows a connection to be switched according to the outer VLAN ID. Figure 4-2 shows an example of S-VLAN Cross-connect.

Advanced Ethernet Package v1.10.doc	Date: 06.07.2006
Copyright © Siemens COM FN A SB	Version: 1.10
	Page 11 of 16



In Port	In VLAN	Dest. Port	Out VLAN
1	10	7	110
2	10	5	120
3	30	6	130
4	40	7	140

Figure 4-2 S-VLAN Cross-connect Example

VLAN Cross-connect allows reuse of VLAN IDs over multiple ports whilst ensuring that they are isolated and that traffic can not be switched from one port to another (e.g. VLAN 10 in ports 1 and 2). This increases the effective number of VLANs available from 4K per system to 4K per port. It also enables each DSLAM to be provisioned identically thereby simplifying provisioning.

By enabling S-VLAN Cross-connect, the benefits of not having to learn MAC addresses for point-to-point connections together with VLAN reuse for ports allows greater scalability when compared to the basic switching concept for Ethernet.

4.2 S+C VLAN Cross-connect

S+C VLAN Cross-connect is taken from the ATM world of Cross-connect based on VP (Virtual Path) and VC (Virtual Channel). It performs switching based on the S and C VLAN values which increases the number of switching entries from 4K VLANs per port when using S-VLAN Cross-connect to a theoretical maximum of 16 million VLAN combinations.

Table 3 summarizes the VLAN scalability options for different options. It is obvious that VLAN Cross-connect provides an additional level of scalability for Ethernet domains.

VLAN Options	VLAN Scalability
Single Tagged VLAN with MAC Learning	4K VLANs per domain
Double Tagged VLAN (Q-in-Q) with MAC Learning	16M VLANs per domain
S-VLAN Cross-connect	4K VLANs per port
S+C VLAN Cross-connect	16M VLANs per port

Table 3 - VLAN Scalability

S+C VLAN Cross-connect provides a greater level of flexibility whereby, for instance, small DSLAMs can be grouped together under a single outer VLAN by translating both the inner and outer VLANs. Figure 4-3 shows an example of 10 DSLAMs each with 100 customers (C-VLANs) and a specific service (S-VLAN 1). Each DSLAM has the same identical configuration. At the Metro Node, all 10 DSLAMs are combined into the same S-VLAN (S-VLANs 10), and the C-VLANs are changed to ensure that the S+C VLAN combination is unique.

Ingress			Egress		
Port	S-VLAN	C-VLAN	Port	S-VLAN	C-VLAN
1	1	1-100	20	10	1-100
2	1	1-100	20	10	101-200
...					
10	1	1-100	20	10	901-1000

Figure 4-3 S+C VLAN Cross-connect Example

The hiD 6650/6670 supports a maximum of 216K VLAN Cross-connect entries per Line Interface Card¹.

4.3 VLAN Cross-connect Resiliency

Siemens has implemented VLAN Cross-connect protection together with the VLAN Cross-connect functionality which enables an automatic level of protection that can be used for VLAN switched connections.

Each end-to-end VLAN connection can be configured with a backup path. Using IEEE 802.1ag OAM, the paths are monitored and in the event of a failure, the originating node is informed and initiates a switchover to the backup path.

¹ Note that the total number of VLAN Cross-connect entries is affected by the total number of MAC Addresses. If MAC learning and VLAN Cross-connect are used in the same node, the total number of VLAN Cross-connect entries per card can not exceed 216K minus the total number of MAC addresses learned per node.

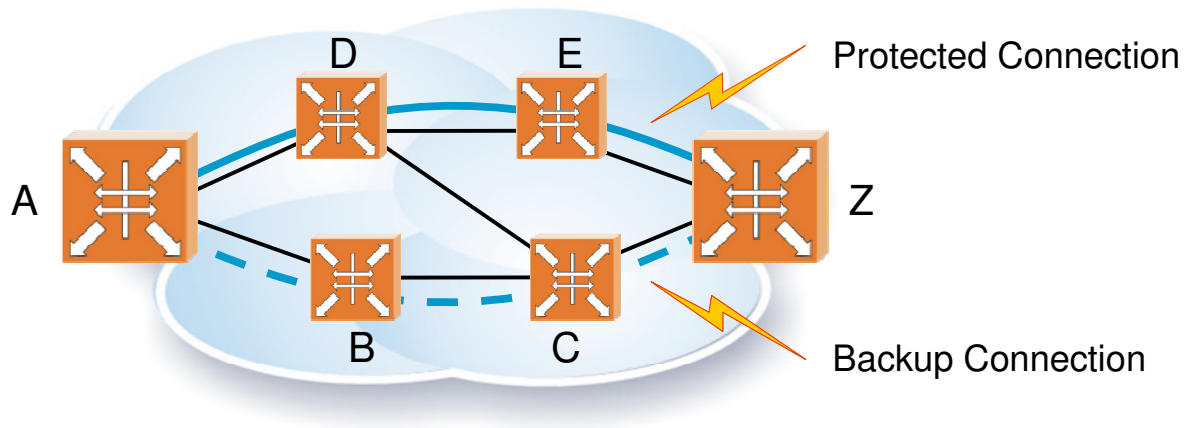


Figure 4-4 VLAN Cross-connect Resiliency

Figure 4-4 shows an example of a network. A primary path is established along the top path and a secondary path is established along the bottom path. If a fault in the top path causes the OAM messages to be interrupted, the originating node will switch all traffic to the bottom path.

Since the failure message needs to be detected by the originating node and then the protection activated, the recovery time is approximately 100ms.

VLAN Cross-connect protection works over meshed and ring topologies. The 2 alternative paths are provisioned so that a failure will not cause both paths to fail.

Using Siemens' CAC (Connection Admission Control) mechanism, bandwidth can be allocated in advance so that in the case of a path failure, bandwidth is set aside for the committed (CIR – Committed Information Rate) services. This ensures that even in the case of a failure, service levels remain unaffected.

In addition VLAN Cross-connect and standard bridging can work together in the same network over the same links. The decision as to which protection protocol to use is per VLAN and is dependant on whether bridging or VLAN Cross-connect is used.

Table 4 shows the different resiliency protocols supported over different architectures.

Architecture	Bridged VLANs with MAC learning	VLAN Cross-connect (No MAC Learning)	MPLS Tunnels
Meshed	STP/RSTP/MSTP LAG	Global Restoration LAG	Fast Reroute MPLS Global Restoration
Ring	STP/RSTP/MSTP LAG ERP ²	Global Restoration LAG	Fast Reroute MPLS Global Restoration
Mixed (Meshed + Ring)	STP/RSTP/MSTP/LAG ERP ³	Global Restoration LAG	Fast Reroute MPLS Global Restoration

Table 4 Summary of Resiliency options

4.4 Provisioning

Siemens' ACI-E Element Management System (EMS) supports VLAN Cross-connect provisioning. The ACI-E is a GUI based EMS which supports service profiles, mass provisioning and other time-saving mechanisms to ensure that the operations side of the network is efficient and thus lower OPEX costs.

The ACI-E will include a network planning tool which will help in configuring the network configuration.

In addition Siemens' APM-E Network Management System allows the same point and click provisioning as with bridging mode and provides an end-to-end view.

In the same way as the APM-E can provision end-to-end VLANs by clicking on both end-points of the connection, it can also do the same with VLAN Cross-connect paths. It will also define backup paths as well.

By using VLAN Cross-connect, DSLAMs can be identically provisioned with an inner VLAN per port and an outer VLAN per service. When the VLANs reach the aggregation switch (the SURPASS hiD 6650/6670), the outer VLANs can be switched and translated to VLANs per service per DSLAM. Simplifying the provisioning process makes the installation and operations processes quicker and less prone to provisioning mistakes.

5 Summary

As can be seen from the above document, Siemens' Advanced Ethernet Package provides an additional level of functionality that can help carriers solve scalability, flexibility and security issues.

VLAN Manipulation can easily integrate into any network configuration and enable a carrier to seamlessly implement advanced services like triple play.

² Note that for pure ring architectures, either STP/RSTP/MSTP or ERP should be used

³ Note that for networks which have both rings and meshed architecture, ERP can be used for ring protection, and STP/RSTP/MSTP can be used for the meshed portion of the network. In addition, BPDU messages can be transparently transferred across the ERP ring.

VLAN Cross-connect (both S-VLAN Cross-connect and S+C VLAN Cross-connect) is a useful complementary feature which could resolve some of the weaker areas of the Ethernet protocol (e.g. security). Combined with the VLAN Cross-connect resilience functionality which provides a protection mechanism for VLAN switched connections, this functionality provides the same resiliency as standard Ethernet bridging.

Since bridging, VLAN Manipulation and VLAN Cross-connect features can all be combined within the same node (and even the same port), different services can use different connections. For example, multipoint services like video can use MAC learning and VLAN Manipulation, whereas point-to-point services like Broadband DSL can use VLAN Cross-connect.

This flexibility makes the SURPASS hiD 6650/6670 the ideal platform for Carriers planning to provide multiple services such as triple play and advanced business applications.