SONET Interoperability Forum

WORK GROUP: Architecture

TITLE: Intercarrier Interface Recommendations

DATE: June 1998

EDITOR: Name: Cypryan (Kip) T. Klish, II
Voice: 919 992 3801
email: cypryan_klish@nt.com

ABSTRACT: The purpose of this document is to provide implementation requirements for interfaces between network providers and between network providers and end customers. These requirements may reduce the cascading of network failures between jurisdictional boundaries. A second purpose of this document is to increase the understanding of the problems that arise from inter-carrier communications.

TABLE OF CONTENTS

Table Of Figures

1. Scope, Purpose And Field Of Application

1.1 Scope

Implementation requirements for Synchronous Optical Network (SONET) inter-carrier interfaces are within the scope of this document. This document version supersedes SIF-010-1997.

1.2 Purpose

The purpose of this document is to provide implementation requirements for interfaces between network providers and between network providers and end customers. These requirements may reduce the cascading of network failures between jurisdictional boundaries. A second purpose of this document is to increase the understanding of the problems that arise from inter-carrier communications.

1.3 Application

This document has application to SONET interfaces that cross-jurisdictional boundaries.

2. References

1. ANSI T1.105-1995 Digital Hierarchy-Optical Interface Rates and Formats Specification (SONET)
2. ANSI T1.105.01-1998 - Synchronous Optical Network (SONET) - Automatic Protection Switching
3. ANSI T1.105.02-1995 - Synchronous Optical Network (SONET) - Payload Mappings
4. ANSI T1.105.04-1995 - Synchronous Optical Network (SONET) - Data Communication Channel Protocols and Architectures
5. ANSI T1.105.05-1994 - Synchronous Optical Network (SONET) - Tandem Connection Maintenance
6. ANSI T1.105.06-1996 - Synchronous Optical Network (SONET) - Physical Layer Specifications

7. ANSI T1.105.07-1996 - Synchronous Optical Network (SONET) - Sub STS-1 Interface Rates and Formats Specifications
8. ANSI T1.105.09-1996 - Synchronous Optical Network (SONET) - Timing and Synchronization
9. ANSI T1.224-1992 - Operations, Administration, Maintenance, and Provisioning (OAM&P) - Protocols for Interfaces between Operations Systems in Different Jurisdictions
10. ANSI T1.227-1995 - Operations, Administration, Maintenance, and Provisioning (OAM&P) - Extension to Generic Network Information Model for Interfaces between Operations Systems across Jurisdictional Boundaries to Support Fault Management (Trouble Administration)
11. T1.228-1995 - Operations, Administration, Maintenance, and Provisioning (OAM&P) - Services for Interfaces between Operations Systems across Jurisdictional Boundaries to Support Fault Management (Trouble Administration)
12. ITU-T G.707 - Network node interface for the synchronous digital hierarchy
13. ITU-T M.3010 - Principles of a Telecommunications Management Network (TMN)
14. GR-253-CORE - Synchronous Optical Network (SONET): Common Generic Criteria (a module of FR-440)
15. GR-1042-CORE - Generic Requirements for Operations Interfaces Using OSI Tools - Information Model Overview: Synchronous Optical Network (SONET) Transport Information Model
16. GR-2869-CORE - Generic Requirements for Operations Based on the Telecommunications Management Network (TMN) Architecture

3. Definitions

Definitions for most of the terms in this document are provided in the references, especially the ANSI T1.105 series of standards, and are not repeated here.

Inter-carrier interface: A SONET facility which is connected at either end to NEs in different administrative domains.

Isolated Sub-Domain: A portion of a management domain which is non-contiguous to the rest of the management domain, being separated by an intermediate carrier.

Private Network: A network in which all network elements and all network media are dedicated to a single customer or use. A private network therefore cannot contain any shared resources.

4. Acronyms

This section defines the acronyms used throughout this document.

Acronym	Definition
AIS	Alarm Indication Signal
ANSI	American National Standards Institute
ATIS	Alliance for Telecommunications Industry Solutions
ATM	Asynchronous Transfer Mode
BISs	Boundary Intermediate Systems
BLSR	Bi-directional Line Switched Ring
CLNP	ConnectionLess mode Network Protocol
CMIP	Common Management Information Protocol
CMISE	Common Management Information Service Element
CNM	Customer Network Management
CPE	Customer Premises Equipment
DCC	Data Communications Channel
DCN	Data Communications Network
DT	Data Transfer
EB	Electronic Bonding
EBG	Electronic Bonding Gateway
EML	Element Manager Layer
FDDI	Fiber Distributed Data Interface
FTAM	File Transfer, Access and Management
GNE	Gateway Network Element
IEC	InterExchange Carrier
ICI	InterCarrier Interface
IDRP	Inter-Domain Routing Protocol
IDT	Integrated Digital Terminal
INE	Intermediate Network Element
IS-IS	IS to IS intra-domain routing information exchange protocol
IS	Intermediate System
ISO	International Organization for Standardization
ITU	International Telecommunications Union
IWF	InterWorking Function
LEC	Local Exchange Carrier
LTE	Line Terminating Equipment
MD	Mediation Device
MF	Mediation Function
MIB	Management Information Base
NE	Network Element
NEF	Network Element Function
NET	Network Entity Title

NMA	Network Monitoring and Analysis
NML	Network Management Layer
NNI	Network-Network Interface
NSAP	Network Service Access Point
OAM&P	Operations, Administration, Maintenance & Provisioning
OSI	Open System Interconnection
OSS	Operational Support System
PDU	Protocol Data Unit
PM	Performance Monitoring
POTS	Plain Old Telephone Service
PRS	Primary Reference Source
RDT	Remote Digital Terminal
SONET	Synchronous Optical NETwork
SPE	Synchronous Payload Envelope
STE	Section Terminating Equipment
STS	Synchronous Transport Signal
SYNC	Synchronization
TMN	Telecommunications Management Network
UNI	User-Network Interface
UPSR	Unidirectional Path Switched Ring
VCI	Virtual Circuit (channel) Identifier
VPI	Virtual Path Identifier
VT	Virtual Tributary

5. Terminology

The following terms are used within this document:

Interface NE: A network element that forms part of the inter-carrier interface with respect to section and line DCC termination. Interface NEs are distinguished by positional location relative to the ICI and functional capability: they are the first STE or STE and LTE capable NEs adjacent to the ICI.

Non-Interface NE: A network element that does not form part of the inter-carrier interface. A non-interface NE is either not STE or STE and LTE capable, or if it is STE or STE and LTE capable, is not the first such NE adjacent to the ICI.

Path Originating NE: For purposes of this document, a path originating NE is one at which POH is generated.

6. Architectures

6.1 Inter-Carrier-Interface Interface NE Architectures

An inter-carrier interface may consist of from two to four interface NEs. This is because these recommendations place no restrictions on the functionality of interface NEs with respect to LTE functionality or STE functionality. In short, an interface NE may be STE capable NE or an STE and LTE capable NE. This gives rise to the ICI architecture cases described in the following subparagraphs.

This is a change from the first edition of this document, which restricted interface NEs to being both STE and LTE devices, and therefore permitted only a single ICI NE architectural case consisting of two interface NEs, one on each side of the ICI.

6.1.1 Two Interface NE ICI Architecture

If the two NEs immediately adjacent to an ICI are both STE and LTE, then the architecture is complete with those two NEs. Figure 1 depicts this architecture. NEs A2 and B1 are both interface NEs immediately adjacent to the ICI and are also both STE and LTE capable NEs.

Accordingly, the ICI spans only these two NEs, and NEs A1 and B2 are therefore not interface NEs.

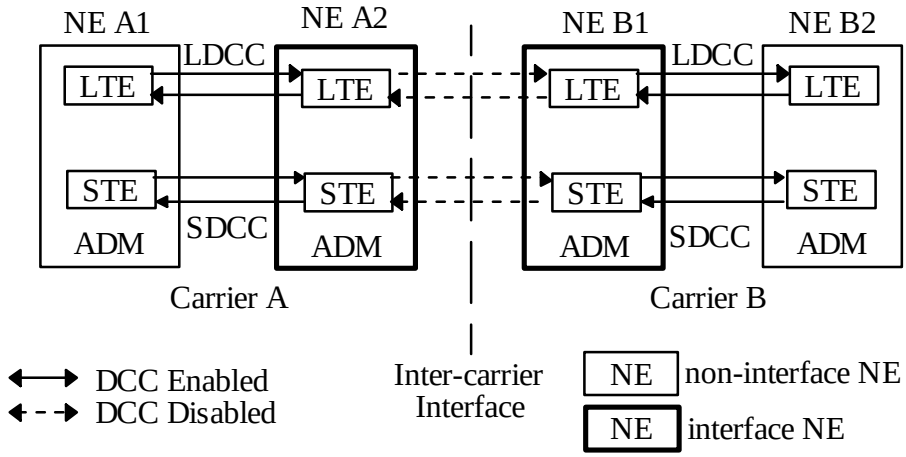

Figure 1: Two Interface NE ICI Architecture

6.1.2 Three Interface NE ICI Architecture

If the one of the NEs immediately adjacent to an ICI is an STE-only NE, and the first NE on the other side of the ICI is both STE and LTE, then the ICI spans three interface NEs, since an LTE-capable NE must be part of the ICI on the side that has the STE-only NE closest to the ICI.

Figure 2 depicts an ICI where two networks, Carrier A and Carrier B meet. One of the NEs immediately adjacent to the ICI, NE A2, is an STE-only interface NE, the other, NE B1 is both STE and LTE capable. As a result, the ICI spans three interface NEs; NE A1, an LTE capable NE becomes the third interface NE because it is the first LTE capable encountered as one moves away from the ICI on the Carrier A network side of the ICI. Thus, NEs A1, A2, and B1 are all interface NEs. NE B2 is a non-interface NE because STE and LTE capable interface NE B1 terminates both the LDCC and SDCC.

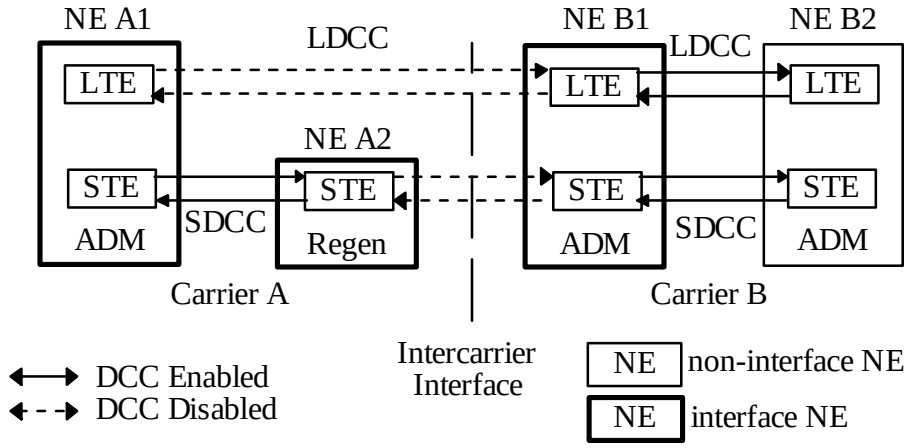

Figure 2: Three Interface NE ICI Architecture

Note that the STE-only NE and the LTE-capable NE that form one side of the ICI need not be adjacent, they may be separated by one or more additional STE-only NEs. Figure 3 illustrates this configuration:

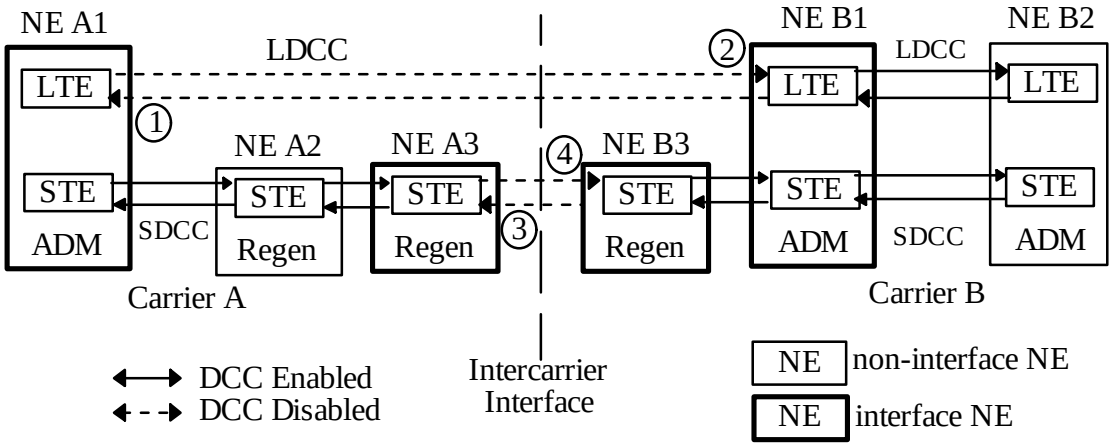

Figure 3: Non-adjacent Interface NEs

NE A2 of Figure 3 is an STE-only non-interface NE that separates interface NEs A1 and A3. Since interface NE A3 is the closest STE capable NE to the ICI, SDCC is disabled at it, and the STE only, non-interface NE A2 plays no role other than to make interface NEs A1 and A3 architecturally non-adjacent. NE B2 is also a non-interface NE as SDCC termination is provided by interface NE B3 and LDCC termination is provided by interface NE B1. Circled numbers one

through four indicate the targets for the four DCC disabling operations required to fully disable DCC traffic across this ICI.

6.1.3 Four Interface NE Architecture

If both of the NEs immediately adjacent to an ICI are STE only NEs, then the ICI spans four interface NEs since LTE capable NEs are needed on both sides of the ICI so that the LDCC can be disabled.

Figure 4 illustrates this architecture. Two networks, Carrier A and Carrier B network meet at the ICI shown. Immediately adjacent to the ICI, the NEs on either side, A2 and B1 are both STE only interface NEs. As result, LTE capable NEs A1 and B2 are also interface NEs, since they are the closest LTE capable NEs to the ICI.

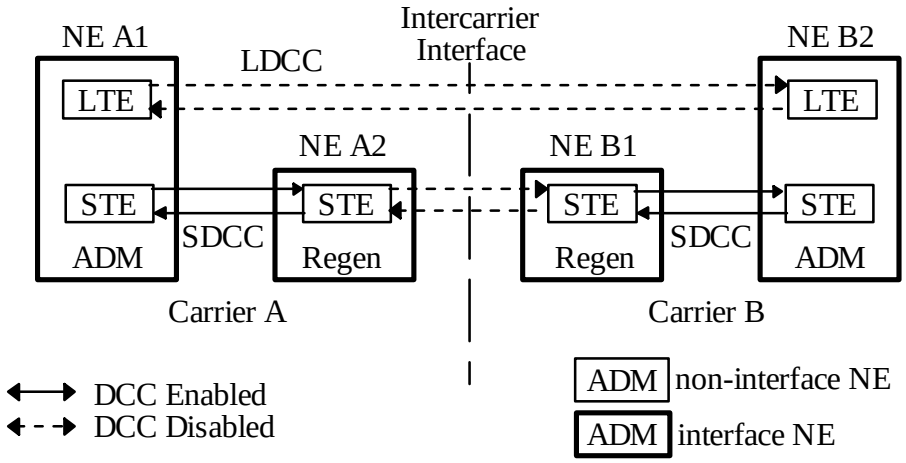

Figure 4: Four Interface NE ICI Architecture

As in the case of the three interface NE ICI architecture, the STE-only and LTE capable NEs need not be adjacent.

6.2 Inter-Carrier Interface Network Architectures

The following inter-carrier interface architectures were considered as part of this effort.

6.2.1 Linear Systems

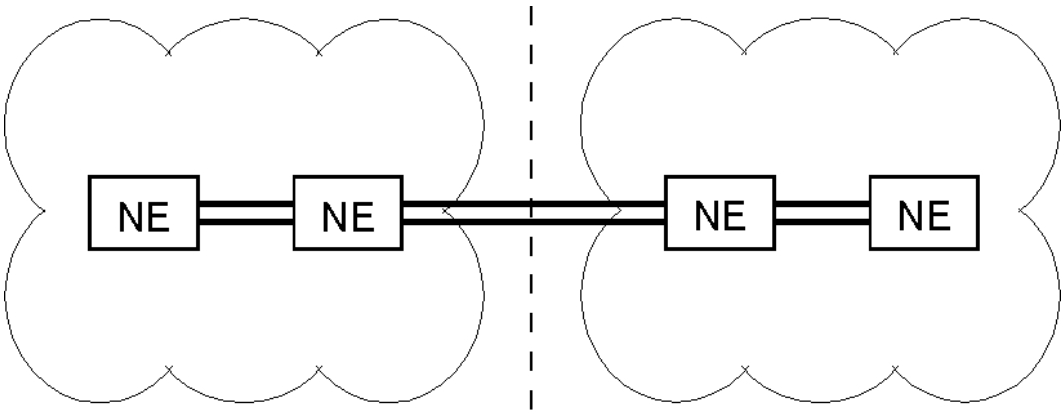

Figure 5: Linear Systems

The figure shows the interconnection of two SONET linear systems. The two (or more) SONET interface NEs on either side of the inter-carrier interface are configured in a linear chain architecture.

6.2.2 Ring to Linear Systems

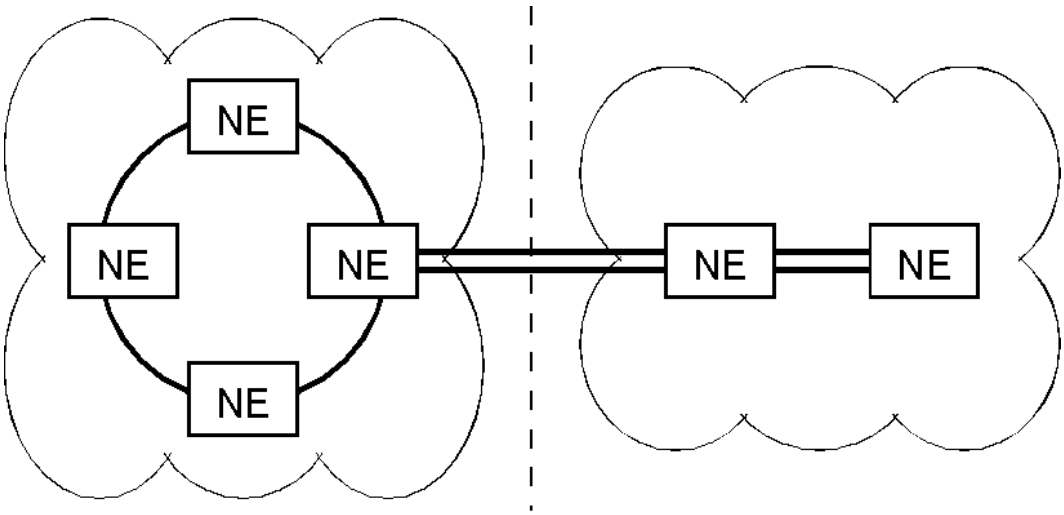

Figure 6: Ring to Linear Systems

The figure shows the interconnection of a SONET linear system with a SONET ring (UPSR or BLSR). The SONET NE(s) on the right side of the inter-carrier interface are configured in a linear chain architecture. The SONET NE(s) on the left side of the inter-carrier interface are configured in a SONET ring architecture. This ring can be either a UPSR or BLSR.

6.2.3 Ring to Ring Systems

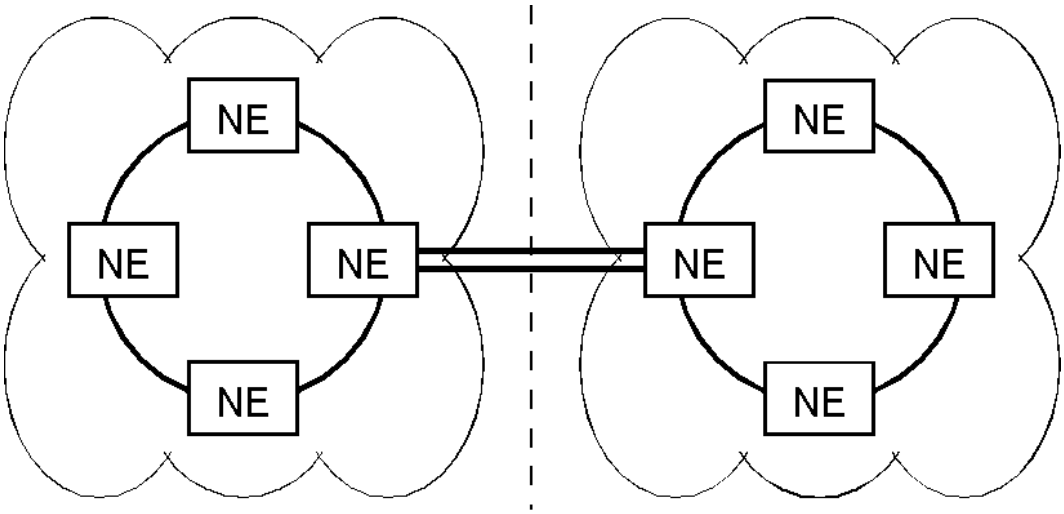

Figure 7: Ring to Ring System

The figure shows the interconnection of two SONET ring systems. The SONET NEs, one (or more) on each side of the inter-carrier interface, are configured in SONET ring architectures. Each ring may be either a UPSR or BLSR.

6.2.4 Ring to Ring (Dual Node) Systems

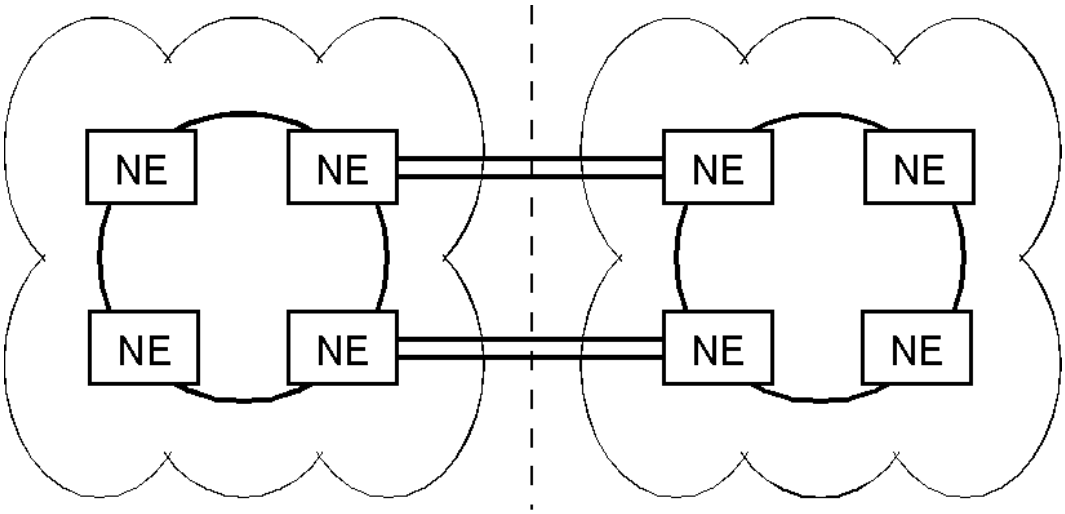

Figure 8: Ring to Ring (Dual Node) Systems

The figure shows the interconnection of two SONET ring systems in a dual ring interconnection configuration. The SONET NEs, two (or more) on each side of the inter-carrier interface, are configured in SONET ring architectures. Each ring may be either a UPSR or BLSR. Dual ring interconnection requires additional coordination between rings, including primary and secondary nodes, additional selector functionality, etc.

6.3 Carrier-Premises Interface Architectures

The following carrier-premises interface architectures were considered as part of this effort.

6.3.1 Customer Premises As Part Of The Carrier's Domain

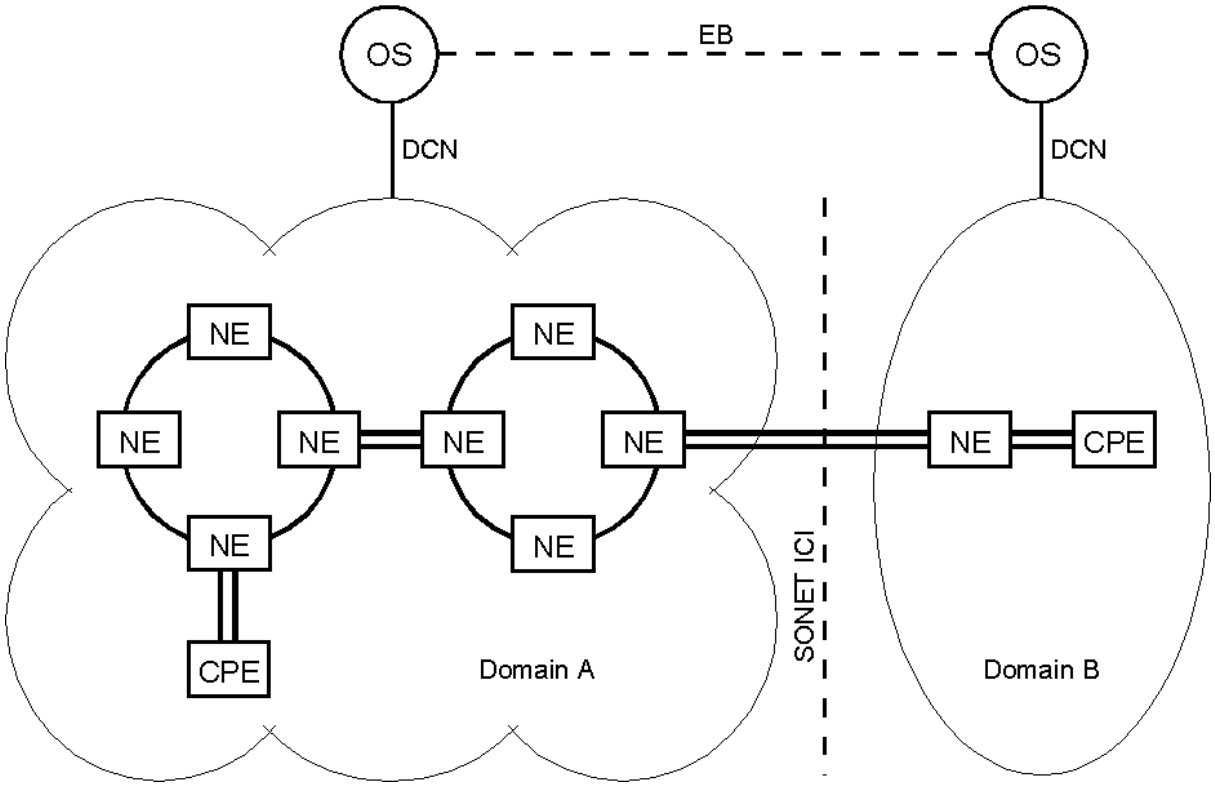

Figure 9: Customer Premises as Part of the Carrier's Domain

The figure shows customer premises equipment within the domain of carrier B. In this architecture, the customer premises equipment is part of B's management domain and is managed by carrier B through the use of the OS at B. The communication of management information between A and B can be performed through the use of an Electronic Bonding interface as shown.

6.3.2 Customer Premises As Its Own Domain

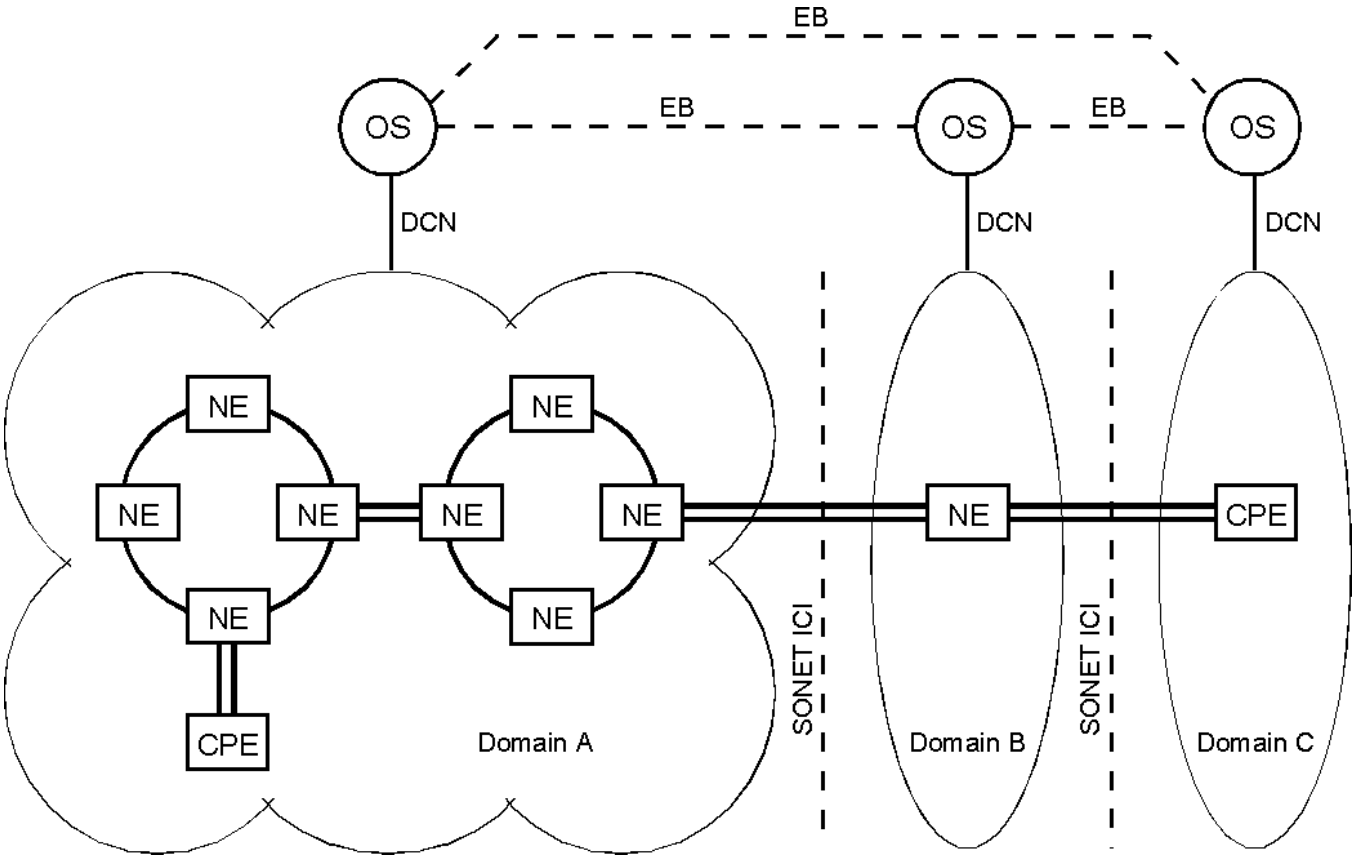

Figure 10: Customer Premises as Its Own Domain

The figure shows customer premises equipment within the domain of the customer C. In this architecture, the customer premises equipment is part of C's management domain and is managed by the customer through the use of an OS or craft interface terminal at C. The communication of management information between A and B and C can be performed through the use of Electronic Bonding interfaces as shown.

6.3.3 Customer Premises As An Isolated Sub-Domain

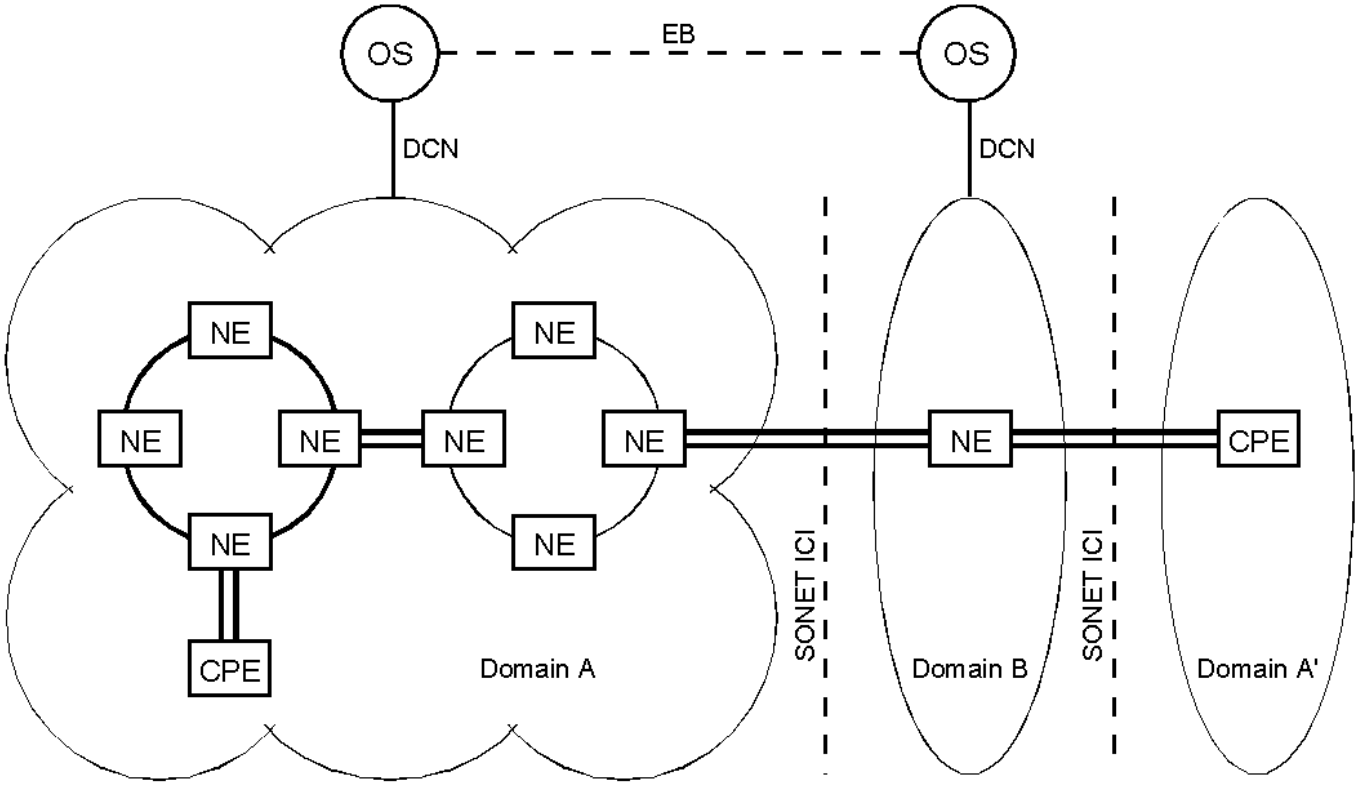

Figure 11: Customer Premises as an Isolated Sub-Domain

The figure shows customer premises equipment as an isolated sub-domain, non-contiguous to the domain of the managing carrier A. In this architecture, the customer premises equipment is part of A's management domain and the desire is to manage this customer premises equipment by carrier A through the use of the OS at A. While the communication of management information between A and B can be performed through the use of an Electronic Bonding interface as shown, the absence of a management or operations system within the isolated sub-domain A' precludes the communication of management information between A and A' through the use of an Electronic Bonding interface. The use of the DCC to provide connectivity from A to A' through B has been considered.

6.4 Private Network Architectures

The following private network architecture was considered as part of this effort.

6.4.1 Shared Ring Systems

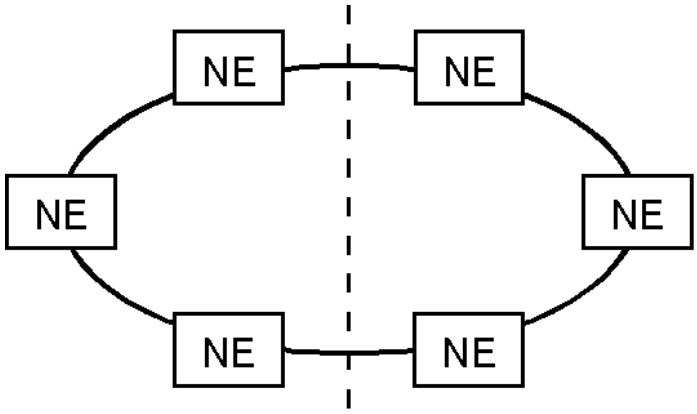

Figure 12: Shared Ring Systems

The figure shows the inter-carrier interface bisecting a SONET ring system. The six SONET NEs are configured in a single SONET ring system. This ring may be either a UPSR or BLSR. This scenario requires careful coordination between administrative domains because of the complex relationships between SONET NEs in a ring. Such shared ring systems can be treated as private networks, dedicated to a single use, and isolated from the management domains of both carriers.

7. Cascade Of Faults Through The Inter-Carrier Interface

A fault is considered to have cascaded through the inter-carrier interface if a fault on one side of the inter-carrier interface causes a service outage or outages to traffic that is completely contained on the other side of the inter-carrier interface. Faults which cause service outages only to traffic which traverse the inter-carrier interface, or to traffic on that side of the inter-carrier interface on which the fault originated, are not considered cascaded faults.

Three mechanisms for cascading of faults through the inter-carrier interface have been identified:

- Faults cascaded through the DCC.
- Faults cascaded through the SONET overhead bytes.
- Faults cascaded through the SONET clock synchronization messaging.

7.1 Cascade Of Faults Through The DCC

7.1.1 Current Situation

7.1.1.1 Primary Use Of The DCC

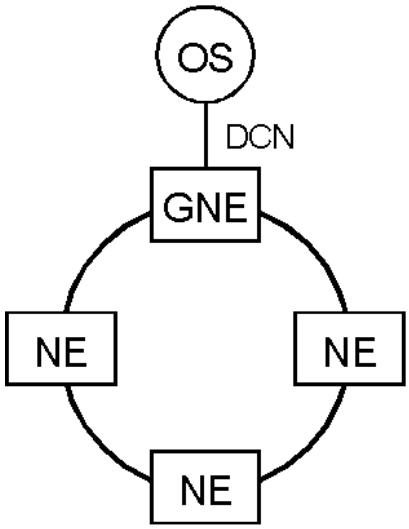

Figure 13: Normal Use of the DCC

Rather than deploy an external operations interface to every SONET NE, the DCC is used to carry operations information to a Gateway NE which does have an external operations interface, as shown in the figure. For OS-OS communications, traditional transport services (e.g., Frame Relay Service) are usually used rather than the DCC. The DCC use is usually restricted to intra-carrier communications.

7.1.1.2 Motivations For Inter-Carrier Use Of The DCC

The DCC bandwidth is available, though limited, and therefore there is a great temptation to use the DCC to carry inter-carrier management data. Alternatives include using a separate communications channel either 1) out of band, 2) in-band within the SONET payload, or 3) in-band within some other portion of the SONET signal. The added expense of these alternatives motivates carriers to consider the use of the DCC.

7.1.1.3 Current Inter-Carrier Interfaces

No standard use of the DCC has been defined for inter-carrier interfaces. Requirements for direct communications between NEs at an inter-carrier interface have not been identified. Electronic

Bonding standards are defined to exchange data between carriers' OSs; the operations data that may be exchanged using Electronic Bonding may apply to SONET or to any other network technology. SONET-specific operations data for Electronic Bonding is currently being defined and standardized. Electronic Bonding assumes that the OS of one carrier would communicate with the OS of another carrier using a traditional transport service (e.g., Frame Relay Service). To date the DCC is used between carriers via bilateral agreement since there are no standard solutions.

7.1.2 Considerations for Inter-Carrier Use Of The DCC

Inter-carrier use of the DCC could be through a single pair of NEs that are on separate rings, between two rings using dual-homing, between NEs that are on the same ring but in different carrier administrative domains, or any other of the architectures discussed and illustrated previously in Section 6.2.

The following sub-sections of Section 7.1.2 discuss problems that make this approach not viable.

7.1.2.1 Routing Considerations

Different methods of routing across the inter-carrier interface are possible, and each method has different impacts on the kinds of faults that can propagate across the interface. Administrative and operational considerations also affect the feasibility of the solution.

These possibilities were considered:

1. Same Level 1 Area (Level 1 Routing only)
2. Same Level 2 Area (Level 2 Routing)
3. Inter-domain Routing using only IS-IS
4. Inter-domain Routing using IDRP
5. Tunneling

7.1.2.1.1 Same Level 1 Area (Level 1 Routing Only)

All systems in all administrations are in the same Level 1 Area.

Pros:

1. Only Level 1 routing is required

Cons:

1. Detailed cooperation between administrations is required. Since all systems must be in the same area, they should all share the same Area Address. [NOTE: IS-IS implementations are required to support at least 3 area addresses per area, but this

feature is intended for managing area boundaries, such as moving area boundaries and splitting and joining areas.]

2. The size of one carrier's network affects the routing table size for every IS in the network, including those in the other carriers' networks. Sometimes an increase in the number of systems in the network may require reprovisioning, and sometimes it may require replacement or upgrade of equipment that has insufficient memory or processing power.
3. The size of one carrier's network affects the amount of routing protocol traffic and routing protocol processing time for every IS in the network, including those in the other carriers' networks. As a result of this and the previous item, network growth is very limited.
4. When there are multiple interfaces between the same two carriers, intra-carrier data will be routed through the other carrier's equipment, if that is the shortest path.
5. Routing protocol failures in one administration are likely to cause routing problems in other administrations.

7.1.2.1.2 Same Level 2 Area (Level 2 Routing)

All NEs are in the same Level 2 Area, and the inter-carrier interface always falls at a Level 1 Area boundary. There may be additional area boundaries that do not correspond to an inter-carrier interface.

Pros:

1. Less cooperation is required between administrations than in the first case. Area Address assignment must be coordinated so that no two areas are assigned the same Area Address.
2. Level 1 routing protocol failures in one administration will not affect Level 1 routing in another administration.
3. If each administration uses a single area, then intra-carrier data will not be routed across an inter-carrier interface.

Cons:

1. Level 2 Routing protocol failures in one administration can cause Level 2 routing problems in another.
2. The size of one carrier's network affects the routing table size for every Level 2 IS in the network, including those in the other carriers' networks. Sometimes an increase in the number of Level 2 ISs in the network may require reprovisioning, and sometimes it may require replacement or upgrade of Level 2 ISs that have insufficient memory or processing power.

3. The size of one carrier's network affects the amount of routing protocol traffic and routing protocol processing time for every Level 2 IS in the network, including those in the other carriers' networks.
4. Level 2 connectivity is required from the source to the destination of the inter-carrier traffic. As inter-area traffic is never forwarded from one Level 2 IS to another via a Level 1 IS, all Level 2 ISs in the inter-carrier traffic path must be interconnected to form a Level 2 backbone. For example, in a SONET ring that needs two Level 2 INEs for Level 1 Area interconnection, all INEs between the two Level 2 INEs must also be Level 2 INEs going either way around the ring. To provide protection switching for the DCN, all NEs on the ring must be Level 2 INEs, including SONET line- and section-terminating equipment.

7.1.2.1.3 Manually Provisioned Inter-Domain Routing

Each administration is in a different routing domain (Level 2 Area). There is a Level 2 INE on each side of an inter-carrier interface; these ISs are called Boundary Intermediate Systems (BISs). Each BIS is manually provisioned with one or more NSAP prefixes common to all systems on the other side of the boundary. This information is propagated in the Level 2 Link State PDUs (LSPs) to all other Level 2 ISs in the administration (routing domain).

Pros:

1. Intra-domain traffic will not be routed across an inter-carrier interface.
2. Other than the provisioning of reachable prefixes and traffic engineering issues, no special cooperation is required between administrations.
3. This is an academically correct solution, fitting the ISO routing domain and administrative domain hierarchy.
4. It is easier to add new areas and to add connectivity to more domains than in the previous alternatives.
5. This is supported by off-the-shelf IS-IS Level 2 routers.

Cons:

1. Level 2 connectivity is required from the source to the destination of the inter-carrier traffic, just as for Section 7.1.2.1.2 above.
2. Manual provisioning of reachable prefixes is required at each BIS.

7.1.2.1.4 Inter-Domain Routing Using IDRP (ISO 10747)

Each administration is in a different routing domain (Level 2 Area). There is a Level 2 INE on each side of an inter-carrier interface; these ISs are called Boundary Intermediate Systems (BISs). Each BIS runs IDRP to exchange routing information across the inter-carrier interface and with

other BISs in the domain. Since each BIS also operates as a Level 2 INE, it propagates the routing information to other Level 2 INEs via its Level 2 Link State PDUs (LSPs).

Pros:

1. Intra-domain traffic will not be routed across an inter-carrier interface.
2. Other than the provisioning of reachable prefixes and traffic engineering issues, no special cooperation is required between administrations.
3. This is an academically correct solution, fitting the ISO routing domain and administrative domain hierarchy.
4. It is easier to add new areas and to add connectivity to more domains than in the previous alternatives.
5. Manual provisioning of NSAP prefixes is not required.
6. Certain kinds of inter-domain routing policies can be enforced, including policies concerning data priority and security. Also, a domain that is connected to several other domains can selectively choose to relay traffic between some pairs of domains, while prohibiting relaying of traffic between other pairs of domains.

Cons:

1. Level 2 connectivity is required from the source to the destination of the inter-carrier traffic, just as for Sections 7.1.2.1.2 and 7.1.2.1.3 above.
2. Implementations are not widely available.
3. Space and processing requirements on BISs may be very large.

7.1.2.1.5 Tunneling

To support relaying traffic through another routing domain ("transit routing"), as required for the isolated sub-domain of Section 6.3.3, it is possible for the boundary intermediate systems to tunnel data through the other domain. A BIS at the inter-carrier interface of the originating domain would encapsulate the received DT PDU within another DT PDU, and send this encapsulated PDU to the NET of the BIS at the inter-carrier interface of the destination domain. Upon receipt of this PDU, the BIS would extract the enclosed PDU and forward it to the destination domain. This is supported by IDRP and the IDRP mechanism could be adapted for use without IDRP. The same kind of tunneling is employed by IS-IS to perform partition repair. The advantage to tunneling is that it avoids the need for Level 2 connectivity between the exit points in the transit routing domain. However, routing issues would still need to be resolved so that:

1. data from the originating domain can be routed to the tunneling BIS,
2. tunneled data from this BIS can be routed to the BIS at the destination routing domain, and

3. Untunneled data from the destination BIS can be routed to the ultimate destination system.

The most straightforward solution would use inter-domain routing in the source and destination domains and across the inter-carrier interface, and tunneling only within the transit routing domain. Since the tunneled traffic would not cross an inter-carrier interface, it is beyond the scope of this document.

7.1.2.2 Traffic Engineering Considerations

In addition to the routing and network architecture issues discussed above, transit routing to meet the need of Section 6.2.4 imposes additional traffic engineering considerations on the transit routing domain. Normally, the DCN is engineered for the bulk of OAM&P traffic required to manage the network, and this traffic usually travels between a Central Office and the managed NEs. Transverse traffic, or traffic that goes between NEs on opposite sides of a domain, is usually minimal. Transit routing may burden the network with a significant amount of transverse traffic, which must be taken into account in the network architecture and bandwidth allocation.

7.1.2.3 Security Considerations

Security issues become important in the inter-carrier use of the DCC because access to the control network has been given to an outside enterprise. The present implementations of DCC communications do not contain adequate security mechanisms for the more open environment resulting from using the DCC for inter-carrier communications.

7.1.2.3.1 Security Threats

Various threats must be considered. These include:

- Breach of authentication mechanisms
- Breach of access control mechanisms
- Masquerading
- Alteration of information
- Loss of confidentiality
- Traffic analysis
- Theft of service
- Denial of service

7.1.2.3.2 Security Mechanisms

The services that are required to counter these threats are:

- Authentication (of user, network element)
- Data integrity
- Data confidentiality
- Access control

Mechanisms used to support these services are:

- Authentication exchange
- Digital signature
- Encryption
- Data integrity
- Access control

To implement OSI security mechanisms would likely require an upper layer security mechanism, the authentication functional unit of ACSE, a trusted entity for the issuance of keys, appropriate modifications to the MIB, and implementing the access control mechanisms for FTAM and CMISE. The upper layer security mechanism for TL1 over OSI is not currently available.

Such mechanisms would allow the carrier to handle most of the security threats. For example, a breach of authentication threat is avoided by employing a combination of authentication exchange, digital signature, and encryption.

7.1.2.3.3 Unresolved Security Issues

Traffic analysis and denial of service are problematic.

Because traffic analysis does not rely on the content of what is sent, an intervening network can be in a position to use the timing and volume of the through traffic to understand a competitor's business strategy and quality of service characteristics, as well as the size and type of the carrier's network.

Denial of service is a problem because the DCC is already congestion-limited for use in a single carrier's network. An additional increment of traffic from carrier A to its remote network elements in isolated sub-domains may cause the failure of the network for carrier B as they pass through. Conversely, a high traffic load on carrier B's DCC may make it impossible for carrier A to administer its remote equipment. Maliciously caused congestion is a particular concern. Another issue is the fact that, as the other security services are implemented, their overhead can contribute to the traffic load, raising the likelihood of congestion.

Schemes for congestion control could be implemented, but are beyond the scope of this document.

7.1.2.4 Restrict Functions Available To Outside Carrier

In addition to the security threats of Section 7.1.2.3, there are security issues related to the assignment of access privileges. We would need to provide security procedures to restrict the functions that the outside carrier could perform on NEs across the inter-carrier interface. We need to ensure that only the functions, which have been prearranged, can be carried out between the NEs. For example the agreed interface may have defined read access between the NEs. The NEs would then need to ensure that any write requests coming from the inter-carrier interface would be denied. This implies additional software would need to be written at the NEs.

7.1.2.5 Standard Message Set

One motivation for the use of the DCC across the inter-carrier interface is NE-NE communications. We would need to define and implement a standard inter-carrier message set for the NEs to implement inter-carrier use of the DCC. Other than the message set for the interface between the RDT and the IDT in TR-303 we are unaware of standard CMIP message sets between NEs. We do not see the need to have the TR-303 interface span inter-carrier interfaces.

7.1.2.6 Restrict Messages To Designated NEs

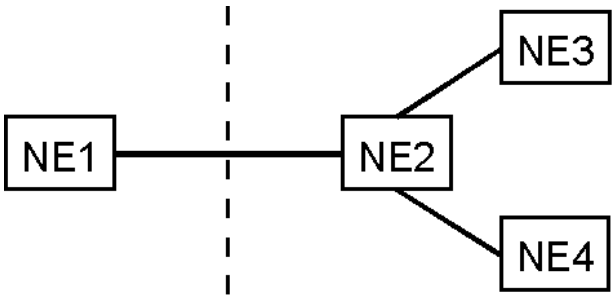

Figure 14: Restricted Messages Example

If the NE to be accessed is a NE other than the boundary NE at the carrier interface, additional complexities arise. In the figure, suppose the target NE is NE3 and we want to ensure that no outside commands go to NE 4. In this case we must filter messages, either at NE2 or at NE4. It is more economical to filter messages at NE2 since this will reduce the amount of extra traffic in the control network and will also limit the number of sites at which the filtering software must be implemented. This implies additional software would need to be written at the NEs.

7.1.2.7 Partitioning Access Within An NE

If the NE provides service to other customers or carriers than the one that is accessing the NE,

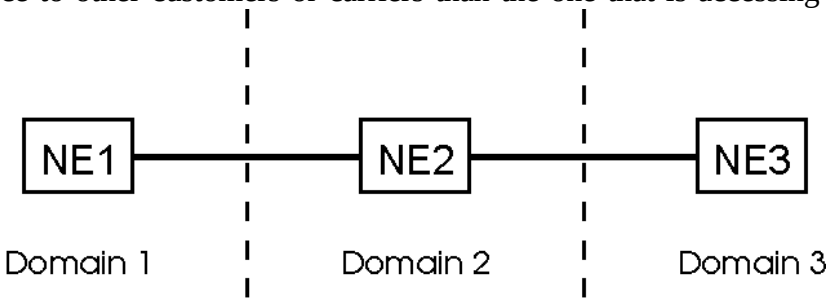

Figure 15 : Partitioning Access within a NE

then additional complexities arise. In the figure, suppose NE2 is providing services to customers in Domain 1 and Domain 3. Any messages that are received from NE1 must not be allowed to access information within NE2 concerning the service provided to Domain 3. Similarly any NE3 messages must not be allowed access to information within NE2 concerning the service provided to Domain 1.

7.1.2.8 Maintenance Of The Inter-Carrier DCC

Since separate authorities handle either end of the DCC the maintenance of the DCC may be more complex. The two authorities may have different maintenance procedures and will rely on separate and perhaps different types of OSs to maintain their DCCs. Maintenance procedures for the inter-carrier use of the DCC would need to be worked out between the authorities.

7.1.2.9 Billing For The Inter-Carrier Use Of The DCC

If any billing strategy other than a flat fee were used, additional functions at the terminating NEs would need to be added to calculate the use of the DCC so that proper billing records can be maintained. These are functions not traditionally found at these NEs and so may not be easy to add. These billing facilities would need to be sensitive to the traffic across the inter-carrier interface, as well as to the source and destination of the traffic within the billing carrier.

7.1.3 Requirements For The DCC

Section 7.1.1 has reviewed the ways in which the DCC is currently used, and Section 7.1.2 has reviewed the issues involved in using the DCC as a means of communication of management information across inter-carrier interfaces. Significant obstacles exist in providing the DCC across inter-carrier interfaces, primarily in the areas of routing, traffic congestion and management, and security. Solutions to these obstacles that would be more effective than the existing alternatives to the inter-carrier use of the DCC have not been found. The following Requirement is therefore imposed:

> **Requirement: To prevent the cascade of faults across inter-carrier interfaces, the inter-carrier use of the DCC is prohibited. In particular:**

1. SONET NEs are required to ignore the DCC received across an inter-carrier interface.

2. SONET NEs are required to ignore the DCC received across a carrier-premises interface.

3. SONET NEs are required to ignore the DCC received across a carrier-private network interface.

7.1.4 Alternatives To The Inter-Carrier Use Of The DCC

The following alternatives to the inter-carrier use of the DCC are proposed to meet the needs for the transmission of management information across the inter-carrier interface.

7.1.4.1 Alternative For Inter-Carrier Interface: Electronic Bonding

Electronic Bonding (EB) is the term given to an effort to implement an OSI/CMISE interface for the exchange of customer network management information between OSs in different administrations (e.g., IEC-LEC). In TMN terms, this interface is a service level X interface. This mechanized operations interface currently supports generic (i.e., POTS, specials, etc.) trouble reporting based on the OSI/CMISE model defined in the ANSI T1 Trouble Administration Standard (T1.227 and T1.228). In 1996, contributions on additional functional areas, fault and performance management were submitted to T1 to be incorporated in the EB interface standards.

7.1.4.1.1 Electronic Bonding Architecture

The carrier EB architecture consists of an EB gateway with an external OSI/CMISE interface to another carrier's EB gateway and an internal interface to back-end OSs. This architecture allows customers to access the carrier's back-end OS SONET service management capabilities via a single OSI/CMISE interface to an EB gateway that provides security and data mapping interfaces for the back-end systems. An EB gateway has the following features:

- interfaces with the customer
- provides security
- stores management information
- interfaces with service provider back-end OSs
- translates CNM messages to and from back-end OS capabilities

The EB gateway provides uniform single point security. Possible security features include:

- customer authentication
- customer data partitioning
- non-repudiation

- message integrity
- access control
- intrusion detection

The EB gateway provides a single well-defined interface that can be designed to shield service provider OSs from network failures in external domains.

7.1.4.1.2 Comparison Of Electronic Bonding To The SONET DCC

	Electronic Bonding	**SONET DCC**
Definition	Term for exchange of CNM information between OSs in different administrations	A message oriented operations communications channel using SONET section overhead bytes
Purpose	To facilitate the exchange of CNM information between OSs in different administrations	To extend the reach of the operations communications network to NEs beyond the gateway NE
Technology	Technology Independent	SONET Specific
TMN Layer/Interface	Defined as a Service Layer X Interface	Typically supports Element Management Layer - Network Element Layer Q interface or non-standard interface
Protocols	Defined as OSI/CMISE	CMISE over OSI 7 layer stack TL1 over OSI 7 layer stack or others
Related Standards	T1.224, T1.227, and T1.228	GR-253-CORE (SONET Req.) T1.105.04 (SONET DCC) GR-1042-CORE (OSI/CMISE) GR-1042-IMD (OSI/CMISE)

As can be seen from the table, there are substantial differences between EB and the DCC. The differences stem primarily from the reasons these capabilities were developed in the first place: the EB being a means of facilitating the exchange of CNM information; and the DCC being an

extension of the SONET operations communications network. From these clearly distinct roles flows the major difference: The EB interface is an OSI/CMISE service layer X interface while the DCC, which is not an interface, typically supports an EML-NEL Q interface or non-standard interface.

7.1.4.1.3 Recommendation For The Use Of Electronic Bonding

Electronic bonding has been designed for the transmission of management information across the inter-carrier interface, and is the most suitable mechanism.

> **Recommendation: The use of electronic bonding for the transmission of management information across the boundary between administrative domains is hereby recommended for all cases in which an OS exists on both sides of the interface.**

7.1.4.2 Alternatives For Isolated Sub-Domains

It is known that the need exists to manage isolated sub-domains, as illustrated in Section 6.3.3, and it is anticipated that this need will grow as SONET increasingly penetrates to the premises. These isolated sub-domains do not contain an OS, and the use of electronic bonding to transport management information is therefore impossible. Transmission of the DCC across the intermediate carrier poses all of the issues discussed in Section 7.1.2, however, and is therefore prohibited in Section 7.1.3.

> **Recommendation: It is recommended that the management of isolated sub-domains be accomplished by transporting the management information from the primary carrier through the intermediate carrier to the isolated sub-domain in one of the following ways:**
>
> - **Use of a separate dedicated facility to carry the management information through the intermediate carrier.**
> - **Tunneling of the management information through the intermediate carrier by using bandwidth within the SONET payload.**

Each of these alternatives has advantages and disadvantages, and one or more of these alternatives may be impossible in specific applications.

7.1.4.2.1 Use Of A Separate Dedicated Facility

In one implementation of this alternative, the SONET DCC would be separated from the SONET signal within the primary carrier A at its boundary with the intermediate carrier B. The SONET DCC would be transported through B on a separate dedicated facility, such as a dial-up modem over POTS, 56 kbps leased line, fractional T-1, or frame relay service. The SONET DCC would be reinserted in the SONET signal within the isolated sub-domain A' at its boundary with B.

Another implementation of this alternative is to separate the management information packets, sourced within the primary carrier A and destined for isolated sub-domain A', at a point earlier than the boundary with the intermediate carrier B. The separation of the management information data stream could occur anywhere within the DCN, perhaps at or near the OS itself. Similarly, the management information data stream could emerge at any point within the isolated sub-domain A'.

The key point is that a separate dedicated facility transports the management information from within the primary carrier A to within the isolated sub-domain A' without ever being transported over the DCC of the intermediate carrier B.

The advantages of this alternative include that the management circuit is up even when the transmission path is down, allowing remote diagnostics of the far end during service outages. The disadvantages of this alternative include the one-time acquisition and installation of the terminating equipment and the recurring expenses and OAM&P of the separate dedicated facility and its termination equipment.

7.1.4.2.2 Tunneling Of The DCC Within The SONET Payload

A number of methods can be used to provide tunneling of the DCC within the SONET payload, depending on the mapping of the payload, including:

- Dedicated VT1.5 for DS1 mapped payloads.
- ATM cells for ATM-mapped payloads.
- FDDI packets for FDDI-mapped payloads.

For the VT1.5 alternative, the management information is carried over a DS1 mapped into a VT1.5 on a SONET MUX within the primary carrier A. The signal is then carried through the network to the isolated sub-domain A' and demuxed there back to a DS1.

For the ATM cell alternative, the management information is carried over a VCI/VPI pair selected from the ATM switch, and mapped into the ATM payload of the SONET signal within the primary carrier A. The signal is carried to the isolated sub-domain A' and the ATM cells are extracted by ATM equipment at the isolated sub-domain.

For the FDDI packet alternative, the management information is carried within FDDI packets through an FDDI router, and mapped into the FDDI payload of the SONET signal within the primary carrier A. The signal is carried to the isolated sub-domain A' and the FDDI packets are extracted by FDDI router equipment at the isolated sub-domain.

The advantages of this alternative include that no separate dedicated facility is required, and no additional facility, terminating equipment, and operations expenses are incurred. The disadvantages of this alternative include the requirement to use customer bandwidth to provide management visibility of equipment within the isolated sub-domain A' to operations systems

within the primary carrier A. An additional disadvantage of this alternative is that some mappings do not provide any divisible small portion of the bandwidth, such as the DS-3 mapped STS-1, in which the smallest divisible signal is one third of the capacity.

7.1.4.3 Alternatives For Private Networks

For private network architectures, such as the shared ring architecture of Section 6.4.1, the DCC can be turned on within the private network. However, per Section 7.1.3, the DCC shall not be propagated outside the private network across any carrier-private network interface. Any of the alternatives for the management of isolated sub-domains, discussed in Section 7.1.4.2, may be used to transport management information into and out of the private network.

7.2 Cascade Of Faults through the SONET Overhead Bytes.

There are cases where the overhead bytes of the SONET frame received over the inter-carrier interface can cause a cascade failure, as previously defined in Section 7.

One simple example is the case where a NE vendor has implemented a proprietary embedded operations channel using a non-standard overhead byte in the SONET frame. If both carriers on either side of the inter-carrier interface employ NEs from the same vendor and the proprietary operations channel is not blocked over the inter-carrier interface, either carrier may be able to control NEs across the inter-carrier interface into the other carrier's network and affect their network operations.

Another example is the case where non-standard or erroneous K1/K2 byte values in a protected shared ring architecture can cause an NE to switch to its protection fibers while its neighboring NE does not switch, resulting in a break in the ring which could affect local ring traffic as well as inter-carrier interface traffic.

The following requirements are therefore imposed on the NEs that sit at either end of the inter-carrier interface.

7.2.1 Requirements For Section Overhead Bytes

B1 - Section Parity, E1 - Local Orderwire - Interface NEs must generate these bytes per GR-253-CORE, ANSI, or ITU standards as listed in Section 2. Non-standard uses of these bytes are prohibited over the inter-carrier interface.

A1, A2 - Framing - Interface NEs must properly generate A1/A2. Interface NEs must generate AIS-L downstream when unable to properly detect incoming A1/A2. This prevents invalid frames from being propagated through a network.

C1 - Section Trace or STS ID - Interface NEs must not assume this contains an STS-ID and must not perform routing or protection switching based on this byte.

D1-3 - Section DCC - The Section DCC is addressed in Section 7.1 of this document.

F1 - Section User Channel - Interface NEs must have the ability to ignore the incoming value in this byte received over the inter-carrier interface and must not pass it through to the rest of the network. A carrier must block this byte received over the inter-carrier interface unless jointly agreed to by both carriers. Note that some NE vendors use this byte as a proprietary embedded operations channel.

7.2.2 Requirements For Line Overhead Bytes

B2 - Line Parity; E2 - Express Orderwire; H1, H2, H3 - Pointer; K1, K2 - Protection Switching; M1 - Far End PM - Interface NEs must generate these bytes per GR-253-CORE, ANSI, or ITU standards as listed in Section 2. Non-standard uses of these bytes are prohibited over the inter-carrier interface.

D4-12 - Line DCC - The Line DCC is addressed in Section 7.1 of this document.

Z1, Z2 - Growth - Interface NEs must have the ability to ignore the incoming value in this byte received over the inter-carrier interface and must not pass it through to the rest of the network. A carrier must block this byte received over the inter-carrier interface unless jointly agreed to by both carriers.

S1 - Timing Info - The synchronization subsystem of interface NEs shall not pass the incoming S1 byte value received over the inter-carrier interface to the rest of the receiving network. This does not mean that the interface NE shall not receive or process the received S1 byte according to applicable management standards, nor does this imply that the synchronization subsystem of interface NEs shall not make the received S1 byte available internally to NE management applications or to external management systems. It prohibits only:

- The propagation of an S1 byte received across the ICI within the network the receiving interface NE is part of.
- The consideration or use of an S1 byte value received across the ICI in the generation of a new S1 byte that is generated by the receiving NE for use within its own (receiving) network.
- The clocking an outbound signal using a clock selected by using an S1 byte received across the ICI.

Note that interface_NEs must still generate a valid S1 byte per GR-253-CORE, ANSI, or ITU standards as listed in section 2. Note also that if the ICI is between a stratum 1 capable carrier

and a small carrier or private network which is not stratum 1 capable, then these requirements may be waived if an agreement between the two parties is reached. See section 7.3.2 for additional discussion of this case.

7.2.3 Requirements For Path Overhead Bytes

B3 - Path Parity - Path originating NEs must generate this byte per GR-253-CORE, ANSI, or ITU standards as listed in Section 2. Non-standard uses of this byte are prohibited over the inter-carrier interface.

F2 - Path User Channel -This byte must be processed according to GR-253-CORE, ANSI, or ITU standards as listed in Section 2. Non-standard (proprietary) use of the F2 byte is specifically prohibited. In cases where a carrier deploys equipment that makes proprietary use of the F2 byte, it is the responsibility of that carrier to ensure that:

- The F2 byte contents of paths entering their network are not lost and are transparently available at the intercarrier interface where the paths exit the carrier's network.

- Their proprietary use of the F2 bytes does not propagate faults across the intercarrier interface.

7.3 Cascade Of Faults Through The SONET Synchronization Subsystem

Synchronization faults may be propagated across the ICI through two mechanisms: the actual selection of a synchronization clock source and through the use of synchronization messages contained in the S1 byte. This section discusses both mechanisms and provides the network operator with recommendations for the prevention of synchronization fault propagation across the ICI.

Two broad categories of SONET clock synchronization messaging across an inter-carrier interface are considered: 1) interfaces where both carriers involved are capable of providing reliable and consistent stratum-1 traceable timing to their NEs, and 2) interfaces where one of the two carriers involved is not capable of providing reliable and consistent stratum-1 traceable timing to its NEs. Interface 1 is typical of an interface between two large carriers. Interface 2 is more likely to be a carrier-customer interface or an interface between a large carrier and a small one.

7.3.1 Clock Synchronization Messaging Between Large Carriers

The general principle for inter-carrier interfaces is that each network operator provides its own stratum-1 traceable timing to its own NEs. Therefore, NEs shall ignore synchronization source

messaging received across the inter-carrier interface. No transfer of timing between networks is recommended under normal operating conditions. This is also applicable to a shared ring architecture. This recommendation is possible since the clock differences between the two sources are negligible and the errors introduced will be small. The shared ring architecture and other private network architectures can also be handled as in Section 7.3.2.

7.3.2 Clock Synchronization Messaging With A Private Network Or Small Carrier

In cases where a SONET signal crosses from a public to a private network or a small carrier that does not have a stratum-1 traceable synchronization source, the private network/small carrier should derive timing from the carrier that has stratum-1 traceable timing source. In such cases specific agreements must be made between the parties. This synchronization is recommended since the large difference in a stratum-1 traceable clock and a free running clock will cause excessive errors across the interface.

If an agreement is made between a stratum 1 capable carrier and a private network/small carrier to allow the private network/small carrier to derive timing from the stratum 1 capable carrier, then the two parties may also agree to accept synchronization messages across the ICI.

The discussion contained in this section is specific to the stratum 1 capable carrier to private network/small carrier case. If specific agreements between the parties are reached as described above, these agreements override the S1 byte requirements of section 7.2.2.

7.3.3 Requirements For Clock Synchronization Messaging

Synchronization of SONET clocks across the inter-carrier interface provides an opportunity for the cascade of faults across the inter-carrier interface. Stratum-1 traceable timing will generally be available for both sides of the inter-carrier interface. Refer to section 7.2.2 for S1 byte requirements.