INSTALLATION AND
OPERATION MANUAL

ACE-3600

RNC-Site Gateway

Version 5.2

data communications
The Access Company

ACE-3600

RNC-Site Gateway

Version 5.2

Installation and Operation Manual

Notice

This manual contains information that is proprietary to RAD Data Communications Ltd. ("RAD"). No part of this publication may be reproduced in any form whatsoever without prior written approval by RAD Data Communications.

Right, title and interest, all information, copyrights, patents, know-how, trade secrets and other intellectual property or other proprietary rights relating to this manual and to the ACE-3600 and any software components contained therein are proprietary products of RAD protected under international copyright law and shall be and remain solely with RAD.

The ACE-3600 product name is owned by RAD. No right, license, or interest to such trademark is granted hereunder, and you agree that no such right, license, or interest shall be asserted by you with respect to such trademark. The RAD name, logo, logotype, and the terms EtherAccess, TDMoIP and TDMoIP Driven, and the product names Optimux and IPmux, are registered trademarks of RAD Data Communications Ltd. All other trademarks are the property of their respective holders.

You shall not copy, reverse compile or reverse assemble all or any portion of the Manual or the ACE-3600. You are prohibited from, and shall not, directly or indirectly, develop, market, distribute, license, or sell any product that supports substantially similar functionality as the ACE-3600, based on or derived in any way from the ACE-3600. Your undertaking in this paragraph shall survive the termination of this Agreement.

This Agreement is effective upon your opening of the ACE-3600 package and shall continue until terminated. RAD may terminate this Agreement upon the breach by you of any term hereof. Upon such termination by RAD, you agree to return to RAD the ACE-3600 and all copies and portions thereof.

This product is manufactured and sold under license to U.S. Patent Re. 36,633.

For further information contact RAD at the address below or contact your local distributor.

International Headquarters **RAD Data Communications Ltd.**	**North America Headquarters** **RAD Data Communications Inc.**
24 Raoul Wallenberg Street Tel Aviv 69719, Israel Tel: 972-3-6458181 Fax: 972-3-6498250, 6474436 E-mail: market@rad.com	900 Corporate Drive Mahwah, NJ 07430, USA Tel: (201) 5291100, Toll free: 1-800-4447234 Fax: (201) 5295777 E-mail: market@rad.com

Publication No. 493-200-11/08

Limited Warranty

RAD warrants to DISTRIBUTOR that the hardware in the ACE-3600 to be delivered hereunder shall be free of defects in material and workmanship under normal use and service for a period of twelve (12) months following the date of shipment to DISTRIBUTOR.

If, during the warranty period, any component part of the equipment becomes defective by reason of material or work manship, and DISTRIBUTOR immediately notifies RAD of such defect, RAD shall have the option to choose the appropriate corrective action: a) supply a replacement part, or b) request return of equipment to its plant for repair, or c) perform necessary repair at the equipment's location. In the event that RAD requests the return of equipment, each party shall pay one-way shipping costs.

RAD shall be released from all obligations under its warranty in the event that the equipment has been subjected to misuse, neglect, accident or improper installation, or if repairs or modifications were made by persons other than RAD's own authorized service personnel, unless such repairs by others were made with the written consent of RAD.

The above warranty is in lieu of all other warranties, expressed or implied. There are no warranties which extend beyond the face hereof, including, but not limited to, warranties of merchantability and fitness for a particular purpose, and in no event shall RAD be liable for consequential damages.

RAD shall not be liable to any person for any special or indirect damages, including, but not limited to, lost profits from any cause whatsoever arising from or in any way connected with the manufacture, sale, handling, repair, maintenance or use of the ACE-3600, and in no event shall RAD's liability exceed the purchase price of the ACE-3600.

DISTRIBUTOR shall be responsible to its customers for any and all warranties which it makes relating to ACE-3600 and for ensuring that replacements and other adjustments required in connection with the said warranties are satisfactory.

Software components in the ACE-3600 are provided "as is" and without warranty of any kind. RAD disclaims all warranties including the implied warranties of merchantability and fitness for a particular purpose. RAD shall not be liable for any loss of use, interruption of business or indirect, special, incidental or consequential damages of any kind . In spite of the above RAD shall do its best to provide error-free software products and shall offer free Software updates during the warranty period under this Agreement.

RAD's cumulative liability to you or any other party for any loss or damages resulting from any claims, demands, or actions arising out of or relating to this Agreement and the ACE-3600 shall not exceed the sum paid to RAD for the purchase of the ACE-3600. In no event shall RAD be liable for any indirect, incidental, consequential, special, or exemplary damages or lost profits, even if RAD has been advised of the possibility of such damages.

This Agreement shall be construed and governed in accordance with the laws of the State of Israel.

Product Disposal

To facilitate the reuse, recycling and other forms of recovery of waste equipment in protecting the environment, the owner of this RAD product is required to refrain from disposing of this product as unsorted municipal waste at the end of its life cycle. Upon termination of the unit 's use, customers should provide for its collection for reuse, recycling or other form of environmentally conscientious disposal.

General Safety Instructions

The following instructions serve as a general guide for the safe installation and operation of telecommunications products. Additional instructions, if applicable, are included inside the manual.

Safety Symbols

⚠ **Warning**

This symbol may appear on the equipment or in the text. It indicates potential safety hazards regarding product operation or maintenance to operator or service personnel.

⚡

Danger of electric shock! Avoid any contact with the marked surface while the product is energized or connected to outdoor telecommunication lines.

⏚

Protective ground: the marked lug or terminal should be connected to the building protective ground bus.

Warning

Some products may be equipped with a laser diode. In such cases, a label with the laser class and other warnings as applicable will be attached near the optical transmitter. The laser warning symbol may be also attached.

Please observe the following precautions:

- Before turning on the equipment, make sure that the fiber optic cable is intact and is connected to the transmitter.
- Do not attempt to adjust the laser drive current.
- Do not use broken or unterminated fiber-optic cables/connectors or look straight at the laser beam.
- The use of optical devices with the equipment will increase eye hazard.
- Use of controls, adjustments or performing procedures other than those specified herein, may result in hazardous radiation exposure.

ATTENTION: The laser beam may be invisible!

In some cases, the users may insert their own SFP laser transceivers into the product. Users are alerted that RAD cannot be held responsible for any damage that may result if non-compliant transceivers are used. In particular, users are warned to use only agency approved products that comply with the local laser safety regulations for Class 1 laser products.

Always observe standard safety precautions during installation, operation and maintenance of this product. Only qualified and authorized service personnel should carry out adjustment, maintenance or repairs to this product. No installation, adjustment, maintenance or repairs should be performed by either the operator or the user.

Handling Energized Products

General Safety Practices

Do not touch or tamper with the power supply when the power cord is connected. Line voltages may be present inside certain products even when the power switch (if installed) is in the OFF position or a fuse is blown. For DC-powered products, although the voltages levels are usually not hazardous, energy hazards may still exist.

Before working on equipment connected to power lines or telecommunication lines, remove jewelry or any other metallic object that may come into contact with energized parts.

Unless otherwise specified, all products are intended to be grounded during normal use. Grounding is provided by connecting the mains plug to a wall socket with a protective ground terminal. If a ground lug is provided on the product, it should be connected to the protective ground at all times, by a wire with a diameter of 18 AWG or wider. Rack-mounted equipment should be mounted only in grounded racks and cabinets.

Always make the ground connection first and disconnect it last. Do not connect telecommunication cables to ungrounded equipment. Make sure that all other cables are disconnected before disconnecting the ground.

Connecting AC Mains

Make sure that the electrical installation complies with local codes.

Always connect the AC plug to a wall socket with a protective ground.

The maximum permissible current capability of the branch distribution circuit that supplies power to the product is 16A. The circuit breaker in the building installation should have high breaking capacity and must operate at short-circuit current exceeding 35A.

Always connect the power cord first to the equipment and then to the wall socket. If a power switch is provided in the equipment, set it to the OFF position. If the power cord cannot be readily disconnected in case of emergency, make sure that a readily accessible circuit breaker or emergency switch is installed in the building installation.

In cases when the power distribution system is IT type, the switch must disconnect both poles simultaneously.

Connecting DC Power

Unless otherwise specified in the manual, the DC input to the equipment is floating in reference to the ground. Any single pole can be externally grounded.

Due to the high current capability of DC power systems, care should be taken when connecting the DC supply to avoid short-circuits and fire hazards.

DC units should be installed in a restricted access area, i.e. an area where access is authorized only to qualified service and maintenance personnel.

Make sure that the DC power supply is electrically isolated from any AC source and that the installation complies with the local codes.

The maximum permissible current capability of the branch distribution circuit that supplies power to the product is 16A. The circuit breaker in the building installation should have high breaking capacity and must operate at short-circuit current exceeding 35A.

Before connecting the DC supply wires, ensure that power is removed from the DC circuit. Locate the circuit br eaker of the panel board that serv ices the eq uipment and switch it to the OFF position. W hen co nnecting the DC supply wires , first co nnect the ground wire to the corresponding terminal, th en the positive pole and last the negative pole. Switch the ci rcuit breaker back to the ON position.

A readily accessible disconnect device that is suitably rated and approved should be incorporated in the building installation.

If the DC power supply is floating, the switch must disconnect both poles simultaneously.

Connecting Data and Telecommunications Cables

Data and telecommunication interfaces are classified according to their safety status.

The following table lists the status of several standard interfaces. If the stat us of a given port differs from the standard one, a notice will be given in the manual.

Ports Safety	Status	
V.11, V.28, V.35, V.36, RS-530, X.21, 10 BaseT, 100 BaseT, Unbalanced E1, E2, E3, STM, DS-2, DS-3, S-Interface ISDN, Analog voice E&M	SELV	Safety Extra Low Voltage: Ports which do not present a safety hazard. Usually up to 30 VAC or 60 VDC.
xDSL (without feeding voltage), Balanced E1, T1, Sub E1/T1	TNV-1	Telecommunication Network Voltage-1: Ports whose normal operating voltage is within the limits of SELV, on which overvoltages from telecommunications networks are possible.
FXS (Foreign Exchange Subscriber)	TNV-2	Telecommunication Network Voltage-2: Ports whose normal operating voltage exceeds the limits of SELV (usually up to 120 VDC or telephone ringing voltages), on which overvoltages from telecommunication networks are not possible. These ports are not permitted to be directly connected to external telephone and data lines.
FXO (Foreign Exchange Office), xDSL (with feeding voltage), U-Interface ISDN	TNV-3	Telecommunication Network Voltage-3: Ports whose normal operating voltage exceeds the limits of SELV (usually up to 120 VDC or telephone ringing voltages), on which overvoltages from telecommunication networks are possible.

Always connect a given port to a port of the same safety status. If in doubt, seek the assistance of a qualified safety engineer.

Always make sure that the equipment is grounded before connecting telecommunication cables. Do not disconnect the ground connection before disconnecting all telecommunications cables.

Some SELV and non-SELV circuits use the same connectors. Use caution when connecting cables. Extra caution should be exercised during thunderstorms.

When using shielded or c oaxial cables, verify th at there is a go od ground connection at both ends. The grounding and bonding of the ground connections should comply with the local codes.

The telecommunication wiring in the building may be damaged or present a fire hazard in case of contact between exposed external wires and the AC power line s. In order to reduce the risk, there are restrictions on the diameter of wires in the telecom cables, between the equipment and the mating connectors.

Caution To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cords.

Attention Pour réduire les risques s'incendie, utiliser seulement des conducteurs de télécommunications 26 AWG ou de section supérieure.

Some ports are suitable for connection to intra-building or non-exposed wiring or cabling only. In such cases, a notice will be given in the installation instructions.

Do not attempt to tamper with any carrier-provided equipment or connection hardware.

Electromagnetic Compatibility (EMC)

The equipment is designed and approved to comply with the electromagnetic regulations of major regulatory bodies. The following instructions may enhance the performance of the equipment and will provide better protection against excessive emission and better immunity against disturbances.

A good ground connection is essential. When installing the equipment in a rack, make sure to remove all traces of paint from the mounting points. Use suitable lock-washers and torque. If an external grounding lug is provided, connect it to the ground bus using braided wire as short as possible.

The equipment is designed to comply with EMC requirements when connecting it with unshielded twisted pair (UTP) cables. However, the use of shielded wires is always recommended, especially for high-rate data. In some cases, when unshielded wires are used, ferrite cores should be installed on certain cables. In such cases, special instructions are provided in the manual.

Disconnect all wires which are not in permanent use, such as cables used for one-time configuration.

The compliance of the equipment with the regulations for conducted emission on the data lines is dependent on the cable quality. The emission is tested for UTP with 80 dB longitudinal conversion loss (LCL).

Unless otherwise specified or described in the manual, TNV-1 and TNV-3 ports provide secondary protection against surges on the data lines. Primary protectors should be provided in the building installation.

The equipment is designed to provide adequate protection against electro-static discharge (ESD). However, it is good working practice to use caution when connecting cables terminated with plastic connectors (without a grounded metal hood, such as flat cables) to sensitive data lines. Before connecting such cables, discharge yourself by touching ground or wear an ESD preventive wrist strap.

FCC-15 User Information

This equipment has been tested and found to comply with the limits of the Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the Installation and Operation manual, may cause harmful interference to the radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Canadian Emission Requirements

This Class A digital apparatus meets all the requirements of the Canadian Interference-Causing Equipment Regulation.

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

Warning per EN 55022 (CISPR-22)

Warning This is a class A product. In a domestic environment, this product may cause radio interference, in which case the user will be required to take adequate measures.

Avertissement Cet appareil est un appareil de Classe A. Dans un environnement résidentiel, cet appareil peut provoquer des brouillages radioélectriques. Dans ces cas, il peut être demandé à l'utilisateur de prendre les mesures appropriées.

Achtung Das vorliegende Gerät fällt unter die Funkstörgrenzwertklasse A. In Wohngebieten können beim Betrieb dieses Gerätes Rundfunkströrungen auftreten, für deren Behebung der Benutzer verantwortlich ist.

Mise au rebut du produit

Afin de faciliter la réutilisation, le recyclage ainsi que d'autres formes de récupération d'équipement mis au rebut dans le cadre de la protection de l'environnement, il est demandé au propriétaire de ce produit RAD de ne pas mettre ce dernier au rebut en tant que déchet municipal non trié, une fois que le produit est arrivé en fin de cycle de vie. Le client devrait proposer des solutions de réutilisation, de recyclage ou toute autre forme de mise au rebut de cette unité dans un esprit de protection de l'environnement, lorsqu'il aura fini de l'utiliser.

Instructions générales de sécurité

Les instructions suivantes servent de guide général d'installation et d'opération sécurisées des produits de télécommunications. Des instructions supplémentaires sont éventuellement indiquées dans le manuel.

Symboles de sécurité

Avertissement

Ce symbole peut apparaitre sur l'équipement ou dans le texte. Il indique des risques potentiels de sécurité pour l'opérateur ou le personnel de service, quant à l'opération du produit ou à sa maintenance.

Danger de choc électrique ! Evitez tout contact avec la surface marquée tant que le produit est sous tension ou connecté à des lignes externes de télécommunications.

Mise à la terre de protection : la cosse ou la borne marquée devrait être connectée à la prise de terre de protection du bâtiment.

Avertissement

Certains produits peuvent être équipés d'une diode laser. Dans de tels cas, une étiquette indiquant la classe laser ainsi que d'autres avertissements, le cas échéant, sera jointe près du transmetteur optique. Le symbole d'avertissement laser peut aussi être joint.

Veuillez observer les précautions suivantes :

- Avant la mise en marche de l'équipement, assurez-vous que le câble de fibre optique est intact et qu'il est connecté au transmetteur.
- Ne tentez pas d'ajuster le courant de la commande laser.
- N'utilisez pas des câbles ou connecteurs de fibre optique cassés ou sans terminaison et n'observez pas directement un rayon laser.
- L'usage de périphériques optiques avec l'équipement augmentera le risque pour les yeux.
- L'usage de contrôles, ajustages ou procédures autres que celles spécifiées ici pourrait résulter en une dangereuse exposition aux radiations.

ATTENTION : Le rayon laser peut être invisible !

Les utilisateurs pourront, dans certains cas, insérer leurs propres émetteurs-récepteurs Laser SFP dans le produit. Les utilisateurs sont avertis que RAD ne pourra pas être tenue responsable de tout dommage pouvant résulter de l'utilisation d'émetteurs-récepteurs non conformes. Plus particulièrement, les utilisateurs sont avertis de n'utiliser que des produits approuvés par l'agence et conformes à la réglementation locale de sécurité laser pour les produits laser de classe 1.

Respectez toujours les précautions standards de sécurité durant l'installation, l'opération et la maintenance de ce produit. Seul le personnel de service qualifié et autorisé devrait effectuer l'ajustage, la maintenance ou les réparations de ce produit. Aucune opération d'installation, d'ajustage, de maintenance ou de réparation ne devrait être effectuée par l'opérateur ou l'utilisateur.

Manipuler des produits sous tension

Règles générales de sécurité

Ne pas toucher ou altérer l'alimentation en courant lorsque le câble d'alimentation est branché. Des tensions de lignes peuvent être présentes dans certains produits, même lorsque le commutateur (s'il est installé) est en position OFF ou si le fusible est rompu. Pour les produits alimentés par CC, les niveaux de tension ne sont généralement pas dangereux mais des risques de courant peuvent toujours exister.

Avant de travailler sur un équipement connecté aux lignes de tension ou de télécommunications, retirez vos bijoux ou tout autre objet métallique pouvant venir en contact avec les pièces sous tension.

Sauf s'il en est autrement indiqué, tous les produits sont destinés à être mis à la terre durant l'usage normal. La mise à la terre est fournie par la connexion de la fiche principale à une prise murale équipée d'une borne protectrice de mise à la terre. Si une cosse de mise à la terre est fournie avec le produit, elle devrait être connectée à tout moment à une mise à la terre de protection par un conducteur de diamètre 18 AWG ou plus. L'équipement monté en châssis ne devrait être monté que sur des châssis et dans des armoires mises à la terre.

Branchez toujours la mise à la terre en premier et débranchez-la en dernier. Ne branchez pas des câbles de télécommunications à un équipement qui n'est pas mis à la terre. Assurez-vous que tous les autres câbles sont débranchés avant de déconnecter la mise à la terre.

Connexion au courant du secteur

Assurez-vous que l'installation électrique est conforme à la réglementation locale.

Branchez toujours la fiche de secteur à une prise murale équipée d'une borne protectrice de mise à la terre.

La capacité maximale permissible en courant du circuit de distribution de la connexion alimentant le produit est de 16A. Le coupe-circuit dans l'installation du bâtiment devrait avoir une capacité élevée de rupture et devrait fonctionner sur courant de court-circuit dépassant 35A.

Branchez toujours le câble d'alimentation en premier à l'équipement puis à la prise murale. Si un commutateur est fourni avec l'équipement, fixez-le en position OFF. Si le câble d'alimentation ne peut pas être facilement débranché en cas d'urgence, assurez-vous qu'un coupe-circuit ou un disjoncteur d'urgence facilement accessible est installé dans l'installation du bâtiment.

Le disjoncteur devrait déconnecter simultanément les deux pôles si le système de distribution de courant est de type IT.

Connexion d'alimentation CC

Sauf s'il en est autrement spécifié dans le manuel, l'entrée CC de l'équipement est flottante par rapport à la mise à la terre. Tout pôle doit être mis à la terre en externe.

A cause de la capacité de courant des systèmes à alimentation CC, des précautions devraient être prises lors de la connexion de l'alimentation CC pour éviter des courts-circuits et des risques d'incendie.

Les unités CC devraient être installées dans une zone à accès restreint, une zone où l'accès n'est autorisé qu'au personnel qualifié de service et de maintenance.

Assurez-vous que l'alimentation CC est isolée de toute source de courant CA (secteur) et que l'installation est conforme à la réglementation locale.

La capacité maximale permissible en courant du circuit de distribution de la connexion alimentant le produit est de 16A. Le coupe-circuit dans l'installation du bâtiment devrait avoir une capacité élevée de rupture et devrait fonctionner sur courant de court-circuit dépassant 35A.

Avant la connexion des câbles d'alimentation en courant CC, assurez-vous que le circuit CC n'est pas sous tension. Localisez le coupe-circuit dans le tableau desservant l'équipement et fixez-le en position OFF. Lors de la connexion de câbles d'alimentation CC, connectez d'abord le conducteur de mise à la terre à la borne correspondante, puis le pôle positif et en dernier, le pôle négatif. Remettez le coupe-circuit en position ON.

Un disjoncteur facilement accessible, adapté et approuvé devrait être intégré à l'installation du bâtiment.

Le disjoncteur devrait déconnecter simultanément les deux pôles si l'alimentation en courant CC est flottante.

Declaration of Conformity

Manufacturer's Name:	RAD Data Communications Ltd.
Manufacturer's Address:	24 Raoul Wallenberg St. Tel Aviv 69719 Israel

Declares that the product:

Product Name:	ACE-3600

Conforms to the following standard(s) or other normative document(s):

EMC: EN	55022:1998+ A1:2000, A2:2003	Information technology equipment – Radio disturbance characteristics – Limits and methods of measurement.
	EN 50024:1998+ A1:2001, A2:2003	Information technology equipment – Immunity characteristics – Limits and methods of measurement.
Safety:	EN 60950-1:2001	Information technology equipment – Safety – Part 1: General requirements.

Supplementary Information:

The product herewith com plies with the requirements of the EMC Directive 89/336/EEC, the Low Voltage Directive 2006/95/EC and the R&TTE Directive 99/5/EC for wired equipment. The product was tested in a typical configuration.

Tel Aviv, 17 May 2007

Haim Karshen

VP Quality

European Contact: RAD Data Communications GmbH, Otto-Hahn-Str. 28-30, 85521
Ottobrunn-Riemerling, Germany

Glossary

Address	A coded representation of the origin or destination of data.
Agent	In SNMP, this refers to the managed system.
ANSI	American National Standards Institute.
Backhaul	Transporting traffic between distributed sites (typically access points) and more centralized points of presence. See Cellular Backhaul.
Balanced	A transmission line in which voltages on the two conductors are equal in magnitude, but opposite in polarity, with respect to ground.
Bandwidth	The range of frequencies passing through a given circuit. The greater the bandwidth, the more information can be sent through the circuit in a given amount of time.
Baud	Unit of signaling speed equivalent to the number of discrete conditions or events per second. If each signal event represents only one bit condition, baud rate equals bps (bits per second).
Bit	The smallest unit of information in a binary system. Represents either a one or zero ("1" or "0").
Bridge	A device interconnecting local area networks at the OSI data link layer, filtering and forwarding frames according to media access control (MAC) addresses.
Buffer	A storage device. Commonly used to compensate for differences in data rates or event timing when transmitting from one device to another. Also used to remove jitter.
Byte	A group of bits (normally 8 bits in length).
Carrier	A continuous signal at a fixed frequency that is capable of being modulated with a second (information carrying) signal.
Cell	The 53-byte basic information unit within an ATM network. The user traffic is segmented into cells at the source and reassembled at the destination. An ATM cell consists of a 5-byte ATM header and a 48-byte ATM payload, which contains the user data.
Channel	A path for electrical transmission between two or more points. Also called a link, line, circuit or facility.
Circuit Emulation	In ATM, a connection over a virtual circuit-based network providing service to the end users that is indistinguishable from a real point-to point, fixed-bandwidth circuit.

Circuit Emulation Service	New technology for offering circuit emulation services over packet-switched networks. The service offers traditional TDM trunking (at n x 64 kbps, fractional E1/T1, E1/T1 or E3/T3) over a range of transport protocols, including Internet Protocol (IP), MPLS and Ethernet.
Clock	A term for the source(s) of timing signals used in synchronous transmission.
Concentrator	Device that serves as a wiring hub in a star-topology network. Sometimes refers to a device containing multiple modules of network equipment.
Congestion	A state in which the network is overloaded and starts to discard user data (frames, cells or packets).
Congestion Control	A resource and traffic management mechanism to avoid and/or prevent excessive situations (buffer overflow, insufficient bandwidth) that can cause the network to collapse. In ATM networks, congestion control schemes may be based on fields within the ATM cell header (CLP, EFCI within the PTI) or may be based on a more sophisticated mechanism between the ATM end-system and ATM switches. The ATM Forum has developed a mechanism based on rate control for ABR-type traffic. In Frame Relay networks, congestion is handled by the FECN, BECN and DE bits.
CORBA	The acronym for Common Object Request Broker Architecture, OMG's open, vendor-independent architecture and infrastructure that computer applications use to work together over networks. One of its most important uses is in servers that must handle large number of clients, at high hit rates, with high reliability, such as network management systems.
Data	Information represented in digital form, including voice, text, facsimile and video.
dBm	A measure of power in communications: the decibel in reference to one milliwatt (0 dBm = 1 milliwatt and -30 dBm = .001 milliwatt).
Diagnostics	The detection and isolation of a malfunction or mistake in a communications device, network or system.
Differential Delay	Differential delay is caused when traffic is split over different lines that may traverse shorter and longer paths. Products like the RAD IMX-2T1/E1 inverse multiplexer compensate for any differential delay (up to 64 msec) between the T1 lines, to properly reconstruct the original stream.
Encapsulation	Encapsulating data is a technique used by layered protocols in which a low level protocol accepts a message from a higher level protocol, then places it in the data portion of the lower-level frame. The logistics of encapsulation require that packets traveling over a physical network contain a sequence of headers.

Ethernet	A local area network (LAN) technology which has extended into the wide area networks. Ethernet operates at many speeds, including data rates of 10 Mbps (Ethernet), 100 Mbps (Fast Ethernet), 1,000 Mbps (Gigabit Ethernet), 10 Gbps, 40 Gbps, and 100 Gbps.
Flow Control	A congestion control mechanism that results in an ATM system implementing flow control.
Frame	A logical grouping of information sent as a link-layer unit over a transmission medium. The terms packet, datagram, segment, and message are also used to describe logical information groupings.
Framing	At the physical and data link layers of the OSI model, bits are fit into units called frames. Frames contain source and destination information, flags to designate the start and end of the frame, plus information about the integrity of the frame. All other information, such as network protocols and the actual payload of data, is encapsulated in a packet, which is encapsulated in the frame.
Full Duplex	A circuit or device permitting transmission in two directions (sending and receiving) at the same time.
Gateway	Gateways are points of entrance and exit from a communications network. Viewed as a physical entity, a gateway is that node that translates between two otherwise incompatible networks or network segments. Gateways perform code and protocol conversion to facilitate traffic between data highways of differing architecture.
GUI (Graphical User Interface)	Pronounced "gooey," this software interface is based on pictorial representations and menus of operations and files. Opposite of command line interface.
Half Duplex	A circuit or device capable of transmitting in two directions, but not at the same time.
Impedance	The combined effect of resistance, inductance and capacitance on a transmitted signal. Impedance varies at different frequencies.
Interface	A shared boundary, defined by common physical interconnection characteristics, signal characteristics, and meanings of exchanged signals.
IP Address	Also known as an Internet address. A unique string of numbers that identifies a computer or device on a TCP/IP network. The format of an IP address is a 32-bit numeric address written as four numbers from 0 to 255, separated by periods (for example, 1.0.255.123).
J1	Digital interconnection protocol similar to T1 and E1 used in Japan.
Jitter	The deviation of a transmission signal in time or phase. It can introduce errors and loss of synchronization in high speed synchronous communications.

Laser	A device that transmits an extremely narrow and coherent beam of electromagnetic energy in the visible light spectrum. Used as a light source for fiber optic transmission (generally more expensive, shorter lived, single mode only, for greater distances than LED).
Loading	The addition of inductance to a line in order to minimize amplitude distortion. Used commonly on public telephone lines to improve voice quality, it can make the lines impassable to high speed data, and baseband modems.
Loopback	A type of diagnostic test in which the transmitted signal is returned to the sending device after passing through all or part of a communications link or network.
Manager	An application that receives Simple Network Management Protocol (SNMP) information from an agent. An agent and manager share a database of information, called the Management Information Base (MIB). An agent can use a message called a traps-PDU to send unsolicited information to the manager. A manager that uses the RADview MIB can query the RAD device, set parameters, sound alarms when certain conditions appear, and perform other administrative tasks.
Master Clock	The source of timing signals (or the signals themselves) that all network stations use for synchronization.
Modular	Modular interfaces enable field-changeable conversion.
MPLS (Multiprotocol Label Switching)	A standards-approved technology that allows core network routers to operate at higher speeds without needing to examine each packet in detail, and allows more complex services to be developed, enabling discrimination on a QoS basis. MPLS speeds up network traffic flow by bringing Layer 2 information to Layer 3 (IP) and facilitating network management. It forwards traffic using a label that instructs the routers and the switches in the network where to forward the packets based on pre-established IP routing information. MPLS is called multiprotocol because it works with TDM, Ethernet, IP, ATM, and Frame Relay network protocols.
Network	(1) An interconnected group of nodes. (2) A series of points, nodes, or stations connected by communications channels; the collection of equipment through which connections are made between data stations.
NMS (Network Management System)	The system that controls the network configuration, fault and performance management, and diagnostic analysis.
Node	A point of interconnection to a network.
Packet	An ordered group of data and control signals transmitted through a network, as a subset of a larger message.
Payload	The 48-byte segment of the ATM cell containing user data. Any adaptation of user data via the AAL will take place within the payload.

Physical Layer	Layer 1 of the OSI model. The layer concerned with electrical, mechanical, and handshaking procedures over the interface connecting a device to the transmission medium.
Policing	A method for verifying that the incoming VC complies with the user's service contract.
Port	The physical interface to a computer or multiplexer, for connection of terminals and modems.
Protocol	A formal set of conventions governing the formatting and relative timing of message exchange between two communicating systems.
Pseudowire	Point-to-point connections set up to emulate (typically Layer 2) native services like ATM, Frame Relay, Ethernet, TDM, or SONET/SDH over an underlying common packet-switched network (Ethernet, MPLS or IP) core. Pseudowires are defined by the IETF PWE3 (pseudowire emulation edge-to-edge) working group.
Router	An interconnection device that connects individual LANs. Unlike bridges, which logically connect at OSI Layer 2, routers provide logical paths at OSI Layer 3. Like bridges, remote sites can be connected using routers over dedicated or switched lines to create WANs.
Routing	The process of selecting the most efficient circuit path for a message.
Single Mode	Describing an optical wave-guide or fiber that is designed to propagate light of only a single wavelength (typically 5-10 microns in diameter).
SNMP (Simple Network Management Protocol)	The Internet standard protocol for managing nodes on an IP network.
Space	In telecommunications, the absence of a signal. Equivalent to a binary 0.
Sync	See Synchronous Transmission.
T1	A digital transmission link with a capacity of 1.544 Mbps used in North America. Typically channelized into 24 DS0s, each capable of carrying a single voice conversation or data stream. Uses two pairs of twisted pair wires.
Telnet	The virtual terminal protocol in the Internet suite of protocols. It lets users on one host access another host and work as terminal users of that remote host. Instead of dialing into the computer, the user connects to it over the Internet using Telnet. When issuing a Telnet session, it connects to the Telnet host and logs in. The connection enables the user to work with the remote machine as though a terminal was connected to it.

Timeslot	A portion of a serial multiplex of timeslot information dedicated to a single channel. In E1 and T1, one timeslot typically represents one 64 kbps channel.
Traffic Policing	Mechanism whereby any traffic which violates the traffic contract agreed to at connection setup, is detected and discarded.
Traffic Shaping	A method for smoothing the bursty traffic rate that might arrive on an access virtual circuit so as to present a more uniform traffic rate on the network.

Quick Start Guide

Only an experienced technician should carry out the installation of ACE-3600. If you are familiar with ACE-3600, use this quick start guide to prepare the unit for operation.

1. Installing ACE-3600

The physical installation of ACE-3600 includes the following steps:

1. Mount and secure the unit in a 19" rack using the complemented RM-36 kit. The rack mounting kit installation instructions are provided separately.
2. Determine the required configuration of ACE-3600, according to your application (for typical application configurations, refer to *Chapter 5*).
3. Connect the network/user interfaces as required for the application (see procedure: *Connecting the Interface Cables*).
4. Connect the external clock source (if applicable) to the unit's station clock port (see procedure: *Connecting the Clock Source*).
5. Connect the ASCII terminal to the RS-232 control port, or connect the network management station/hub to the Ethernet control port (see procedure: *Connecting the Control Cable*).
6. Make sure that the unit is properly grounded and then connect power to the unit.

Note *Detailed installation instructions are available in Chapter 2.*

Connecting the Interface Cables

➤ To connect the interface cables to ACE-3600:

1. Carefully remove the dust covers from the STM-1/OC-3c ports of the SDH/SONET modules. Then, insert the appropriate SFP transceivers into the STM-1/OC-3c ports.

Note *Lock the wire latch of each SFP transceiver by lifting it up until it clicks into place. For more information, refer to Chapter 2.*

2. To each plugged-in SFP transceiver, connect a fiber optic cable: one for RX (incoming) and one for TX (outgoing) data.
3. Insert an appropriate SFP transceiver into the GbE port of the interface module (one GbE port per interface module), and then connect the fiber optic cables. Remember to lock the transceiver's wire latch by lifting it up until it clicks into place.

Connecting the Clock Source

➤ To connect ACE-3600 to a dedicated clock source:

- Connect an E1/T1/J1-compliant cable to the specific clock source unit/device on the remote end, and then to the RJ-45 connector designated STATION CLK on the ACE-3600 unit end.

Connecting the Control Cable

➤ To connect the Ethernet control interface:

1. Connect one end of an Ethernet cable (not supplied) to the control device or the network management station hub.
2. Connect the other end of the Ethernet cable to the RJ-45 connector designated ETH in ACE-3600.

➤ To connect the terminal control cable:

1. Connect the DB-9 end of the RS-232 adapter cable (supplied) to the 9-pin DCE connector of the management station.
2. Connect the RJ-45 end of the adapter cable to the RJ-45 connector designated CONTROL in ACE-3600.

Connecting the Power

➤ To connect ACE-3600 to AC power:

1. Connect the power cable to the AC power connector on the ACE-3600 front panel.
2. Connect the power cable to the mains outlet.

   The unit is turned on automatically upon connection to the mains.

Note *To connect ACE-3600 to DC power, refer to the DC power supply connection supplement.*

2. Starting and Configuring ACE-3600

Configure ACE-3600 using an ASCII-based terminal or a network management station.

Starting a Terminal Session for the First Time

➤ To start the terminal session:

1. Connect an ASCII terminal to the ACE-3600 control port.
2. Configure the ASCII terminal connection to 19200 bps, N, 8, 1, and then set the terminal emulator to VT100 emulation for optimal viewing of system menus.
3. Power up the ACE-3600 unit. Verify that the PS1 and PS2 LEDs in the front panel are lit.
4. If you are using HyperTerminal, set the terminal mode to 132-column mode for optimal view of system menus (Properties › Settings › Terminal Setup › 132 column mode).
5. Check the state of the power supply LEDs as follows:
   - Green – power supply is OK
   - Red – power supply failure.
6. Check the main module's RDY green LED:
   - On: Self-test has been completed successfully.
   - Blinking: Self-test has failed (display the self-test results to check the failure source).

Logging In

According to your user privileges, you may log in as super user, technician or user. You must have "super user" privileges to be able to configure ACE-3600.

➤ To log in as a super user:

1. When connected to the terminal, press ESC to display the login screen.
2. Enter your user name ("su" for full configuration and monitoring access) and "1234" default password when prompted, and then press ‹Enter›.

Setting the Date and Time

Set the current date and time in order to log events properly.

➤ To set the date and time:

- On the Date and Time menu (Configuration › System › Date and Time), enter the current date and time or configure the SNTP parameters.

Configuring the Physical Ports

Configure the physical layer parameters for:

- ATM-155 ports
- Gigabit Ethernet ports.

➤ **To configure the ATM-155 ports:**

- On the ATM-155 menu (**Configuration > Physical layer > Port > ATM-155**), set the required physical layer parameters.

➤ **To configure the Gigabit Ethernet ports:**

- On the Ethernet menu (**Configuration > Physical layer > Port > Ethernet**), set the required physical layer parameters.

Configuring the Protection Parameters

If required, set the system, Ethernet and/or SDH/SONET protection/redundancy parameters.

➤ **To configure the protection parameters:**

- On the Protection menu (**Configuration > System > Protection**), select the protection type and then set the parameters in the relevant submenu.

Configuring the Application Parameters

The application layer configuration includes:

- Router parameters (essential for cross-network management)
- ATM parameters
- MPLS parameters (for LDP functionality, if required)
- Multiservice over PSN parameters (if traffic is to be carried over a packet-switched network).

➤ **To configure the router functionality:**

- On the router Interface menu (**Configuration > Applications > Router > Interface**), enter the required routing parameters.

➤ **To configure the ATM functionality:**

- On the ATM menu (**Configuration > Applications > ATM**), select the ATM functionality type and then set the parameters in the relevant submenu.

➤ **To configure the MPLS functionality:**

- On the MPLS menu (**Configuration > Applications > MPLS**), enter the MPLS dynamic range and then set the parameters in the relevant submenu.

➤ **To configure the multiservice over PSN functionality:**

- On the Multiservice over PSN menu (**Configuration > Applications > Multiservice over PSN**), select the PSN functionality type and then set the parameters in the relevant submenu.

Setting the Clock Source

Set the source from which ACE-3600 should derive its timing.

➤ To set the clock source:

- On the Clock menu (Configuration > System > Clock), select the type of source and then set the clock parameters in the relevant submenu.

Defining the Manager IP

➤ To define the manager IP address:

- On the Manager List menu (Configuration > System > Management > Manager List), set the IP and trap mask parameters (per manager).

Contents

Chapter 1. Introduction

Chapter 2. Installation and Setup

Chapter 3. Operation

Chapter 4. Configuration

Chapter 1

Introduction

1.1 Overview

ACE-3600 is an advanced carrier-class gateway, optimized for transporting 3G/3.5G voice and HSDPA data traffic over next-generation core PSNs (packet-switched networks), including Layer-2, MPLS or IP. Its modular physical architecture, hardware redundancy features and aggregation abilities make ACE-3600 a customizable, fail-safe and high-end traffic concentrator for third-generation cellular operators and carriers.

Typically located at the 3G RNC site, the unit interconnects with the RNC and converts up to 4 simultaneous fiber optic STM-1/OC-3c (ATM-155) links to virtual pseudowire (PW) connections that are established over a packet-switched network, using the unit's Gigabit Ethernet interface. Both the Gigabit Ethernet and the four STM-1/OC-3c links can be protected using an additional interface module (optional).

Since traffic timing synchronization plays a critical role in cellular backhaul applications, ACE-3600 can distribute the ATM timing over the packet-switched network.

Additional features of ACE-3600 include (see *Features* for more details):

- Advanced pseudowire connectivity verification using VCCV-BFD messages
- End-to-end fault propagation between legacy and packet-switched networks
- A choice of clock synchronization modes
- Full system redundancy protection
- Full OAM and statistics collection features
- Self-diagnostic tools
- Inband and out-of-band management via various management access types and user interfaces.

Product Options

Chassis Options

The ACE-3600 chassis is 2U high and fully modular.

The chassis has a passive backplane that includes pin connectors with which the main modules and interface modules engage. The chassis supports the following modules:

- Up to two main modules (main cards; A and B)
- Up to two interface modules, each with four STM-1/OC-3c ports and one Gigabit Ethernet port (the second module is used for redundancy protection).

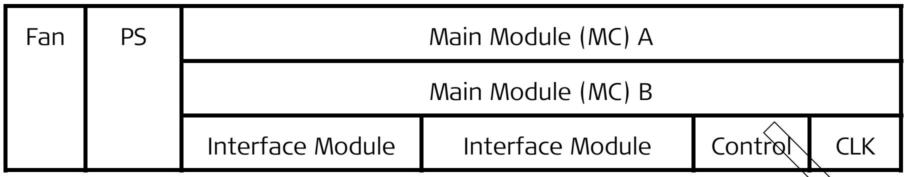


Figure 1-1. ACE-3600 2D Chassis Illustration

Main Module (Main Card) Options

The main modules (A and B) provide the overall functionality of the ACE-3600 unit and support the operation of the STM-1/OC-3c and Gigabit Ethernet interfaces. The main modules can be replaced (field-replaceable) when necessary.

Two identical main modules are typically ordered for enabling the full redundancy protection feature, as explained in *Main Modules Protection* on page *1-10*.

In the current version of ACE-3600, one main module type is available:

MC-155-4/GBE Supports the ATM-155 and GbE interfaces, for delivering ATM traffic over packet-switched networks and STM-1/OC-3c links.

Interface Module Options

ACE-3600 can be ordered with 1 or 2 interface modules, while each module includes:

STM-1/OC-3c UNI × 4 Four fiber optic ports for ATM-155 UNI traffic, each using SFP transceivers. The ATM-155 (155 Mbps) interface performs physical layer and ATM mapping into STM-1/OC-3c according to ITU I.432.

Gigabit Ethernet × 1 One Gigabit Ethernet port for pseudowire/Ethernet-based traffic over a PSN, using fiber optic or electrical interface via an SFP transceiver.

For more detailed information about the interface module options, refer to *Table 1-1* and on page *1-25*. For three-dimensional illustration of these modules, refer to *Chapter 2*.

Note *The ACE-3400 and ACE-3402 modules are not compatible with ACE-3600.*

Power Options

ACE-3600 can be either AC-powered or DC-powered, and has one or two hot-swappable power supplies (as ordered).

License Packs

The available software license packs are:

LDP Enables the label distribution protocol (LDP) functionality

Applications

ATM over PSN Application

In a typical ATM over PSN application (see *Figure 1-2*), 3G cellular traffic (ATM) is transmitted over the PSN by the remote peers (ACE-3100 and ACE-3200) using pseudowires that comprise uniquely formatted Ethernet packets. ACE-3600 receives the Ethernet packets via its Gigabit Ethernet interface and converts it back to ATM-155 traffic, carried by up to four STM-1/OC-3c links towards the RNC. In such application, ACE-3600 can serve as the clock distributor for the remote peers.

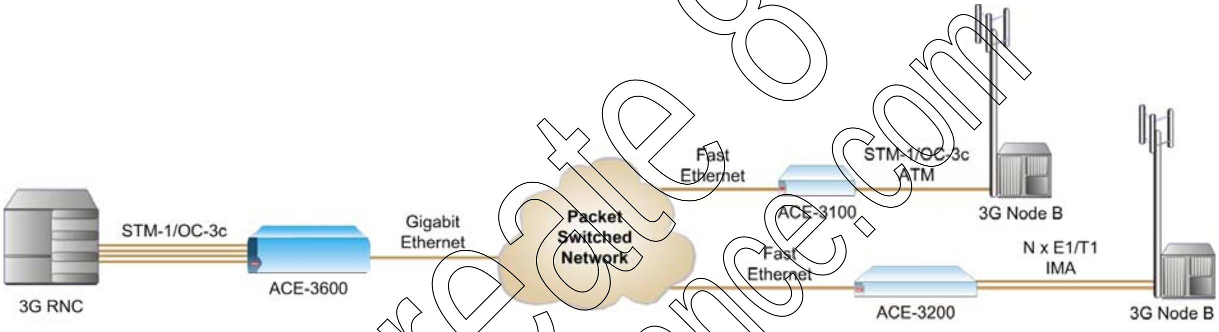


Figure 1-2. 3G Backhaul over a Packet-Switched Network

HSDPA in a Hybrid Backhaul Solution

The following figure demonstrates how voice (R99) and data (HSDPA) traffic can be separated in a hybrid backhaul solution. ACE-3600 is configured to send the data traffic over the packet-switched network, and the voice traffic over an ATM or SDH network.

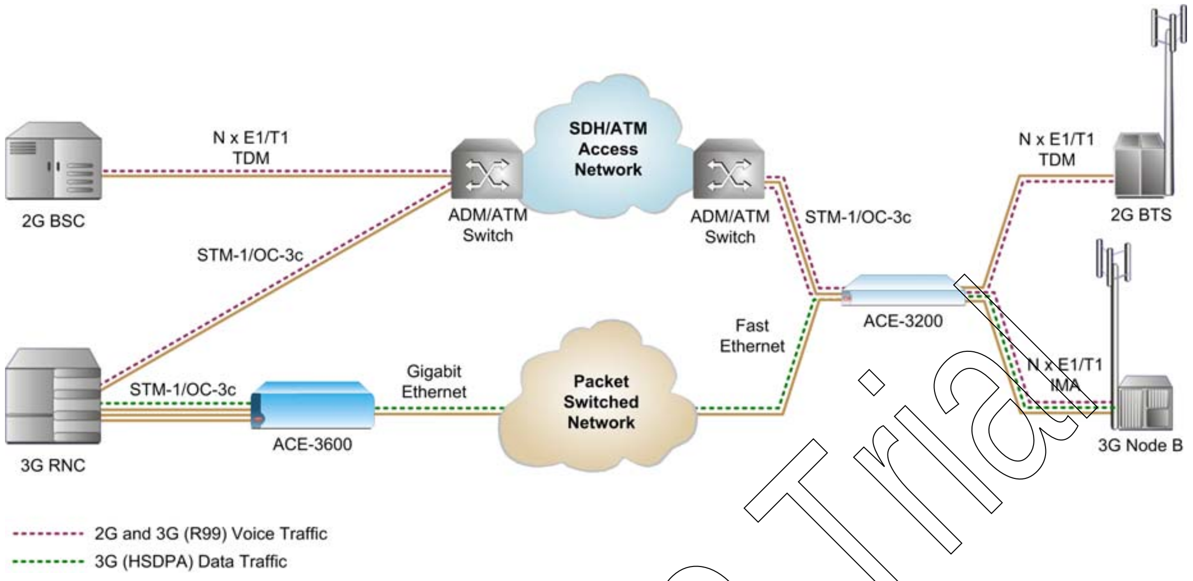


Figure 1-3. Hybrid Backhaul Solution

Features

ATM over PSN Capabilities

ACE-3600 creates and utilizes up to 1024 data pseudowire (PW) connections to emulate ATM services over packet-switched networks.

Two encapsulation methods are supported according to IETF's 'draft-ietf-pwe3-atm-encap':

- 1:1 (one-to-one) VC/VP encapsulation – Each VCC/VPC is mapped to a single pseudowire (PW) connection
- N:1 (N-to-one) VC/VP encapsulation – Several VCs or VPs are encapsulated to a single PW connection.

ACE-3600 allows single or multiple cells to be encapsulated per frame.

For more information about the ATM over PSN functionality, see *ATM over PSN Functionality* on page *1-11*. For detailed description of the ATM over PSN encapsulation modes, refer to *Appendix E*.

LDP, PHP and MPLS over GRE

ACE-3600 uses the MPLS label distribution protocol (LDP) to automatically assign and distribute pseudowires and tunnel labels between MPLS peers (up to 512 peers). When LDP is enabled, labels (tunnels or PWs) are set automatically. It is still possible, however, to manually create tunnels or PWs with static labels.

Note *The LDP functionality requires a software license.*

Additionally, ACE-3600 supports advanced MPLS label handling using Penultimate Hop Popping (PHP), a packet-level modification process in which the label switched router (LSR) removes the last label of MPLS packets before they are passed to an adjacent label edge router (LER).

Lastly, MPLS (multiprotocol label switching) can be used over generic routing encapsulation (GRE) to establish point-to-point tunnel connection over an IP network. This tunneling service is used to transfer MPLS packets over an IP network without using the IP addressing scheme. For a detailed description, refer to *Appendix E*.

ATM Switching and Policing Capabilities

ACE-3600 provides full ATM switching capabilities, including scheduling and shaping of ATM-based traffic.

Operators can assign each virtual connection (VC) or virtual path (VP) to a service class, define the QoS parameters and shape the ATM egress traffic according to CBR, VBR and UBR+. ATM traffic policing allows operators to discard, tag or count non-conformant cells per configuration.

Up to 1024 VP and VC connections can be established with full UNI/NNI VPI and VCI ranges.

Quality of Service (QoS) over PSN

Over packet-switched networks, QoS is provided according to the network type:

- Layer-2 network – outgoing pseudowire packets are assigned a dedicated VLAN ID according to 802.1Q and marked for priority using 802.1p bits
- MPLS network – outgoing pseudowire packets are assigned to a specific MPLS tunnel and marked for priority using EXP bits
- IP network – outgoing pseudowire packets are marked for priority using ToS or DSCP bits.

Clock Synchronization

ACE-3600 provides robust clock synchronization and flexible timing modes, including:

- Interface-based synchronization – the clock is recovered from the RX traffic of a selected interface, in accordance with G.823 and depending on the network's SLA
- Unicast clock distribution – the master clock is distributed with a dedicated stream towards up to 512 remote PSN peers
- Multicast clock distribution – The master clock is distributed towards the PSN using a single IP multicast clock stream (IGMPv2 host).

The clock steam is generated at a rate of 170 PPS (64 bytes each) for every remote site.

For detailed information about the different system timing modes, see *Appendix D.* For information about clock encapsulation over a PSN, see *Appendix E*.

OAM and Diagnostics

ACE-3600 provides comprehensive monitoring and diagnostic capabilities, including:

- Pseudowire connectivity check – ACE-3600 periodically verifies the connectivity status of pseudowire connections, using VCCV-BFD messages according to the 'draft-ietf-bfd-base' requirements. If a failure is detected, a notification is sent to both the remote peer and the ATM connection of the specific PW. This allows complete monitoring over the pseudowire connections in real-time. For more information, refer to *Appendix F*.
- External and internal physical loopbacks on STM-1/OC-3c ports
- Cell test towards the ATM ports.

In addition, ATM and PSN port alarms are propagated over the packet-switched network from end to end, towards both the BTS/Node B side and the BSC/RNC side. This includes the mapping of:

- Packet-switched network alarms to ATM alarms
- ATM alarms over the PSN to the remote customer equipment (CE)
- Physical failures of ATM ports, over the packet-switched network towards both the local and remote CE.

For conventional ATM cross-connects (XCs), OAM is supported according to ITU I.610 requirements:

- F4 and F5 OAM
- Configurable OAM mode per connection point
- Segment/intermediate mode for user connections and end-to-end mode for the management connection
- AIS and RDI cell detection and generation upon physical layer and ATM layer failures
- CC cell generation and LOC state detection per VP/VC
- Loopback location ID and configurable loopback source ID per device. For detailed information about the ATM OAM functionality, refer to *Appendix C*.

Performance Monitoring

Performance monitoring is provided by Ethernet and IP-layer network condition statistics, such as packet sequence errors (loss or misorder) and packet delay variation (jitter), which are monitored and stored by the device.

ACE-3600 collects statistics per physical port and per connection for 15-minute intervals. Statistics for the last 6 hours are stored in the device and can be retrieved at the network management station.

ACE-3600 maintains a cyclic event log file that stores up to 4096 time-stamped events. In addition, an internal system log agent can send all reported events to a centralized repository or remote server.

Full System Redundancy

To ensure a fail-safe and continuous operation, ACE-3600 supports:

- 1+1 protection on STM-1/OC-3 ports – ACE-3600 allows two STM-1/OC-3c ports to work in the automatic protection switching (APS) mode, in which the two interfaces send identical data, and either of them can take the place of the other if an error is detected in one of them. For more detailed information about this feature, see *APS on STM-1/OC-3c Ports* on page *1-18*.

- Ethernet redundancy – To allow reliable and uninterrupted service over packet-switched networks, two Gigabit Ethernet interfaces can be set to work in the 1:1 or 1+1 automatic protection switching modes, according to IEEE 802.3ad. For more information, see *Gigabit Ethernet Port Redundancy* on page *1-19*.
- Main module protection – ACE-3600 allows the installation of two main modules, to ensure continuous operation when one module is reset, restarted, or stops operating for any reason. In such a case, the redundant main module immediately takes over the unit, using its own pre-configured settings.
- Dual power supply – ACE-3600 has two hot-swappable power supplies that allow the unit to be connected to two power sources. If one power supply/source fails, the other continues to provide the required power. This ensures non-interruption of the unit's operation in case of a power failure.
- Multiple fans – To ensure continuous and proper cooling of the unit, ACE-3600 supports multiple internal fans. If one of the fans fails, the others can continue their operation. Fan trays are field-replaceable.

Management

ACE-3600 can be managed by up to 16 authenticated users simultaneously, using inband or out-of-band access, via:

- The dedicated RS-232 or 100BaseT port (out-of-band)
- Dedicated ATM VC defined on an STM-1/OC-3c ATM port (inband)
- The Gigabit Ethernet uplink port, using IP-based connection (raw IP or over PW).

Complete control over the unit's functions can be attained via the following supported applications –

- Menu-driven terminal utility for management via a local ASCII-based terminal connection. Telnet access is supported via IP-based connection.
- ConfiguRAD – Web-based element management utility, embedded in ACE-3600 for IP-based, installation-free access to the unit from any computer equipped with a standard Web browser.
- RADview-EMS – RAD's CORBA-based element management system, providing a dedicated PC/Unix-based GUI for controlling and monitoring the unit from a network management station. It also includes northbound CORBA interface for integration into any third-party NMS (network management system). For more information, refer to the RADview-EMS/NGN User's Manual.

For more information about configuration alternatives, see *Chapter 3*.

The unit can be managed by and report to up to 16 different users simultaneously. Accounts of existing and new users can be defined/changed remotely, using a dedicated RADIUS server.

In addition, ACE-3600 allows retrieval of the current date and time from a centralized location, by synchronizing with an SNTP (System Network Timing Protocol) server.

Software upgrades and preset configuration files can be downloaded/uploaded to/from ACE-3600 via TFTP or XMODEM.

Security

ACE-3600 supports the Secure Socket Layer (SSL) protocol for enabling secure Web access to the unit. If enabled, the SSL protocol encrypts the data between the TCP and HTTP Web layers.

Telnet-like management can be secured using a Secure Shell (SSH) client/server program. Instead of sending plain-text ASCII-based commands and login requests over the network, SSH provides a secure communication channel.

User access to the unit is restricted via user name and password (for more information, see *Management* on page *1-21*).

In addition, ACE-3600 supports SNMP version 3, providing secure access to the device by authenticating and encrypting packets transmitted over the network.

1.2 Physical Description

ACE-3600 is a modular unit, 17.3" wide and 2U high. It can be mounted in a 19" rack or used as a desktop unit.

Figure 1-4 shows a 3D front view of ACE-3600.

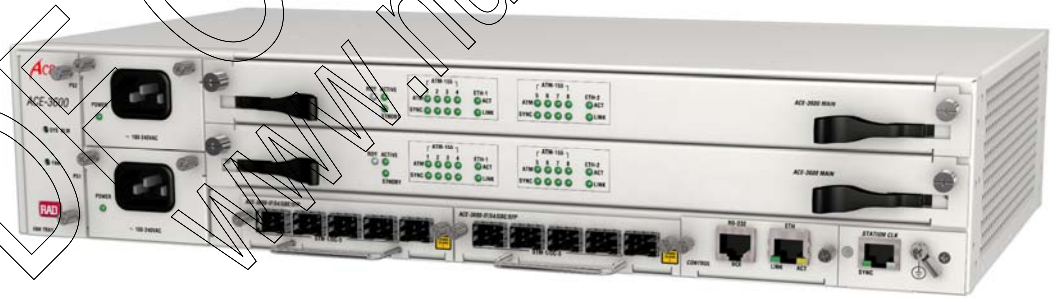


Figure 1-4. ACE-3600 Front View

The unit is fully accessible from the front panel, which includes the interface ports, control connectors, main modules, fan tray, LED indicators and power connectors.

For information about the unit's physical installation and required cable connections, refer to *Chapter 2*. For information about the unit's operation and LED indicators, refer to *Chapter 3*.

1.3 Functional Description

This section shows the ACE-3600 block diagram and provides detailed descriptions of the following functional features:

- *Main Modules Protection* (see page *1-10*)
- *ATM over PSN Functionality* (see page *1-11*)
- *ATM Switching/Aggregation Functionality* (see page *1-13*)
- *MPLS Utilization* (see page *1-16*)
- *Fault Propagation and PSN Connectivity Checks* (see page *1-18*)
- *Ports Protection* (see page *1-18*)
- *Physical Loopback Tests* (see page *1-20*)
- *SNMP and Alarm Traps* (see page *1-21*)
- *Management* (see page *1-21*).

Block Diagram

The following diagram illustrates the internal functional structure of ACE-3600 and its main module (main card) and ports.

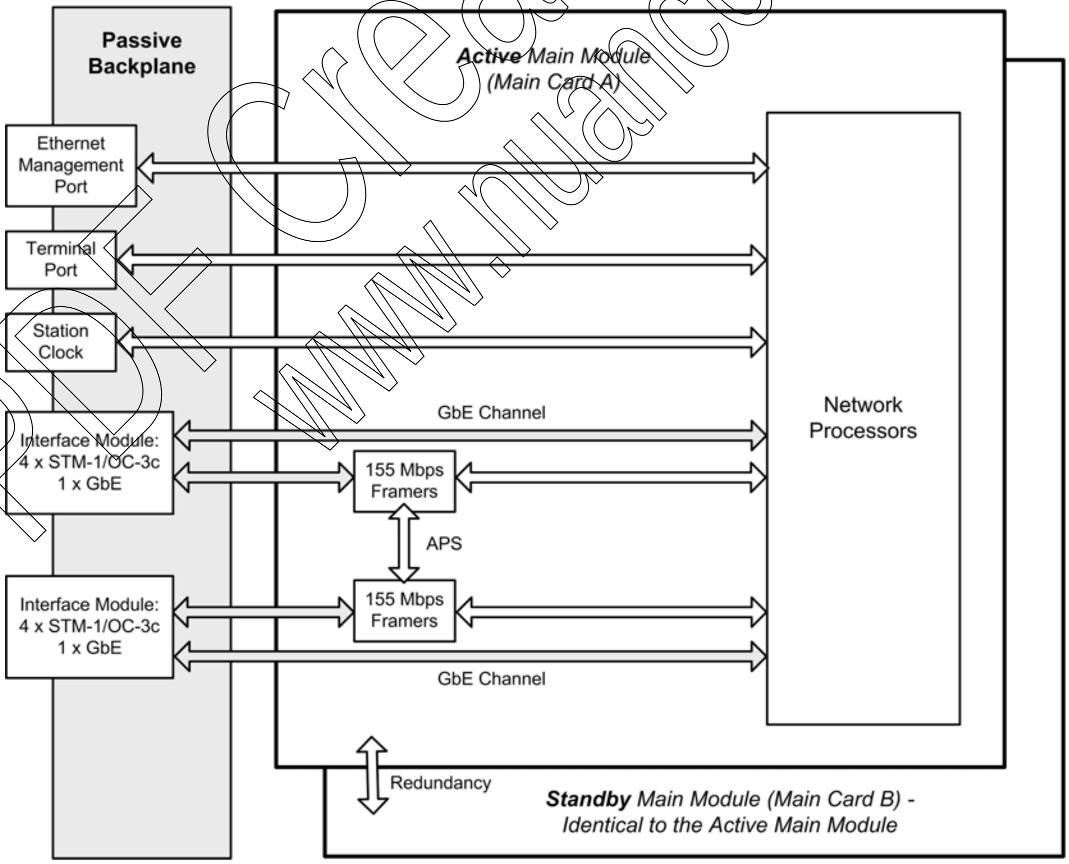

Passive Backplane
Active Main Module (Main Card A)
Ethernet Management Port
Terminal Port
Station Clock
Interface Module: 4 x STM-1/OC-3c 1 x GbE
GbE Channel
155 Mbps Framers
APS
155 Mbps Framers
Interface Module: 4 x STM-1/OC-3c 1 x GbE
GbE Channel
Network Processors
Redundancy
Standby Main Module (Main Card B) - Identical to the Active Main Module

Figure 1-5. ACE-3600 Block Diagram

As shown in *Figure 1-5*, the main module (main card) is the core component of ACE-3600, and all traffic types are processed by it.

Main Modules Protection

In addition to APS on STM-1/OC-3 ports, ACE-3600 supports main modules (main cards) redundancy protection, which protects the unit's data matrix and main CPU in cases of unexpected module reset.

In this protection mode, one main card is the active one (which controls the unit and processes all traffic), and the second is the standby module, ready to take the place of the active one at any moment. Once the standby module becomes the active module, the other becomes the standby module, and vice-versa.

When two main modules are installed and configured to work in redundancy mode, both receive the same traffic simultaneously (received via any of the unit's interfaces). The transmitter on the standby card, however, is always disabled.

Requirements for Main Module Protection

The protection mechanism is available provided that:

1. The two installed main modules are identical, in terms of:
   - Hardware version
   - Software version
   - Configuration database.
2. Inter-module communication is valid.
3. Redundancy support is configured to ON.

Triggers for Main Module Protection Switching

The module on standby becomes the active module when:

- The active card performs reset;

  Or –
- The user invokes a manual switch causing the standby module to become the active card;

  Or –
- The self-test results for the standby card are better than those for the active card.

Configuration of the Active and Standby Module

The displayed configuration menus (as described in *Chapter 4* and *Chapter 6*) are always related to the currently active card. If a switching occurs when viewing one of the menus, the standby card takes over, logs all users out and then displays the Login screen.

A new configuration is always performed on the currently active card. In order to synchronize the standby module with a new configuration, the database update command should be activated. This command transfers the new database to the standby module. Once the transfer is complete, the standby module performs automatic restart.

ATM over PSN Functionality

This section describes the unit's ATM over PSN capabilities in terms of:

- *Queues and Buffers*
- *Timeout Mechanism*
- *PSN Buffer Allocations.*

Queues and Buffers

The traffic sent by the Gigabit Ethernet interface is mapped to four strict priority transmit queues, as follows:

- Queue 1 (highest) – Reserved for clock distribution traffic; can store up to 50 frames.
- Queue 2 – Reserved for management traffic and highest priority data; can store up to 500 frames.
- Queue 3 – Used for the second priority data; can store up to 500 frames.
- Queue 4 – Used for the lowest priority data; can store up to 500 frames.

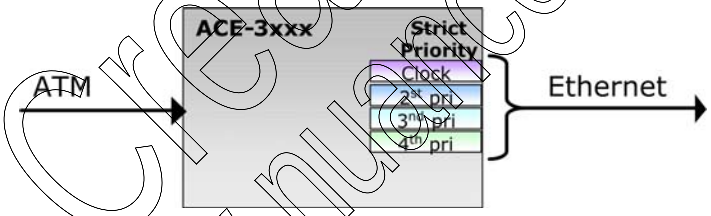


Figure 1-6. Ethernet Queue Priority

PSN Buffer Allocations

- In the PSN to ATM direction –
  - Frames are received on the Ethernet port and are mapped to a VPC/VCC based on the incoming PW label.
  - Each frame is stored in a buffer of 1600 bytes.
  - Each VPC/VCC transmit channel can store up to 50 buffers.
  - The Tx priority of each Tx channel is determined by the connection service category.
  - If a frame is received for a specific VCC/VPC that already occupies 50 buffers, the frame is dropped and the Rx congestion counter is increased.
- In the ATM to PSN direction –
  - Cells are received on the VCC/VPC and are mapped to a PW based on the incoming VPI/VCI.

  - Each incoming cell is either concatenated to an existing PW packet or starts a new PW packet.
  - Each PW packet is stored in a 1600 byte buffer.
  - Upon transmission, each PW is mapped to one of the three Ethernet transmission queues.
  - Each transmission queue can store up to 500 buffers.
  - If a PW frame is directed to a transmission queue which its 500 buffers are full, the frame is dropped and the Tx congestion counter is increased.
- Data buffer pool –
  - The buffers used for data transmission (in both directions) are allocated from a single pool.
  - Each buffer size is 1600 bytes.
  - The number of buffers in the pool is set to the maximum numbers of buffers that can be acquired (max. VC ×50 + ETH queue×500).

Timeout Mechanism

ACE-3600 has a built-in a timer that defines pseudowire (PW) timeouts in the range between 100 to 5,000,000 microseconds (μs). Each specific PW can be configured to work with the timeout function enabled or disabled. If a timeout state is reached, the PW frame is closed and forwarded.

The timer accuracy is +500 microseconds.

The timer process comprises the following stages:

1. When the first cell of a packet is received, the arrival time of the cell is saved, and the cell is stored.
2. A background timer process task is entered every 500 microseconds, and performs the following:
   - Scans and traces all PWs that are set with Timer Enabled.
   - If the PW already has cell/cells stored, the timer task compares the current time with the arrival time of the first cell (which was stored in the 1st stage).
   - If the current time minus the arrival time is larger than the timer settings, a timeout state takes effect and the frame is forwarded for transmission. Alternatively, if no timeout has been reached, no action is taken.

ATM Switching/Aggregation Functionality

This section describes:

- *ATM Layer Functionality*
- *ATM Traffic Shaping*
- *ATM Cell Scheduling*
- *ATM Policing*
- *ATM Buffer Allocations*
- *ATM OAM Functionality*
- *Continuity Check (CC)*.

ATM Layer Functionality

ACE-3600 supports the following ATM layer features:

- Up to 1024 VP and VC connections are supported with full UNI/NNI VP range (0–255/4095) and VCI range (0–65535).
- Quality of Service (QoS) for delay-sensitive applications –
  - The required QoS parameters can be defined according to application requirements
  - Each VC or VP can be assigned to a service class
  - Egress traffic can be shaped as the application requires.
- Rate limiting on STM-1/OC-3c uplink traffic – Each STM-1/OC-3c port can be configured to have an outbound rate limit in cells/sec.

ATM Traffic Shaping

ACE-3600 controls the ATM traffic transmitted to the public network using a built-in shaper. Single or dual leaky bucket shaping applies on each VP/VC, and a traffic descriptor is assigned to each VC/VP.

The traffic shaping improves ATM services by:

- Providing improved service, since bursty traffic is smoothened
- Enabling flexible and accurate traffic adaptation for the required service.

Shaping prevents network congestion and achieves increased network utilization.

Shaping is supported for all VCCs. The TD (traffic descriptor) that is assigned to a VC sets both the connection priority (according to strict priority queues, see *Figure 1-7*) and the shaping parameters.

Each side of a VP/VC cross connection (XC) can be either shaped or unshaped according to its traffic descriptor (TD). The shaping can be set to one of the following:

- CBR shaped
- CBR unshaped

- VBR1 shaped
- UBR+ shaped
- UBR unshaped

The shaping parameters are defined according to the following service categories:

- CBR shaped – PCR and CDVT
- VBR1 shaped – PCR, CDVT, SCR and MBS
- UBR+ – PCR, CDVT and MDCR
- ACE-3600 has a built-in shaper, of a single/dual leaky bucket type.
- PCR/SCR granularity in the worst case is 0.39%
- Minimum PCR/SCR supported is 100 cells/second
- Recommended CDVT values are displayed in the relevant Traffic Descriptor (TD) configuration screen (CDVT values cannot be enforced accurately).

ATM Cell Scheduling

Each ATM port's egress cell traffic is hierarchically matched to four strict-priority queues, and the traffic is transmitted according to these four outbound queue levels of priority:

- First priority queue – CBR-shaped and CBR-unshaped cells are transmitted first
- Second priority queue – VBR cells
- Third priority queue – UBR+ cells
- Fourth priority queue – UBR cells are transmitted last.

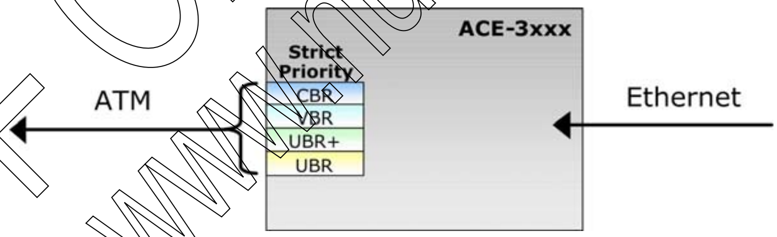


Figure 1-7. ATM Queues Priority

ATM Policing

The ATM policing function defines which non-conformant ATM cells should be discarded, tagged or counted by ACE-3600, per user configuration. The following policing modes are supported according to ATMF TM4.1:

- CBR.1
- VBR.1
- VBR.2
- VBR.3
- UBR.1
- UBR.2

The policing is configurable per a receive channel. Multiple channels can be mapped to a single policing policy (group policing).

The granularity of the CDVT is 10ns. The minimum CDVT depends upon the port type:

Port Type	Minimum CDVT
TDM	1 cell time at line rate
UPI multi-PHY	4 cell time at line rate
UPI single-PHY	16 cell time at line rate
IMA	1 cell time at minimum IMA group rate
Equal-rate-slow-PHY (ERSP)	1 cell time at line rate

ATM Buffer Allocations

ACE-3600 has three types of fixed congestion thresholds:

- Global – the maximum number of cells that can be allocated/buffered for all service categories is 64,000.
- Service category – the maximum number of cells that can be allocated/buffered for each traffic class is 16,000.
- Per connection – the maximum number of cells that can be allocated/buffered for each connection is 1024.

ATM OAM Functionality

ACE-3600 provides F4/F5 OAM support that complies with ITU-I.610 (AIS, RDI and CC). OAM cells are inserted into the VP/VC cell stream ahead of the shaper, enabling accurate conformance to shaping parameters.

Four operating modes are supported:

- End-to-end (for a host only)
- Segment
- Intermediate
- Loopback – OAM loopback cells are used to determine connectivity at specific points in a network or between networks. OAM cells are part of the F4 and F5 OAM service, which allows fault management for VPs and VCs. Loopback cells can be defined as Segment or End-to-End.

For in-depth information about the supported OAM modes, refer to *Appendix C*.

Continuity Check (CC)

CC is used to check service availability in the following manner:

- The transmitting (Tx) end sends a CC cell periodically over a predefined VCC or VPC and verifies that the VCC/VPC is intact.

- F4/F5 Continuity Check (CC) cell is generated or terminated and is user-configurable per VCC/VPC. It is optionally supported on all VCCs/VPCs.
- CC cells are sent once every second, regardless of user traffic presence.
- LOC is declared when no user data cells or CC are received for 3.5 consecutive seconds. User data cells do not include AIS cells.

MPLS Utilization

ACE-3600 provides the following MPLS-related features:

- *Label Distribution Protocol (LDP)*
- *Penultimate Hop Popping (PHP)*.

Label Distribution Protocol (LDP)

With an appropriate license, ACE-3600 optionally allows using the label distribution protocol (LDP) to automatically assign and distribute pseudowires and tunnel labels between MPLS peers (up to 32 peers). When LDP is enabled, labels (tunnels or PWs) are set automatically.

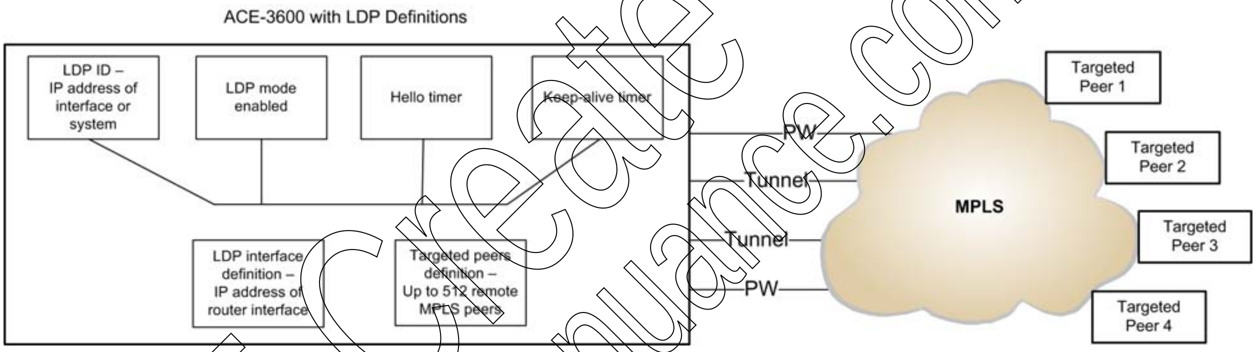

ACE-3600 with LDP Definitions
LDP ID – IP address of interface or system
LDP mode enabled
Hello timer
Keep-alive timer
LDP interface definition – IP address of router interface
Targeted peers definition – Up to 512 remote MPLS peers
PW
Tunnel
Tunnel
PW
MPLS
Targeted Peer 1
Targeted Peer 2
Targeted Peer 3
Targeted Peer 4

Figure 1-8. LDP Definitions and Connectivity

For more information, refer to *Configuring the LDP Signaling Protocol* in Chapter 4.

Penultimate Hop Popping (PHP)

Penultimate Hop Popping (PHP) is a packet-level modification process in which the label switched router (LSR) removes (pops) the last label of MPLS packets before they are passed to an adjacent label edge router (LER). PHP mode is relevant only when some signaling protocols are in use.

When PHP mode is enabled:

- The receiving LER advertises an implicit null label (a reserved label value of 3) for directly connected routes. The implicit null label causes the previous hop (penultimate) router to remove the most outer label before transmitting the packet to the LER.
- Every packet received over MPLS (regardless of the number of labels) is regarded as data packet and is forwarded to the PW module.
- The control (IP) traffic is received as raw IP.

- Configuration of PW connections with static ingress tunnel label is allowed in order to allow backward compatibility.

When PHP mode is disabled:

- The receiving LER advertises an actual label value to the previous hop. This label is used when packets are transmitted to the LER.
- After the tunnel label is established, all the traffic coming from the previous hop, arrive over the tunnel label. This specifically includes IP control traffic (such as LDP, Ping, etc.) that is transmitted over a tunnel label and not as raw IP.
- PW traffic over MPLS must be received with two MPLS labels: tunnel and PW label.
- Every packet received with single label is forwarded to the host in order to allow control (IP) traffic over the MPLS tunnel.
- It is not possible to configure a PW connection without an ingress tunnel label (for either dynamic or static mode).
- Traffic received as raw IP works normally.

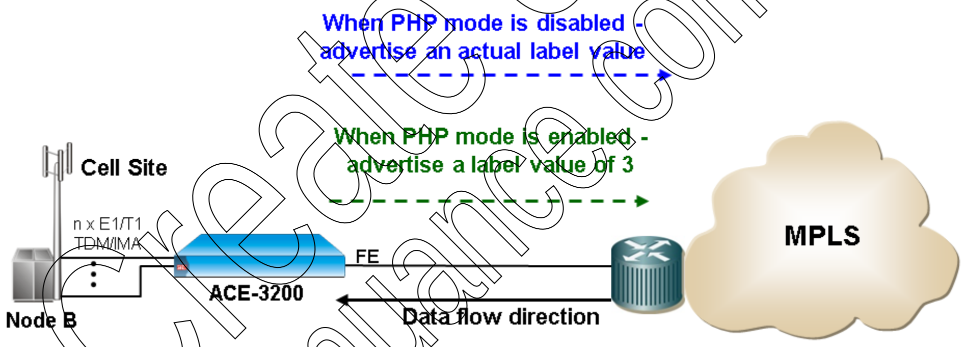

When PHP mode is disabled - advertise an actual label value
When PHP mode is enabled - advertise a label value of 3
Cell Site
n x E1/T1
TDM/IMA
Node B
ACE-3200
FE
Data flow direction
MPLS

Figure 1-9. Label Advertising in PHP Mode

PHP is enabled by default, meaning that all the control traffic is expected to be received as raw IP.

PHP mode settings affect only the ingress tunnel behavior when it is established with LDP. They do not affect PWs configured for an IP-based PSN type (MPLSoIP, UDPoIP).

The following diagram shows how PHP mode availability affects configuration:

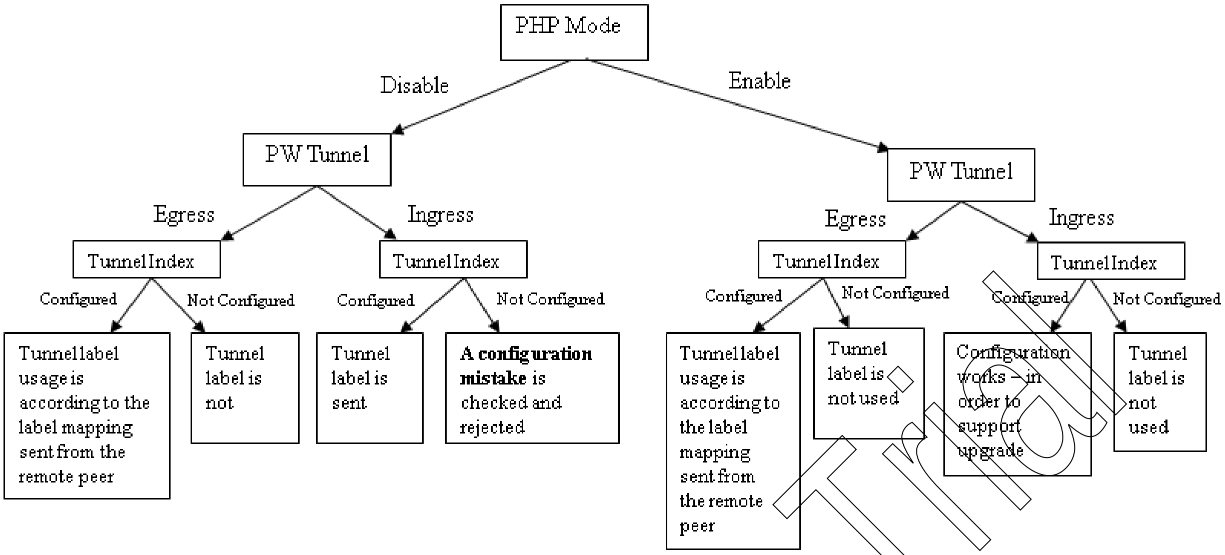

PHP Mode
Disable
Enable
PW Tunnel
Egress
Ingress
Tunnel Index
Configured
Not Configured
Tunnel label usage is according to the label mapping sent from the remote peer
Tunnel label is not
Tunnel label is sent
A configuration mistake is checked and rejected
PW Tunnel
Egress
Ingress
Tunnel Index
Configured
Not Configured
Tunnel label usage is according to the label mapping sent from the remote peer
Tunnel label is not used
Configuration works – in order to support upgrade
Tunnel label is not used

Figure 1-10. PHP Mode Configuration Options

For more information about encapsulation with or without PHP, refer to *Appendix E*.

Fault Propagation and PSN Connectivity Checks

The ACE-3600 alarm forwarding mechanism translates PSN and ATM link failures to alarms that are sent to the customer equipment on each end of the application. ACE-3600 sends either F4 or F5 Segment/End-to-End AIS alarms towards the ATM backbone side, and performs VCCV-BFD connectivity checks with the PSN side.

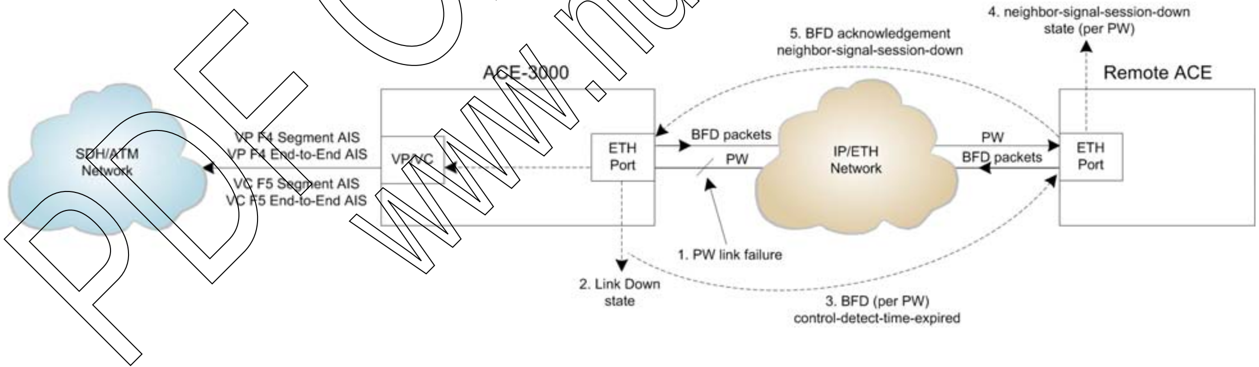


Figure 1-11. PW Link Failure and Alarm Forwarding/Acknowledgement over a PSN

For more detailed information, refer to *Appendix F*.

Ports Protection

APS on STM-1/OC-3c Ports

Automatic protection switching (APS) is a link-level protection mechanism for ensuring service continuity in the case of interface failure/error. In ACE-3600, the STM-1/OC-3c interfaces can be configured to work in APS mode, in which the unit's two interface modules (each includes 4 STM-1/OC-3c ports) transmit simultaneously over working fibers and protection fibers.

In the receive direction, each node monitors the corresponding link for SD and SF conditions, and selects the better of the protected RX links. If an interface's uplink traffic fails, the other continues and compensates for the loss, allowing uninterrupted service. This form of APS is called 1+1 protection.

APS in ACE-3600 functions according to G.841 Annex B or Clause 7.1, Linear MSP (multiplex section protection; compatible with 1:n bidirectional switching), and allows a channel to be bridged on the transmit direction at the SONET/SDH path level. The protocol used between the devices to handle the switching is carried out using K1 and K2 bytes from the line header of the SONET/SDH frame.

The APS path information (APS TX) may be sourced from either the receive side or the transmit side of a channel. ACE-3600 logs and monitors all errors across the APS receive stream.

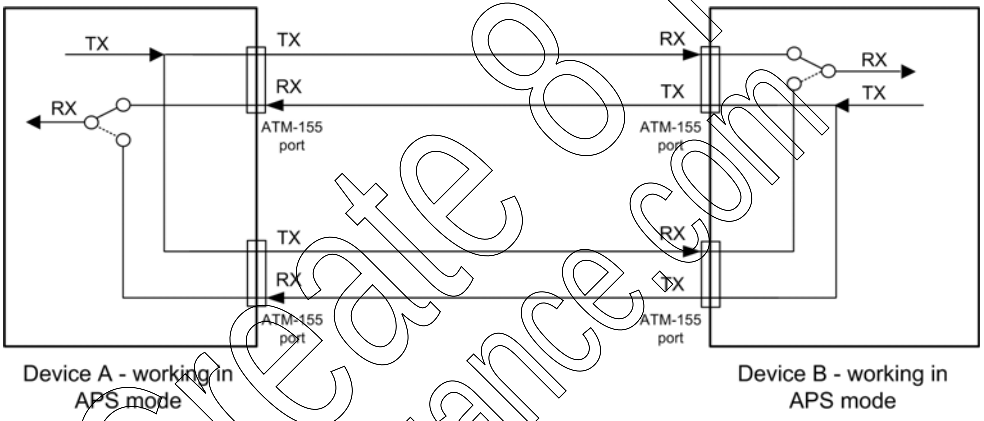


Figure 1-12. Two nodes working and communicating in APS mode

Gigabit Ethernet Port Redundancy

The Gigabit Ethernet interfaces can be set to work in 1:1 protection mode, or in 1+1 link aggregation mode according to IEEE 802.3ad.

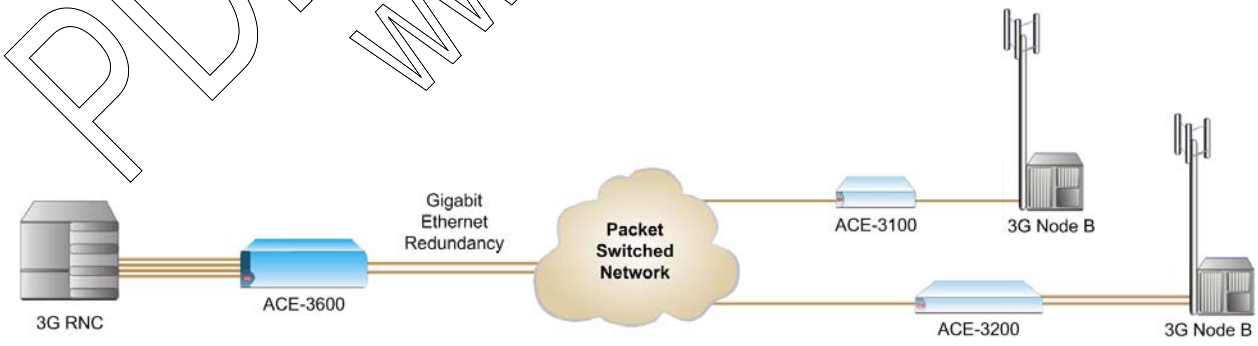


Figure 1-13. ACE-3600 Using Ethernet Redundancy

When working in the 1+1 link aggregation mode:

- Both GBE ports share the same MAC and IP address
- Traffic is received on both ports

- Traffic is transmitted only via the active GbE port
- When a physical failure (loss of carrier) is detected on the active GbE port, the redundant port becomes active and the errored one switches to standby mode.

GbE link redundancy in 1:1 mode is not based on an existing standard, and works as follows:

- Both GbE ports share the same MAC and IP address
- RX and TX are enabled only on the active port
- When a physical failure (loss of carrier) is detected on the active port, the redundant port becomes the active one in both TX and RX directions. ARP is sent from the active port, so that all L2 switches can update their MAC tables.

Note

- *1:1 protection mode can be used when ACE-3600 is connected to L2 switches (same one or different ones). It cannot work with routers, since both ports share the same IP address.*
- *1+1 link aggregation mode (802.3ad) can work with either L2 switches or routers, but both ports must be connected to the same switch/router that supports 802.3ad.*

Physical Loopback Tests

ACE-3600 supports two types of user-defined physical loopback operations on ATM ports:

- Internal loopback – returns the transmitted data at the physical layer to the receive path. The internal physical loopback includes a configurable timeout mechanism that ends the loopback operation after expiry of the user-defined period.
- External loopback – returns the received data at the physical layer to the transmit path.

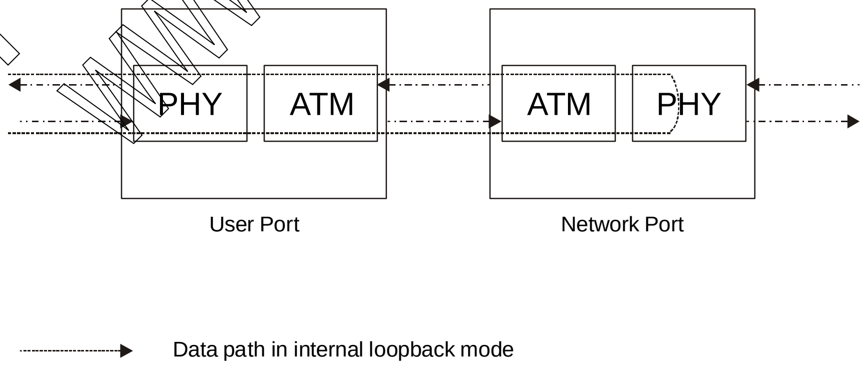


Figure 1-14. Data Path in Internal Loopback Mode

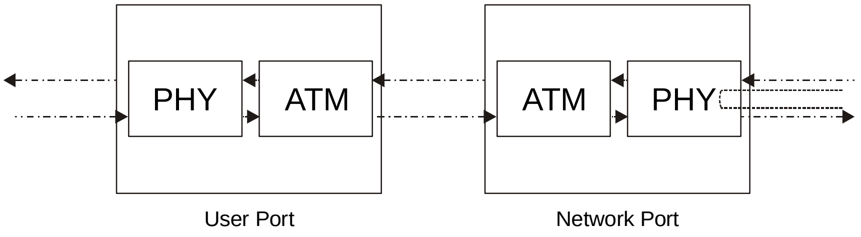


Figure 1-15. Data Path in External Loopback Mode

The physical loopback includes a configurable timeout mechanism to terminate the loopback operation upon expiry of the assigned period.

SNMP and Alarm Traps

SNMP Traps

SNMP traps are automatically sent by the agent towards the NMS (network management station) to report errors in the device or in the affected service. To enable fault isolation by the NMS, the traps include specific information about the problem status, such as: start/end time), port number/type and the type of problem, such as: LOS, LOF, LCD, and so on.

Standard SNMP traps, such as cold start and authentication failure, are also supported. Additionally, alarm traps to be sent are user-selectable and can be masked per manager.

Alarm Traps

ACE-3600 supports a hierarchical alarm traps mechanism. This mechanism generates alarm traps according to a configurable alarm traps mask per manager. All traps are reported in the system event log, even when masked.

Traps can also be disabled when selected for masking by manager. The recording of events in the event log cannot be disabled.

All alarm traps are listed in *Chapter 6*.

Management

Cross-Network Management

Management traffic streams can pass through ACE-3600 transparently, using predefined destination subnet IDs. ACE-3600 delivers the management traffic over pseudowire or ATM VC connections, allowing frames to pass over a packet-switched network or from one network to another without interruption.

If the originating management subnet is received on the inband GbE port, it can be translated to an ATM VC subnet, and vice-versa, as needed in the application.

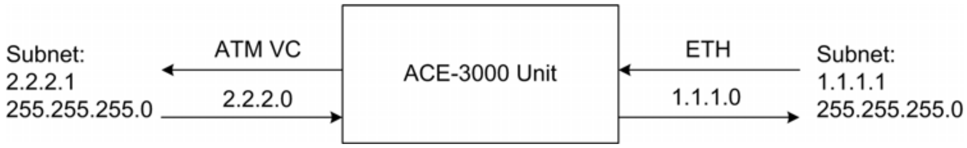


Figure 1-16. Ethernet to ATM VC Subnet Conversion

Management Security

Access via terminal, Telnet or ConfiguRAD is password-protected and can be secured using SSL protocol or SSH-protected client/server connection. The system logs out automatically and displays the login screen after 15 minutes of inactivity (time during which no character was sent to the terminal/Telnet).

After three unsuccessful login attempts, ACE-3600 locks up and prohibits additional attempts for 15 minutes. Each attempt to login (valid or invalid) to ACE-3600 results in sending events/traps to the log file or NMS.

Three user access levels are supported:

- su – super user, full read and write access, not including access to hidden screens for internal/debugging use.
- tech – limited write access to alarm configuration, clearing of alarms and access to diagnostics.
- user – read-only.

SNMP (simple network management protocol) version 3.0 adds security and remote configuration capabilities to the previous versions (SNMPv1/SNMPv2). This includes:

- Message integrity –ensuring that a packet has not been tampered with during transit
- Authentication –determining that the message originates from a valid source
- Encryption – scrambling the contents of a packet prevent interception by unauthorized sources
- Security models – authentication strategies that are applied on single users or entire user groups
- Security levels – set the permitted level of security within security models.

A chosen combination of a security model and a security level determines which security mechanism is employed when handling SNMP packets.

1.4 Technical Specifications

Interface Modules	*Number of Modules*	Up to 2 per unit (field-replaceable modules)
STM-1/OC-3c Interface	*Number of Ports*	Up to 8 in total, 4 per single interface module (4+4 in automatic protection switching mode)
	Data Rate	155 Mbps
	Operation Mode	• ATM UNI • SDH or SONET (user-selectable)
	Compliance	• Physical layer and ATM mapping into STM-1 according to I.432 • Automatic protection switching (APS) according to G.841 Annex B or Clause 7.1, Linear MSP (multiplex section protection) compatible with 1:n bidirectional switching)
	Jitter Performance	• Output: according to G.825 • Tolerance: according to G.823 • Transfer: according to G.783
	Framing	STM-1/STS3c
	Interface Type	Fiber optic via SFP transceiver; see *Table 1-1* on page *1-25*
	Connector	LC, see *Table 1-1* on page *1-25*
Gigabit Ethernet Interface	*Number of Ports*	2 in total, 1 per single interface module
	Data Rate	1000 Mbps
	Compliance	IEEE 802.3z, 802.1Q, 802.1p
	Operation Mode	Full duplex
	Max. Frame Size	1600 bytes
	Interface Types	See *Table 1-1* on page *1-25*
	Connector	RJ-45 or fiber optic via SFP transceiver; see *Table 1-1* on page *1-25*

Ethernet Control Port	*Interface Type*	100BaseTX
	Operation Mode	Full-duplex; autonegotiation disabled
	Compliance	IEEE 802.3
	Connector	RJ-45
Terminal Control Port	*Interface Type*	RS-232/V.24 (DCE)
	Data Rate	9.6, 19.2, 38.4, 57.6 or 115.2 kbps, user-configurable
	Connector	RJ-45 (RJ-45 to DB-9 adapter cable is supplied)
Station Clock Port	*Interface Type*	E1, T1 or J1, user-configurable
	Impedance	• Unbalanced E1: 75Ω (via an adapter cable; for more information, refer to *Chapter 2*) • Balanced E1: 120Ω (HDB3) • T1: 100Ω (B8Zs, AMI)
	Connector	RJ-45
ATM Connections		Up to 1024 VPs/VCs
PW Connections		Up to 1024
Power Supply	*Number of Units*	2, hot-swappable
	Type	• AC: 100 to 240 VAC (±10%), 47–63 Hz • DC: 24 VDC or -48 VDC nominal
Power Consumption		• AC: 120 VA max • DC: 80W max
Physical	*Height*	8.74 cm (3.4 in / 2U)
	Width	44.0 cm (17.3 in)
	Depth	25.0 cm (9.0 in)
	Weight	8.0 kg (17.6 lb) – with two main modules installed
Fan Tray		Field-replaceable with two independent cooling fans

Environment		
	Operating Temperature	0°–50°C (32°–122°F)
	Storage Temperature	-20°–70°C (-4°–158°F)
	Humidity	Up to 90%, non-condensing

Table 1-1. STM-1/OC-3c and Gigabit Ethernet SFP Transceiver Types

Ordering Name, Interface, Connector	Wavelength, Fiber Type [nm], [µm]	Relevant Standards	Transmitter Type	Input Power [dBm]		Output Power [dBm]		Typical Max. Range*	
				(min)	(max)	(min)	(max)	[km]	[miles]
SFP-1, STM-1/OC-3c, LC	1310, 62.5/125 multimode	ANSI T1 646-1995 (STM-1)	LED	-30	-14	-20	-14	2	1.2
SFP-2, STM-1/OC-3c, LC	1310, 9/125 single mode	G.957 S1.1 (STM-1)	Laser, short haul	-28	-8 -15		-8	15	9.3
SFP-3, STM-1/OC-3c, LC	1310, 9/125 single mode	G.957 L1.1 (STM-1)	Laser, long haul	-34 -10		-5	0	40	24.8
SFP-4, STM-1/OC-3c, LC	1550, 9/125 single mode	G.957 L1.2 (STM-1)	Laser, long haul	-34 -10		-5	0	80	49.7
SFP-5, 1000BaseSX, LC	850, 50/125 multimode	IEEE 802.3 (Gigabit Ethernet)	VCSEL	-17	0 -9.	5	0 0.	55	0.3
SFP-6, 1000BaseLX10, LC	1310, 9/125 single mode	IEEE 802.3 (Gigabit Ethernet)	Laser	-20	-3 -9.	5	-3 10		6.2
SFP-10a, STM-1/OC-3c, LC	Tx – 1310 Rx – 1550, 9/125 single mode (single fiber)	G.957 (STM-1)	Laser (WDM)	-28	-8 -14		-8 20		12.4
SFP-10b STM-1/OC-3c, LC	Tx – 1550 Rx – 1310, 9/125 single mode (single fiber)	G.957 (STM-1)	Laser (WDM)	-28	-8 -14		-8 20		12.4
SFP-13, STM-1/OC-3c, SC	Tx/Rx – 1310, 9/125 single mode (single fiber)	G.957 (STM-1)	Laser (WDM)	-29	-8 -15		-8 20		12.4
SFP-17a, 1000BaseBx10, LC	TX – 1310 RX – 1490, 9/125 single mode (single fiber)	IEEE 802.3 (Gigabit Ethernet)	Laser (WDM)	-20	-3 -9		-3 10		6.2
SFP-17b 1000BaseBx10, LC	TX – 1490 RX – 1310, 9/125 single mode (single fiber)	IEEE 802.3 (Gigabit Ethernet)	Laser (WDM)	-20	-3 -9		-3 10		6.2

Note *Typical range is calculated using common peripheral equipment and environment conditions. It may therefore vary according to user specific equipment and environment conditions.*

Chapter 2

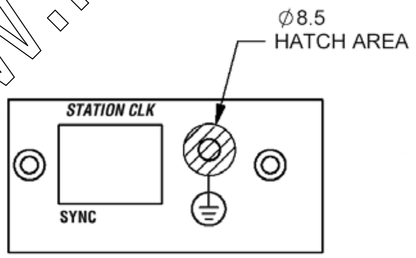
Installation and Setup

This chapter describes the physical installation and setup of ACE-3600, and includes the following topics:

- *Site Requirements and Prerequisites*
- *Package Contents*
- *Equipment Needed*
- *Mounting the Unit*
- *Removing/Installing Field-Replaceable Parts*
- *Connecting to Networks and Devices*
- *Connecting to the Clock Source*
- *Connecting to Power*.

Warning

- No internal settings, adjustment, maintenance and repairs should be performed by either the operator or the user. Such activities must be performed only by skilled personnel who are aware of the hazards involved. Always observe standard safety precautions during installation, operation and maintenance of this product.
- A grounding cable must be connected to the dedicated grounding screw, located in the hatch area next to the ACE-3600 station clock port (see figure below). The other side of the cable must be connected to a proper grounding (Earth) point.



2.1 Site Requirements and Prerequisites

AC-powered ACE-3600 units should be installed within 1.5 meters (5 feet) of an easily accessible and grounded AC outlet capable of furnishing the required voltage supply, in the range of 100 to 240 VAC, 47 to 63 Hz.

Allow at least 90 cm (36 inches) of frontal clearance to allow operator access and module replacement. For cable connections and continuous product operation, allow at least 15 cm of frontal clearance and at least 15 cm at the rear of the unit.

ACE-3600 has internal cooling fans and its ambient* operating temperature is 0°–50° C (32°–122°F), at a relative humidity of up to 90%, non-condensing.

Note *Since the ACE-3600 unit and adjacent devices generate their own heat, the actual ambient temperature may be higher than the room temperature, if several units are placed next to or on top of each other. Such placement is allowed as long as the ambient temperature does not exceed the specified above.*

DC-powered units should apply the same clearance and temperature requirements.

2.2 Package Contents

The ACE-3600 package contains the following items:

- ACE-3600 unit
- AC power cord or DC connection kit (if a DC-powered unit was ordered)
- CBL-RJ45/D9/F/STR – Control port adapter cable (RJ-45 to DB-9)
- RM-36 – Hardware kit for mounting one unit into a 19-inch rack
- Technical Documentation CD – Contains the relevant PDF documents for ACE-3600, including the DC power connection supplements and the relevant RADview manuals.

2.3 Equipment Needed

ACE-3600 is delivered completely assembled and requires only the following hand tools:

- Mounting ACE-3600 in a 19" rack requires a 3 mm Phillips screwdriver and an RM-36 hardware kit (see *Mounting the Unit*).
- Removing/installing hot-swappable power supplies or field-replaceable interface modules requires a flathead screwdriver.
- Removing/installing a main card module or a patch panel adapter requires a 3 mm Phillips screwdriver.

Power Cable

AC-powered ACE-3600 is equipped with an appropriate power cord (country or region dependent) to be connected from the mains to the power socket of the hot-swappable power unit (accessible from the front panel).

DC-powered ACE-3600 is equipped with an appropriate DC connection kit, which should be used for preparing the DC cable connection.

Interface Cables

Refer to the following table to determine what cables and connectors are required for installation. *Appendix A* specifies the wiring of all connector pinouts.

Table 2-1. Required Interface Cables

Interface	Required Cable Type
Terminal Control	RJ-45 to DB-9, RS-232/V.24 compliant cable for ASCII-based terminal control (supplied)
Ethernet or electrical GbE	Cat. 5, RJ-45 to RJ-45, IEEE 802.3 compliant cable for Ethernet control (not supplied)
STM-1/OC-3 or fiber optic GbE	Fiber optic cable that matches the ordered interface type (not supplied). For more information, see *Table 1-1* in Chapter 1.
Station clock	RJ-45 to RJ-45, E1/T1 compliant cable for connecting the unit to an external clock source (if required; not supplied).

2.4 Mounting the Unit

ACE-3600 can serve as a desktop unit, or be mounted in a 19" rack.

- For rack mounting instructions, refer to the RM-36 Installation Kit Manual.
- If ACE-3600 is to be used as a desktop unit, place and secure the unit on a stable, non-movable surface.

Refer to the clearance and temperature requirements in *Site Requirements and Prerequisites*.

2.5 Removing/Installing Field-Replaceable Parts

ACE-3600 is a modular unit that allows the following parts to be replaced:

Main module	See *Removing/Installing the Main Module*
Interface modules	See *Removing/Installing the Interface Modules*
Fans	See *Removing/Installing the Fan Tray/Fans*
Power supply	See *Removing/Installing the Hot-Swappable Power Supply Units* on page *2-12* (in *Section 2.8*).
Control ports module	See *Removing/Installing the Control Ports Module* on page *2-7*.
Station Clock port module	Replacement may be performed only in rare cases, when you are specifically instructed to do so by an authorized *Technical Support* representative.

Warning

- The unit's power supply delivers up to 240 Volts! Removing or installing field-replaceable parts while the unit is turned on can therefore be dangerous. To prevent electrocution, DO NOT TOUCH exposed electrical parts!
- When removing or installing a hot-swappable power supply unit: disconnect the power supply cable from the unit that you are removing or installing!

Removing/Installing the Main Module

The main module (main card) of ACE-3600 can be removed and re-inserted/replaced when necessary.

Caution Do not install the ACE-3400 or ACE-3402 main modules in ACE-3600, since they are incompatible.

ACE-3600 allows the installation of two main modules: one used for normal operation and one for protection/backup. For more information about the main module redundancy feature, refer to *Chapter 1*.

➤ To remove a main module card:

1. Using a Philips screwdriver, unscrew and remove the module's two tightening screws.
2. Carefully pull the module's two black plastic latches outwards together at the same time (see *Figure 2-1*).

Caution Never pull the plastic latches when the tightening screws are in place.

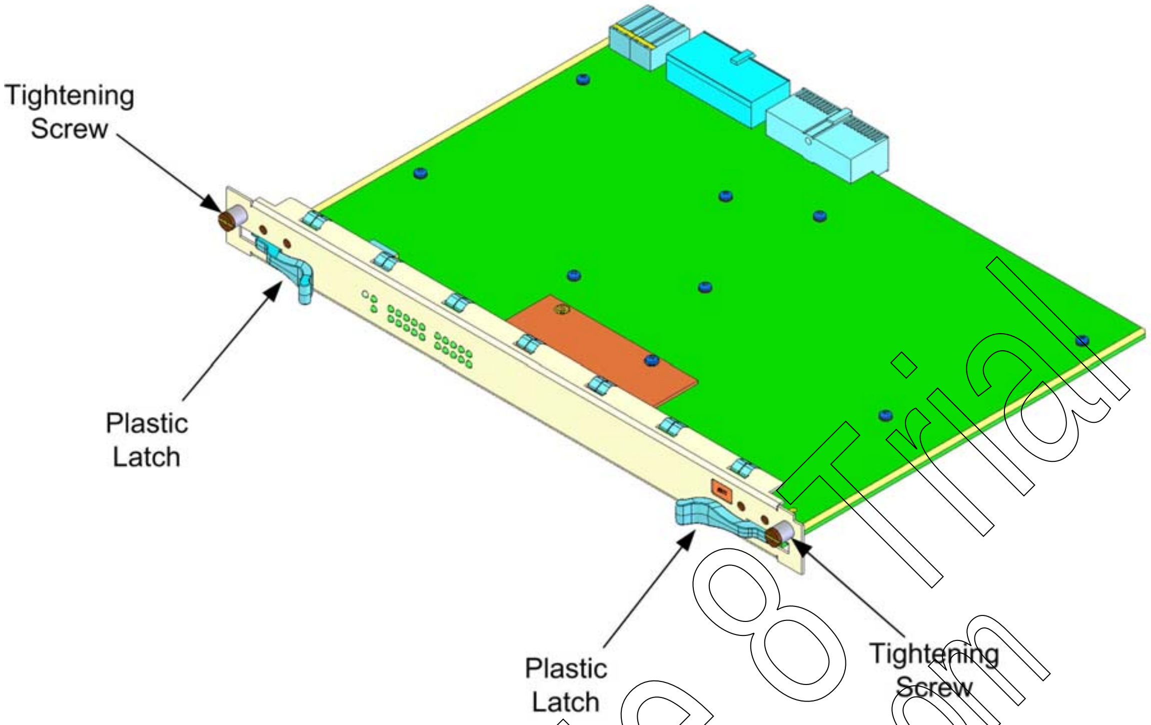


Figure 2-1. ACE-3600 Main Module

3. Carefully pull the main module card out of the chassis.

➤ To install a main module:

1. Carefully insert the module into the appropriate main module slot of ACE-3600, until the module's rear connectors engage the mating connector on the backplane and the module fits into place.
2. Close the two plastic latches inwards.
3. Secure the module card using the two tightening screws and a Philips screwdriver.

Removing/Installing the Interface Modules

When required, the interface modules can be removed and re-inserted/replaced.

Warning

This module includes Class 1 lasers. For your safety:

- Do not look directly into the optical connectors while the module is operating. Remember that the module starts operating as soon as it is inserted in ACE-3600, and that the laser beam is invisible.
- Do not attempt to adjust the laser drive current.

➤ To remove an interface module:

1. Using a flathead screwdriver, unscrew and remove the module's two tightening screws.
2. Carefully pull the module out of the chassis.

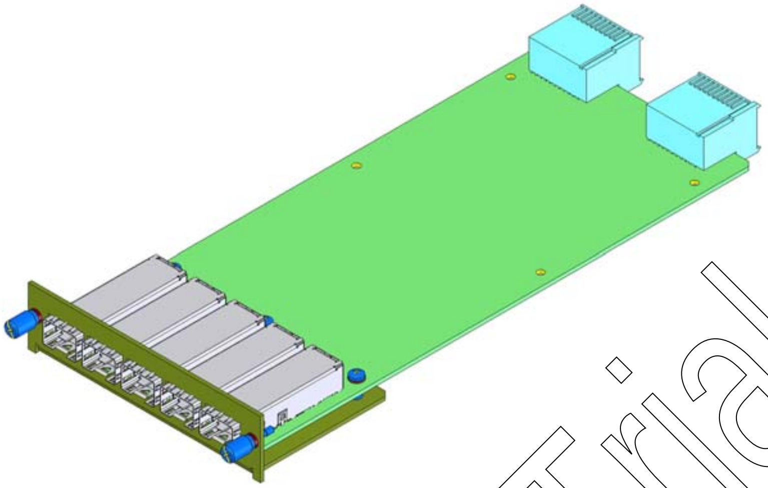


Figure 2-2. ACE-3600 Interface Module

➤ To install the interface module:

1. Carefully insert the module into the appropriate interface slot of ACE-3600, until the module's rear connector engages the mating connector on the backplane and the module fits into place.
2. Secure the module using the two tightening screws and a flathead screwdriver.

Note *If two interface modules are installed in ACE-3600, the second module is used as the redundancy protection module.*

Removing/Installing the Fan Tray/Fans

This section provides instructions for removing and installing the fan tray and its fans.

Fan Tray Description

The fan tray includes two independently controlled exhaust fans that provide cooling for the unit by exhausting the heated air from the chassis outwards. ACE-3600 automatically monitors and adjusts the proper operation of its internal fans.

The fan tray can be removed from ACE-3600 to allow replacement/cleaning of fans, after which it can easily be installed back to its place.

Note

- *If one of the fans stops working, the Fan LED indicator (on the front of the tray) becomes red. In such a case, you should replace the fan tray at the earliest.*
- *ACE-3600 requires the cooling fans at all times. If you completely remove the fan tray, another working fan tray should take its place immediately.*
- *The fan tray can be removed when ACE-3600 is operating.*

Removing the Fan Tray

➤ To remove the fan tray:

1. Using a flathead screwdriver, unscrew the two screws that tighten the tray to the unit.
2. Carefully pull the fan tray out of the chassis.

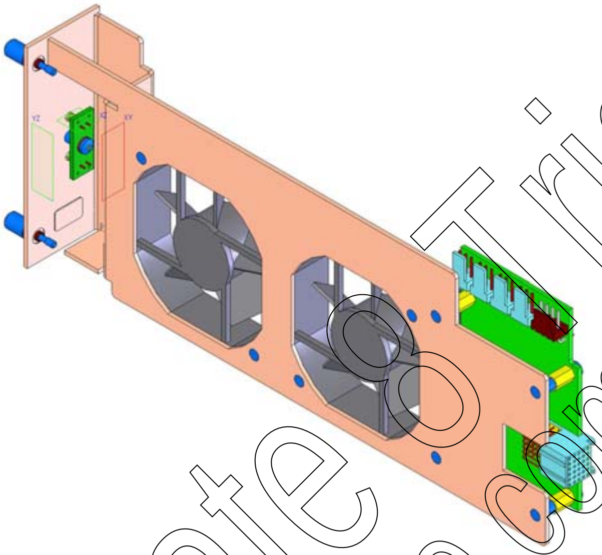


Figure 2-3. Fan Tray (3D Rear View)

Installing the Fan Tray

➤ To install the fan tray into the ACE-3600 chassis:

1. Carefully check the fan tray for foreign objects and dirt that may have been trapped inside, and remove them.
2. Insert the fan tray in the left chassis slot, and slide it inside until its rear connector engages the mating connector on the backplane.
3. Secure the fan tray by tightening its two screws using a flathead screwdriver.

Removing/Installing the Control Ports Module

The control ports module includes the out-of-band Ethernet and the RS-232/V.24 terminal control ports. Removal of this module is necessary only in rare cases of malfunctioned ports or when the ACE-3600 is to be totally dismantled for maintenance purposes.

➤ To remove the control ports module:

1. Using a flathead screwdriver, unscrew the two screws that tighten the module to the unit.
2. Carefully pull the module out of the chassis.

➤ **To install the control ports module:**

1. Carefully insert the module into the appropriate interface slot of ACE-3600, until the module's rear connector engages the mating connector on the backplane and the module fits into place.
2. Secure the module using the two tightening screws and a flathead screwdriver.

2.6 Connecting to Networks and Devices

To interconnect with SDH/SONET networks/equipment or packet-switched networks within the required application, ACE-3600 requires the appropriate cable connections.

Figure 2-1 illustrates the front panel of typical ACE-3600 unit. *Appendix A* specifies the ACE-3600 connector pinouts of each interface.

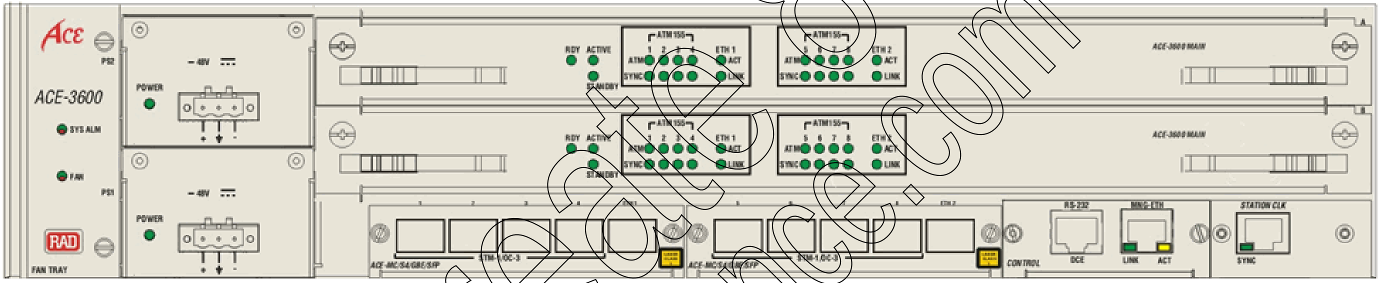


Figure 2-4. ACE-3600 Front Panel (DC-Powered Unit)

Warning

ACE-3600 includes Class 1 lasers. For your safety, do not look directly into the optical connectors while the unit is operating. The laser beam is invisible.

Use **of controls or performing** procedures other than those specified herein may result in hazardous radiation exposure.

The ACE-3600 cables installation includes the following steps:

1. Determine the required configuration of ACE-3600, according to your application (for more information, see *Chapter 5*).
2. Connect the STM-1/OC-3c interface cables (see *Connecting to SDH/SONET Network Equipment*.
3. Connect the Ethernet interface cables (see *Connecting to Packet-Switched Network Equipment* and *Connecting to Ethernet-based (Out-of-Band) Control Station*).
4. Connect ACE-3600 to the clock source (see *Connecting to the Clock Source*).
5. Connect the power cables (see *Connecting to Power*).

Connecting to SDH/SONET Network Equipment

To interconnect ACE-3600 with SDH/SONET networks or equipment (usually RNC equipment), up to 8 fiber optic STM-1/OC-3 cables should be connected to the unit's interface modules, which utilize Small Form-Factor Pluggable (SFP) transceivers that are plugged into the module's empty SFP slot (SFP cage).

➤ **To connect the STM-1/OC-3c fiber optic interface cables:**

1. Lock the wire latch of the SFP transceiver by lifting it up until it clicks into place, as illustrated in *Figure 2-5*.

Note *The SFP module you are installing may have a different wire latch or closing mechanism. In such a case, refer to its manufacturer instructions.*

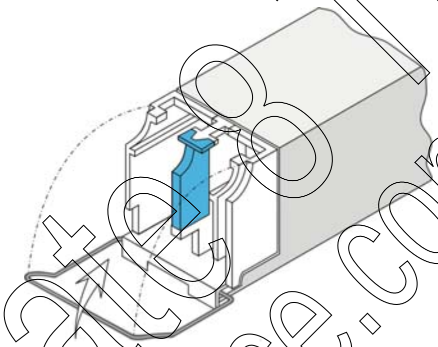


Figure 2-5. SFP Wire Latch Locking Direction

2. Carefully remove the dust covers from the SFP unit.
3. Install the SFP transceiver by inserting it into the GbE module's empty slot (SFP cage), until it clicks into place.

Note *If the SFP does not click into place, remove the SFP, lock it properly and then re-insert the SFP module into the port cage.*

4. Remove the protective rubber caps from the SFP transceiver.

   Two LC connectors are revealed.

5. To each LC connector, connect a fiber optic cable: one for RX and one for TX data.
6. Connect the fiber optic cables to the SDH/SONET equipment (RNC).

Connecting to Packet-Switched Network Equipment

To allow ACE-3600 to interconnect with packet-switched networks, connect fiber optic or electrical GbE cables to the unit's interface module, via appropriate SFP transceivers that are inserted into the module's GbE cage. An appropriate SFP is required for both the fiber optic and electrical Gigabit Ethernet interface types.

Using Fiber-Optic GbE Interface

To install a fiber optic GbE port, perform steps 1–5 of the connection procedure described in the previous section (see *Figure 2-5*), using an appropriate fiber optic GbE SFP transceiver. Then, connect a fiber optic cable between the GbE port and the packet-switched network equipment.

Using Electrical GbE Interface

To install an electrical GbE port, insert an electrical GbE-compliant SFP unit into the interface module's GbE port cage. Then,

➤ To connect the GbE electrical interface cable:

1. Connect a Cat. 5 cable to the RJ-45 connector of the inserted SFP unit.
2. Connect the other end of the cable to the packet-switched network equipment.

Connecting to Ethernet-based (Out-of-Band) Control Station

The ACE-3600 Ethernet interface terminates in an 8-pin RJ-45 connector (for connector pinouts, see *Appendix A*). The Ethernet (100BaseTX) port can be used for out-of-band management access.

➤ To connect the Ethernet control interface:

1. Connect one end of an Ethernet cable (not supplied) to the control device or the network management station's hub.
2. Connect the other end of the Ethernet cable to the RJ-45 connector designated ETH in ACE-3600.

Connecting to an RS-232 Control Terminal

ACE-3600 can also be managed via the RS-232/V.24 (DCE) terminal control port, which has an 8-pin RJ-45 connector.

➤ To connect the terminal control cable:

1. Connect the DB-9 end of the RS-232 adapter cable (supplied) to the 9-pin DTE connector of the management station.
2. Connect the RJ-45 end of the adapter cable to the RJ-45 connector designated CONTROL in ACE-3600.

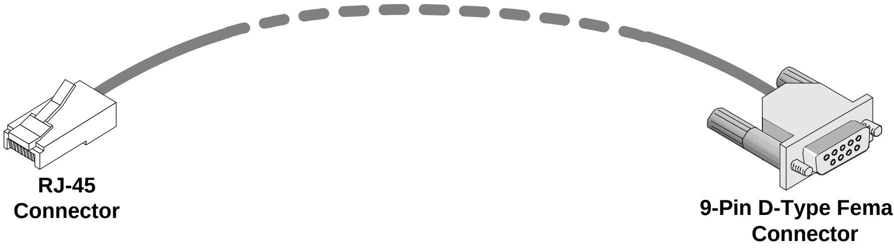


Figure 2-6. RJ-45 to DB-9 Adapter Cable (CBL-RJ45/D9/F/STR)

2.7 Connecting to the Clock Source

ACE-3600 can be connected to a clock source via its dedicated clock port. The station clock port is an RJ-45, E1/T1-based port that receives data for timing purposes only (without processing the incoming data). Although ACE-3600 can receive its required clock source from any of its STM-1/OC-3c ports (as explained in *Chapter 1* and *Appendix D*), the dedicated station clock port provides a strain-free and reliable channel for the clock source.

The station clock source can also be shared with other devices if those are connected to it via an E1/T1 compliant cable, using special cable wiring that carries the clock signal to the other devices. For more information about this sharing connection option, refer to *Appendix A*.

Connecting to a Balanced E1 or T1 Clock Source

➤ To connect ACE-3600 to a dedicated clock source:

- Connect E1/T1 compliant cable to the clock source unit/device on one end, and to the RJ-45 connector designated STATION CLK on the ACE-3600 end.

Connecting to an Unbalanced E1 Clock Source

ACE-3600 can be connected to an unbalanced E1 clock source via the CBL-RJ45/2BNC/E1 adapter cable. ACE-3600 automatically adjusts the line impedance to 75Ω once the unbalanced E1 (120Ω) connection is detected.

➤ To connect the unbalanced E1 interface:

1. Connect the RJ-45 connector of the adapter cable to the station clock port.
2. Connect the external clock source to the receive (RX, green) coaxial connector of the adapter cable marked "←" (see *Figure 2-7*).
3. Connect the clock sharing cable (optional) to the transmit (TX, red) coaxial connector of the adapter cable marked "→".

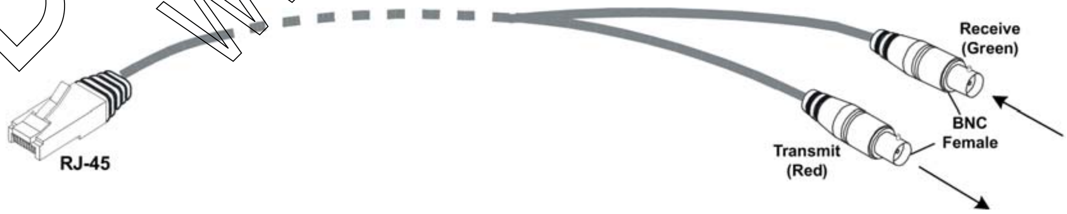


Figure 2-7. RJ-45 to BNC Adapter Cable

Note *Use only the RAD adapter cable (CBL-RJ45/2BNC/E1/X). Other adapter cables may not have the required wiring for detecting the current of the unbalanced interface.*

2.8 Connecting to Power

ACE-3600 has either AC or DC power supply (as ordered), provided via two hot-swappable power supply units. A power cable is supplied with the unit.

Removing/Installing the Hot-Swappable Power Supply Units

ACE-3600 allows its power supply units to be replaced in the field whenever necessary.

➤ To remove a hot-swappable power supply unit:

Warning

To prevent electrocution, DISCONNECT THE POWER SUPPLY CABLE FROM THE POWER SUPPLY UNIT before the removal.

1. Using a flathead screwdriver, unscrew the two tightening screw that secure the unit to the chassis.
2. Carefully pull and remove the power supply unit from the chassis.

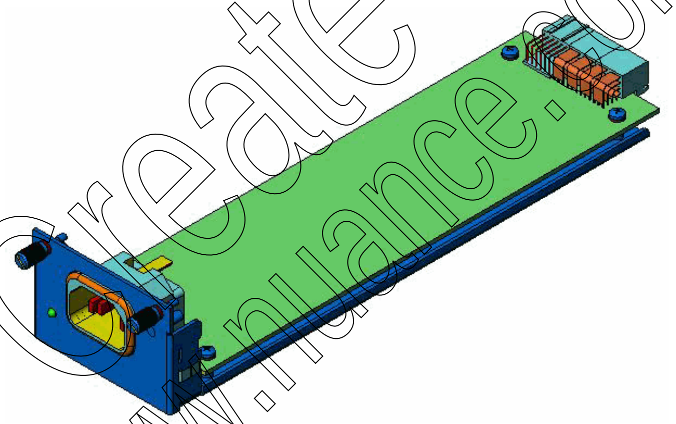


Figure 2-8. AC Power Supply Unit (Schematic Illustration)

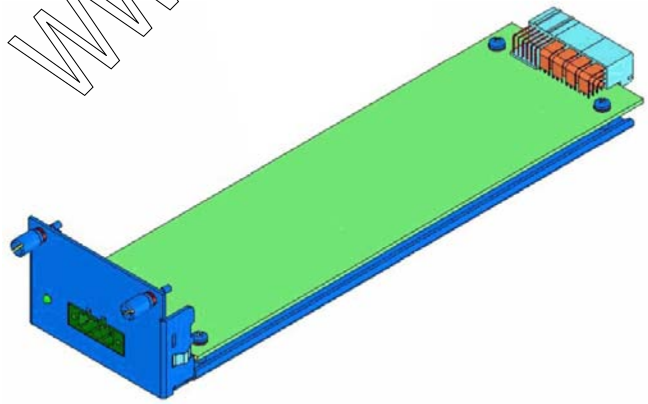


Figure 2-9. DC Power Supply Unit (Schematic illustration)

Warning

To prevent electrocution, KEEP THE POWER SUPPLY CABLE DISCONNECTED FROM THE POWER SUPPLY UNIT as long as the unit is not fully installed.

➤ To install the hot-swappable power supply unit:

Caution Do not install the ACE-3600 power supply units in other products. The power supply units are intended solely for ACE-3600.

1. Carefully slide the new PS unit into its slot until the unit's rear connector engages the mating connector on the backplane, and the PS unit fits into place.
2. Using a flathead screwdriver, secure the PS unit with the two tightening screws.

Connecting to AC Power

AC power is supplied to ACE-3600 via a 3-prong plug. AC power should be supplied through the 1.5m (5 ft) standard power cable terminated by a 3-prong plug. The cable is provided with the unit.

Two power cables may be connected to the unit simultaneously.

⚠ ***Warning***

Before switching on this unit and connecting or disconnecting any other cable, the protective earth terminals of this unit must be connected to the protective ground conductor of the mains power cord. If you are using an extension cord (power cable) make sure it is grounded as well.

⏚ **Any interruption of the protective (grounding) conductor (inside or outside the instrument) or disconnecting of the protective earth terminal can make this unit dangerous. Intentional interruption is prohibited.**

The line fuse is located in an integral-type fuse holder located on the rear panel. Make sure that only fuses of the required rating, as marked on the rear panel, are used for replacement. Do not use repaired fuses or short-circuit the fuse holder. Always disconnect the mains cable before removing or replacing the fuse. Whenever it is likely that the fuse protection has been damaged, make the unit inoperative and secure it against unintended operation.

DO NOT INSTALL AC and DC power supplies together in the same unit.

➤ To connect ACE-3600 to AC power:

1. Connect the power cable to the AC power connector on the unit's front panel.
2. Connect the power cable to the mains outlet.

   The unit is turned on automatically upon connection to the mains.

Connecting to DC Power

➤ To connect ACE-3600 to DC power:

- Refer to the DC power supply connection supplement, located on the Technical Documentation CD or at the back of the official printed version of this manual. Also, refer to the safety instructions at the beginning of this document.

Table 2-2. Typical and Maximum DC Power Consumption

Condition/HW Part	Typical DC Power	Maximum DC Power
ACE-3600 with two main modules (main cards)	65W	75W
ACE-3600 main module in Standby mode	24W	30W
ACE-3600 interface module (STM-1 x 4 ; GbE x 1)	10W	12W
Fan module	4W	6W
Management module	1.5W	2W

Chapter 3

Operation

This chapter describes the following:

- Power-on and power-off procedures
- Description of the ACE-3600 front panel LED indicators and their function
- Default settings
- Configuration alternatives – the different management access options available for ACE-3600
- Menu navigation.

For a detailed explanation of the options and parameters in the management menus, see *Chapter 4*.

3.1 Turning On the Unit

➤ **To turn the ACE-3600 unit on:**

- Connect the unit's power cable(s) to the mains.

  The power supply indicator lights up and remains on as long as ACE-3600 receives power.

Warning

ACE-3600 includes Class 1 lasers. For your safety:

- Do not look directly into the optical connectors while the unit is operating. The laser beams are invisible.
- Do not attempt to adjust the laser drive current.

Once turned on, ACE-3600 requires no operator attention, with the exception of occasional monitoring of front panel indicators. Intervention is required only when:

- ACE-3600 must be configured to its operational requirements
- The alarm LED indicator indicates an alarm
- Diagnostic tests are performed.

3.2 LED Indicators

The front panel of an assembled ACE-3600 includes a series of LED indicators that show the current operating status of the unit and its modules.

Figure 3-1 shows the ACE-3600 front panel:

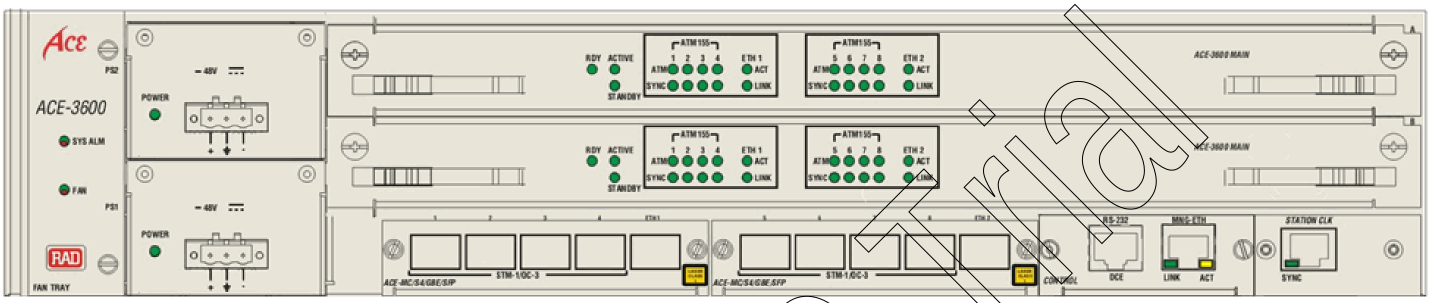


Figure 3-1. ACE-3600 Front Panel

The following list summarizes the function of all LED indicators in ACE-3600:

Hot-Swappable Power Supplies	*POWER (green/red)*	Green: power supply is OK Red: power supply failure
Fan Tray	*SYS ALM (green/red)*	Green: no system alarm is detected Red: at least one system alarm has been detected
	FAN (green/red)	Green: all the fans are working properly Red: at least one fan is not working properly
Main Module	*RDY (green)*	On: self-test has been completed successfully Blinking: self-test has failed
	ACTIVE (green)	On: this main module is in Active mode Off: this main module is not in Active mode
	STANDBY (green)	On: this main module is in Standby mode Off: this main module is not in Standby mode
	ATM-155 SYNC 1–4, 5–8 (green)	On: the port's physical layer is synchronized Off: the port's physical layer is not synchronized Blinking: RDI has been detected
	ATM-155 ATM 1–4, 5–8 (green)	On: ATM cells are being received or transmitted Off: ATM cells are not being received or transmitted

	ETH 1/2 LINK (green)	On: Gigabit Ethernet link is detected Off: Gigabit Ethernet link is not detected
	ETH 1/2 ACT (green)	On: Frames are being received or transmitted Off: Frames are not being received or transmitted
MNG-ETH Control Port	*LINK (green)*	On: Ethernet link is detected Off: Ethernet link is not detected
	ACT (yellow)	On: ETH frames are being received or transmitted Off: ETH frames are not being received or transmitted
Station Clock Port	*SYNC (green)*	On: E1/T1 physical layer is synchronized Off: E1/T1 physical layer is not synchronized

3.3 Default Settings

Login Names

There are three levels of user access rights:

- su – can perform all the activities supported by the ACE-3600 management facility
- tech – can monitor the ACE-3600 operation and initiate diagnostic tests
- user – can monitor the ACE-3600 operation.

The default passwords for these access levels is “1234”. For backward compatibility reasons, the “xxxxxxxxxx” (10 times "x") password is also used as a default password.

Note *For security reasons, it is recommended to periodically change your password, as explained in Chapter 4.*

Configuration Defaults

ACE-3600 comes with factory defaults. It is possible, however, to change these defaults and save any current configuration as user default configuration, as explained in *Saving/Deleting the Default Configuration File* in Chapter 4.

Additional parameters suggest default values that become active only when saving the configuration.

In some cases, values must be entered manually, otherwise the configuration cannot be completed.

3.4 Configuration Alternatives

ACE-3600 can be managed and configured using the following user interface alternatives:

- *Working with an ASCII-based Control Terminal*
- *Working with ConfiguRAD*
- *Working with RADview-EMS.*

Working with an ASCII-based Control Terminal

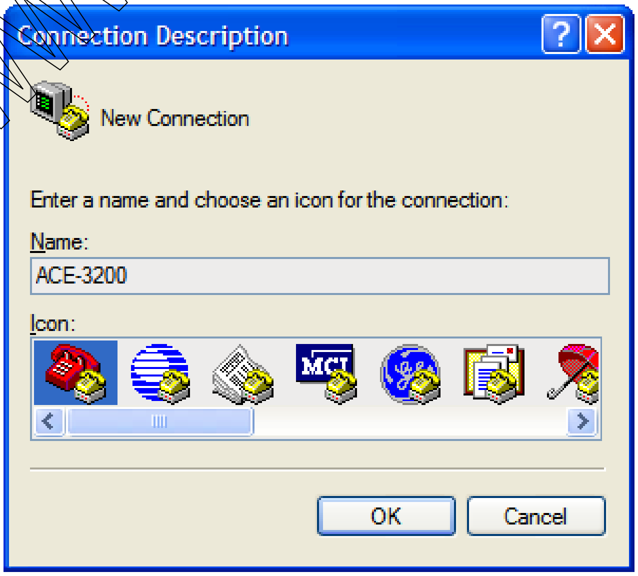
Any standard ASCII terminal or a PC station (running a terminal emulation application), which is equipped with a V.24/RS-232 communication interface, can be used to set up and configure ACE-3600. You can connect the terminal/station directly to the unit's control port for establishing out-of-band management.

The terminal screens interface (see *Figure 3-7*) however, can also be used for inband management (for example, via Telnet).

➤ To set up terminal control using Windows HyperTerminal:

1. Make sure that all the cables are properly connected (for more information, refer to *Chapter 2*).
2. Turn on the control terminal or start the PC terminal emulation (in Windows XP: click Start > All Programs > Accessories > Communications > HyperTerminal to create a new terminal connection.

   The Connection Description dialog box is displayed.



Connection Description

New Connection

Enter a name and choose an icon for the connection:

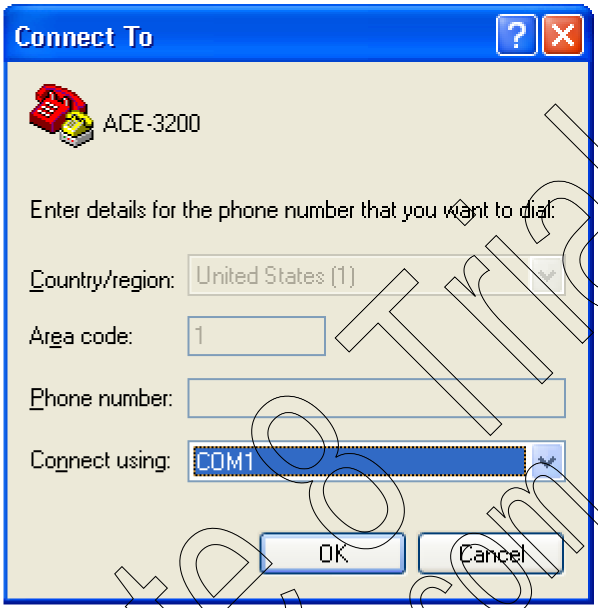
Name: ACE-3200

Icon:

Figure 2. Windows HyperTerminal, Connection Description Dialog Box

3. Enter description for the terminal connection.
4. Select an icon to represent the terminal connection.

   The Connect To dialog box is displayed.



Connect To

ACE-3200

Enter details for the phone number that you want to dial:

Country/region: United States (1)

Area code: 1

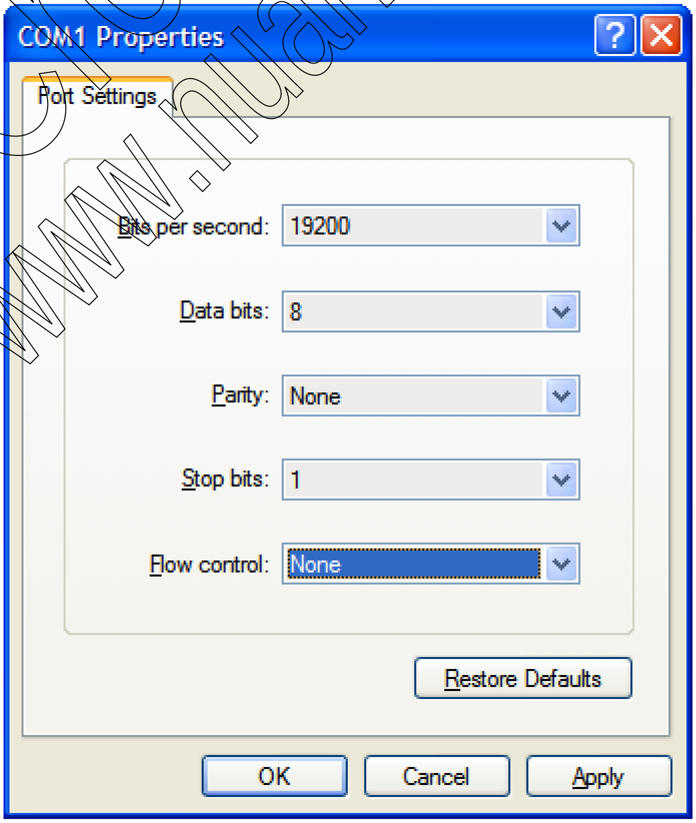
Phone number:

Connect using: COM1

Figure 3. Connect To Dialog Box

5. Select a PC COM port to be used to communicate with ACE-3600.

   The COM Properties dialog box is displayed.



COM1 Properties

Port Settings

Bits per second: 19200

Data bits: 8

Parity: None

Stop bits: 1

Flow control: None

Figure 4. COM1 Properties Dialog Box

6. Configure the communication port parameters to a baud rate of 19,200 bps, 8 bits/character, 1 stop bit, no parity and no flow control.

   The main HyperTerminal window is displayed.

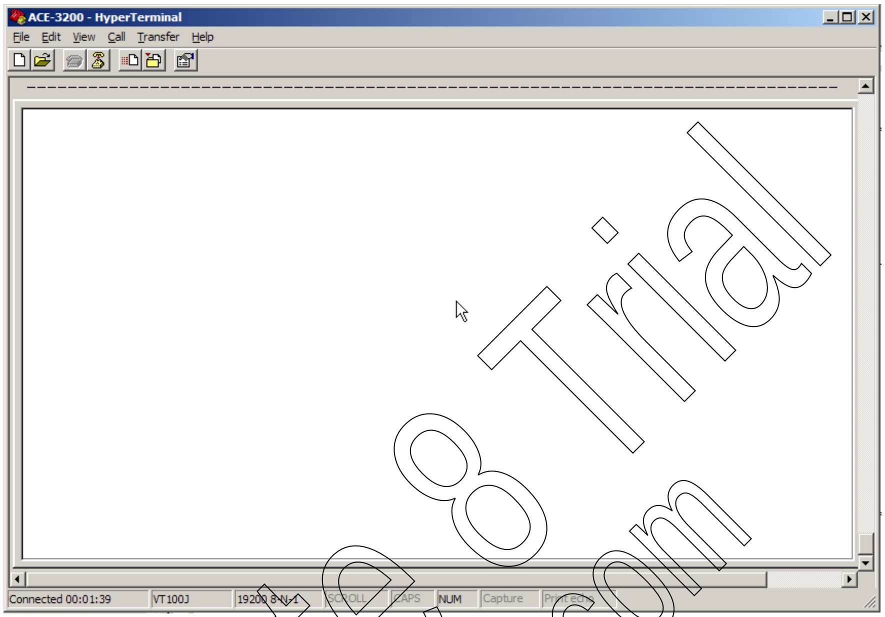


Figure 5. Main HyperTerminal Window

7. Set the terminal emulation to VT100 (Properties› Settings).
8. If you are using the MS-Windows HyperTerminal, set the terminal mode to the 132-column mode for optimal view of system menus: (Properties› Settings› Terminal Setup› 132 column mode).
9. Power-up the unit by connecting the power cable.

   The ACE-3600 self-test results are displayed on the terminal screen. The RDY LED on the left-hand side of the front panel should be green at the end of the test.

Logging In via the Terminal/Telnet Interface

To access the unit's management/configuration/monitoring options, you must log in.

➤ To log in:

1. While connected to the terminal, press ‹ESC› to access the login screen.

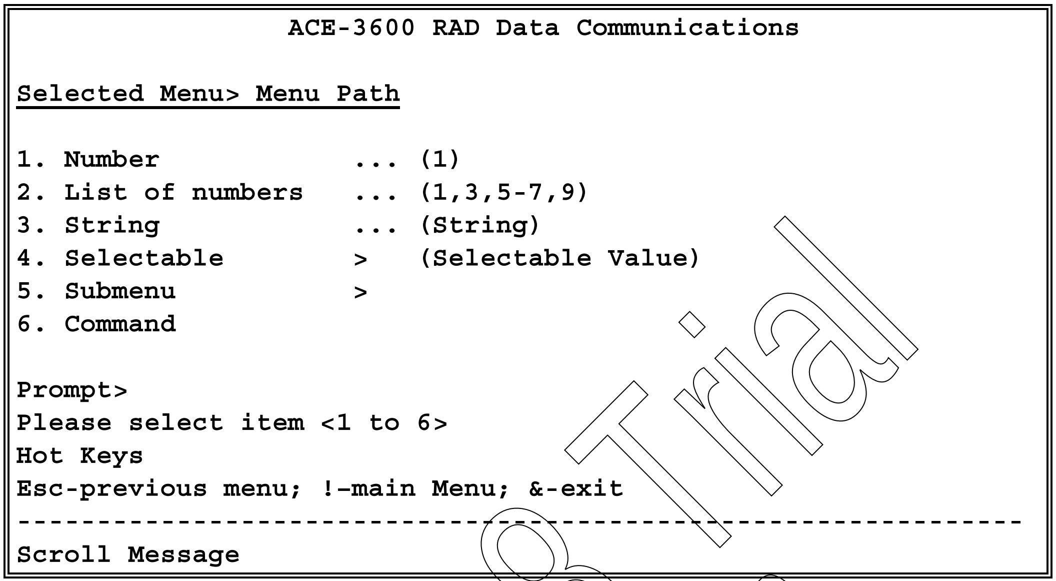
   The following login screen appears:

```
User name      >su
Password       >1234
```

Figure 3-6. Terminal Login Screen

2. Enter your user name (su, tech or user) and your password when prompted. The factory set password is 1234 or xxxxxxxxxx.
3. If you enter an invalid password during three consecutive attempts, the system becomes inaccessible for 15 minutes.

ASCII Screen Format



```
                      ACE-3600 RAD Data Communications

Selected Menu> Menu Path

1. Number               ... (1)
2. List of numbers      ... (1,3,5-7,9)
3. String               ... (String)
4. Selectable           >   (Selectable Value)
5. Submenu              >
6. Command

Prompt>
Please select item <1 to 6>
Hot Keys
Esc-previous menu; !-main Menu; &-exit
-------------------------------------------------------------
Scroll Message
```

Figure 3-7. Terminal Screen Format

In this manual, the parameters appearing on menu screens are described in tables that follow the screen figures. A typical parameters table contains the following three columns:

Parameter Descripti	on	Possible Values

- **Parameter** – specifies the parameter appearing on the screen, including submenus, where applicable.
- Description – describes the purpose or functionally of the parameter.
- Possible Values – provides all the possible values for the parameter, or a range of values, including the default value, if applicable.

Only the user-relevant information is shown in the tables. For example, see *Table 3-2* on page *3-14*.

Principles of Navigation

The main menu categories (see *Figure 3-12* on page *3-14*) lead to submenus and items with selectable parameters (which are explained in *Chapter 4 – 'Configuration'* and *Chapter 6 – 'Statistics, Diagnostics and Troubleshooting'*).

All terminal screens are titled “ACE-3600 – RAD Data Communications”, while the current screen name and path is underlined. The underlined screen name is identical to the item selected in the previous menu.

At any given time, you can press **!** (SHIFT-1) to return the main menu. For more information, refer to *Menu Paths (ASCII or ConfiguRAD)* on page *3-13*.

Hot Keys

Table 3-1 summarizes the functionality of hot keys (keyboard shortcuts) that are available in the different menu screens.

Table 3-1. Hot Keys

Hot Key	Functionality
P/p	Previous menu page (for long menus that exceed a page). Scrolling up for menu items
N/n	Next menu page (for long menus that exceed a page). Scrolling down for menu items
F/f	Forward (next entry) – stay in same menu with next instance (Port) on axis Y
B/b	Backward (previous entry) – stay in same menu with previous instance (Port) on axis Y
CTRL F/f	Forward (next entry) – stay in same menu with next instance (Interval) on axis X
CTRL B/b	Backward (previous entry) – stay in same menu with previous instance (Interval) on axis X
A,a	Add a new entry and display its parameters
R,r	Remove the entry which parameters are currently displayed
G, g	Get (entry), Go
←	Skip left (move to the previous cell)
→	Skip right (move to the next cell)
↓	Skip down (move to the down cell)
CTRL R/r	Scroll right
CTRL L/l	Scroll left
CTRL D/d	Scroll down
CTRL U/u	Scroll up
?	Display help (if available for the specific screen)
TAB	Select next changeable cell (skip read-only cells)
G,g	Select specified cell – row_num, col_num
A,a	Add table entry
R,r	Remove table entry
C,c	Clear all table entries
M,m	Display selected table entry as a menu
S,s	Save table session changes

Hot Key	Functionality
DEL	Clear currently typed string
ESC	Previous menu
!	Go to main menu
&	Exit from the menus; if user presses any key, LOGIN is displayed
@	Spread the messages scrolling area to full screen
$	Display history
#	Display previous command
+	Command filter start
-	Parameter start

Note *The* ***Save (S)*** *operation is essential for updating and applying configuration changes.*

Working with ConfiguRAD

ConfiguRAD is a Web-based remote access terminal management software, embedded within ACE-3600. It provides a user-friendly Web interface for configuring, collecting statistics and monitoring the ACE-3600 unit. It provides the same options that are available via the terminal interface.

Logging In via a Web Browser

Supported Web Browsers

ConfiguRAD allows you to access and control the unit via an Internet connection, and supports the following Web browsers:

- Internet Explorer 6.0 or higher, running on Windows 98, Windows 2000 or Windows XP.
- Netscape Communicator 7.1 or higher, running on Windows NT or Unix.

IP Address Configuration

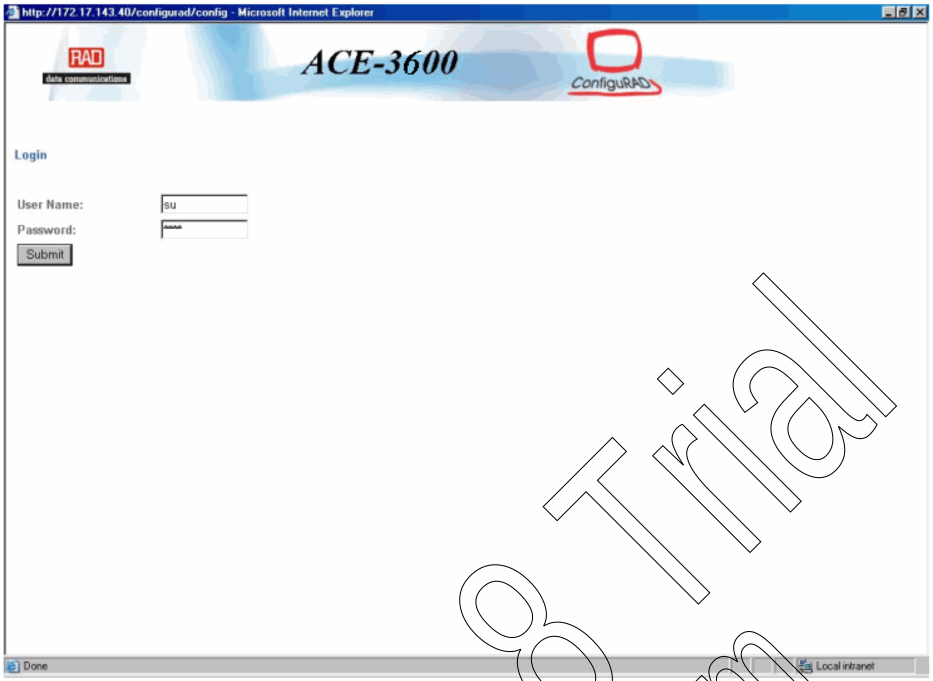
The remote Web login requires a pre-configured IP address for the ACE-3600 unit (host configuration). For more information, refer to *Chapter 4*.

Web Login Procedure

➤ To log in via a Web browser:

1. Connect Ethernet Port 1 to the LAN.
2. Open the Web browser.
3. Disable any pop-up blocking software, such as Google Popup Blocker.
4. In the address field of the browser, enter the IP address of the ACE-3600 unit using the following format: http:// (IP address) and then press <Enter> to command the browser to connect ('IP address' stands for the actual ACE-3600 IP address which has to be assigned via an ASCII terminal).
5. After the opening window is displayed, click LOGIN.
6. Enter your user name and password in the appropriate fields (see *Figure 3-8*).

   The Main menu is displayed (see *Figure 3-9*).



User Name: su
Password: ****

Figure 3-8. User Name and Password Entry Window

Navigating the ConfiguRAD Menus

The ConfiguRAD Web-based interface provides the same options that are available in the terminal control screens. The only difference between ConfiguRAD and the terminal screens is the GUI (Graphical User Interface).

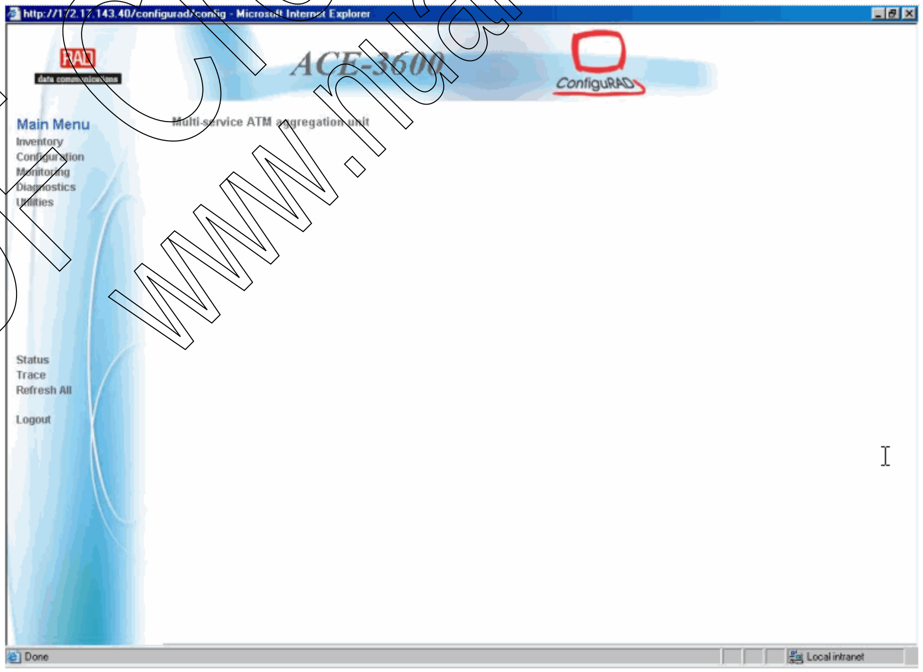


Figure 3-9. ConfiguRAD Main Menu Window

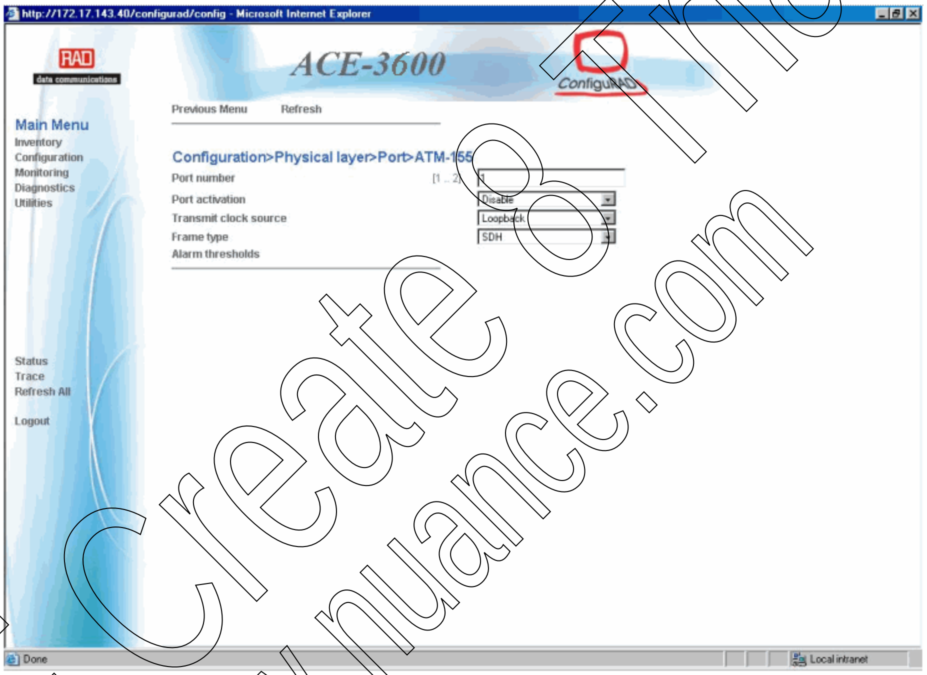
➤ To choose a ConfiguRAD option:

1. Click a link in the ConfiguRAD screen's left pane to display the submenu.

2. Once the target screen is displayed, select a value from the drop-down box or enter it in a text box.

At the left-hand bottom corner ConfiguRAD provides some assisting management tools:

- **Status** – shows the number of users currently managing ACE-3600
- **Trace** – opens an additional pane for system messages, progress indicators (ping, software and configuration file downloads) and alarms. It is recommended to keep the trace pane open all the time.
- **Refresh All** – updates the displayed parameters by retrieving new information from the unit.



Configuration>Physical layer>Port>ATM-155

Port number [1 .. 2] 1
Port activation Disable
Transmit clock source Loopback
Frame type SDH
Alarm thresholds

Figure 3-10. ConfiguRAD Port Configuration Window

Working with RADview-EMS

RADview-EMS is a user-friendly and powerful SNMP-based element management system (EMS), used for planning, provisioning and managing heterogeneous networks. RADview-EMS provides a dedicated graphical user interface for monitoring RAD products via their SNMP agents. RADview-EMS for ACE-3600 is bundled in the RADview-EMS/NGN package for PC (Windows-based) or Unix.

For more details about this network management software, and for detailed instructions on how to install, set-up and use RADview – refer to the RADview-EMS/NGN User's Manual, located on the Technical Documentation CD or on RAD's Web site via the Partners page.

3.5 Menu Paths (ASCII or ConfiguRAD)

Once you have logged-in, navigate the ACE-3600 menus to set and view the unit's configuration parameters, and to perform other essential operations.

Main Menu Paths

Figure 3-11 illustrates the main categories that are available from the main menu.

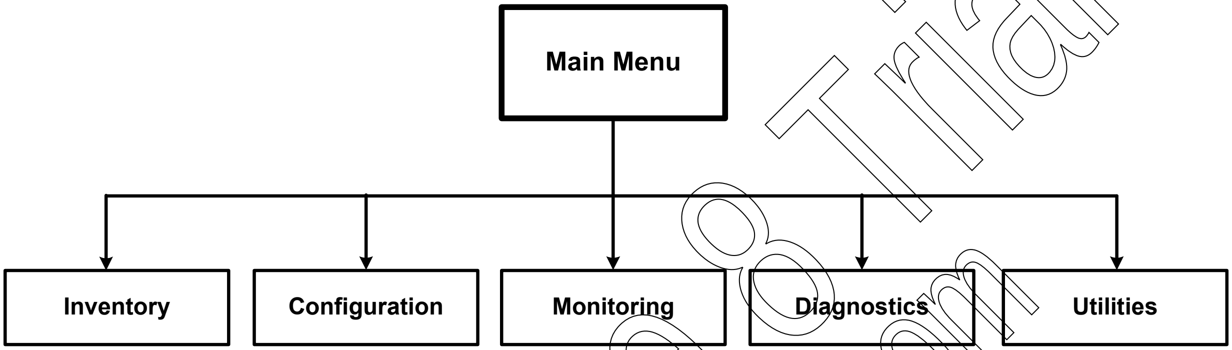
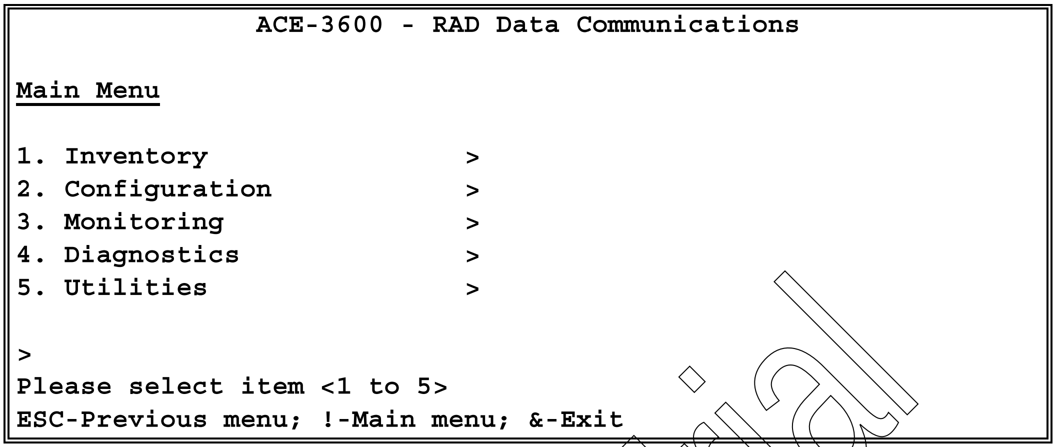


Figure 3-11. Main Menu Tree

Figure 3-12 shows the actual main menu in an ASCII terminal screen. All system configuration and control functions are accessed via this menu.

The main menu options are:

Inventory (type 1) View	system information, HW/SW versions and HW configuration
Configuration (type 2)	Set and configure all the parameters required for the operation of ACE-3600
Monitoring (type 3)	Monitor system performance and statistics
Diagnostics (type 4)	Perform diagnostics
Utilities (type 5)	Upload/download application files, configuration files and backup files



```
                    ACE-3600 - RAD Data Communications

Main Menu

1. Inventory                  >
2. Configuration              >
3. Monitoring                 >
4. Diagnostics                >
5. Utilities                  >

>
Please select item <1 to 5>
ESC-Previous menu; !-Main menu; &-Exit
```

Figure 3-12. Main Menu (Terminal Screen)

Table 3-2. Main Menu Reference Table

Parameter Descripti	on	Reference
Inventory	Displays the unit's hardware and software versions, along with description of major components	Refer to *Section 4.4* in Chapter 4
Configuration	Submenu providing access to the configuration of system, physical level and logical level parameters	Refer to *Chapter 4*
Monitoring	Submenu providing access to monitoring of performance and statistics	Refer to *Chapter 6*
Diagnostics	Submenu providing access to diagnostics and troubleshooting	Refer to *Chapter 6*
Utilities	Submenu providing access to utilities such as uploading /downloading configuration files from/to the unit	Refer to *Section 4.4* in Chapter 4

Configuration Menu Paths

The following figure summarizes the paths available in the configuration process:

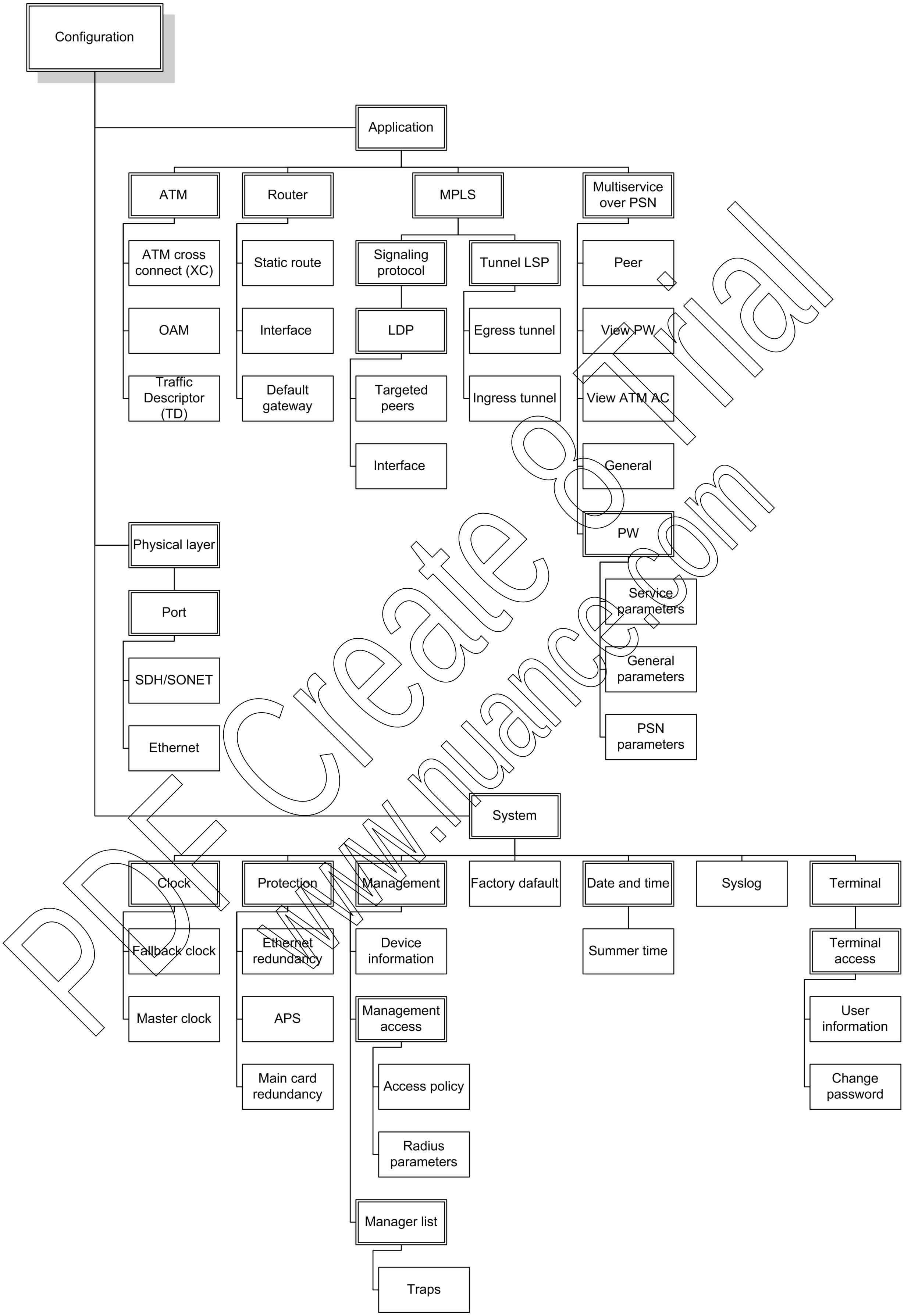


Figure 3-13. Configuration Menu Paths

Utilities Menu Paths

The following figure summarizes the paths available for the additional tasks and options:

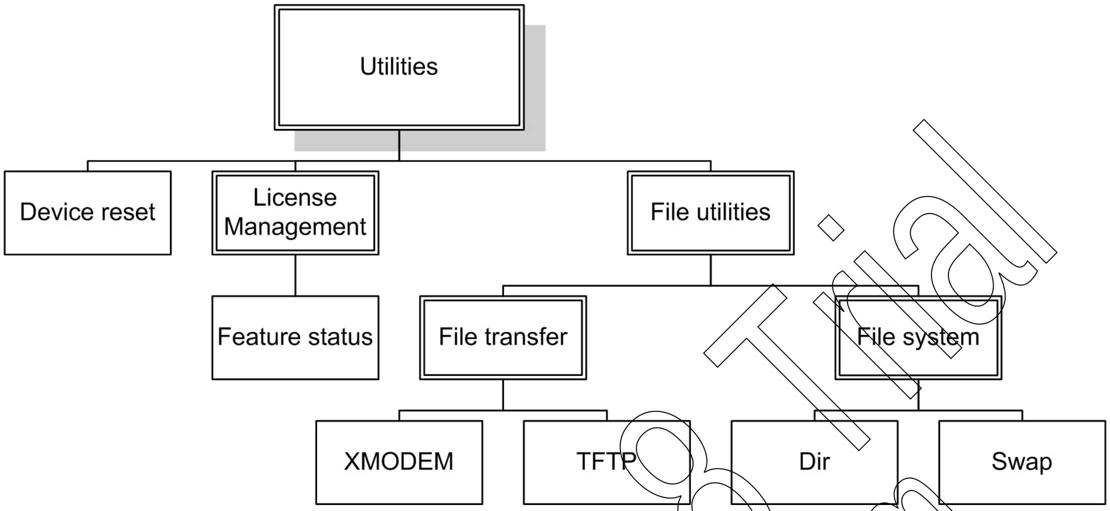


Figure 3-14. Utilities Menu Paths

Diagnostics Menu Paths

The following figure summarizes the paths available for the diagnostics options:

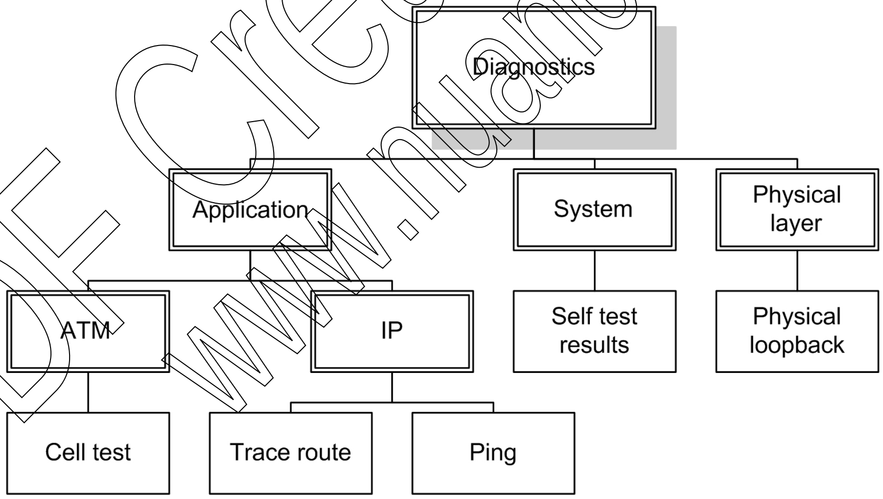


Figure 3-15. Diagnostics Menu Paths

Monitoring Menu Paths

The following figure summarizes the paths available for the monitoring options:

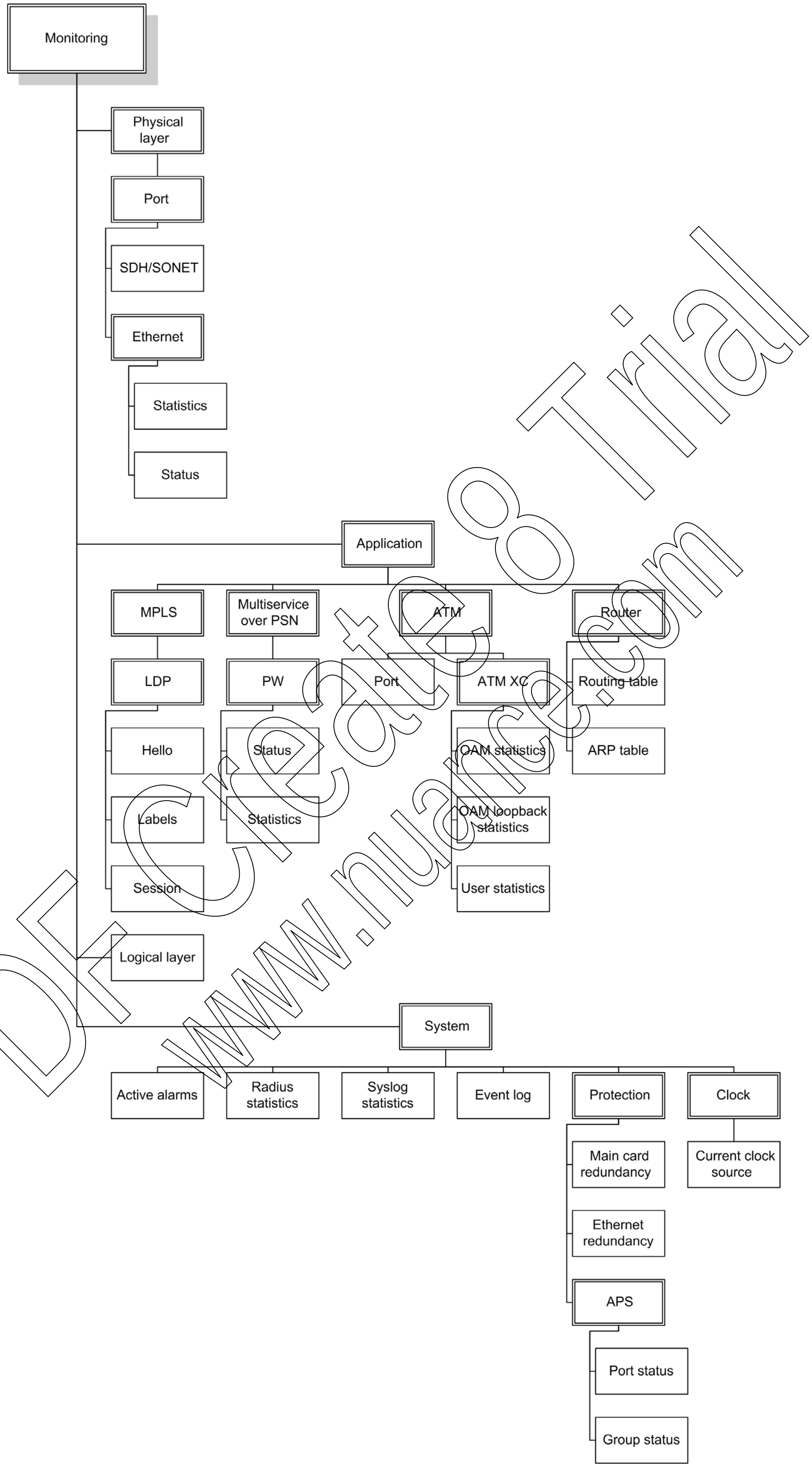


Figure 3-16. Monitoring Menu Paths

3.6 Turning Off the Unit

➤ To turn off the ACE-3600 unit:

- Disconnect the power cord from the power source.

Chapter 4

Configuration

This chapter explains in detail the different configuration options available for ACE-3600.

4.1 Configuration Sequence

Manual Configuration

The initial configuration of ACE-3600 consists of three main configuration stages (assuming there are no ready-made configuration files for download):

1. Configuring for Management (see *Section 4.2*) – Setting initial system parameters that are required for enabling remote/local management access to the unit. This includes:
   - Configuring the terminal control
   - Entering device information, router parameters, authorized managers, and management access definitions
   - Setting the date and time – to allow accurate logging of system events
   - Configuring the system log (Syslog) – to allow logging/sharing of system events on a server.
2. Configuring for Operation (see *Section 4.3*) – Setting the parameters required for functioning in the network application:
   - Configuring the physical layer parameters
   - Configuring the system/port redundancy features
   - Defining the master and fallback clock
   - Configuring the application parameters, which include ATM, bridge, router interface, remote peers (including static routes if necessary), MPLS, and multiservice over PSN parameters.

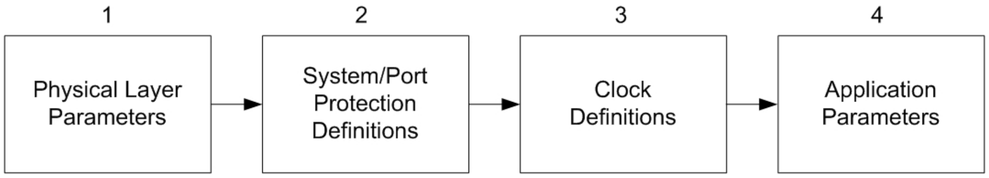


Figure 4-1. Configuring the Unit for Operation

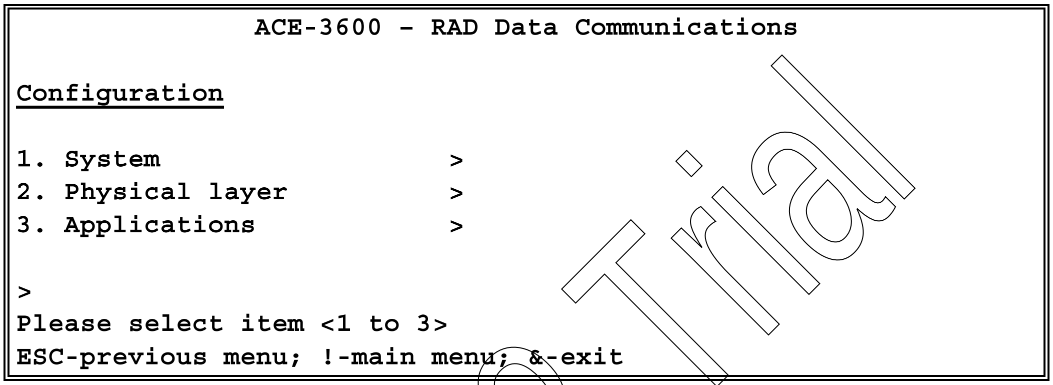
3. Additional Tasks (see *Section 4.4*) – Displaying the inventory, resetting the unit and managing the file system.

All configuration options are available from the Configuration menu.

➤ To access the Configuration menu:

- From the main menu, select **Configuration**.

  The Configuration menu is displayed.



```
                    ACE-3600 - RAD Data Communications

Configuration

1. System                    >
2. Physical layer            >
3. Applications              >

>
Please select item <1 to 3>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-2. Configuration Menu

Preset Configuration

You can download ready-made configuration files containing the full configuration of the unit, provided a configuration was already performed and saved on another ACE-3600 unit.

For more information about downloading a preset configuration, see *Loading a Preset Configuration*.

4.2 Configuring for Management

Before ACE-3600 can work in the intended application, several key parameters must be set in order to allow normal operation and management access. This stage includes:

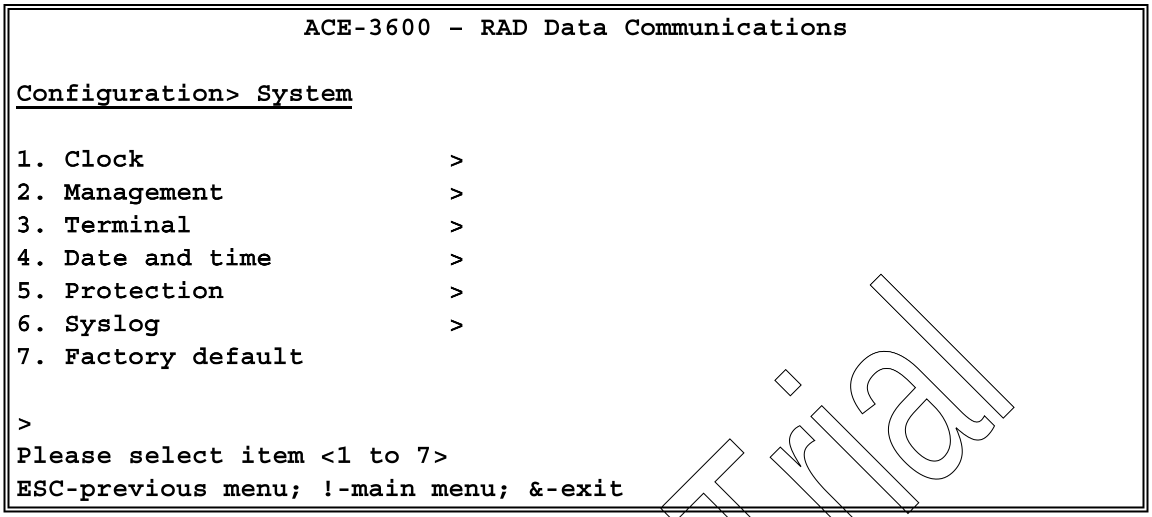
- *Configuring the Terminal Control*
- *Configuring Out-Of-Band Ethernet Control*
- *Setting Management Parameters*
- *Setting the Date and Time*
- *Setting the Syslog Parameters*.

These functions are available from the System menu.

➤ To access the System menu:

- From the Configuration menu, select System.

  The System menu is displayed.



```
                        ACE-3600 - RAD Data Communications

Configuration> System

1. Clock                    >
2. Management               >
3. Terminal                 >
4. Date and time            >
5. Protection               >
6. Syslog                   >
7. Factory default

>
Please select item <1 to 7>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-3. System Menu

Table 4-1. System Menu Parameters

Parameter Description		Possible Values
Clock	Access the system's timing synchronization definitions (ATM/PSN clock options)	Refer to *Setting the Clock*
Management	Access the general management parameters	Refer to *Setting Management Parameters*
Terminal	Access the terminal control parameters	Refer to *Configuring the Terminal Control*
Date and time	Access the date and time definition	Refer to *Setting the Date and Time*
Protection	Access the port protection (APS) or main module (main card) redundancy options	Refer to *Setting the Protection Parameters*
Syslog	Access the Syslog options for logging/sharing system events on a server	Refer to *Setting the Syslog Parameters*
Factory default	Resets all configuration parameters to their factory-default settings	Refer to *Resetting the Unit to Configuration Defaults*

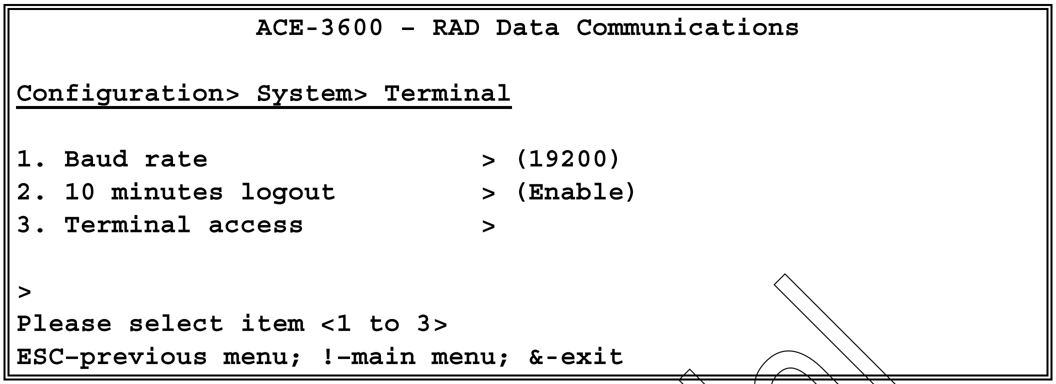
Configuring the Terminal Control

The terminal control parameters determine the control port's baud rate, password used for each control session, and availability of the fixed security timeout.

➤ To access the Terminal menu:

- From the System menu (see *Figure 4-3*), select **Terminal**.

  The Terminal menu is displayed.



```
                    ACE-3600 - RAD Data Communications

Configuration> System> Terminal

1. Baud rate                     > (19200)
2. 10 minutes logout             > (Enable)
3. Terminal access               >

>
Please select item <1 to 3>
ESC-previous menu; !-main menu; &-exit
```

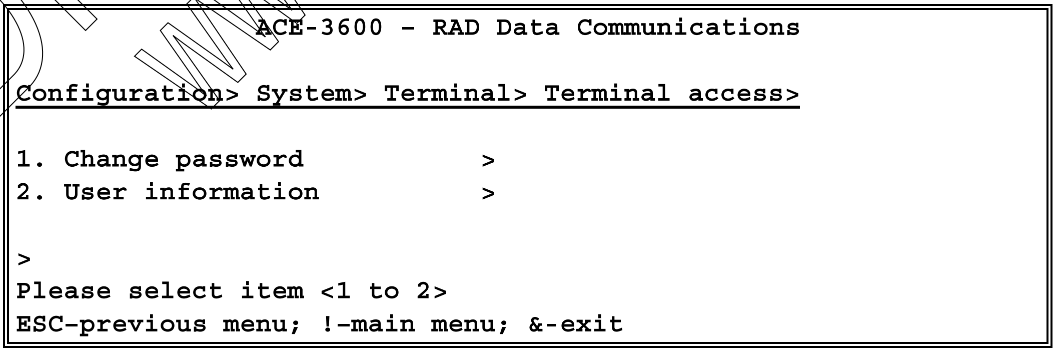
Figure 4-4. Terminal Menu

Table 4-2. Terminal Menu Parameters

Parameter	Description	Possible Values
Baud rate	Terminal baud rate in bits per second (bps)	9600, 19200, 38400, 57600 or 115200 Default: 19200
10 minutes logout	Automatic logout from terminal after 10 minutes of inactivity. ***Note:*** *This parameter does not affect Telnet and Web sessions; for these applications, timeout is always enabled.*	Enable Disable Default: Enable
Terminal access	Terminal access options	See *Using the Terminal Access Options* below

Using the Terminal Access Options

The terminal access options allow you to change user passwords and view user information.



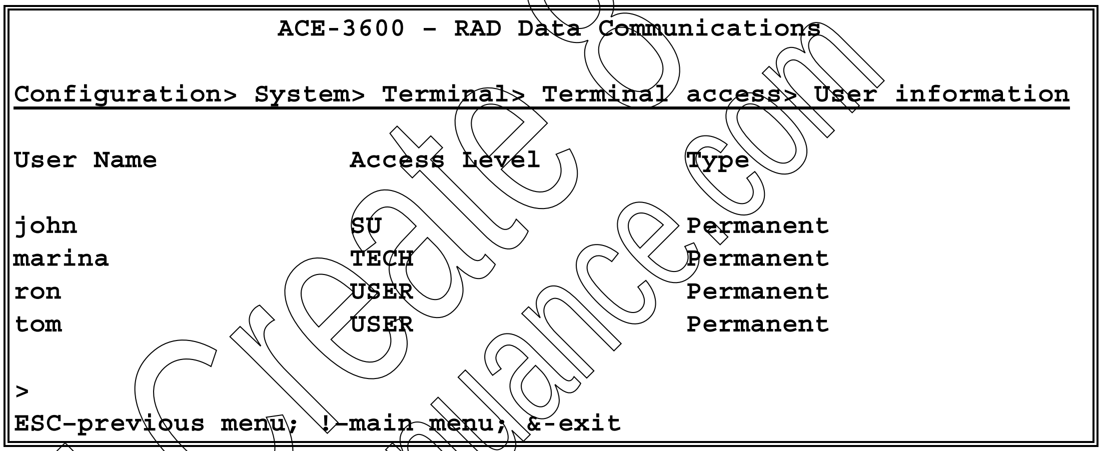
```
                    ACE-3600 - RAD Data Communications

Configuration> System> Terminal> Terminal access>

1. Change password               >
2. User information              >

>
Please select item <1 to 2>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-5. Terminal Access Menu

Table 4-3. Terminal Access Menu Options

Parameter	Description	Possible Values
Change password	Allows you to change your user password.	Refer to *Changing the Password*.

Parameter	Description	Possible Values
	Note: *Depending on the user level, “su” user can change passwords for all user levels; “tech” and “user” may change it only their own passwords.*	
User information	Displays the user name, access level and type of all registered users, in three columns: • User Name – the alphanumerical strings of the user name • Access Level – SU, TECH or USER. • Type – the user's type. Currently, ACE-3600 supports only permanent (non-dynamic) users.	See *Figure 4-6* below



```
                ACE-3600 - RAD Data Communications

Configuration> System> Terminal> Terminal access> User information

User Name                Access Level            Type

john                     SU                      Permanent
marina                   TECH                    Permanent
ron                      USER                    Permanent
tom                      USER                    Permanent

>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-6. Displaying User Information

Configuring Out-Of-Band Ethernet Control

If ACE-3600 is to be managed via an out-of-band LAN connection, the unit's dedicated Ethernet management port (MNG-ETH port) should be configured.

Note *The required parameters are already configured by default. For more information, see Configuring the Ethernet Ports.*

➤ To check/perform the management Ethernet port configuration:

1. From the Configuration menu, select **Physical Layer**.

   The Physical Layer menu appears (see *Figure 4-32*).

2. Select Port.

   The Port menu appears (see *Figure 4-33*).

3. Select Ethernet.

   The Ethernet menu appears (see *Figure 4-34*).

4. Check/enter the following parameters:

Table 4-4. Management Ethernet Port Configuration

Parameter Required	Value
Port number	ETH-MNG
Port activation	Enable
Auto negotiation	Disable
Default type	100BaseT Full Duplex

5. Press **S** to save.

   The unit's Ethernet management port is configured. The manager IP or the router interface must be set separately (for more information, see *Defining the IP Address of Network Managers* and *Configuring the Router Interface*).

Setting Management Parameters

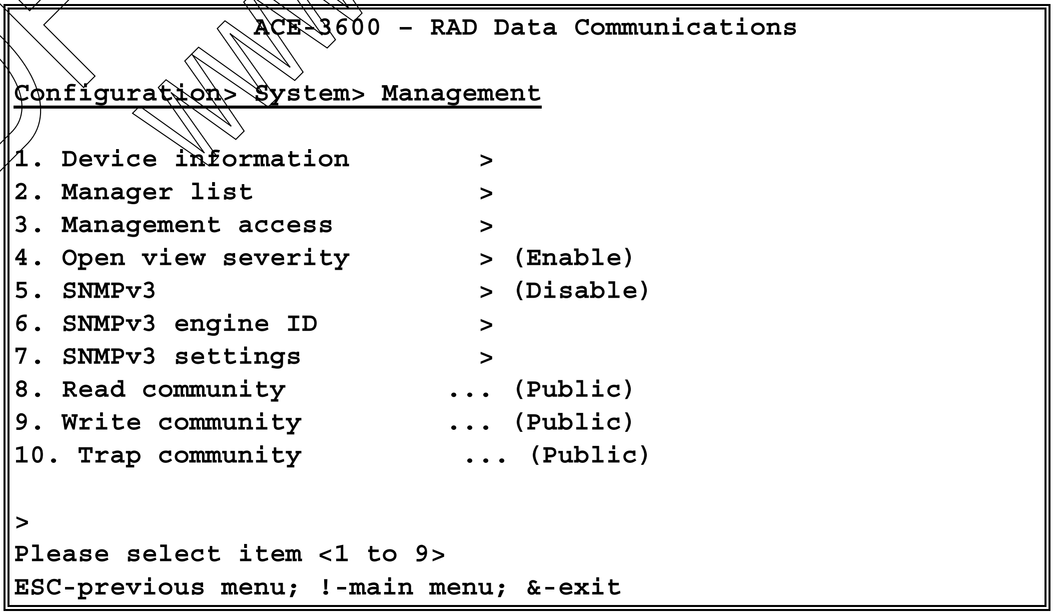
ACE-3600 can be managed by a network management station (NMS). In order to establish proper connection between the unit and the NMS, it is necessary to configure the router interface parameters, IP address of network managers, alarm traps, SNMPv3 parameters (if applicable) read/write communities, and define at least one network manager. In addition, you can view and edit the general device information.

All these functions are available from the Management menu.

➤ To access the Management menu:

- From the System menu (see *Figure 4-3*), select **Management**.

  The Management menu is displayed.



```
               ACE-3600 - RAD Data Communications

Configuration> System> Management

1. Device information          >
2. Manager list                >
3. Management access           >
4. Open view severity          > (Enable)
5. SNMPv3                      > (Disable)
6. SNMPv3 engine ID            >
7. SNMPv3 settings             >
8. Read community            ... (Public)
9. Write community           ... (Public)
10. Trap community            ... (Public)

>
Please select item <1 to 9>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-7. Management Menu

Table 4-5. Management Menu Parameters

Parameter Description		**Possible Values**
Device information	Submenu for entering device information	Refer to *Viewing Device Information* below
Manager list	Submenu for defining network managers	Refer to *Defining the IP Address of Network Managers*.
Management access	Submenu for defining management access	Refer to *Configuring Remote Management Access*.
Open view severity	Option for attaching OpenView severity to alarm traps	• Enable – OpenView severity will be attached to the alarm traps • Disable – OpenView severity will not be attached to the alarm traps Default: Disable
SNMPv3	Enable or disable the SNMPv3 functionality	Enable Disable Default: Disable
SNMPv3 engine ID	Submenu for configuring the SNMPv3 engine	Refer to *Configuring the SNMPv3 Parameters*
SNMPv3 settings	Submenu for configuring the SNMPv3 parameters; available only if the SNMPv3 functionality is enabled (see above)	Refer to *Configuring the SNMPv3 Parameters.*
Read community	String that defines the read community; available only if the SNMPv3 functionality is disabled	Up to 20 alphanumeric characters, case-sensitive Default: Public
Write community	String that defines the write community; available only if the SNMPv3 functionality is disabled	Up to 20 alphanumeric characters, case-sensitive Default: Public
Trap community	String that defines the trap community; available only if the SNMPv3 functionality is disabled	Up to 20 alphanumeric characters, case-sensitive Default: Public

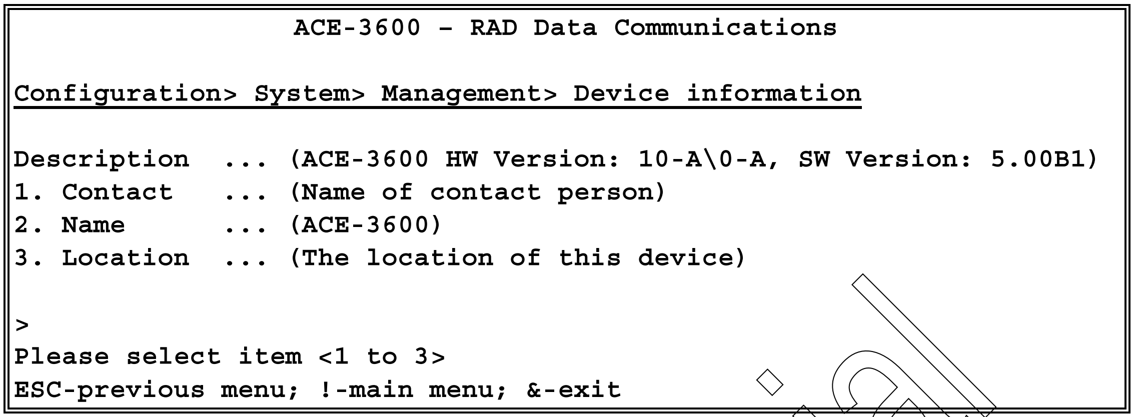
Viewing Device Information

The ACE-3600 management software allows you to assign a name to the unit, specify its location to distinguish it from the other devices installed in your system and assign a contact person.

➤ To access the Device Information menu:

- From the Management menu (see *Figure 4-7*), select Device Information.

The following information screen is displayed.



```
                    ACE-3600 - RAD Data Communications

Configuration> System> Management> Device information

Description  ... (ACE-3600 HW Version: 10-A\0-A, SW Version: 5.00B1)
1. Contact   ... (Name of contact person)
2. Name      ... (ACE-3600)
3. Location  ... (The location of this device)

>
Please select item <1 to 3>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-8. Device Information Menu

Table 4-6. Device Information Menu Parameters

Parameter Description		Possible Values
Description	A read-only string which displays the hardware and software revision information.	Alphanumerical version number using the XY-Z\Q-R (HW) and X.YZQR (SW) format, where: • X – major version number (1–9) • Y – minor version number (0–9) • Z – CSL number in the HW version (A–Z); or bug fixing number in the SW version (0–9) • Q – version number of the chassis in the HW version; or phase of the product in SW version (D – development; E – EOD; A – Alpha; B – Beta) • R – CSL number in the HW version (A–Z); or used in conjunction with Q to indicate a SW phase version (for example: A1 for first Alpha, B1 for first Beta, etc.)
Contact	Enter (type) the name of the contact person who will manage/monitor the unit, along with information of how to contact that person.	Up to 32 alphanumeric characters, case-sensitive. Default: "Name of contact person"
Name	Enter the actual name of the device, or the string attached to the OID excluding the prefix RAD.	Up to 12 alphanumeric characters, case-sensitive. Default: ACE-3600
Location	Enter the physical location of this node.	Up to 32 alphanumeric characters, case-sensitive Default: "The location of this device"

Defining the IP Address of Network Managers

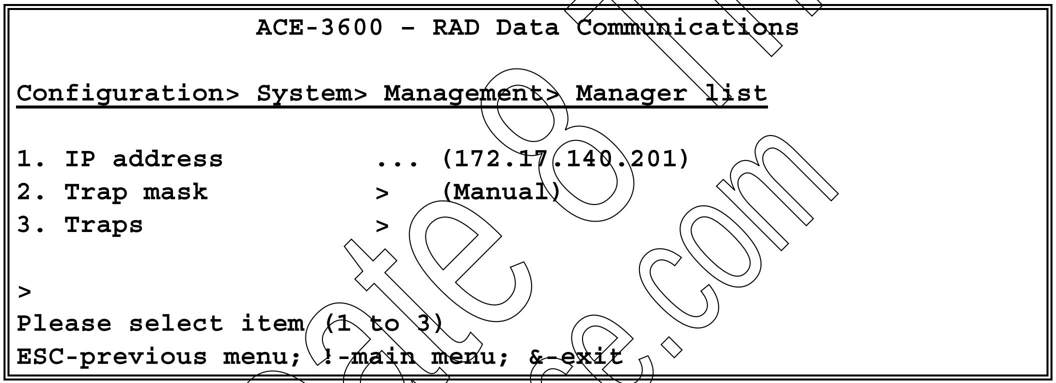
If ACE-3600 is to be managed via a network management station (NMS), it is necessary define the location of network managers who can access the unit via inband or out-of-band management channels. Managers are defined via the Manager List menu.

Note *If the unit is not intended for NMS management, a static route definition is sufficient (for more information, see Setting the Static Route Parameters).*

➤ To access the Manager List menu:

- From the Management menu (see *Figure 4-7*), select Manager list.

  The Manager List menu is displayed.



```
                 ACE-3600 - RAD Data Communications

Configuration> System> Management> Manager list

1. IP address          ... (172.17.140.201)
2. Trap mask           >   (Manual)
3. Traps               >

>
Please select item (1 to 3)
ESC-previous menu; !-main menu; &-exit
```

Figure 4-9. Manager List Menu

Table 4-7. Manager List Menu Parameters

Parameter	Description	Possible Values
IP address	The manager's IP address. *Note:* • *The manager's IP address cannot be the same as the subnet of an existing router interface, unless it is attached to it.* • *Multicast, broadcast, all ones and all zeros IPs are not allowed.* • *Address parts that are not subnet cannot be all zeros or all ones.* • *The manager's IP address cannot be changed dynamically (on-the-fly)*	0.0.0.0 – 255.255.255.255

Parameter	Description	Possible Values
Trap mask	Manually enable/disable mask on a specific alarm, or enable/disable all alarm traps in a single operation.	• All masked – all traps are masked • None masked – No trap is masked • Manual – masking is manually configured on the Traps menu Default: Manual
Traps	Provides access to traps configuration menu. ***Note:*** *This parameter is visible only if a manager is already defined and the trap mask is set as Manual.*	Refer to *Figure 4-10* and *Table 4-8*

Note *Up to 16 managers (management IPs) can be defined per unit.*

Configuring Alarm Traps

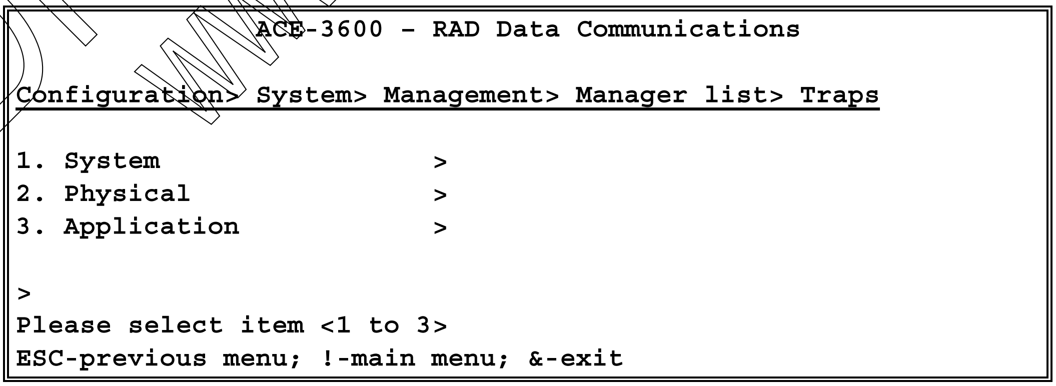
Alarm traps can be configured at the system level, physical layer, ATM and multiservice over PSN layer, via the Traps menu. This configuration defines whether traps are sent for a specific alarm type, using two settings:

- Active – traps are sent for this alarm
- Masked – traps are not sent for this alarm.

➤ To access the Traps configuration menu:

- From the Manager List menu (see *Figure 4-9*), select Traps.

  The Traps menu is displayed.



```
              ACE-3600 - RAD Data Communications

Configuration> System> Management> Manager list> Traps

1. System                 >
2. Physical               >
3. Application            >

>
Please select item <1 to 3>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-10. Traps Menu

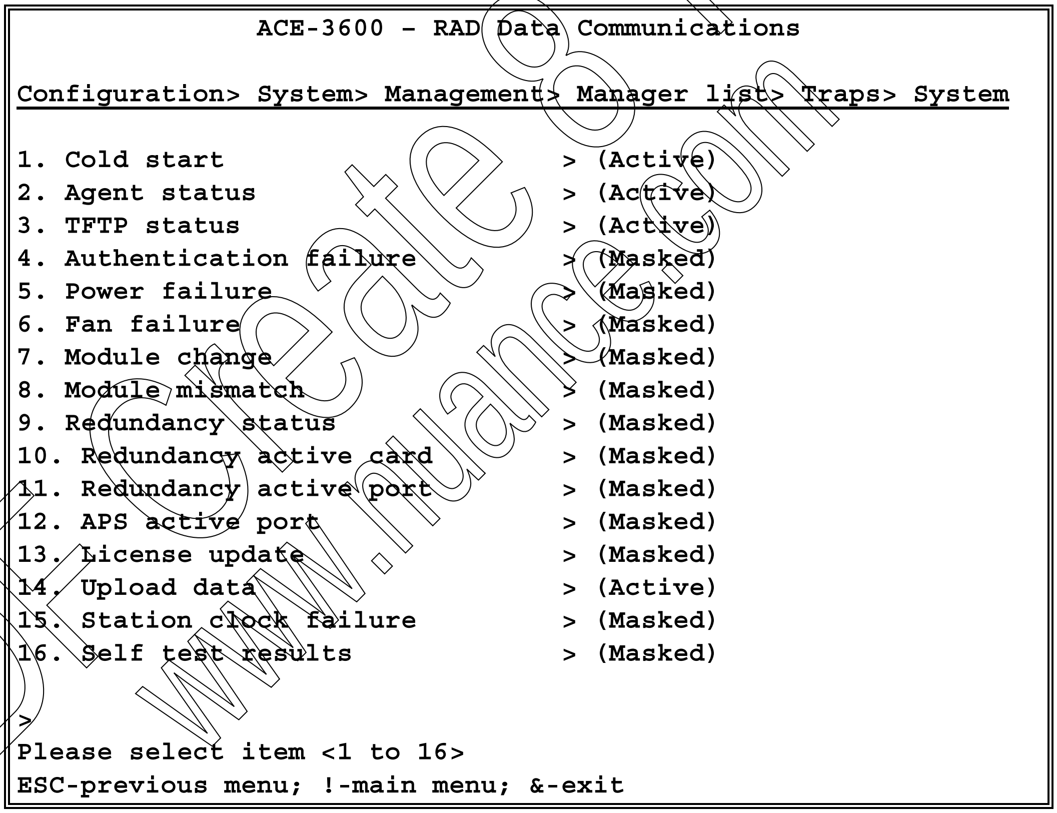
Table 4-8. Traps Configuration Menu Parameters

Parameter	Description	Possible Values
System	Mask configuration menu for system traps	Refer to *Figure 4-11* and *Table 4-9*
Physical	Mask configuration menu for physical traps	Refer to *Figure 4-12* and *Table 4-10*
Application	Mask configuration menu for application-level traps	Refer to *Figure 4-13* and *Table 4-11*

➤ To access the system traps configuration menu:

- From the Traps menu, select **System**.

  The system traps list appears.



```
                  ACE-3600 - RAD Data Communications

Configuration> System> Management> Manager list> Traps> System

1. Cold start                         > (Active)
2. Agent status                       > (Active)
3. TFTP status                        > (Active)
4. Authentication failure             > (Masked)
5. Power failure                      > (Masked)
6. Fan failure                        > (Masked)
7. Module change                      > (Masked)
8. Module mismatch                    > (Masked)
9. Redundancy status                  > (Masked)
10. Redundancy active card            > (Masked)
11. Redundancy active port            > (Masked)
12. APS active port                   > (Masked)
13. License update                    > (Masked)
14. Upload data                       > (Active)
15. Station clock failure             > (Masked)
16. Self test results                 > (Masked)

>
Please select item <1 to 16>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-11. System Traps Configuration Menu

Table 4-9. System Traps Parameters

Parameter	Description	Possible Values
Cold start	Activates or masks the 'cold start' trap (see the Note below)	Active Masked Default: Active

Parameter	Description	Possible Values
Agent status	Activates or masks the 'agent status changed' alarm trap, used by HPOV map application	Active Masked Default: Active
TFTP status	Activates or masks the 'TFTP status changed' alarm trap, used by TFTP upload/download application	Active Masked Default: Active
Authentication failure	Activates or masks the user authentication failure alarm trap	Active Masked Default: Masked
Power failure	Activates or masks the power failure alarm trap	Active Masked Default: Masked
Fan failure	Activates or masks the fan failure alarm trap	Active Masked Default: Masked
Module change	Activates or masks the module change alarm trap, which indicates that a card (module) in the unit has been replaced/changed.	Active Masked Default: Masked
Module mismatch	Activates or masks the module mismatch alarm trap.	Active Masked Default: Masked
Redundancy status	Activates or masks the redundancy status alarm trap.	Active Masked Default: Masked
Redundancy active card	Activates or masks the redundancy switch alarm trap, which indicates that operation has switched to the redundant main module.	Active Masked Default: Masked
Redundancy active port	Activates or masks the Ethernet redundancy switch alarm trap, which indicates that operation has switched to the redundant GbE port	Active Masked Default: Masked
APS active port	Activates or masks the APS switch alarm trap, which indicates that operation has switched to the redundant ATM-155 port	Active Masked Default: Masked

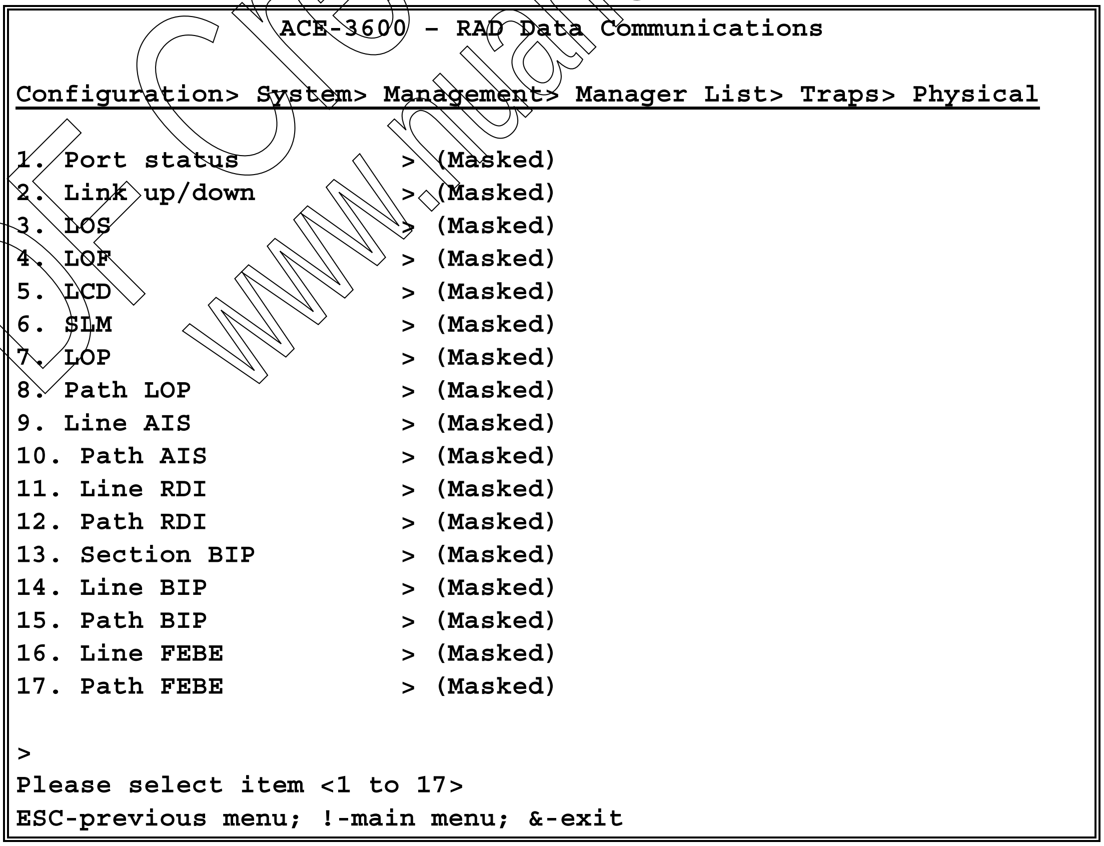
Parameter	Description	Possible Values
License update	Activates or masks the license update status alarm trap. For more information about the License Update feature, see *Section 4.4*.	Active Masked Default: Masked
Upload data	Activates or masks the agent upload alarm trap, which can be generated for completed upload operations	Active Masked Default: Active
Station clock failure	Activates or masks the station clock failure alarm trap	Active Masked Default: Masked
Self test results	Activates or masks an alarm trap regarding any change in the unit's self test results	Active Masked Default: Masked

Note *If "**all masked**" or "**none masked**" was previously selected in the Manager List menu (see Figure 4-9), individual traps cannot be masked or activated.*

➤ To access the physical layer traps configuration menu:

- From the Traps menu (see *Figure 4-10*), select Physical.

The following menu is displayed.



```
              ACE-3600 - RAD Data Communications

Configuration> System> Management> Manager List> Traps> Physical

1. Port status           > (Masked)
2. Link up/down          > (Masked)
3. LOS                   > (Masked)
4. LOF                   > (Masked)
5. LCD                   > (Masked)
6. SLM                   > (Masked)
7. LOP                   > (Masked)
8. Path LOP              > (Masked)
9. Line AIS              > (Masked)
10. Path AIS             > (Masked)
11. Line RDI             > (Masked)
12. Path RDI             > (Masked)
13. Section BIP          > (Masked)
14. Line BIP             > (Masked)
15. Path BIP             > (Masked)
16. Line FEBE            > (Masked)
17. Path FEBE            > (Masked)


>
Please select item <1 to 17>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-12. Physical Traps Configuration Menu

Table 4-10. Physical Traps Parameters

Parameter Description		**Possible Values**
Port status	Activates or masks the "port status" alarm trap, which indicates that the status of one of the ports has changed.	Active Masked Default: Masked
Link up/down	Activates or masks the "link up/down" alarm trap	Active Masked Default: Masked
LOS	Activates or masks the Loss of Signal alarm trap. LOS is the start or end of LOS event at the SONET/SDH or ETH physical level.	Active Masked Default: Masked
LOF	Activates or masks the LOF alarm trap. LOF is the start or end of LOF event at the SONET/SDH physical layer.	Active Masked Default: Masked
LCD	Activates or masks the LCD alarm trap. LCD is the start or end of LCD event at the SONET/SDH physical layer.	Active Masked Default: Masked
SLM	Activates or masks the SLM alarm trap. SLM is the start or end of SLM event at the SONET/SDH physical layer.	Active Masked Default: Masked
LOP	Activates or masks the LOP alarm trap. LOP is the start or end of LOP event at the SONET/SDH physical layer.	Active Masked Default: Masked
Path LOP	Activates or masks the Path LOP alarm trap. Path LOP is the start or end of Path LOP event at the SONET/SDH physical layer.	Active Masked Default: Masked
Line AIS	Activates or masks the Line AIS alarm trap. Line AIS is the start or end of Line AIS event at the SONET/SDH physical layer.	Active Masked Default: Masked
Path AIS	Activates or masks the Path AIS alarm trap. Path AIS is the start or end of Path AIS event at the SONET/SDH physical layer.	Active Masked Default: Masked
Line RDI	Activates or masks the Line RDI alarm trap. Line RDI is the start or end of Line AIS event at the SONET/SDH physical layer.	Active Masked Default: Masked
Path RDI	Activates or masks the Path RDI alarm trap. Path RDI is the start or end of Path RDI event at the SONET/SDH physical layer.	Active Masked Default: Masked
Section BIP	Activates or masks the Section BIP alarm trap.	Active

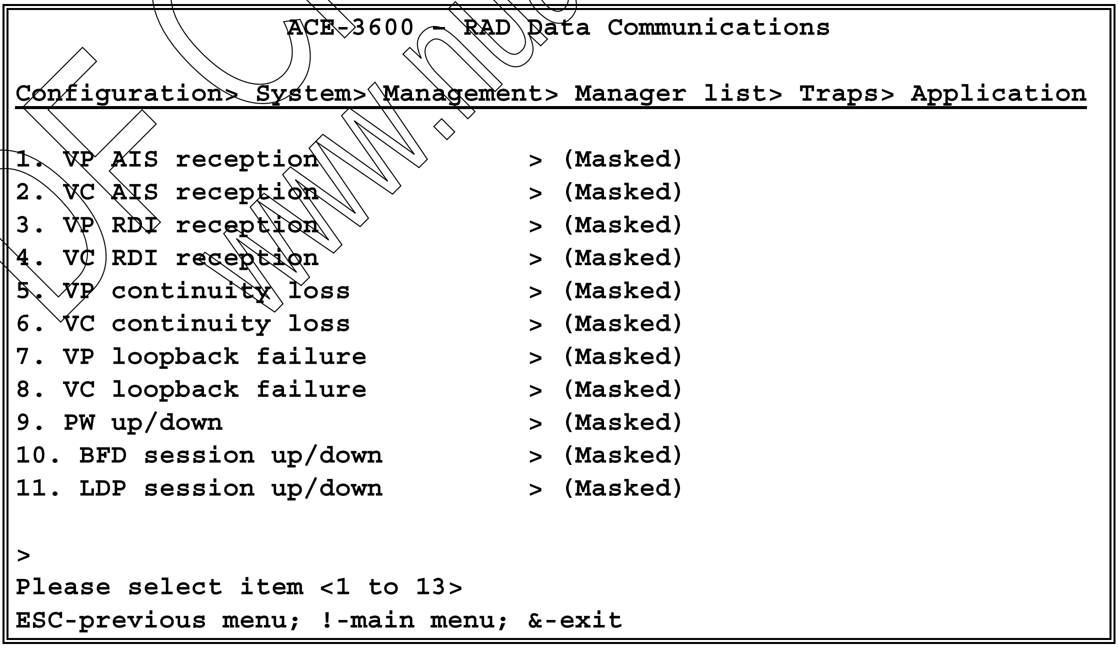
Parameter	Description	Possible Values
	Section BIP is the start or end of section BIP event at the SONET/SDH physical layer.	Masked Default: Masked
Line BIP	Activates or masks the Line BIP alarm trap. Line BIP is the start or end of Line BIP event at the SONET/SDH physical layer.	Active Masked Default: Masked
Path BIP	Activates or masks the Path BIP alarm trap. Path BIP start or end of path BIP event at the SONET/SDH physical layer.	Active Masked Default: Masked
Line FEBE	Activates or masks the Line FEBE alarm trap. Line FEBE start or end of Line FEBE event at the SONET/SDH physical layer.	Active Masked Default: Masked
Path FEBE	Activates or masks the Path FEBE alarm trap. Path FEBE start or end of path FEBE event at the SONET/SDH physical layer.	Active Masked Default: Masked

Note *If "**all masked**" or "**none masked**" was previously selected in the Manager List menu (see Figure 4-9), individual traps cannot be masked or activated.*

➤ To access the application level traps configuration menu:

- From the Traps menu (see *Figure 4-10*), select **Application**.

  The following menu is displayed.



```
                 ACE-3600 - RAD Data Communications

Configuration> System> Management> Manager list> Traps> Application

1. VP AIS reception            > (Masked)
2. VC AIS reception            > (Masked)
3. VP RDI reception            > (Masked)
4. VC RDI reception            > (Masked)
5. VP continuity loss          > (Masked)
6. VC continuity loss          > (Masked)
7. VP loopback failure         > (Masked)
8. VC loopback failure         > (Masked)
9. PW up/down                  > (Masked)
10. BFD session up/down        > (Masked)
11. LDP session up/down        > (Masked)

>
Please select item <1 to 13>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-13. Application Level Traps Configuration Menu

Table 4-11. Application Level Traps Parameters

Parameter Description		Possible Values
VP AIS reception	Activates or masks the "VP Rx AIS" alarm trap. VP RX AIS is the start or end of VP AIS event.	Active Masked Default: Masked
VC AIS reception	Activates or masks the "VC Rx AIS" alarm trap. VC RX AIS is the start or end of VC AIS event.	Active Masked Default: Masked
VP RDI reception	Activates or masks the "VP Rx RDI" alarm trap. VP RX RDI is the start or end of VP RDI event.	Active Masked Default: Masked
VC RDI reception	Activates or masks the "VC Rx RDI" alarm trap. VC RX RDI is the start or end of VC RDI event	Active Masked Default: Masked
VP continuity loss	Activates or masks the "VP continuity loss" alarm trap. Continuity loss is the start or end of VP LOC event.	Active Masked Default: Masked
VC continuity loss	Activates or masks the "VC continuity loss" alarm trap. Continuity loss is the start or end of VC LOC event.	Active Masked Default: Masked
VP loopback failure	Activates or masks the "VP loopback failure" alarm trap. VP loopback failure occurs when the generated loopback cell was not returned.	Active Masked Default: Masked
VC loopback failure	Activates or masks the "VC loopback failure" alarm trap. VC loopback failure occurs when the generated loopback cell was not returned.	Active Masked Default: Masked
PW up/down	Activates or masks the "PW up/down" alarm trap, which indicates whether a pseudowire is up or down.	Active Masked Default: Masked
BFD session up/down	Activates or masks the "BFD session up/down" alarm trap, which indicates whether the BFD connectivity check session is up or down.	Active Masked Default: Masked
LDP session up/down	Activates or masks the "LDP session up/down" alarm trap, which indicates whether the label distribution protocol session is up or down.	Active Masked Default: Masked

Configuring Remote Management Access

ACE-3600 allows you to enable or disable remote access via SNMP, Telnet and Web to the ACE-3600 management system. By disabling remote management access, you prevent unauthorized access to the system when security of the unit's IP address has been compromised.

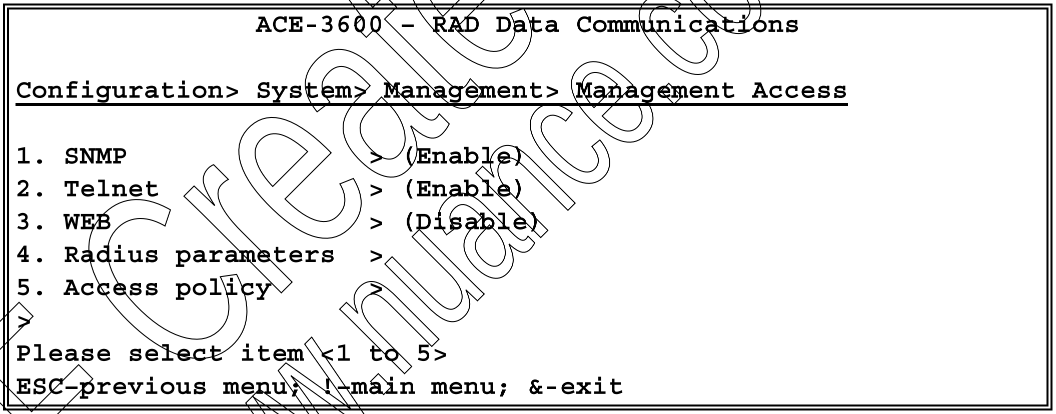
In addition, you can allow users to be defined on a Radius server, which is an easily accessible and centralized server from which ACE-3600 units (as well as other units that support Radius) can authenticate individual users and their passwords. Via the unit's general access policy you can set the availability and priority of both the Radius and local (terminal) login methods.

Note *When remote management access is disabled, ACE-3600 can be managed via a direct ASCII-based terminal connection only.*

➤ To access the Management Access configuration menu:

- From the Management menu (see *Figure 4-7*), select **Management Access.**

The Management Access menu is displayed.



```
                 ACE-3600 - RAD Data Communications

Configuration> System> Management> Management Access

1. SNMP              > (Enable)
2. Telnet            > (Enable)
3. WEB               > (Disable)
4. Radius parameters >
5. Access policy     >
>
Please select item <1 to 5>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-14. Management Access Menu

Table 4-12. Management Access Menu Parameters

Parameter	Description	Possible Values
SNMP	Remote management access via SNMP. ***Note:*** *When SNMP access is disabled, the SNMP agent does not send traps.*	Enable Disable Default: Enable

Parameter	Description	Possible Values
Telnet	Remote management access via Telnet. Secure Telnet access is secured by a Secure Shell (SSH) client/server program, which provides a secure communication channel. *Note:* • *Telnet access cannot be disabled when there are active Telnet or SSH sessions.* • *Secure can be set only when currently there are no active Telnet sessions.*	Enable Disable Secure Default: Enable
WEB	Remote management access via the Web. Secure Web access if secured by a secure socket layer (SSL) protocol, which encrypts the data between the TCP and HTTP Web layers. *Note:* • *Web access cannot be disabled when there are active Web or SSH sessions.* • *Secure can be set only when currently there are no active Web sessions.*	Enable Disable Secure Default: Disable
Radius parameters	Define the Radius server access parameters	See *Setting the Radius Server Parameters*
Access policy	Set the availability and priority of the user access methods	See *Setting the Access Policy*

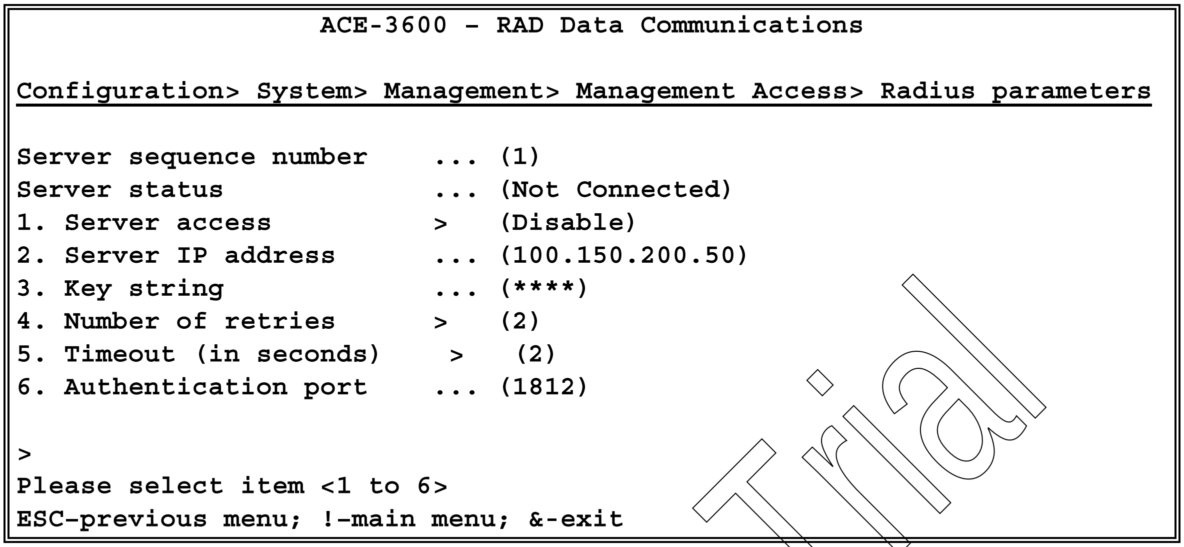
Setting the Radius Server Parameters

If ACE-3600 would be required to authenticate users via a centralized Radius server in a given application, the relevant parameters must be configured.

➤ To access the Radius server options:

- From the Management Access menu (see *Figure 4-14*), select Radius parameters.

  The Radius Parameters menu is displayed.



```
                  ACE-3600 - RAD Data Communications

Configuration> System> Management> Management Access> Radius parameters

Server sequence number     ... (1)
Server status              ... (Not Connected)
1. Server access           >   (Disable)
2. Server IP address       ... (100.150.200.50)
3. Key string              ... (****)
4. Number of retries       >   (2)
5. Timeout (in seconds)     >   (2)
6. Authentication port     ... (1812)

>
Please select item <1 to 6>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-15. Radius Parameters Menu

Table 4-13. Radius Parameters

Parameter	Description	Possible Values
Server sequence number	Number of the server which details are currently displayed. Also indicates the server's priority in the sequence (first, second, third or fourth)	1–4 Default: 1
Server status	Connection status of the server which details are displayed: • Connected – the server is used as the current authentication server • Not Connected – the server is used as a backup authentication server • Disconnected – the server could not be reached/contacted within a specified period.	Connected Not Connected Disconnected Default: Not Connected
Server access	Enable or disable the specific Radius server which details are displayed	Enable Disable Default: Disable
Server IP address	IP of this Radius server	0.0.0.1 – 255.255.255.255
Key string	An non-disclosed string used to encrypt the user password.	
Number of retries	The maximum number of times an authentication request should be re-sent to the server in case of no response.	0–5 Default: 2

Parameter	Description	Possible Values
Timeout (in seconds)	The period in seconds during which ACE-3600 waits for a response from the Radius server.	0–5 Default: 2
Authentication port	The UDP port number used for the authentication channel.	1–65535 Default: 1812

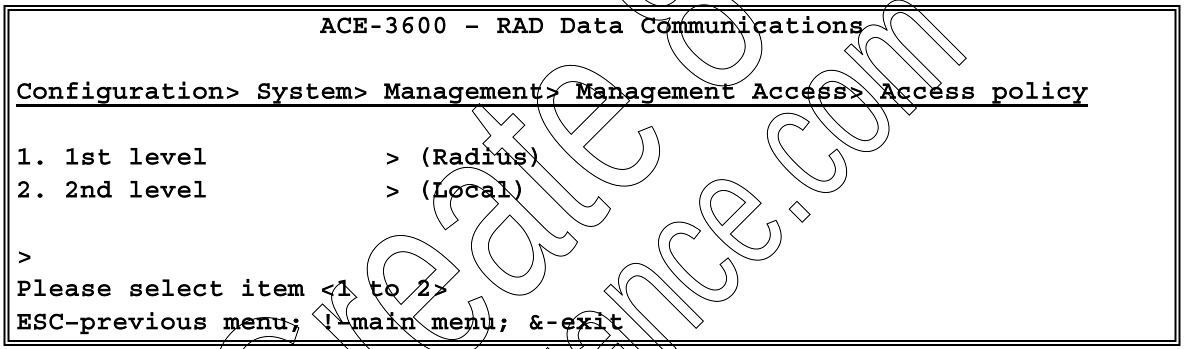
Setting the Access Policy

The general access policy defines the availability and priority of both the Radius (see previous section) and local (terminal) login methods.

➤ To set the access policy:

- From the Management Access menu (see *Figure 4-14*), select Access Policy.

  The Access Policy menu is displayed.



```
                     ACE-3600 - RAD Data Communications

Configuration> System> Management> Management Access> Access policy

1. 1st level           > (Radius)
2. 2nd level           > (Local)

>
Please select item <1 to 2>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-16. Access Policy Menu

Table 4-14. Access Policy Parameters

Parameter Description		Possible Values
1st level	The primary method used by ACE-3600 for authentication of users.	Local Radius Default: Local
2nd level	The secondary method of authentication. Visible only if 'Radius' is selected on the first level.	Local Radius None Default: None

Configuring the SNMPv3 Parameters

ACE-3600 supports SNMP version 3, providing secure access to the device by authenticating and encrypting packets transmitted over the network. The SNMPv3 functionality is optional.

The SNMPv3 configuration includes the following stages:

a. *Configuring the SNMPv3 Engine ID*

b. *Enabling SNMPv3*

c. *Managing SNMPv3 Users*

d. *Adding SNMPv3 Notification Entries*

e. *Assigning SNMPv3 Traps*

f. *Configuring the Target Parameters*

g. *Mapping SNMPv1 to SNMPv3* (if necessary).

Configuring the SNMPv3 Engine ID

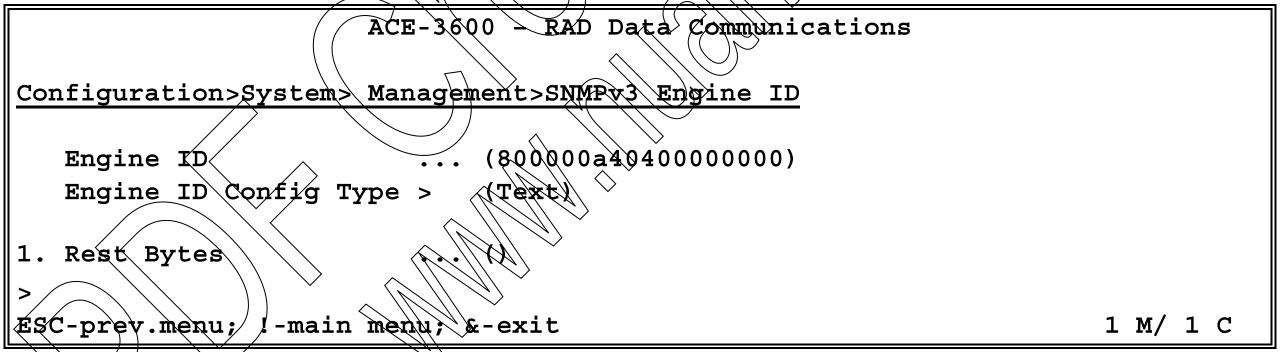
Before enabling the SNMPv3 functionality, you have to define a unique Engine ID.

The Engine ID is an alphanumeric string used to identify the ACE-3600 agent in the SNMPv3 environment. The engine ID must be unique to allow the user to query the SNMP engine. It must be defined prior to enabling SNMPv3 functionality. The length of the string is up to 27 characters.

➤ To define the SNMP engine ID:

- From the SNMP Engine ID menu (Configuration > System > Management > SNMP Engine ID), select Rest Bytes and define the value of the engine ID section reserved for user SNMP engine identification.

  The value is automatically translated into hexadecimal format and appears in the read-only Engine ID field.



```
                      ACE-3600 - RAD Data Communications

Configuration>System> Management>SNMPv3 Engine ID

   Engine ID                 ... (800000a40400000000)
   Engine ID Config Type >       (Text)

1. Rest Bytes                ... ()
>
ESC-prev.menu; !-main menu; &-exit                                      1 M/ 1 C
```

Figure 4-17. SNMPv3 Engine ID Menu

Table 4-15. SNMPv3 Engine ID Parameters

Parameter	Description	Possible Values
Engine ID	An SNMP engine's administratively unique identifier	ff0000ff0400000000 Read-only

Parameter	Description	Possible Values
Engine ID Config Type	IPv4	MAC address Text (MAX length 27 bytes) Octets IPv6 **Default: MAC address**
Rest Bytes	According to the Engine ID Configuration Type	IP Address MAC Address ASCII String (up to 27 characters) Hex String (up to 54 characters) IPv6 Address **Default: Target's MAC address**

Enabling SNMPv3

The general SNMPv3 parameters include the engine boots, the engine time and the SNMP message size. These instructions assume that an SNMP engine ID has already been defined.

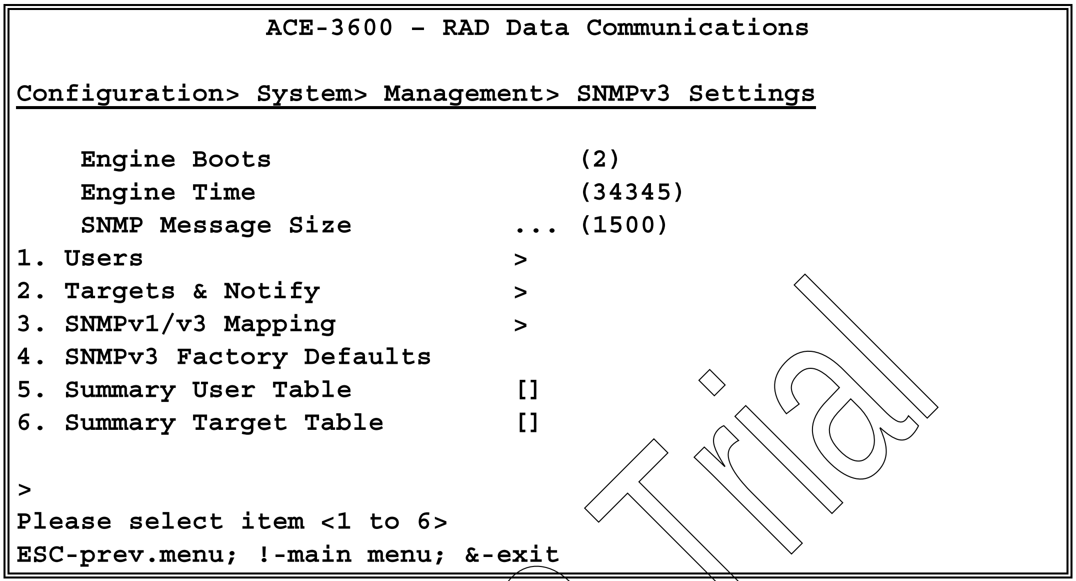
➤ **To access the SNMPv3 general parameters:**

6. On the Management menu (Configuration > System > Management), select **SNMPv3** and then **Enable**.

   The SNMPv3 Settings option becomes available on the Management menu.

7. Select SNMPv3 Settings.

   The SNMPv3 Settings menu is displayed and displays general information and selectable options.



```
                 ACE-3600 - RAD Data Communications

Configuration> System> Management> SNMPv3 Settings

    Engine Boots                      (2)
    Engine Time                       (34345)
    SNMP Message Size             ... (1500)
1. Users                          >
2. Targets & Notify               >
3. SNMPv1/v3 Mapping              >
4. SNMPv3 Factory Defaults
5. Summary User Table             []
6. Summary Target Table           []

>
Please select item <1 to 6>
ESC-prev.menu; !-main menu; &-exit
```

Figure 4-18. SNMPv3 Settings Menu

Table 4-16. SNMPv3 General Information and Options

Parameter Description		Possible Values
Engine boots	Number of times that the SNMP engine has re-initialized since its identification was configured last (read-only)	1–2147483647 (1–7FFFHHHFH) Default: 0
Engine time	Number of seconds since the last SNMP engine boot (read-only)	1–2147483647 Default: 0
SNMP message size	The maximum length of an SNMP message (in octets) that the SNMP engine can send, receive and process (read-only)	484–2147483647 Default: 1500
Users	Add SNMPv3 users or edit existing users	See *Managing SNMPv3 Users*
Targets & Notify	Define the SNMPv3 network management stations to which ACE-3600 should send trap notifications	See *Configuring the Target Parameters*
SNMPv1/v3 Mapping	Option which allows SNMPv1 and SNMPv2 to be mapped (work alongside) SNMPv3	See *Mapping SNMPv1 to SNMPv3*
SNMPv3 Factory Defaults	Selecting this option resets the SNMPv3 configuration and reinstates the factory default settings	
Summary User Table	View the list of current users and their details	See *Viewing the SNMPv3 Information*
Summary Target Table	View the list of current targets and their details	See *Viewing the SNMPv3 Information*

Managing SNMPv3 Users

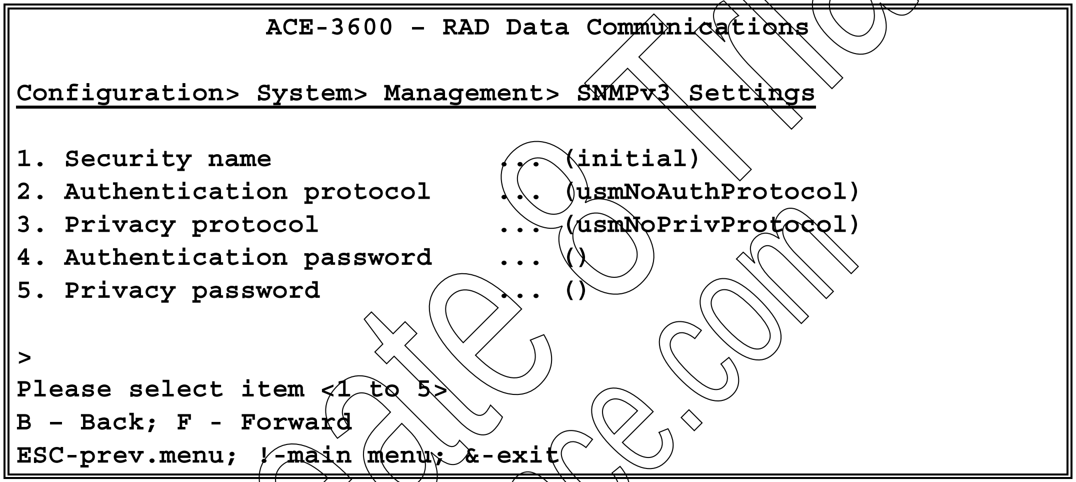
ACE-3600 supports up to 10 SNMPv3 managers with different authorization and privacy attributes.

Note *Access control policy is defined via the **vacmSecurityToGroupTable** and **vacmAccessTable** tables, which can be accessed from an SNMP browser only.*

➤ To add/edit SNMPv3 users:

- From the SNMPv3 Settings menu (see *Figure 4-18*), select Users.

The Users menu is displayed with the details of the first user (if exists).



```
                    ACE-3600 - RAD Data Communications

Configuration> System> Management> SNMPv3 Settings

1. Security name                ...  (initial)
2. Authentication protocol      ...  (usmNoAuthProtocol)
3. Privacy protocol             ...  (usmNoPrivProtocol)
4. Authentication password      ...  ()
5. Privacy password             ...  ()

>
Please select item <1 to 5>
B - Back; F - Forward
ESC-prev.menu; !-main menu; &-exit
```

Figure 4-19. SNMPv3 Users Menu

Note *You can press <F> (Forward) or <B> (Back) to browse through the currently registered users (if such were already registered). The details of one user are displayed at a time.*

Table 4-17. SNMPv3 Users Options

Parameter	Description	Possible Values
Security name	The user's security name. Enter a new name to add a user.	Up to 32 alphanumeric characters
Authentication protocol	The authentication protocol to be used for authenticating the user: • usmNoAuthProtocol – No authentication is performed • usmHMACMD5AuthProtocol – MD5 protocol • usmHMACSHAAuthProtocol – SHA protocol.	usmNoAuthProtocol usmHMACMD5AuthProtocol usmHMACSHAAuthProtocol Default: usmNoAuthProtocol
Privacy protocol	Type of privacy protocol to be used for encryption: • usmNoPrivProtocol – No privacy protocol is not used	usmNoPrivProtocol usmDESPrivProtocol Default: usmNoPrivProtocol

Parameter	Description	Possible Values
	• **usmDESPrivProtocol** – DES protocol	
Authentication password	The user’s authentication password. Not available if authentication is disabled (usmNoAuthProtocol).	A combination of at least 8 alphanumeric characters
Privacy password	The private key used for encryption. Not available if privacy is disabled (usmNoPrivProtocol).	A combination of at least 8 alphanumeric characters

➤ To delete an SNMPv3 user:

1. Navigate to the Users menu (Configuration > System > Management > SNMPv3 Settings > Users).
2. Browse for the specific user by using the <**F**> (forward) or <**B**> (back) keys.
3. Press <**R**> to remove (delete) the user whose details are displayed.

Adding SNMPv3 Notification Entries

You can define which types of notification will be sent to the target management stations (the target stations are defined separately, as explained in *Configuring the Target Parameters*).

➤ To define notifications:

1. From the SNMPv3 Settings menu (see *Figure 4-18*), select **Targets & Notify.**

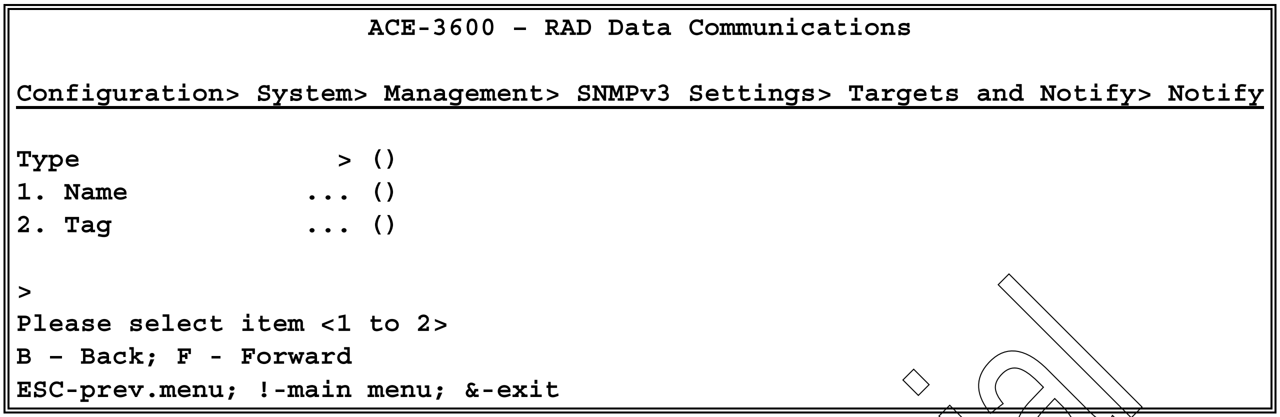
   The Targets & Notify menu is displayed.

2. Select **Notify**.

   The Notify menu is displayed with the details of the first notification (if exists).

Note

- *You can press <**F**> (Forward) or <**B**> (Back) to browse through the currently defined notifications (if such were already defined). The details of one notification are displayed at a time.*
- *Notifications can be defined via Terminal access only. By default, two tags are defined and associated with each notify name according to the default trap mask.*



```
                    ACE-3600 - RAD Data Communications

Configuration> System> Management> SNMPv3 Settings> Targets and Notify> Notify

Type                 > ()
1. Name            ... ()
2. Tag             ... ()

>
Please select item <1 to 2>
B - Back; F - Forward
ESC-prev.menu; !-main menu; &-exit
```

Figure 4-20. Notify Menu (SNMPv3 Settings)

Table 4-18. Notification Entry Parameters

Parameter	Description	Possible Values
Type	Type of the notification to be generated: • 1 – Trap. Any messages generated for selected rows will contain Unconfirmed-Class PDUs. • 2 – Inform. Any messages generated for selected rows will contain Confirmed-Class PDUs. ***Note:*** *if the SNMP entity supports the generation of Unconfirmed-Class PDUs only (not Confirmed-Class PDUs), then this parameter is read-only.*	1 2 Default: 1
Name	ASCII string identifying the notification entry. Enter a new name to add an entry.	A string of up to 32 alphanumeric characters
Tag	A tag value to be associated with the current notification entry. This tag is used to identify the current notification entry when configuring the target address.	0–255

Assigning SNMPv3 Traps to Notifications

One or more traps must be assigned to each notification entry.

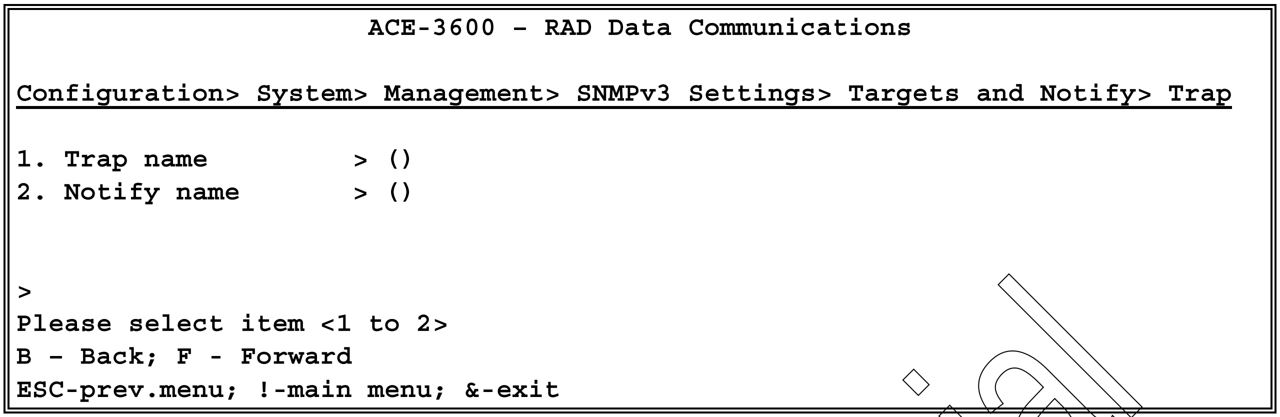
➤ To assign traps to notification entries:

1. From the SNMPv3 Settings menu (see *Figure 4-18*), select **Targets & Notify.**

   The Targets & Notify menu is displayed.

2. Select Trap.

   The Trap menu is displayed.



```
                      ACE-3600 - RAD Data Communications

Configuration> System> Management> SNMPv3 Settings> Targets and Notify> Trap

1. Trap name          > ()
2. Notify name        > ()


>
Please select item <1 to 2>
B - Back; F - Forward
ESC-prev.menu; !-main menu; &-exit
```

Figure 4-21. Notify Menu (SNMPv3 Settings)

3. From the Trap menu, configure the following:
    - Trap name – Select a trap to be assigned to the selected notification
    - Notify Name – Select a tag from the list of previously defined notification tags.

Caution By default, traps are assigned to a Notify name which is identical to the trap name. Deleting existing assignments may impede proper functionality.

Configuring the Target Parameters

A target is a network management station to which ACE-3600 should send trap notifications over SNMPv3. A set of parameters must be configured and assigned to each target. Then, each target must have a valid IP address and IP mask. In addition, a previously configured parameter set and notification tags must be assigned to the target.

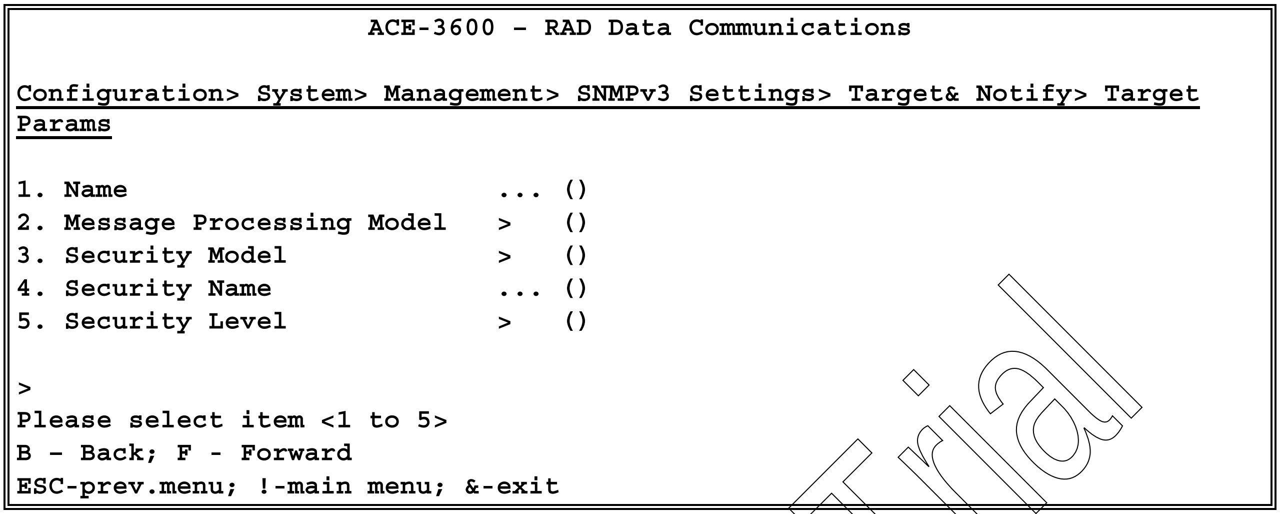
➤ To configure target parameters:

1. From the SNMPv3 Settings menu (see *Figure 4-18*), select Targets & Notify.

    The Targets & Notify menu is displayed.

2. Select Target Parameters ("Target Params").

    The Target Parameters menu is displayed.



```
                        ACE-3600 - RAD Data Communications

Configuration> System> Management> SNMPv3 Settings> Target& Notify> Target
Params

1. Name                         ... ()
2. Message Processing Model      >   ()
3. Security Model                >   ()
4. Security Name                ... ()
5. Security Level                >   ()

>
Please select item <1 to 5>
B - Back; F - Forward
ESC-prev.menu; !-main menu; &-exit
```

Figure 4-22. Target Parameters Menu

Table 4-19. Target Parameters

Parameter Description		Possible Values
Name	An ASCII string identifying current set of target parameters. Enter the name of a new target or use the B and F keys to browse through the targets.	Up to 32 alphanumeric characters
Message Processing Model	The model to be used when generating SNMP messages.	SNMPv1 SNMPv2c SNMPv2u SNMPv3
Security Model	The security model for the SNMP messages	Any SNMPv1 SNMPv2c User-Based Security Model (USM)
Security Name	Identification of the principal on whose behalf SNMP messages are to be generated using this entry. Can be either an SNMPv3 user or an SNMPv1/SNMPv2 community string.	Up to 32 alphanumeric characters
Security Level	The level of security to be used when generating SNMP messages: • noAuthNoPriv – Authorization and privacy are disabled • authNoPriv – Authorization is enabled, privacy is disabled • authPriv – Authorization and privacy are enabled.	noAuthNoPriv authNoPriv authPriv

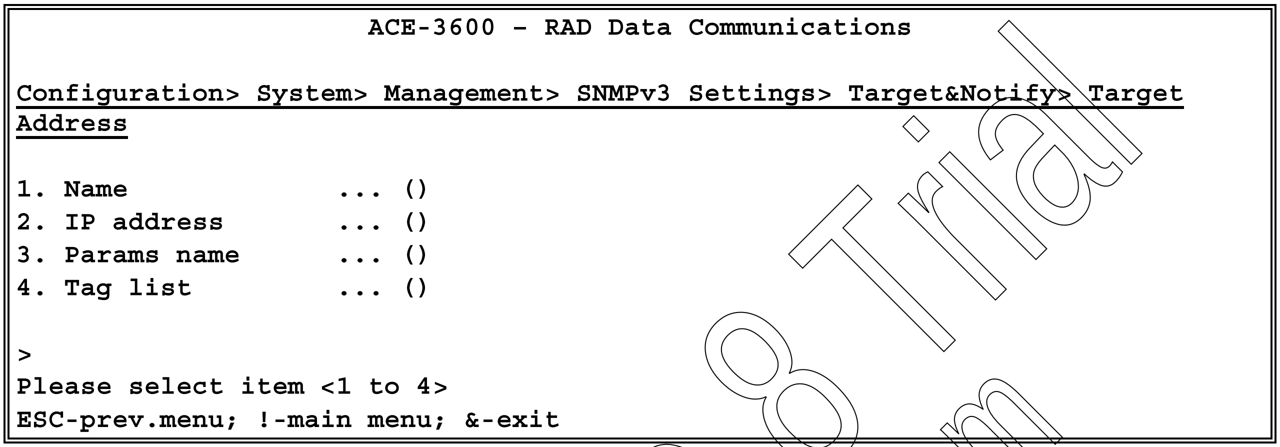
➤ To configure the SNMPv3 target addresses:

1. From the SNMPv3 Settings menu (see *Figure 4-18*), select **Targets & Notify.**

   The Targets & Notify menu is displayed.

2. Select Target Address.

   The Target Address menu is displayed.



```
                      ACE-3600 - RAD Data Communications

Configuration> System> Management> SNMPv3 Settings> Target&Notify> Target
Address

1. Name                ... ()
2. IP address          ... ()
3. Params name         ... ()
4. Tag list            ... ()

>
Please select item <1 to 4>
ESC-prev.menu; !-main menu; &-exit
```

Figure 4-23. Target Address Menu

Table 4-20. Target Address Parameters

Parameter	Description	Possible Values
Name	ASCII string identifying the target. Enter the name of a new target or use the B and F keys to browse through the existing addresses.	Up to 32 alphanumeric characters
IP address	Valid IP address of the target NMS	Must be in the xxx.xxx.xxx.xxx:162 format, where 162 is a standard SNMP port used for sending traps.
Params name	Select the name of the previously defined target parameter set to be assigned to this target	Up to 32 alphanumeric characters
Tag list	Select a tag from the list of previously defined notification tags	0–255

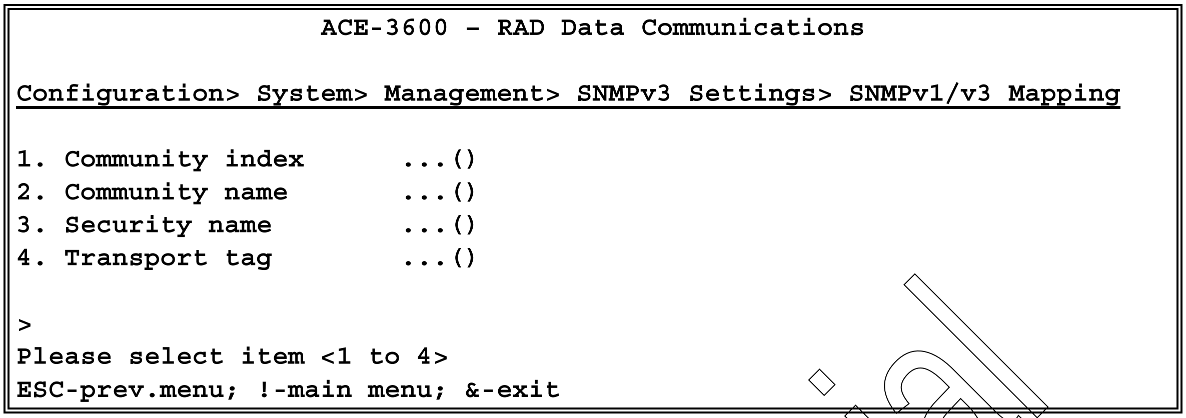
Mapping SNMPv1 to SNMPv3

ACE-3600 supports coexistence of different SNMP versions by mapping SNMPv1/SNMPv2 community names to the SNMPv3 security name values. The mapping is performed according to the RFC 3584 requirements.

➤ To map SNMPv1/SNMPv2 to SNMPv3:

- From the SNMPv3 Settings menu (see *Figure 4-18*), select **SNMPv1/v3 Mapping**.

  The SNMPv1/v3 Mapping menu appears.



```
                    ACE-3600 - RAD Data Communications

Configuration> System> Management> SNMPv3 Settings> SNMPv1/v3 Mapping

1. Community index      ...()
2. Community name       ...()
3. Security name        ...()
4. Transport tag        ...()

>
Please select item <1 to 4>
ESC-prev.menu; !-main menu; &-exit
```

Figure 4-24. SNMPv1/v3 Mapping Menu

Table 4-21. SNMPv1/v3 Mapping Parameters

Parameter Description		Possible Values
Community index	Unique index value of the currently displayed SNMP community. Enter a new index value or use the B and F keys to browse through the defined communities.	Up to 32 alphanumeric characters
Community name	The SNMPv2/SNMPv2 community name for which the information is is presented	Up to 32 alphanumeric characters
Security name	The SNMPv3 security name to be mapped to the SNMPv2/SNMPv2 community name	Up to 32 alphanumeric characters
Transport tag	Specifies a set of the transport endpoints that are used, in either of the following methods: • Specifying the transport endpoints from which an SNMP entity accepts management requests • Specifying the transport endpoints to which a notification may be sent, using the community string matching the corresponding instance of community name.	As previously defined for each target

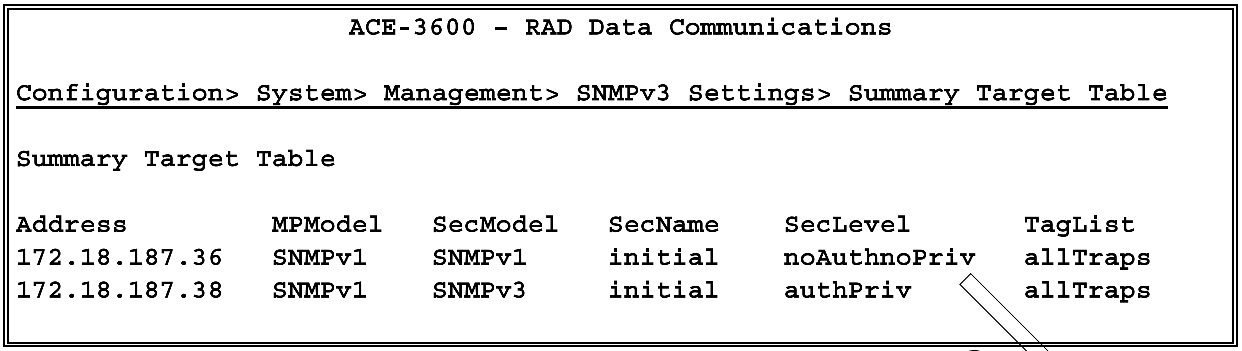
Viewing the SNMPv3 Information

Instead of browsing, you can view the summary of all currently defined SNMPv3 targets, as well as the summary of all currently defined SNMPv3 users.

➤ To view the summary of targets:

- From the SNMPv3 Settings menu (see *Figure 4-18*), select Summary Target Table.

  The list of currently defined targets is displayed.



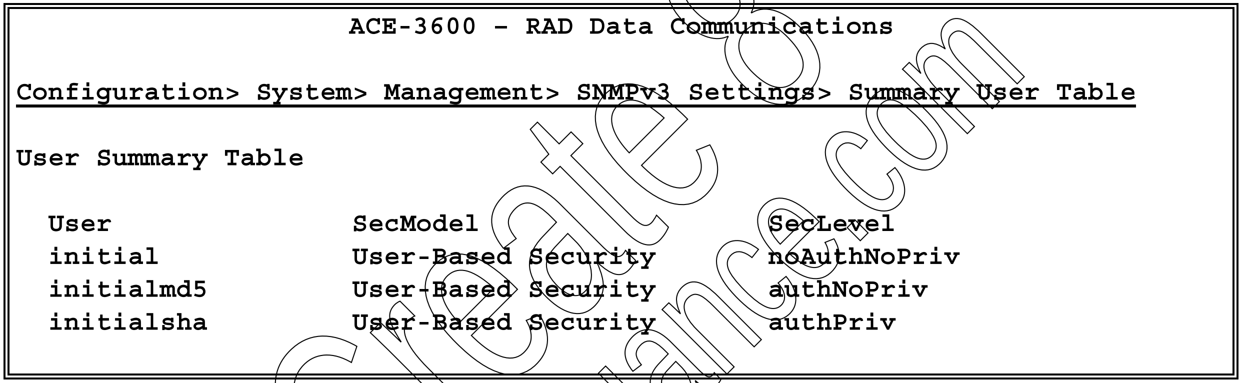
```
                    ACE-3600 - RAD Data Communications

Configuration> System> Management> SNMPv3 Settings> Summary Target Table

Summary Target Table

Address          MPModel    SecModel    SecName     SecLevel       TagList
172.18.187.36    SNMPv1     SNMPv1      initial     noAuthnoPriv   allTraps
172.18.187.38    SNMPv1     SNMPv3      initial     authPriv       allTraps
```

Figure 4-25. SNMPv3 Targets List

➤ To view the summary of users:

- From the SNMPv3 Settings menu (see *Figure 4-18*), select Summary User Table.

  The list of currently defined users is displayed.



```
                    ACE-3600 - RAD Data Communications

Configuration> System> Management> SNMPv3 Settings> Summary User Table

User Summary Table

  User                SecModel                  SecLevel
  initial             User-Based Security       noAuthNoPriv
  initialmd5          User-Based Security       authNoPriv
  initialsha          User-Based Security       authPriv
```

Figure 4-26. SNMPv3 Users List

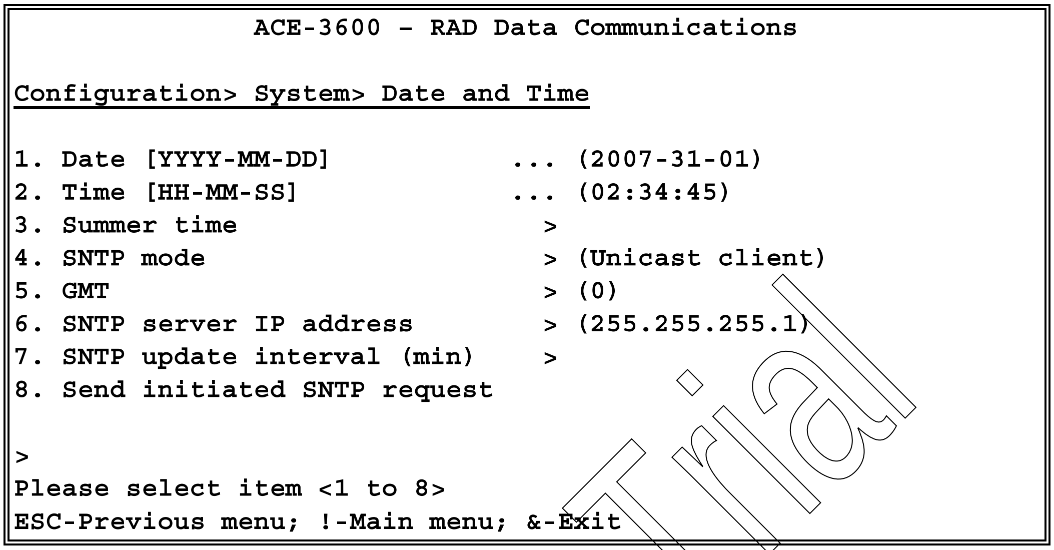
Setting the Date and Time

ACE-3600 allows you to set the date and time of its internal clock. Log events will be recorded according to the set date and time. In addition, you can set the unit to automatically retrieve the current date and time from an SNTP server.

➤ To access the Date and Time options:

- From the System menu (see *Figure 4-3*), select Date and Time.

  The Date and Time menu is displayed.



```
                  ACE-3600 - RAD Data Communications

Configuration> System> Date and Time

1. Date [YYYY-MM-DD]              ... (2007-31-01)
2. Time [HH-MM-SS]                ... (02:34:45)
3. Summer time                      >
4. SNTP mode                        > (Unicast client)
5. GMT                              > (0)
6. SNTP server IP address           > (255.255.255.1)
7. SNTP update interval (min)       >
8. Send initiated SNTP request

>
Please select item <1 to 8>
ESC-Previous menu; !-Main menu; &-Exit
```

Figure 4-27. Date and Time Menu

Table 4-22. Date and Time Menu Parameters

Parameter Description		Possible Values
Date	Date in format of: [YYYY-MM-DD]	2000-01-01 to 2099-12-31
Time	Time in format of: [HH-MM-SS]	00-00-00 to 23-59-59
Summer Time	Access the summer time (daylight saving time) configuration	See *Configuring the Summer Time Parameters*
SNTP mode	Availability and type of the SNTP time retrieval: • Disable – the SNTP service is disabled. • Broadcast client – ACE-3600 works in SNTP mode as a broadcast client. • Unicast client – ACE-3600 works in SNTP mode as a Unicast client.	Disable Broadcast client Unicast client Default: Disable
GMT	The Greenwich Mean Time (GMT) offset of the manually entered time (not relevant in SNTP mode).	-12 to +12, in jumps of 1 (integers only) Default: 0
SNTP server IP address	IP address of the SNTP server. Valid only when the SNTP mode is 'Unicast client'.	0.0.0.0 – 255.255.255.255
SNTP update interval (min)	The required delay in minutes between automatic SNTP request initiations.	1–1440 Default: 60
Send initiated SNTP request	Manual initiation of an SNTP request. An SNTP request is immediately sent to the specified SNTP server address upon selecting this option. Valid only when the SNTP mode is 'Unicast client'.	

Configuring the Summer Time Parameters

The summer time parameters define whether/how the unit should automatically change its internal time when daylight saving time is applied in the geographical region where ACE-3600 is installed. This feature can be disabled, activated on a specific date, or customarily recur.

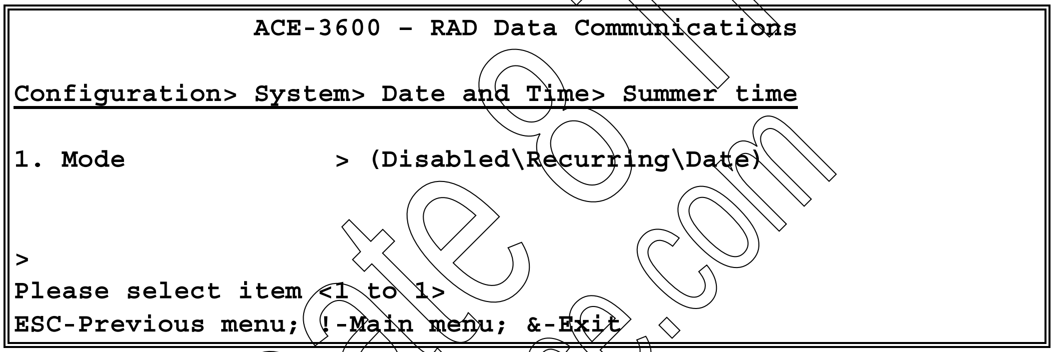
➤ To set the summer time parameters:

1. From the Date and Time menu, select Summer Time.

   The Summer Time menu is displayed.

2. Select the required summer time mode: Disabled, Recurring or Date.

   Based on your selection (see *Table 4-23*), the Summer Time menu displays the relevant options.

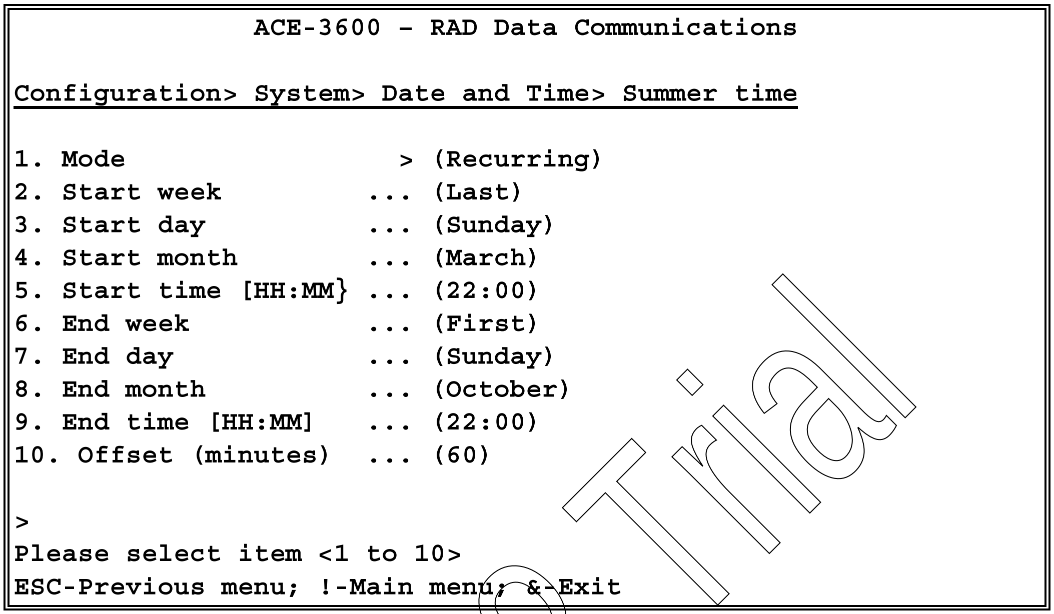


```
                    ACE-3600 - RAD Data Communications

Configuration> System> Date and Time> Summer time

1. Mode              > (Disabled\Recurring\Date)


>
Please select item <1 to 1>
ESC-Previous menu; !-Main menu; &-Exit
```

Figure 4-28. Summer Time Mode Selection

Table 4-23. Summer Time Modes

Parameter	Description	Possible Values
Disabled	The summer time feature is disabled	
Recurring	The daylight saving time shifting is set to recur periodically, as defined in the parameters that appear below	See *Figure 4-29* and *Table 4-24*
Date	The daylight saving time shifting is set to occur once on a given date, as defined in the parameters that appear below	See *Figure 4-30* and *Table 4-25*



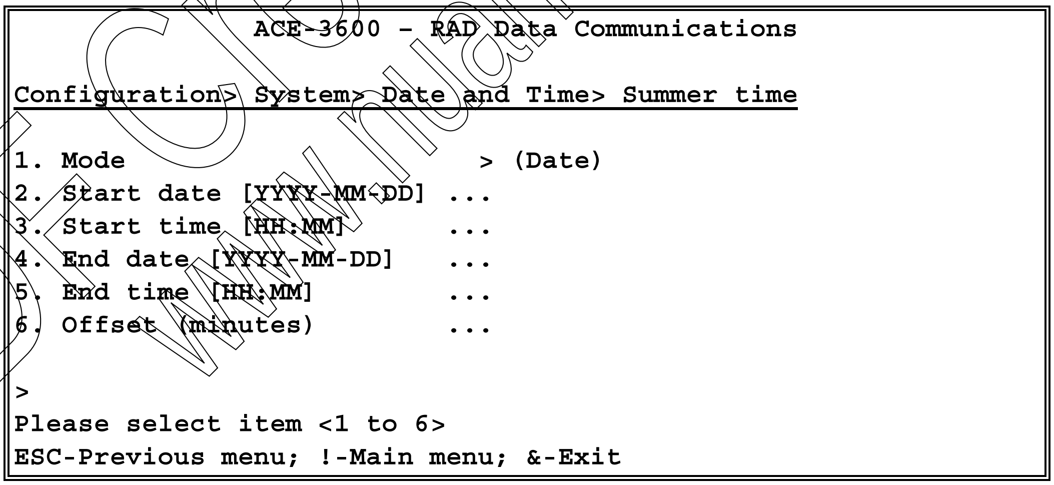
```
                ACE-3600 - RAD Data Communications

Configuration> System> Date and Time> Summer time

1. Mode                  > (Recurring)
2. Start week         ... (Last)
3. Start day          ... (Sunday)
4. Start month        ... (March)
5. Start time [HH:MM} ... (22:00)
6. End week           ... (First)
7. End day            ... (Sunday)
8. End month          ... (October)
9. End time [HH:MM]   ... (22:00)
10. Offset (minutes)  ... (60)

>
Please select item <1 to 10>
ESC-Previous menu; !-Main menu; &-Exit
```

Figure 4-29. Summer Time – Recurring Mode

Table 4-24. Summer Time – Recurring Mode Parameters

Parameter Description		Possible Values
Start week	The chronological week of the month in which the daylight saving time should begin every year	First Second Third Fourth Last
Start day	The specific day of the week on which the daylight saving time should begin every year	Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday
Start month	The specific month in which the daylight saving time should begin every year	January, February, March, April, May, June, July, August, September, October, November, December
Start time [HH:MM]	The specific time (hour and minute) at which the daylight saving time should begin every year	00:00 – 23:59

Parameter	Description	Possible Values
End week	The chronological week of the month in which the daylight saving time should end every year	First Second Third Fourth Last
End day	The specific day of the week on which the daylight saving time should end every year	Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday
End month	The specific month in which the daylight saving time should end every year	January, February, March, April, May, June, July, August, September, October, November, December
End time [HH:MM]	The specific time (hour and minute) at which the daylight saving time should end every year	00:00 – 23:59
Offset (minutes)	The fixed number of minutes that should be added to the local time during the daylight saving time period	0–720 Default: 60



```
              ACE-3600 - RAD Data Communications

Configuration> System> Date and Time> Summer time

1. Mode                         > (Date)
2. Start date [YYYY-MM-DD]    ...
3. Start time [HH:MM]         ...
4. End date [YYYY-MM-DD]      ...
5. End time [HH:MM]           ...
6. Offset (minutes)           ...

>
Please select item <1 to 6>
ESC-Previous menu; !-Main menu; &-Exit
```

Figure 4-30. Summer Time – Date Mode

Table 4-25. Summer Time – Date Mode Parameters

Parameter Description		Possible Values
Start date [YYYY-MM-DD]	The specific date (year-specific) on which the daylight saving time begins	0001-01-01 to 9999-12-31
Start time [HH:MM]	The specific time (hour and minute) at which the daylight saving time begins	00:00 – 23:59

Parameter	Description	Possible Values
End date [YYYY-MM-DD]	The specific date (year-specific) on which the daylight saving time ends. The end date cannot precede or be the same as the start date.	0001-01-01 to 9999-12-31
End time [HH:MM]	The specific time (hour and minute) at which the daylight saving time ends, on the end date	00:00 – 23:59
Offset (minutes)	The fixed number of minutes that should be added to the local time during the daylight saving time period	0–720 Default: 60

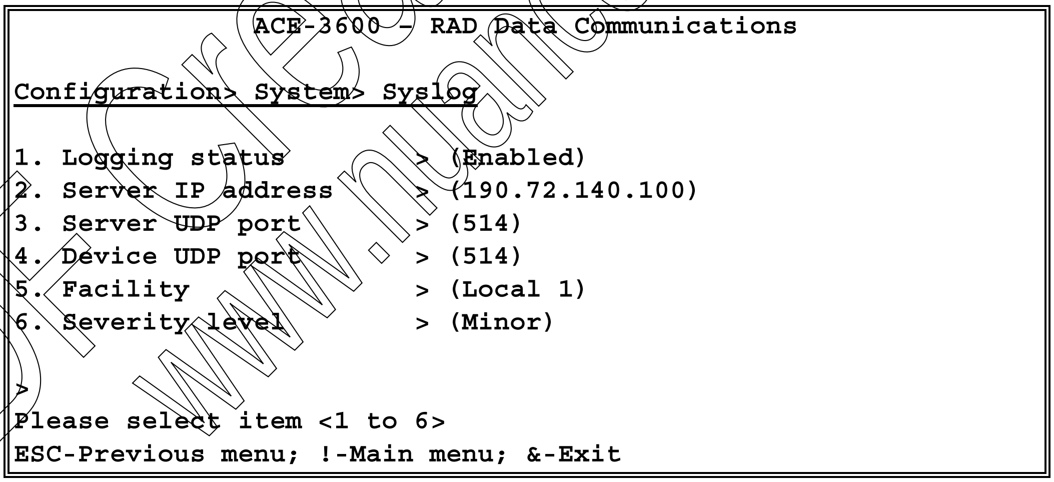
Setting the Syslog Parameters

Once the date and time are set, system events are logged accordingly. To allow logging/sharing of system events on a server instead of internally, you need to configure the Syslog server parameters.

➤ To access the Syslog server options:

- From the System menu (see *Figure 4-3*), select Syslog.

The Syslog menu is displayed.



```
                 ACE-3600 - RAD Data Communications

Configuration> System> Syslog

1. Logging status         > (Enabled)
2. Server IP address      > (190.72.140.100)
3. Server UDP port        > (514)
4. Device UDP port        > (514)
5. Facility               > (Local 1)
6. Severity level         > (Minor)


>
Please select item <1 to 6>
ESC-Previous menu; !-Main menu; &-Exit
```

Figure 4-31. Syslog Menu

Table 4-26. Syslog Server Parameters

Parameter Description		Possible Values
Logging status	Determines whether logging to the Syslog server is enabled or disabled. When disabled, ACE-3600 logs the events internally.	Enabled Disabled Default: Disabled
Server IP address	IP address of the Syslog server to which the event logs are sent.	0.0.0.0 – 255.255.255.255

Parameter	**Description**	**Possible Values**
Server UDP port	The UDP port of the Syslog server. ***Note:*** *The port cannot be changed when the logging status is enabled.*	1–65535 Default: 514
Device UDP port	The local UDP port from which the Syslog messages are sent. ***Note:*** *The port cannot be changed when the logging status is enabled.*	1–65535 Default: 514
Facility	Identifies the software module, task or function from which the Syslog messages are sent.	Local 1 – Local 7 Default: Local 1
Severity level	Only events that their severity equals or exceeds the selected severity level are sent. The severity levels are: • Critical – corresponds to the Emergency (0) severity level of Syslog • Major – corresponds to the Alert (1) and Critical (2) severity levels of Syslog • Minor – corresponds to the Error (3) severity level of Syslog • Warning – corresponds to the Warning (4) severity level of Syslog • Event – corresponds to the Notice (5) severity level of Syslog • Info – corresponds to the Informational (6) severity level of Syslog • Debug – corresponds to the Debug (7) severity level of Syslog ***Note:*** *The severity level can be changed only when the logging status is disabled.*	Critical Major Minor Warning Event Info Debug Default: Major

4.3 Configuring for Operation

This section describes in detail how to configure the parameters needed for normal operation of the unit:

- *Configuring the Physical Layer Parameters*
- *Setting the Protection Parameters*
- *Setting the Clock Source*
- *Configuring the Application Parameters*.

Configuring the Physical Layer Parameters

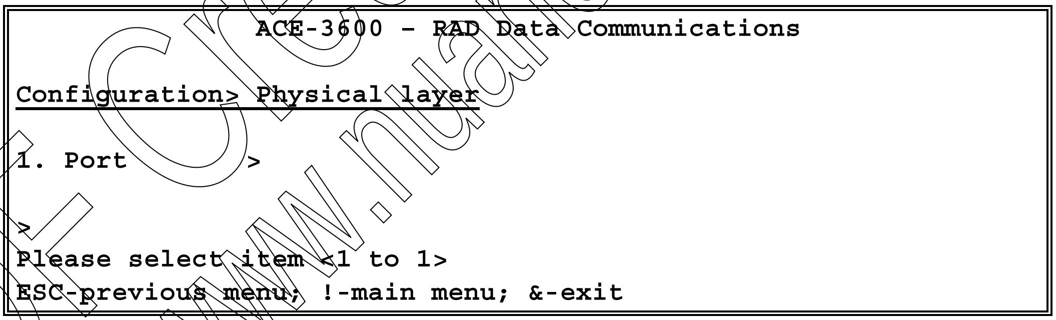
This stage consists of configuring the physical layer parameters of the Ethernet and SDH/SONET ports.

Note *In some menus you are required to select the port number. In general, for SDH/SONET ports, the number can be 1–4 or 5–8 depending on the number of installed modules and their location in the chassis.*

➤ To access the physical layer port options:

1. From the Configuration menu (see *Figure 4-2*), select Physical Layer.

   The Physical Layer menu is displayed.

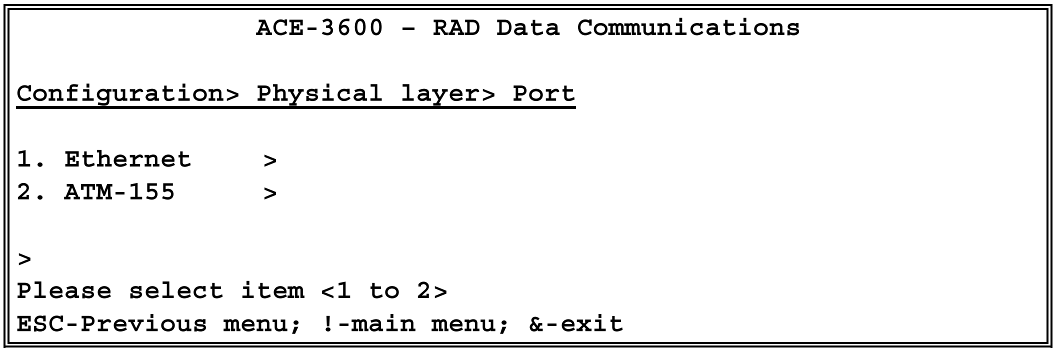


```
                 ACE-3600 - RAD Data Communications

Configuration> Physical layer

1. Port          >

>
Please select item <1 to 1>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-32. Physical Layer Menu

2. From the Physical Layer menu, select Port.

   The Port menu is displayed.



```
                 ACE-3600 - RAD Data Communications

Configuration> Physical layer> Port

1. Ethernet       >
2. ATM-155        >


>
Please select item <1 to 2>
ESC-Previous menu; !-main menu; &-exit
```

Figure 4-33. Port Menu

Table 4-27. Port Menu Parameters

Parameter	Description	Possible Values
Ethernet	Ethernet port configuration submenu	Refer to *Figure 4-34* and *Table 4-28*
ATM-155	SDH/SONET port configuration menu	Refer to *Figure 4-35* and *Table 4-29*

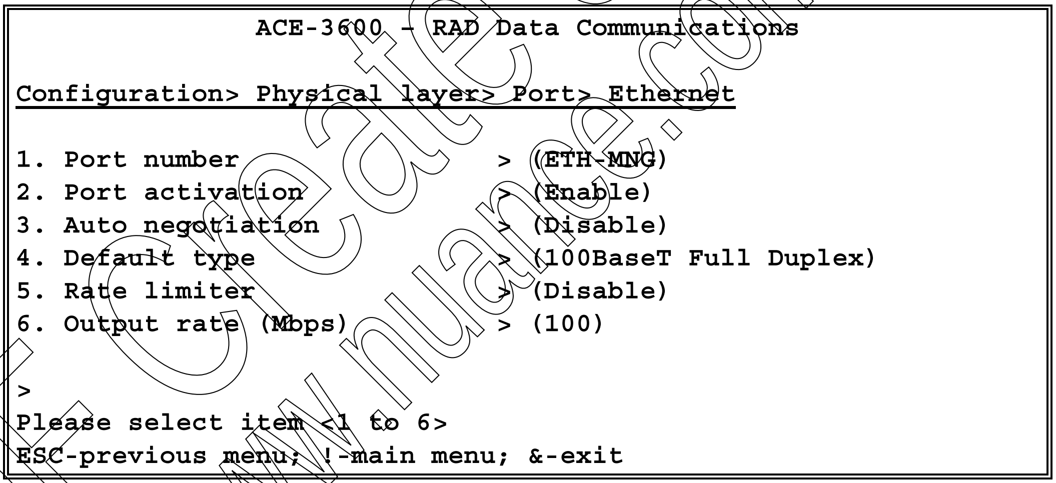
Configuring the Ethernet Ports

ACE-3600 includes two electrical or fiber optic Gigabit Ethernet ports for user data and inband management, and a built-in 100BaseT port for out-of-band management. The physical layer setting of each port is configured individually via the Ethernet port configuration menu.

➤ To access the Ethernet port settings:

- From the Port menu (see *Figure 4-33*), select Ethernet.

  The Ethernet port configuration menu is displayed.



```
                ACE-3600 - RAD Data Communications

Configuration> Physical layer> Port> Ethernet

1. Port number                  > (ETH-MNG)
2. Port activation              > (Enable)
3. Auto negotiation             > (Disable)
4. Default type                 > (100BaseT Full Duplex)
5. Rate limiter                 > (Disable)
6. Output rate (Mbps)           > (100)

>
Please select item <1 to 6>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-34. Ethernet Port Configuration Menu

Table 4-28. Ethernet Port Configuration Parameters

Parameter	Description	Possible Values
Port number	Select the Ethernet port that you want to configure. For each selected port, different parameters may be displayed and saved. ETH-MNG is the out-of-band Ethernet management port.	GbE-1 GbE-2 ETH-MNG Default: ETH-MNG

Parameter	Description	Possible Values
Port activation	Status of the selected port in both the RX and TX directions. When the port is disabled, the TX and RX paths are disabled. Log file events or traps are not sent from this port upon physical layer events. *Note:* • *The port cannot be disabled when it belongs to a redundancy group (see Setting the Ethernet Redundancy).* • *The ETH-MNG port is disabled only terms of events and alarms.*	Enable Disable Default: Enable
Auto negotiation	Status of the autonegotiation mode for the selected port. Valid only when Port activation is set on 'Enable'. The autonegotiation mode is disabled for the out-of-band Ethernet management port (ETH-MNG), since it cannot respond in this mode.	Disable only – when ETH-MNG is selected Enable or Disable – When any GbE port is selected Default: Disable – for ETH-MNG Enable – for any GbE port
Max capacity advertised	Identifies the set of capabilities advertised by the local autonegotiation entity. Visible only for the GbE ports and only if autonegotiation is enabled.	1000BaseT Full Duplex
Default type	The default rate and duplex mode, to be used if auto-negotiation is disabled.	10BaseT Half Duplex 10BaseT Full Duplex 100BaseT Half Duplex 100BaseT Full Duplex 1000BaseT Full Duplex (for GbE ports) Default: 100BaseT Full Duplex (for the ETH-MNG port) 1000BaseT Full Duplex (for the GbE ports)
Rate limiter	Enable or disable rate limiting on the displayed Ethernet port. *Note: This option is not relevant for the ETH-MNG port.*	Enable Disable Default: Disable
Output rate (Mbps)	Set the Mbps rate for the Ethernet port. Visible only if the Rate limiter option (see above) is enabled.	1–1000

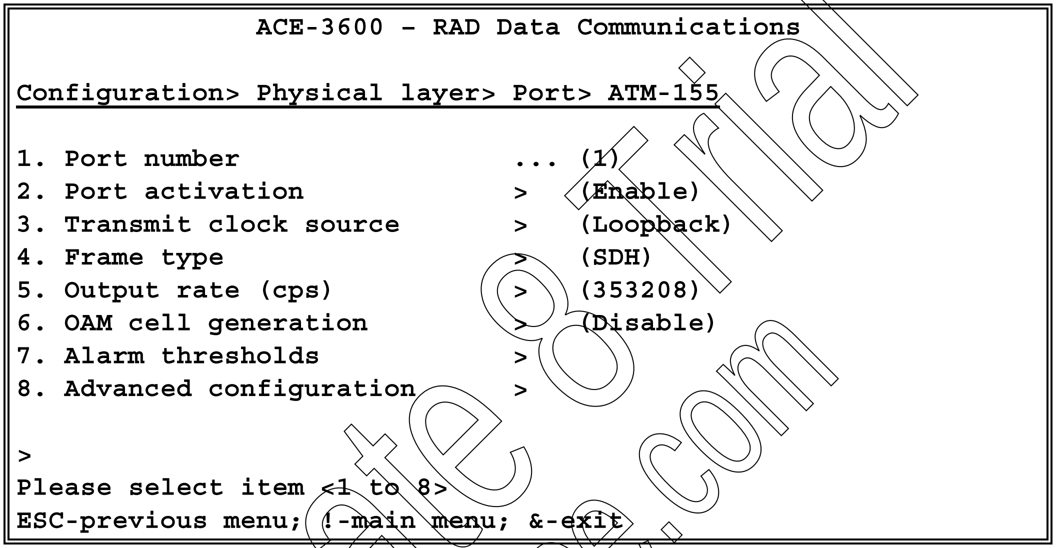
Configuring the ATM-155 Ports

The SDH/SONET ports (up to 8) in ACE-3600 are used for ATM-155 (155 Mbps) fiber optic uplink, and are configured via the ATM-155 menu.

➤ To access the ATM-155 configuration menu:

- From the Port menu (see *Figure 4-33*), select ATM-155.

The ATM-155 configuration menu is displayed.



```
                ACE-3600 - RAD Data Communications

Configuration> Physical layer> Port> ATM-155

1. Port number                     ...  (1)
2. Port activation                 >    (Enable)
3. Transmit clock source           >    (Loopback)
4. Frame type                      >    (SDH)
5. Output rate (cps)               >    (353208)
6. OAM cell generation             >    (Disable)
7. Alarm thresholds                >
8. Advanced configuration          >

>
Please select item <1 to 8>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-35. ATM-155 Port Configuration Menu

Table 4-29. ATM-155 Port Configuration Parameters

Parameter	Description	Possible Values
Port number	The specific ATM-155 port number for which the details are displayed	1–8
Port activation	Enable/disable the SDH/SONET port in both Rx and Tx directions. No log file events or traps are sent from this port upon physical layer events. You can disable the port even if XC connections exist. ***Note:*** • *The port cannot be disabled if it is in Loopback state or if it works in APS mode.*	Enable Disable **Default: Enable**
Transmit clock source	The source of the port's transmit (Tx) clock. Not valid for ports 1 and 2 if APS is active. For more information about the loopback and system TX clock source, see *Appendix D.*	System
Frame type	The cell frame type. The frame type can be changed dynamically (on-the-fly).	SONET SDH **Default: SDH**

Parameter	Description	Possible Values
Output rate	The ATM-155 port's output rate in cells per second. *Note:* • *The output rate must be equal to or higher than the* ***minimum output rate****, which is defined in the Advanced Configuration menu (see Figure 4-37).* • *The output rate value that you enter is automatically rounded downwards to the closest possible granular value, which is calculated based on the minimum output rate value. The granularity difference will be less significant if the entered output rate is closer to the minimum output rate (see Advanced Configuration below). If you would like to calculate granularity differences for your specific application, an Excel sheet can be obtained from Technical Support.*	100–353208 Default: 353208
OAM cell generation	Enable or disable the automatic generation of OAM cells in case of physical layer failure.	Enable Disable Default: Disable
Alarm thresholds	Provides access to the ATM-155 port's alarm thresholds configuration menu.	Refer to *Figure 4-36*
Advanced configuration	Provides access to the ATM-155 port's advanced configuration menu.	Refer to *Figure 4-37*

Note

- *Two SDH/SONET ports that are intended to work in APS (1+1 protection) mode must have identical parameter values.*
- *In APS mode, any parameter change that is applied on the Port 1 is automatically applied on Port 2. Parameters that are displayed for Port 2 cannot be modified and are read-only as long as the APS mode is in effect.*
- *If OAM cells generation is enabled in APS mode, the cells are generated only if both Port 1 and Port 2 have a failure.*

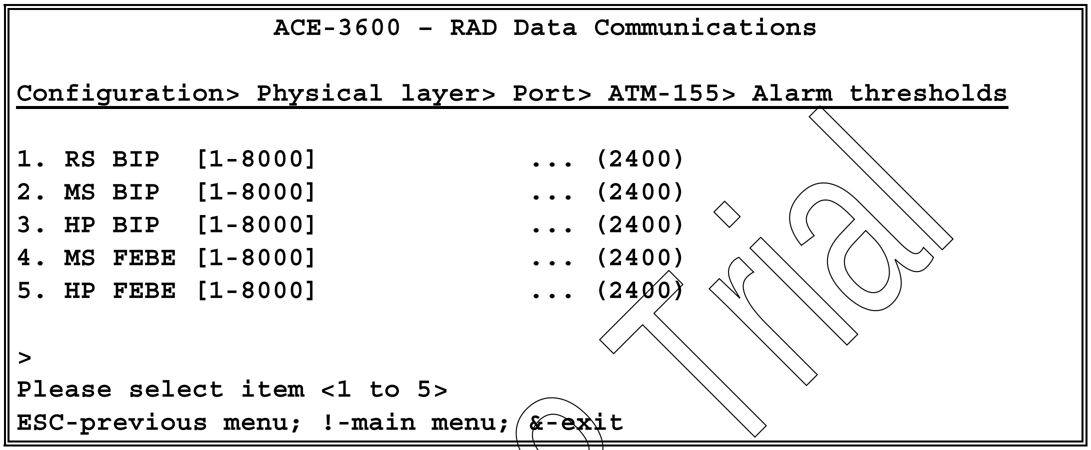
Configuring the SDH/SONET Port's Alarm Thresholds

The alarm thresholds define the number of errored SDH/SONET frames that can be detected before a physical alarm state is initiated. Each of the five alarm categories (RS/Section BIP, MS/Line BIP, HP/Path BIP, MS/Line FEBE and HP/Path HEBE) has a specific threshold, which can be set individually.

➤ To access the Alarm Thresholds configuration menu:

- From the ATM-155 menu (see *Figure 4-35*), select **Alarm Thresholds**.

  The Alarm Thresholds menu is displayed.



```
                    ACE-3600 - RAD Data Communications

Configuration> Physical layer> Port> ATM-155> Alarm thresholds

1. RS BIP   [1-8000]              ... (2400)
2. MS BIP   [1-8000]              ... (2400)
3. HP BIP   [1-8000]              ... (2400)
4. MS FEBE  [1-8000]              ... (2400)
5. HP FEBE  [1-8000]              ... (2400)

>
Please select item <1 to 5>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-36. Alarm Thresholds Menu

Table 4-30. Alarm Thresholds Menu Parameters

Parameter	Description	Possible Values
RS/Section BIP	RS/Section BIP alarm threshold. "RS BIP" is for SDH and "Section BIP" is for SONET frame type.	1–8000 Default: 2400
MS/Line BIP	MS/Line BIP alarm threshold. "MS BIP" is for SDH and "Line BIP" is for SONET frame type.	1–8000 Default: 2400
HP/Path BIP	HP/Path BIP alarm threshold. "HP BIP" is for SDH and "Path BIP" is for SONET frame type.	1–8000 Default: 2400
MS/Line FEBE	MS/Line FEBE alarm threshold. "MS BIP" is for SDH and "Line BIP" is for SONET frame type.	1–8000 Default: 2400
HP/Path FEBE	HP/Path FEBE alarm threshold. "HP BIP" is for SDH and "Path BIP" is for SONET frame type.	1–8000 Default: 2400

Note *Physical layer events/traps are triggered and sent only when the set alarm threshold is exceeded.*

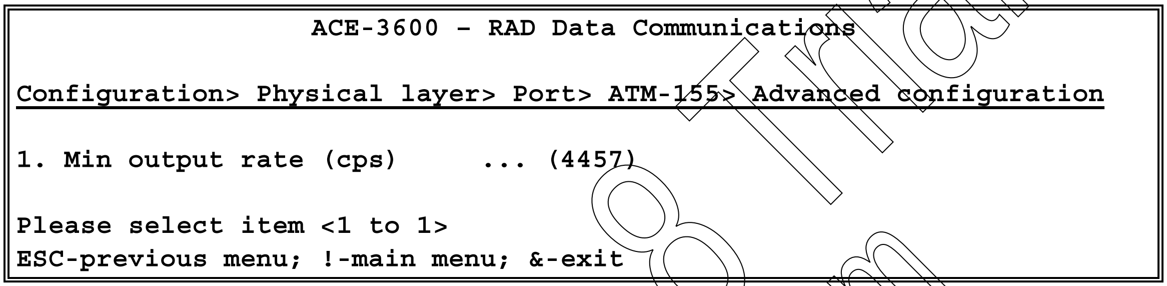
Setting the SDH/SONET Port's Minimum Output Rate

The SDH/SONET port's minimum output rate defines the lowest possible value that can be entered in the general SDH/SONET output rate definition, as explained in *Table 4-29* (*ATM-155 Port Configuration Parameters*). The minimum output rate is set in the Advanced Configuration menu.

➤ To access the advanced configuration menu:

- From the ATM-155 menu (see *Figure 4-36*), select Advanced Configuration.

  The Advanced Configuration menu is displayed.



```
                    ACE-3600 - RAD Data Communications

Configuration> Physical layer> Port> ATM-155> Advanced configuration

1. Min output rate (cps)      ... (4457)

Please select item <1 to 1>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-37. Advanced Configuration Menu

Table 4-31. Advanced Configuration Parameters

Parameter Description		Possible Values
Min output rate (cps)	The minimum cell output rate that may be configured for the ATM-155 ports, in cells per second (cps).	100–353208 Default: 4457

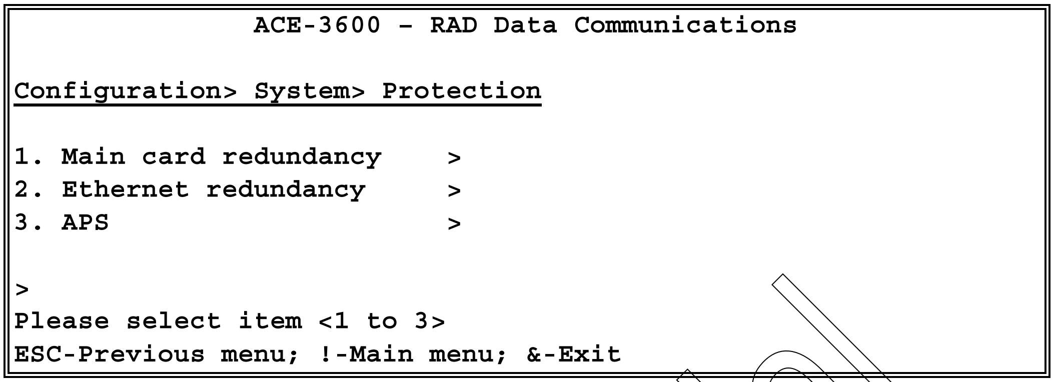
Setting the Protection Parameters

As described in *Chapter 1*, ACE-3600 supports full system redundancy, including main module (main card) redundancy, Ethernet port redundancy and automatic protection switching (APS) for its ATM-155 ports.

➤ To access the protection options:

- From the System menu, select Protection.

  The Protection menu is displayed.



```
                    ACE-3600 - RAD Data Communications

Configuration> System> Protection

1. Main card redundancy     >
2. Ethernet redundancy      >
3. APS                      >

>
Please select item <1 to 3>
ESC-Previous menu; !-Main menu; &-Exit
```

Figure 4-38. Protection Menu

Table 4-32. Protection Options

Parameter	Description	Possible Values
Main card redundancy	Access the main module protection options	See *Setting the Main Module Redundancy*
Ethernet redundancy	Access the GbE port protection options	See *Setting the Ethernet Redundancy*
APS	Access the ATM-155 port protection options	See *Setting Automatic Protection Switching (APS)*

Setting the Main Module Redundancy

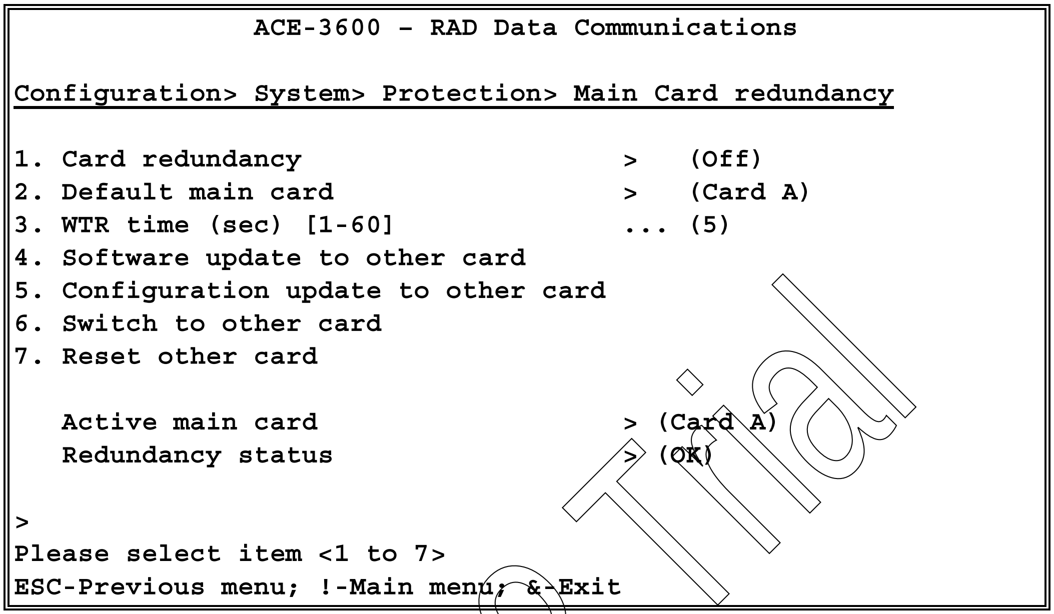
ACE-3600 supports the installation of two main modules (main cards) in order to ensure fail-safe operation. If the unit was ordered with two main modules, you can activate the main module protection feature. Alternatively, if the module protection is disabled, you can select the main module that the unit should use by default.

Additional features include: setting the WTR time, updating software or configuration, switching between modules and performing reset. All these functions are available via the Card Redundancy menu.

➤ To access the Card Redundancy menu:

- From the Protection menu (see *Figure 4-3*), select Main Card Redundancy.

  The Main Card Redundancy menu is displayed.



```
                    ACE-3600 - RAD Data Communications

Configuration> System> Protection> Main Card redundancy

1. Card redundancy                     >   (Off)
2. Default main card                   >   (Card A)
3. WTR time (sec) [1-60]               ... (5)
4. Software update to other card
5. Configuration update to other card
6. Switch to other card
7. Reset other card

   Active main card                    > (Card A)
   Redundancy status                   > (OK)

>
Please select item <1 to 7>
ESC-Previous menu; !-Main menu; &-Exit
```

Figure 4-39. Card Redundancy Menu

Table 4-33. Card Redundancy Menu Options

Parameter Description		Possible Values
Card redundancy	Enables or disables the module redundancy protection.	On Off Default: Off
Default main card	Defines which is the active module in case the redundancy protection is turned off. Module A (Card A) is located on top of module B (Card B).	Card A Card B Default: Card A
WTR time (sec)	Wait to Restore time, in seconds. Defines the length of delay that is required between two consecutive switch operations. The WTR time can be changed only when the redundancy protection is turned off.	1–60 Default: 5
Software update to other card	Updates/copies the current software version (of the active module) onto the standby module.	
Configuration update to other card	Updates/copies the current configuration (of the active module) onto the standby module.	

Parameter	Description	Possible Values
Switch to other card	Switches the control over ACE-3600 to the other installed main module. Available only when the redundancy protection is turned on.	
Reset other card	Resets the standby module (not the active module).	
Active main card	Indicates which main module (card) is currently the active one. Module A (Card A) is located on top of module B (Card B).	Card A Card B
Redundancy status	Displays the current redundancy status. There are four status types: • OK – redundancy is up and running fine • Card A/B absent – the specified module is physically missing • Communication loss – the two main modules are not communicating • Mismatch – the two modules differ in their hardware, software or configuration.	OK Card A absent Card B absent Communication loss Hardware mismatch Software mismatch Configuration mismatch

Note

- *All redundancy options are not applied or activated during the software/configuration update process. A device reset is necessary first.*
- *The software/configuration update and the switch operations are not available if there is a hardware mismatch (the two modules are not identical), when a module is absent or when the redundancy protection is turned off.*
- *In case Card Redundancy is used, it is recommend to perform a configuration update to the standby card once the configuration is finished.*

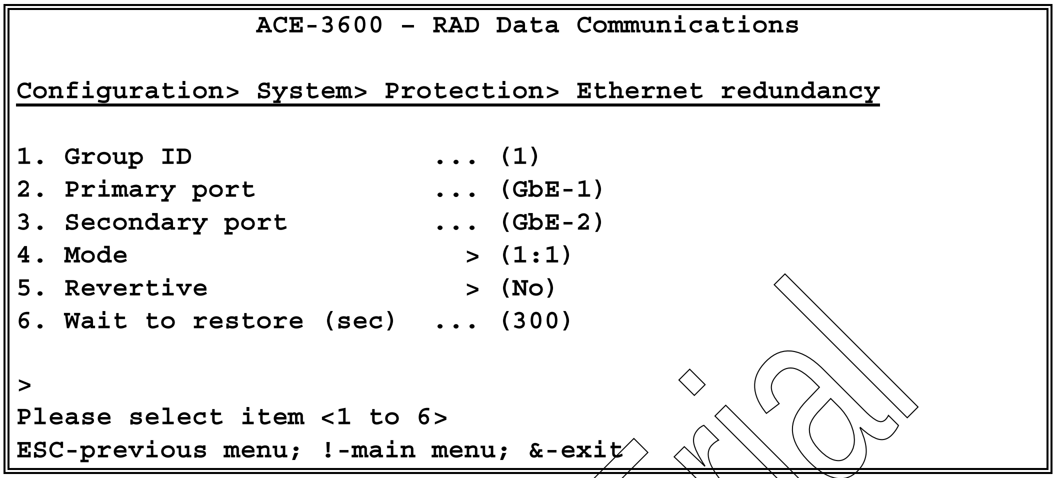
Setting the Ethernet Redundancy

ACE-3600 allows its two Gigabit Ethernet ports (if two are installed) to work in redundancy mode, allowing reliable and uninterrupted service over packet-switched networks. The Gigabit Ethernet ports support the 1:1 and 1+1 automatic protection switching modes according to IEEE 802.3ad.

➤ To access the Ethernet port redundancy options:

- From the Protection menu (see *Figure 4-38*), select Ethernet Redundancy.

  The Ethernet Redundancy menu is displayed.



```
                 ACE-3600 - RAD Data Communications

Configuration> System> Protection> Ethernet redundancy

1. Group ID                  ... (1)
2. Primary port              ... (GbE-1)
3. Secondary port            ... (GbE-2)
4. Mode                        > (1:1)
5. Revertive                   > (No)
6. Wait to restore (sec)     ... (300)

>
Please select item <1 to 6>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-40. Ethernet Redundancy Menu

Table 4-34. Ethernet Redundancy Parameters

Parameter Description		Possible Values
Group ID	ID of the Ethernet redundancy group. Only one group can be configured.	1
Primary port	The primary (protected) GbE port in the redundancy group. See Note after this table.	GbE-1, GbE-2 **Default: GbE-1**
Secondary port	The secondary (protection) GbE port in the redundancy group. See Note after this table.	GbE-1, GbE-2 **Default: GbE-2**
Mode	The method of redundancy. For more information, refer to *Ethernet Redundancy* in Chapter 1.	1+1 (Link aggregation) 1:1 Default: **1:1**

Parameter	Description	Possible Values
Revertive	If 'Revertive' is enabled ('Yes' is selected), the port protection switching is reverted back to the primary link as it was before the link failure, since the primary link is up again. The revert is performed once the WTR time is concluded (see below).	Yes No Default: No
Wait to restore (sec)	Wait to Restore time, in seconds. WTR is the set delay time required before the primary port returns to be the active port, once the port becomes available after recovering from an error. Relevant only if 'Revertive' mode is enabled (see above). This parameter cannot be changed dynamically (on-the-fly).	1–720 Default: 300

Note

The GbE port can be selected if:

- *The port is active*
- *Autonegotiation is enabled*
- *A router interface configuration is missing.*

Setting Automatic Protection Switching (APS)

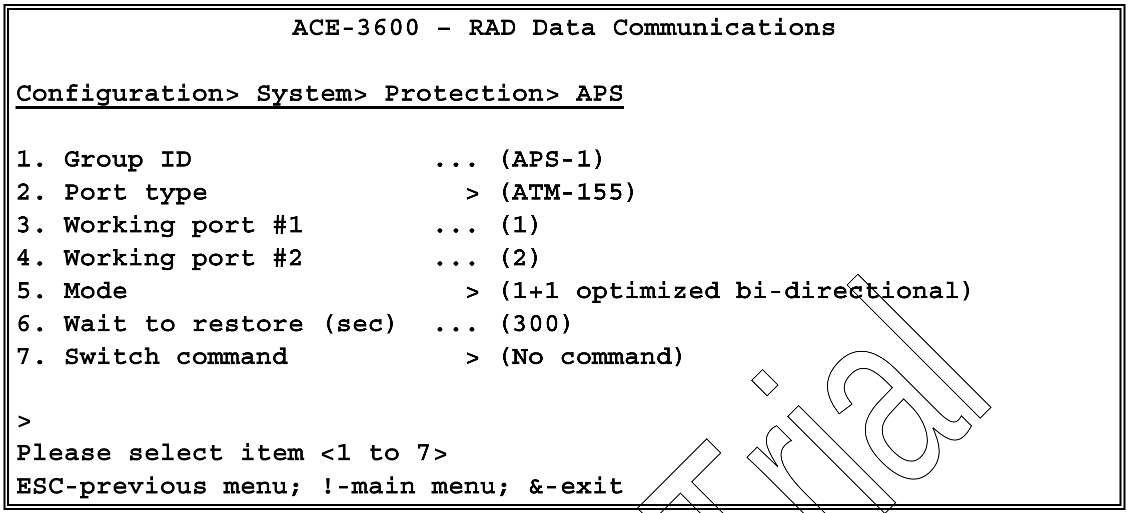
As explained in *Chapter 1*, two ATM-155 ports can work correspondingly in APS mode. The APS configuration screen allows you to specify the two working ports and their operational mode, which can be either of the following:

- 1+1 optimized bi-directional – according to G.841, Annex B
- 1+1 compatible bi-directional – according to G.841, Clause 7.1, Linear multiplex section protection (MSP); compatible with 1:n bidirectional switching.

➤ To access the APS configuration menu:

- From the Physical Layer menu (see *Figure 4-32*), select APS.

  The APS configuration menu is displayed.



```
                ACE-3600 - RAD Data Communications

Configuration> System> Protection> APS

1. Group ID                ...  (APS-1)
2. Port type                 >  (ATM-155)
3. Working port #1         ...  (1)
4. Working port #2         ...  (2)
5. Mode                      >  (1+1 optimized bi-directional)
6. Wait to restore (sec)   ...  (300)
7. Switch command            >  (No command)

>
Please select item <1 to 7>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-41. APS Configuration Menu

Table 4-35. APS Configuration Parameters

Parameter	Description	Possible Values
APS group ID	ID string of the APS group of which details are displayed. ACE-3600 supports four APS groups.	Up to 32 alphanumeric characters, case-sensitive Default: APS-1
Port type	The physical port type	ATM-155
Working port #1	The APS working port #1	1–4
Working port #2	The APS working port #2. The second port is automatically selected if APS is enabled on port #1.	5–8
Mode	The APS operation mode	1+1 optimized bi-directional 1+1 compatible bi-directional Default: 1+1 optimized bi-directional
WTR time (sec)	Wait to Restore time, in seconds. In APS mode, WTR is the set delay time required before the primary port returns to normal operation, once the port becomes available after recovering from an error. This parameter cannot be changed dynamically (on-the-fly).	1–720 Default: 300

Parameter	Description	Possible Values
Switch command – options available for the 1+1 optimized bi-directional APS mode	The APS port switching command. Available only if the APS mode is enabled (if an APS group ID exists). There are four possible switch commands in the 1+1 optimized bi-directional mode: • No command – the initial state, if no command was applied since the unit's initialization. • Force Switch – the service is switched from the primary port to the secondary port. Can be selected only when No Command or Clear is the current state. • Lockout –freeze the transmitted K-bytes and the selector's position (the traffic is taken from the port which is currently primary) until the lockout is cleared. Lockout is considered a local request that is not signaled over the K-bytes. Can be selected only when No Command or Clear is the current state. • Clear – Clear the current command (Force Switch or Lockout). If the 'Lockout' command is cleared, the selector and the transmitted K-bytes return to their previous state. If the 'Force Switch' command is cleared, the primary line returns to be the currently active line, and the local request for lockout is cleared.	No command Force switch Lockout Clear Default: No command
Switch command – options available for the 1+1 compatible bi-directional APS mode	The APS port switching command. Available only if the APS mode is enabled (if an APS group ID exists). There are four possible switch commands in the 1+1 compatible bi-directional mode: • No command – the initial state, if no command was applied since the unit's initialization. • Force Switch to working – switches the normal traffic from the protection port to the working port, unless an equal or higher priority request exists. Since a forced switch has a higher priority than SF or SD on a working port, this command is carried out regardless of the current condition of the working port. For more general information about the APS functionality, refer to *Chapter 1*. • Force switch to protection – switches the normal traffic of the working port to the	Force switch to working Force switch to protection Manual switch to working Manual switch to protection Lockout of protection Clear Default: No command

Parameter	Description	Possible Values
	protection port, unless an equal or higher priority switch command is in effect, or if an SF condition exists on the protection port. • Manual switch to working – switches the traffic from the protection port back to the working port, unless an equal or higher priority request is in effect. Since a manual switch has lower priority than SF or SD on a working port, this command is carried out only if the working port is not in SF or SD condition. • Manual switch to protection – switches the traffic from the working port to the protection port, unless a failure condition exists on the protection port or an equal/higher priority switch command is in effect. The command is carried out by issuing a manual switch request for the normal traffic signal. • Lockout of protection – denies the access of all normal traffic signals (as well as extra traffic signals, if applicable) to the protection port by issuing a "Lockout of protection" request, unless an equal protection switch command is in effect. • Clear – clears all externally initiated switch commands and the WTR time, on the node to which the command was addressed. *Notes:* • *Only one command can be applied at a time* • *Issuing a 'force switch' or 'lockout' is possible only if 'No Command' or 'Clear' is the current command status.* • *'No Command' is only an initial state and cannot be selected as a user command.* • *'Clear' is availale only if the current command value is 'force switch' or 'lockout'.*	

Note

The APS mode cannot be activated if:

- *Connections are already configured on the ATM-155 Port 2.*
- *The transmit (TX) clock of any port is set on Loopback mode.*
- *Port activation is disabled.*
- *The physical layer port configuration for both Port 1 and Port 2 is not identical.*

Setting the Clock Source

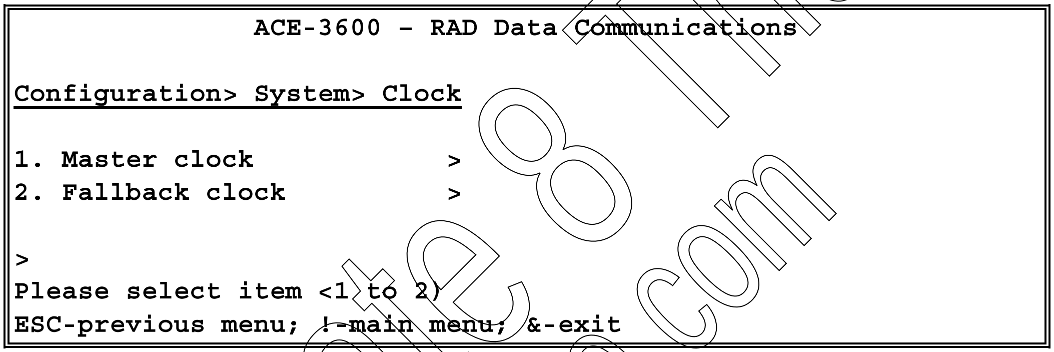
ACE-3600 requires a distinct clock source and a defined system clock in order to fulfill its purpose in a given backhauling application. For more information about the system clock, see *Appendix D*.

Accordingly, you have to select the clock source type, as well as the ports of the master (primary) and fallback (secondary) system clocks, which will be used as the source clocks for all STM-1/OC-3c ports.

➤ To access the Clock options:

- From the System menu (see *Figure 4-3*), select Clock.

The Clock menu is displayed.



```
                 ACE-3600 - RAD Data Communications

Configuration> System> Clock

1. Master clock               >
2. Fallback clock             >

>
Please select item <1 to 2)
ESC-previous menu; !-main menu; &-exit
```

Figure 4-42. Clock Menu

Table 4-36. Clock Menu Options

Parameter	Description	Possible Values
Master Clock	Access the master (primary) clock settings	See *Setting the Master Clock*
Fallback clock	Access the fallback (secondary) clock settings. For more information about the master and fallback clock sources, refer to *Appendix D*.	See *Setting the Fallback Clock*

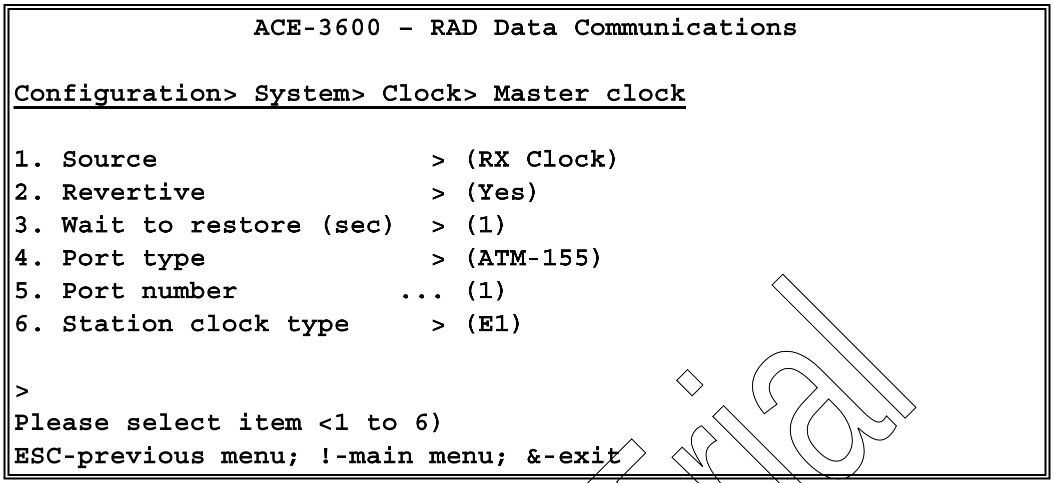
Setting the Master Clock

The master clock is used as the primary clock source of ACE-3600 and must be set prior to starting any backhauling service. The master clock can be derived from either the RX clock of a specific interface or the station clock. For more information about the master clock functionality, refer to *Appendix D*.

➤ To access the master clock options:

- From the Clock menu (see *Figure 4-42*), select Master Clock.

The Master Clock menu is displayed.



```
                    ACE-3600 - RAD Data Communications

Configuration> System> Clock> Master clock

1. Source                  > (RX Clock)
2. Revertive               > (Yes)
3. Wait to restore (sec)   > (1)
4. Port type               > (ATM-155)
5. Port number           ... (1)
6. Station clock type      > (E1)

>
Please select item <1 to 6)
ESC-previous menu; !-main menu; &-exit
```

Figure 4-43. Master Clock Menu

Table 4-37. Master Clock Parameters

Parameter	Description	Possible Values
Source	The clock source type	• RX Clock – the clock is derived from the incoming traffic of one of the unit's ports. • Station – the clock is provided from the station clock port. Default: RX Clock
Revertive	Indicates whether the Revertive mode is enabled, i.e. – whether the master clock will return to be the system clock after a period of unavailability (if unavailability occurs).	Yes No Default: Yes
Wait to restore (sec)	The number of waiting seconds before the master clock will return to be the system clock (if the Revertive mode is enabled).	1–720 Default: 1
Port type	Type of the master clock port. Visible only if RX Clock was selected as the clock source.	ATM-155
Port number	Number of the port that is used as the master clock. ***Note:*** *It is not permitted to set both the master and fallback clocks on the same port number.*	1–8 for one of the ATM-155 ports 1 (non-selectable) for the station clock port

Parameter	Description	Possible Values
Station clock type	The type of the station clock's circuit line, if the station clock was selected to serve as the system clock.	E1 T1 Default: E1

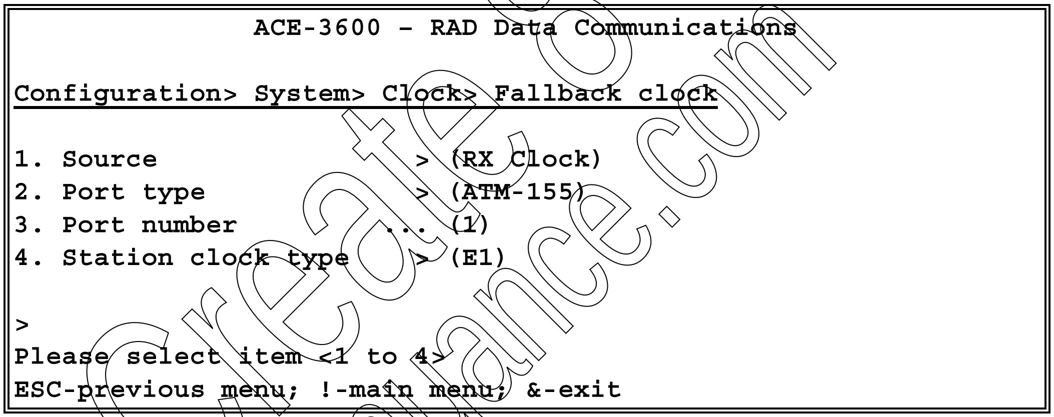
Setting the Fallback Clock

The fallback clock is used as the secondary clock source of ACE-3600 in cases when the master clock is down/unreachable. For more information about the fallback clock functionality, refer to *Appendix D*.

➤ To access the fallback clock options:

- From the Clock menu (see *Figure 4-42*), select Fallback Clock.

  The Fallback Clock menu is displayed.



```
                    ACE-3600 - RAD Data Communications

Configuration> System> Clock> Fallback clock

1. Source                > (RX Clock)
2. Port type             > (ATM-155)
3. Port number         ... (1)
4. Station clock type    > (E1)

>
Please select item <1 to 4>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-44. Fallback Clock Menu

Table 4-38. Fallback Clock Parameters

Parameter Description		Possible Values
Source	The clock source type	• RX Clock – the clock is derived from the incoming traffic of one of the unit's ports. • Station – the clock is provided from the station clock port. • None – No port is assigned to be a system clock source.
Port type	Type of the master clock port. ***Note**: Visible only if RX Clock was selected as the clock source.*	ATM-155

Parameter	Description	Possible Values
Port number	Number of the port that is used as the master clock. ***Note:*** *It is not permitted to set both the master and fallback clocks on the same port number.*	1–8 for one of the ATM-155 ports 1 (non-selectable) for the station clock port Pseudowire channel number for PSN clock
Station clock type	The type of the station clock's circuit line, if the station clock was selected to serve as the system clock.	E1 T1 Default: E1

Configuring the Application Parameters

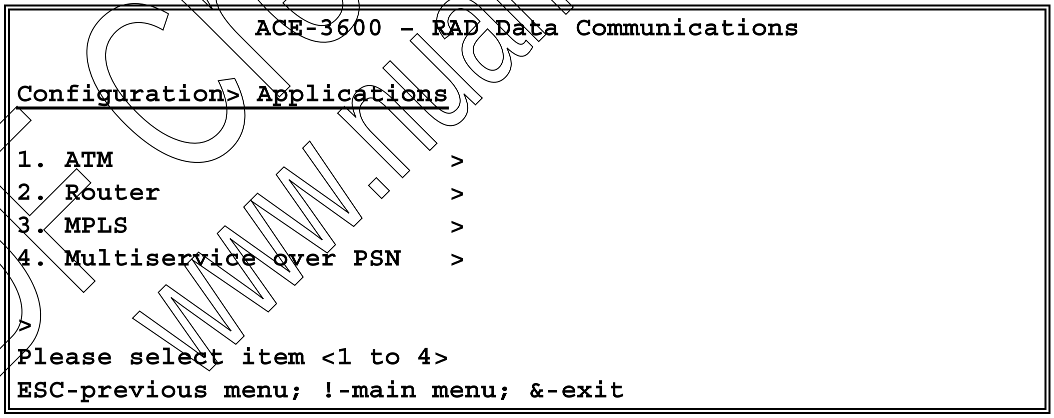
This stage consists of configuring the application parameters, which include the ATM, router, MPLS and PSN functionality categories.

The application parameters are configured according to the nature of the specific application in which ACE-3600 is used. To learn about a typical application, refer to *Chapter 5*.

➤ To access the Application functionality options:

- From the Configuration menu (see *Figure 4-2*), select **Applications**.

  The Applications menu is displayed.



```
             ACE-3600 - RAD Data Communications

Configuration> Applications

1. ATM                          >
2. Router                       >
3. MPLS                         >
4. Multiservice over PSN        >


>
Please select item <1 to 4>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-45. Applications Menu

Table 4-39. Application Functionality Categories

Parameter	Description	Possible Values
ATM	Provides access to the ATM functionality parameters	Refer to *Configuring ATM Parameters* below
Router	Provides access to the router functionality parameters	Refer to *Configuring Router Parameters*

MPLS	Provides access to the MPLS functionality parameters	Refer to *Configuring MPLS Parameters*
Multiservice over PSN	Provides access to the PSN functionality parameters	Refer to *Configuring Multiservice over PSN Parameters*

Configuring ATM Parameters

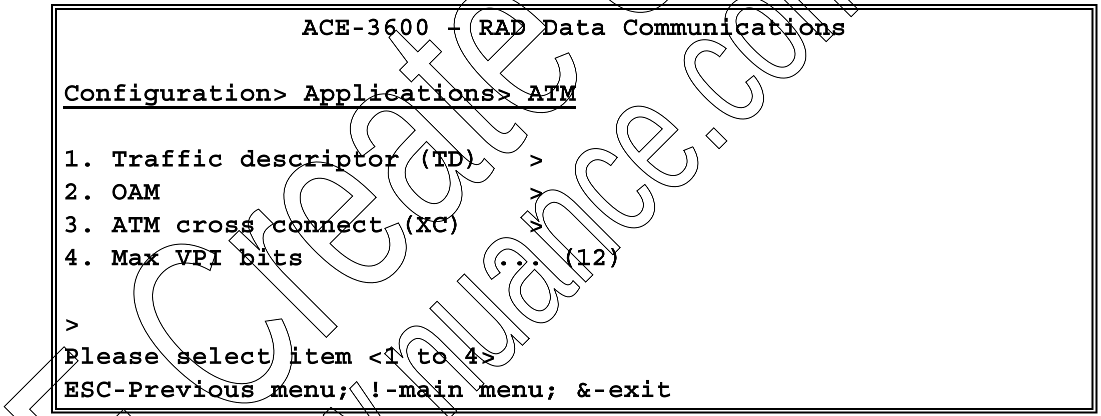
The ATM functionality configuration includes the following tasks:

- *Configuring Traffic Descriptors*
- *Configuring OAM Parameters*
- *Configuring the ATM Cross-Connect (XC) Parameters*.

➤ To access the ATM configuration menu:

- From the Applications menu, select ATM.

The ATM menu displayed.



```
                    ACE-3600 - RAD Data Communications

Configuration> Applications> ATM

1. Traffic descriptor (TD)     >
2. OAM                         >
3. ATM cross connect (XC)      >
4. Max VPI bits            ... (12)

>
Please select item <1 to 4>
ESC-Previous menu; !-main menu; &-exit
```

Figure 4-46. ATM Menu

Table 4-40. ATM Menu Parameters

Parameter	Description	Possible Values
Traffic descriptor (TD)	Provides access to the traffic descriptors configuration	Refer to *Figure 4-47*
OAM	Provides access to the OAM loopback configuration	Refer to *Figure 4-48*
ATM cross connect (XC)	Provides access to the ATM XC parameters configuration	Refer to *Figure 4-50*
Max VPI bits	Defines whether the ATM ports work in UNI (8 bits) or NNI (12 bits) mode. Cannot be changed when connections exist.	• 8 – For UNI • 12 – For NNI Default: 12

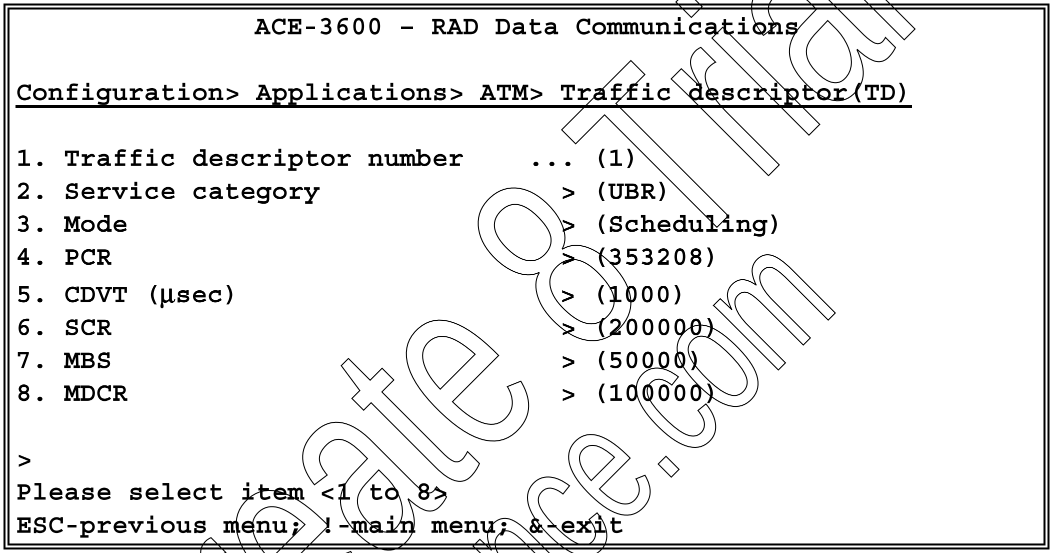
Configuring Traffic Descriptors

Traffic descriptors (TDs) determine the ATM traffic's service category, shaping mode and other distinct parameters, and are configured as ATM application parameters. Each traffic descriptor is configured individually via the Traffic Descriptor menu.

➤ To access the Traffic Descriptor menu:

- From the ATM menu (see *Figure 4-46*), select Traffic descriptor (TD).

    The Traffic Descriptor menu is displayed.



```
                 ACE-3600 - RAD Data Communications

Configuration> Applications> ATM> Traffic descriptor(TD)

1. Traffic descriptor number    ... (1)
2. Service category               > (UBR)
3. Mode                           > (Scheduling)
4. PCR                            > (353208)
5. CDVT (µsec)                    > (1000)
6. SCR                            > (200000)
7. MBS                            > (50000)
8. MDCR                           > (100000)

>
Please select item <1 to 8>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-47. Traffic Descriptors Menu

Table 4-41. Traffic Descriptors Menu Parameters

Parameter	Description	Possible Values
Traffic descriptor number	The traffic descriptor's serial number. Use the Forward (F) and Backward (B) keys to browse through the existing traffic descriptors.	1–99999 Default: 1 *Note: The default traffic descriptor is always 1 and this assignment cannot be changed or deleted.*
Service category	The service category for the currently configured traffic descriptor. ***Note:*** *CBR-CES is not selectable – it is created automatically when a CES XC is created.*	CBR VBR1 VBR2 VBR3 UBR+ UBR UBR1 UBR2 CBR-CES Default: UBR

Parameter	**Description**	**Possible Values**
Mode	Determines whether the TD is shaped or not. ***Note:*** • *The shaping mode cannot be changed for an existing traffic descriptor.* • *Shaped mode cannot be configured for UBR service category.* • *Unshaped mode cannot be configured for VBR1 and UBR+ service categories.*	Scheduling Scheduling&Shaping Policing Default: Scheduling
PCR	Peak cell rate in cells per second. ***Note:*** *In unshaped mode, this parameter is not applicable.*	100–353208
CDVT	Cell delay variation tolerance in µsec. ***Note:*** • *In unshaped mode, this parameter is not applicable.* • *The CDVT value cannot be enforced accurately.*	1–80000
SCR	Sustainable cell rate in cells per second. ***Note:*** • *Must be lower than the PCR.* • *In unshaped mode, this parameter is not applicable.* • *Valid only for VBR1 TD type.*	100–353208
MBS	Max burst size in cells. ***Note:*** *Valid only for VBR1 TD Type.*	1–8388608
MDCR	Minimum desired cell rate in cells. Set to zero (0) in unshaped mode. ***Note:*** • *Must be lower than the PCR, with a difference greater than 100.* • *Valid only for UBR+ TD type.*	100–353208

Note

- *The traffic descriptor type is not configurable; it is automatically set by the system according to the service category (for more information, see ATM Cell Scheduling in Chapter 1).*
- *The shaping parameters' visibility depends on the TD's service category.*
- *ACE-3600 supports up to max XC × 2 traffic descriptors.*
- *A TD cannot be deleted or modified while a VP/VC XC is using it.*

Configuring OAM Parameters

The OAM configuration consists of:

- *Configuring OAM Loopback Parameters*
- *Configuring OAM Descriptors*.

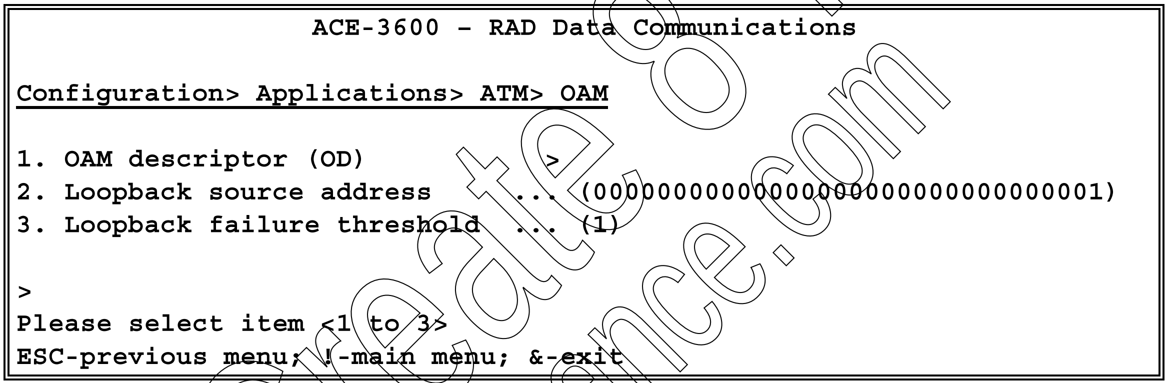
Configuring OAM Loopback Parameters

The OAM loopback function allows ACE-3600 to send OAM loopback cells in case of a link failure. The OAM loopback configuration menu allows you to define the loopback source address and failure threshold.

➤ To access the OAM loopback configuration menu:

- From the ATM menu (see *Figure 4-46*), select OAM.

The OAM configuration menu is displayed.



```
                    ACE-3600 - RAD Data Communications

Configuration> Applications> ATM> OAM

1. OAM descriptor (OD)           >
2. Loopback source address     ... (00000000000000000000000000000001)
3. Loopback failure threshold  ... (1)

>
Please select item <1 to 3>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-48. OAM Menu

Table 4-42. OAM Parameters

Parameter	Description	Possible Values
OAM descriptor (OD)	Access the OAM descriptor options	See *Configuring OAM Descriptors* below
Loopback source address	The unit's OAM loopback source address. For more information about the OAM loopback functionality, refer to *Appendix C*.	00–FF ×16 (Hex) Default: See *Figure 4-48* above
Loopback failure threshold	Number of lost loopback cells before a loopback failure state is declared.	1–16 Default: 1

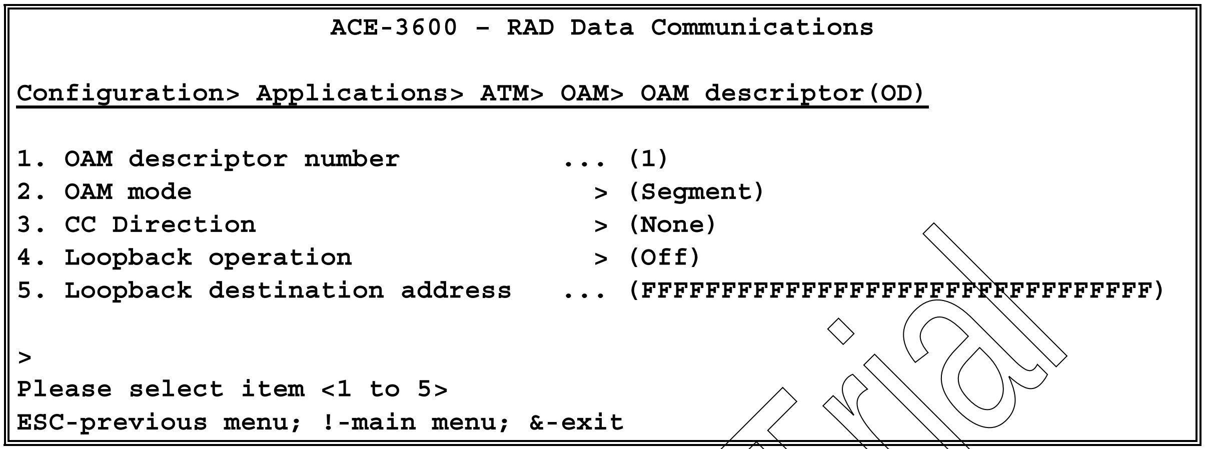
Configuring OAM Descriptors

You can define up to 256 OAM descriptors, which can be set to work in End-to-End, Segment or Intermediate mode. Each descriptor's continuity check direction can be set accordingly.

➤ To access the OAM descriptors configuration menu:

- From the OAM menu, select **OAM descriptor (OD)**.

The OAM Descriptor menu is displayed.



```
                    ACE-3600 - RAD Data Communications

Configuration> Applications> ATM> OAM> OAM descriptor(OD)

1. OAM descriptor number          ... (1)
2. OAM mode                         > (Segment)
3. CC Direction                     > (None)
4. Loopback operation               > (Off)
5. Loopback destination address   ... (FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF)

>
Please select item <1 to 5>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-49. OAM Descriptors Menu

Table 4-43. OAM Descriptor Parameters

Parameter	Description	Possible Values
OAM descriptor number	The identifying number of the specific OAM descriptor which details are displayed. Use the Forward (F) and Backward (B) keys to browse through the OAM descriptors. *Note:* • *1, 2 and 3 are default OAM descriptors and cannot be deleted or modified.* • *OAM descriptor cannot be changed while being used by connections.*	1–256
OAM mode	The OAM mode of the descriptor	End-to-End Segment Intermediate
CC direction	OAM continuity check function mode. Not valid in Intermediate OAM mode.	None Source Sink Both Default: None
Loopback operation	OAM loopback function mode. Not valid in Intermediate OAM mode.	On Off
Loopback destination address	The OAM loopback address that is transmitted on each OAM loopback cell. The destination address parameter is visible only if the loopback operation is set to On.	00 – FF×16 (Hex) Default: FF × 16* * 16 times FF (Hex)

Note *An OAM descriptor cannot be modified when it is being used by connections.*

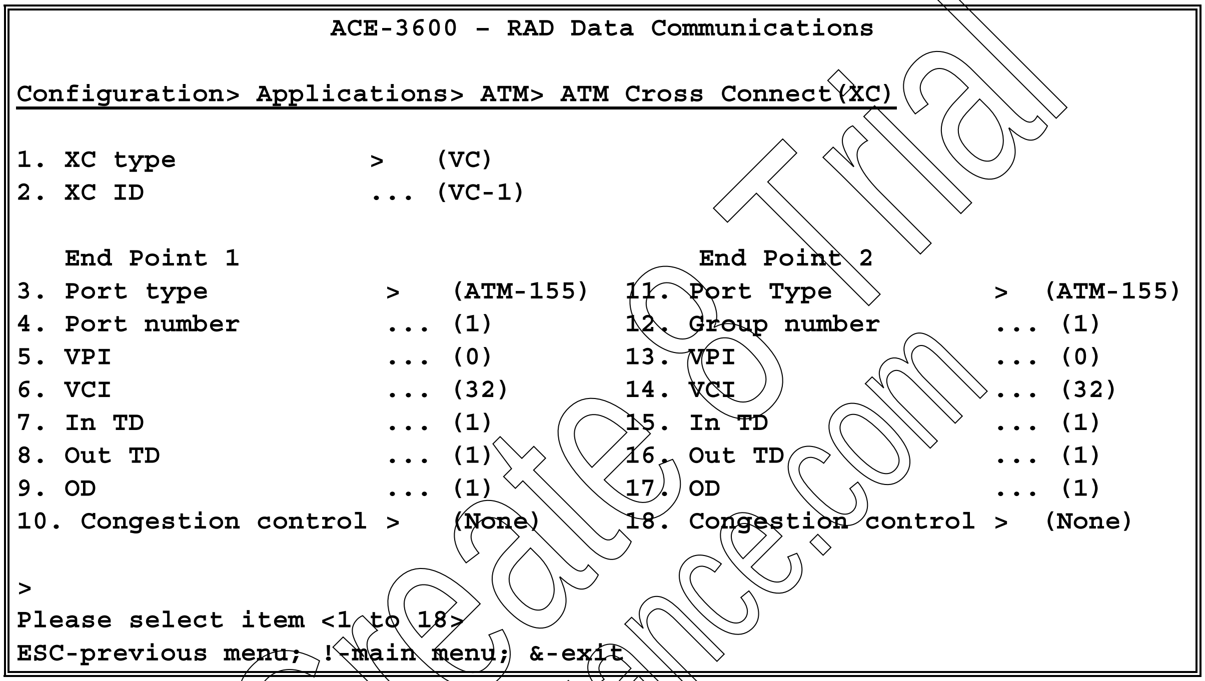
Configuring the ATM Cross-Connect (XC) Parameters

ATM cross-connects deliver the ATM-based traffic over VC or VP connections. Each ATM XC is configured individually on the ATM XC menu.

➤ To access the ATM XC menu:

- From the ATM menu (see *Figure 4-46*), select **ATM cross connect (XC)**.

  The ATM XC menu is displayed.



```
                         ACE-3600 - RAD Data Communications

Configuration> Applications> ATM> ATM Cross Connect(XC)

1. XC type              >    (VC)
2. XC ID                ...  (VC-1)

   End Point 1                                End Point 2
3. Port type             >    (ATM-155)  11. Port Type          >   (ATM-155)
4. Port number           ...  (1)        12. Group number       ...  (1)
5. VPI                   ...  (0)        13. VPI                ...  (0)
6. VCI                   ...  (32)       14. VCI                ...  (32)
7. In TD                 ...  (1)        15. In TD              ...  (1)
8. Out TD                ...  (1)        16. Out TD             ...  (1)
9. OD                    ...  (1)        17. OD                 ...  (1)
10. Congestion control >    (None)       18. Congestion control >   (None)

>
Please select item <1 to 18>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-50. ATM XC Menu

Table 4-44. ATM XC Parameters

Parameter	Description	Possible Values
XC type	The XC type; can be either VP or VC.	VP VC Default: VC
XC ID	A unique ID for the cross-connection. For example: VC-1, VC-2, VC-3 (or VP-1, VP-2, VP-3) and so on. You can manually assign an available number as the XC ID. Max number of total XCs is 1024.	Up to 9 alphanumeric characters, case-sensitive Default: next XC index
Port type	The channel's port type.	ATM-155
Port number	The channel's port number.	1–4 for ATM-155

Parameter	Description	Possible Values
VPI	The channel's VPI. *Note:* • *Two VP XC with the same VPI on the same port cannot be configured.* • *Two VC XC with the same VPI/VCI on the same port cannot be configured.*	0–255 for UNI 0–4095 for NNI
VCI	The channel's VCI for VC XC (valid only for a VC XC). *Note: Two VC XC with the same VPI/VCI on the same port cannot be configured.*	32–65535
In TD	The channel's policing descriptor. *Note:* • *The traffic descriptor must be created first.* • *It is possible to change the TD after the XC is created, provided that the XC is of the same service category and mode.* • *When the TD is set to 0, the policing for the selected ATM channel is stopped.*	0–99999 Default: 0
Out TD	The channel's policing descriptor. *Note:* • *The traffic descriptor must be created first.* • *The traffic descriptor's PCR cannot be higher than the output rate.* • *It is possible to change the TD after the XC is created, providing that the XC is of the same service category and mode.* • *A CBR-CES category TD cannot be used.*	1–99999 Default: 1
OAM descriptor (OD)	The channel's OAM descriptor. *Note:* • *The OAM descriptor must be created first.* • *Cannot be set to end-to-end.* • *The maximum number of endpoints (VCL/VPL) with an OAM descriptor and OAM Loopback is 128.*	1–256 Default: 1
Congestion control	The channel's congestion control mode.	None

Note *Items 3–9 and items 10–16 appear on two separate columns under the ATM XC menu (see Figure 4-50). All items, except XC ID (item no. 2) and TD (item no. 7) – cannot be changed dynamically (on-the-fly).*

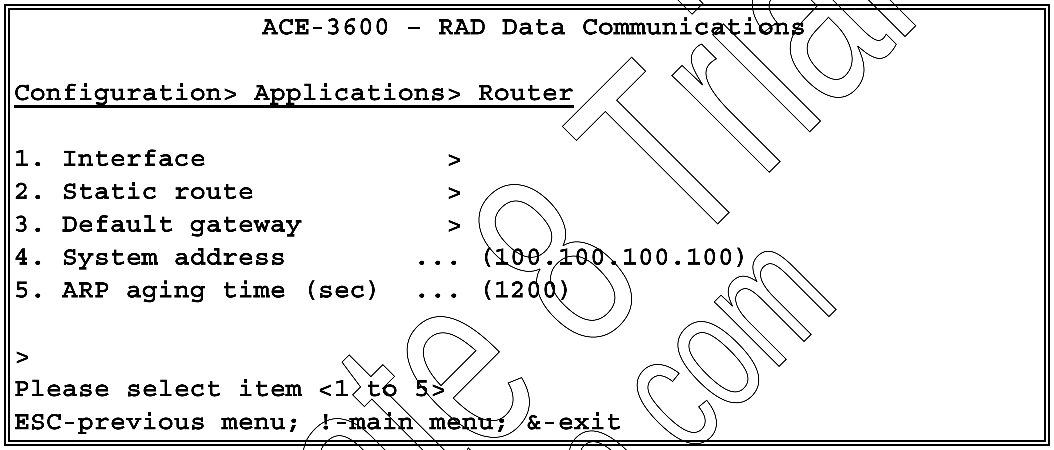
Configuring Router Parameters

The router functionality allows ACE-3600 to establish an IP link with the management station(s), and allows management traffic to be carried transparently through the unit towards specified targets, over pseudowire connections or other channels.

➤ To access the router options:

- From the Applications menu (see *Figure 4-45*), select Router.

  The Router menu is displayed.



```
                ACE-3600 - RAD Data Communications

Configuration> Applications> Router

1. Interface                    >
2. Static route                 >
3. Default gateway              >
4. System address           ... (100.100.100.100)
5. ARP aging time (sec)     ... (1200)

>
Please select item <1 to 5>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-51. Router Menu

Table 4-45. Router Parameters

Parameter	Description	Possible Values
Interface	Access the router interface configuration	See *Configuring Router Parameters* below
Static route	Access the static route parameters	See *Setting the Static Route Parameters*
Default gateway	Access the default gateway definitions	See *Setting the Default Gateway*
System address	The unique IP address that represents this ACE-3600 unit (does not represent an IP subnet). *Note:* • *This IP address cannot be included in the subnet of one of the interfaces.* • *Cannot be changed when the LDP ID has the same address.*	0.0.0.0 – 255.255.255.255 (any valid IP address)
ARP aging time (sec)	The period in seconds that must pass before ARP entries are discarded	300–100000 Default: 1200

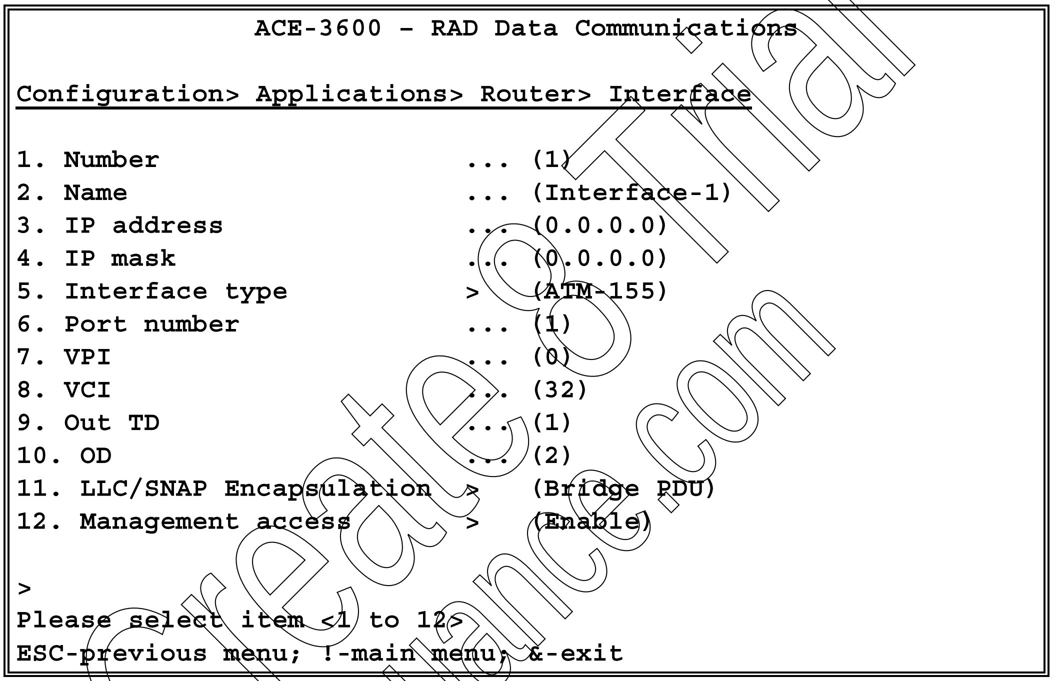
Configuring the Router Interface

A router interface setting is essential for management connections to ACE-3600. Each required router interface is configured individually and includes various parameters as described below.

➤ To access the router interface configuration:

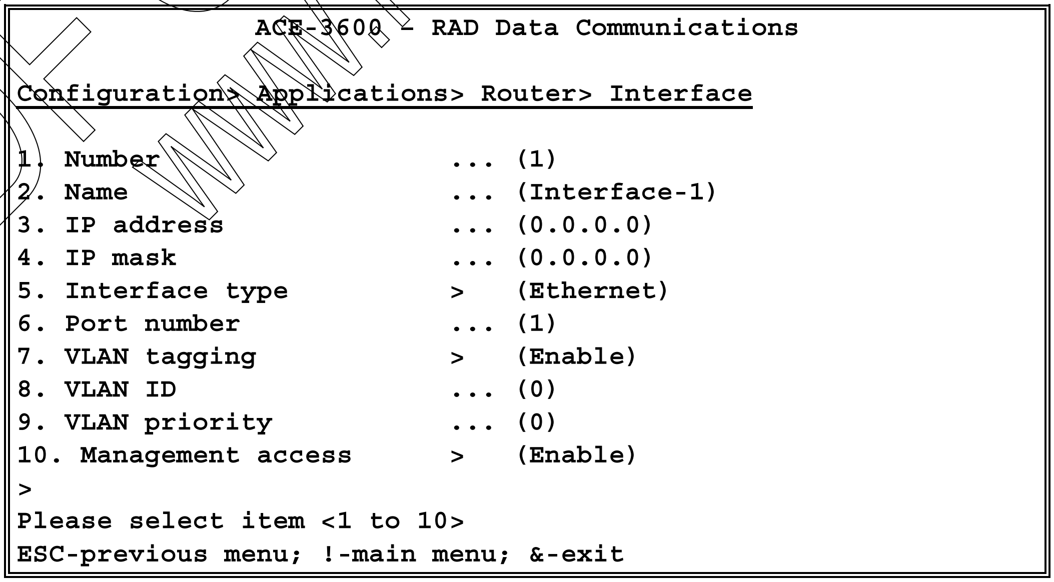
- From the Router menu (see *Figure 4-51*), select **Interface**.

  The Interface menu is displayed.



```
                ACE-3600 - RAD Data Communications

Configuration> Applications> Router> Interface

1. Number                       ... (1)
2. Name                         ... (Interface-1)
3. IP address                   ... (0.0.0.0)
4. IP mask                      ... (0.0.0.0)
5. Interface type               >   (ATM-155)
6. Port number                  ... (1)
7. VPI                          ... (0)
8. VCI                          ... (32)
9. Out TD                       ... (1)
10. OD                          ... (2)
11. LLC/SNAP Encapsulation      >   (Bridge PDU)
12. Management access           >   (Enable)

>
Please select item <1 to 12>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-52. Interface Menu for ATM-155 Interface Type



```
                ACE-3600 - RAD Data Communications

Configuration> Applications> Router> Interface

1. Number                      ... (1)
2. Name                        ... (Interface-1)
3. IP address                  ... (0.0.0.0)
4. IP mask                     ... (0.0.0.0)
5. Interface type              >   (Ethernet)
6. Port number                 ... (1)
7. VLAN tagging                >   (Enable)
8. VLAN ID                     ... (0)
9. VLAN priority               ... (0)
10. Management access          >   (Enable)
>
Please select item <1 to 10>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-53. Interface Menu for Ethernet Interface Type

Table 4-46. Router Interface Parameters

Parameter	Description	Possible Values
Number	Unique ID number of the router interface which details are displayed.	1–1024
Name	An optional name that describes this interface (does not have to be a unique name)	Up to 32 alphanumeric characters; case-sensitive
IP address	IP address of the router interface. ***Note:*** *The IP address cannot be included in the subnet of one of the configured interfaces.*	0.0.0.0 – 255.255.255.255 (any valid IP address) Default: 0.0.0.0
IP mask	Subnet mask of the router interface. ***Note:*** *The IP mask address should always be a sequence of all ones. It cannot include gaps or zeros in between.*	0.0.0.0 – 255.255.255.255 (any valid IP mask)
Interface type	The router interface type. ***Note:*** • *The PW interface type is available only if the PSN license is installed and a PW connection with an appropriate type exists.* • *An Ethernet group is available only if it was previously created.* • *If the router interface is bounded to an ATM VC, check whether the maximum number of XCs has been reached.*	ATM-155 Ethernet PW Ethernet group Default: Ethernet
Port number PW number	Number of the specific port or PW that is used for the router interface, according to the selected interface type (see above). ***Note:*** • *Cannot be changed dynamically (on the fly)* • *Only PW of type AAL5-SDU with router termination type can be selected (must be previously defined).* • *The Ethernet port cannot be selected when it belongs to a redundancy group.*	1–4 for ATM-155 Ethernet: GbE-1 or GbE-2 PW: PW number Ethernet group: 1 GRE Default: GbE-1
VPI	VPI of the PVC connected to the router interface. Not available if Ethernet port type was selected. *Note: A router interface with the same VPI as an existing VP XC on the same port cannot be*	0–255 for UNI (max VPI bits is 8) 0–4095 for NNI (max VPI bits is 12) Default: 0

Parameter	Description	Possible Values
	configured.	
VCI	VCI of the PVC connected to the router interface. Not available for Ethernet, Ethernet group and PW interface type. ***Note:*** *A router interface with the same VPI/VCI as an existing VC XC on the same port cannot be configured.*	32–65535 Default: 32
Out TD	Traffic descriptor of the PVC connected to the router interface. Not available for Ethernet, Ethernet group and PW interface type. ***Note:*** • *A traffic descriptor (TD) must be configured before it can appear on the menu.* • *The descriptor's rate cannot be higher than the port's output rate.* • *A TD with the CBR-CES service category or in Policing mode cannot be used.*	1–99999 Default: 1
OD	OAM descriptor of the PVC connected to the router interface. Not available for Ethernet, Ethernet group and PW interface type. *Note: An OAM descriptor (OD) must be configured before it can appear on the menu and it must be defined as end-to-end or segment.*	1–256 Default: 2
LLC/SNAP Encapsulation	The LLC SNAP encapsulation type. Not visible for the Ethernet, Ethernet group, PW and PPPoE interface types. For more information about this encapsulation, refer to *Appendix E*.	Bridged PDU Routed PDU Default: Routed PDU
VLAN tagging	Indicates whether a VLAN tag is to be inserted into the TX (receive) frames. Available only for Ethernet interface type.	Enable Disable Default: Disable
VLAN ID	Identifies the VLAN that will be carried on the VLAN tag. Available only if VLAN tagging is enabled (see above).	0–4094 Default: 0
VLAN priority	Indicates the priority bit value of the VLAN that will be carried on the VLAN tag. Available only if VLAN tagging is enabled (see above).	0–7 Default: 0

Parameter	Description	Possible Values
Tunnel source IP	The source IP address of the IP header on which the GRE is running. *Note:* • *The IP address must either be a system address or one of the configured router interfaces, otherwise an error message is returned.* • *This parameter only appears if the interface type is set to **GRE**.*	A valid IP address Default: 0.0.0.0
Tunnel destination IP	The destination IP address of the layer on which the GRE is running. *Note:* • *The IP address must be associated with a known route, otherwise an error message is returned.* • *This parameter only appears if the interface type is set to GRE.*	A valid IP address Default: 0.0.0.0
Management access	Enable or disable management access (SNMP, Telnet, SSH, Web, SSL) via this router interface.	Enable Disable Default: Enable

Note

- *All router interface parameters, except 'Management access' – cannot be changed dynamically (on-the-fly).*
- *The number of ATM-type router interfaces is limited to 20.*
- *The maximum number of PW type router interfaces is 2.*

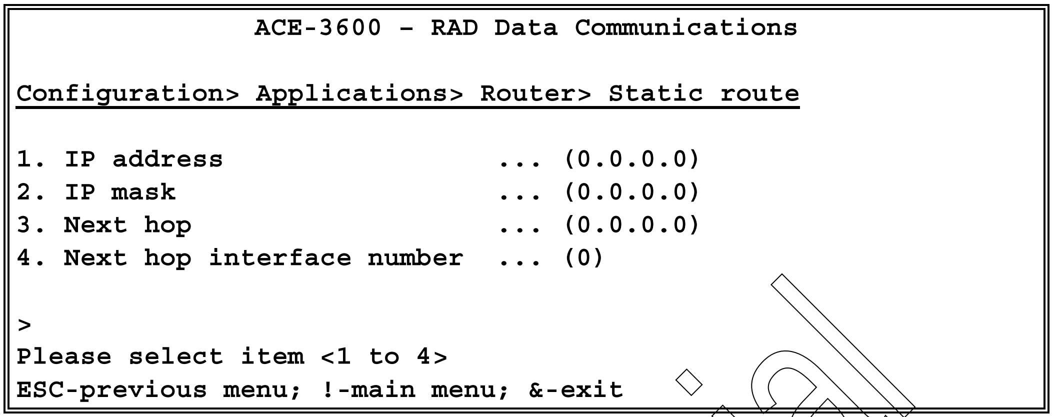
Setting the Static Route Parameters

For remote manager IPs and peers that are located in a subnet different than that of the router interface, you need to assign static route parameters.

➤ To access the static route parameters:

- From the Router menu (see *Figure 4-51*), select **Static Route**.

  The Static Route menu is displayed.



```
                  ACE-3600 - RAD Data Communications

Configuration> Applications> Router> Static route

1. IP address                     ... (0.0.0.0)
2. IP mask                        ... (0.0.0.0)
3. Next hop                       ... (0.0.0.0)
4. Next hop interface number      ... (0)

>
Please select item <1 to 4>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-54. Static Route Menu

Table 4-47. Static Route Parameters

Parameter	Description	Possible Values
IP address	IP address of the static route subnet or station. It is possible to enter a multicast address to support multicast clock distribution.	0.0.0.0 – 255.255.255.255 (any valid IP address)
IP mask	IP mask of the static route subnet.	0.0.0.0 – 255.255.255.255 (any valid IP mask)
Next hop	IP address of the next hop. Must belong to the router interface's subnet. *Note:* • *Multicast, broadcast or all ones address is not allowed.* • *All zeros cannot be assigned to an address part that is not the router interface's subnet.* • *If 0.0.0.0 is used, it indicates that the routing is based on the next hop interface number. This kind of setting is useful when the router interface is of an ATM VC type or PW type.*	0.0.0.0 – 255.255.255.255 Default: 0.0.0.0
Next hop interface number	ID number of the router interface towards which the destination subnet should be router. Available only if the next hop is 0.0.0.0.	A number of a previously configured router interface. For more information, see *Configuring the Router Interface*.

Note

- *The number of static routes is limited to 1041.*
- *A static route cannot be deleted when it is used as a route of an existing peer.*

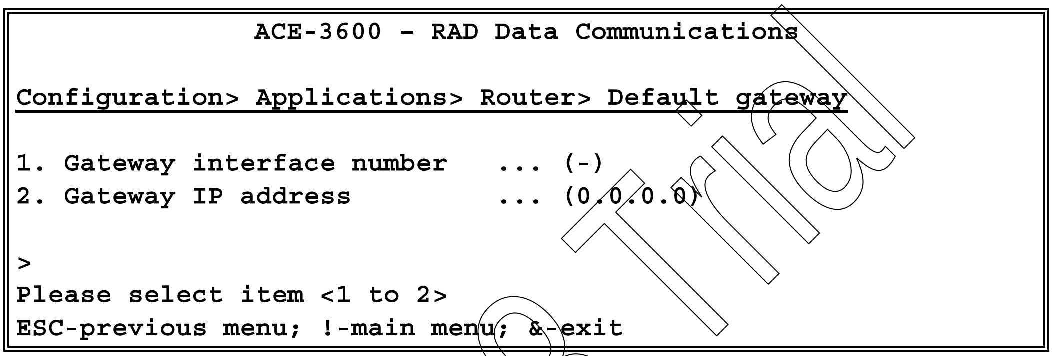
Setting the Default Gateway

One of the router interfaces should be set as the default gateway.

➤ To set the default gateway:

- From the (see *Figure 4-51*), select Default Gateway.

  The Default Gateway menu is displayed.



```
                 ACE-3600 - RAD Data Communications

Configuration> Applications> Router> Default gateway

1. Gateway interface number   ... (-)
2. Gateway IP address         ... (0.0.0.0)

>
Please select item <1 to 2>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-55. Default Gateway Menu

Table 4-48. Default Gateway Parameters

Parameter Description		Possible Values
Gateway interface number	ID number of a defined router interface that should be used as the default gateway. Cannot be changed dynamically (on-the-fly).	Any previously configured router interface
Gateway IP address	The gateway IP address for routing the outgoing IP packets. Visible only when the gateway interface number is configured over an Ethernet port. *Note:* • *The default gateway IP address must be on the same subnet as one of the router interface indicated above* • *The gateway address should not be identical to one of the router IP address.* • *Multicast, broadcast, all ones and all zeros are not allowed.* • *Address parts that are not subnet cannot be all zeros or all ones.* • *Cannot be changed dynamically (on-the-fly).*	0.0.0.0 – 255.255.255.255

Note *You can delete the current default gateway setting by pressing **R**. It cannot be deleted, however, if it is used as a route of an existing peer.*

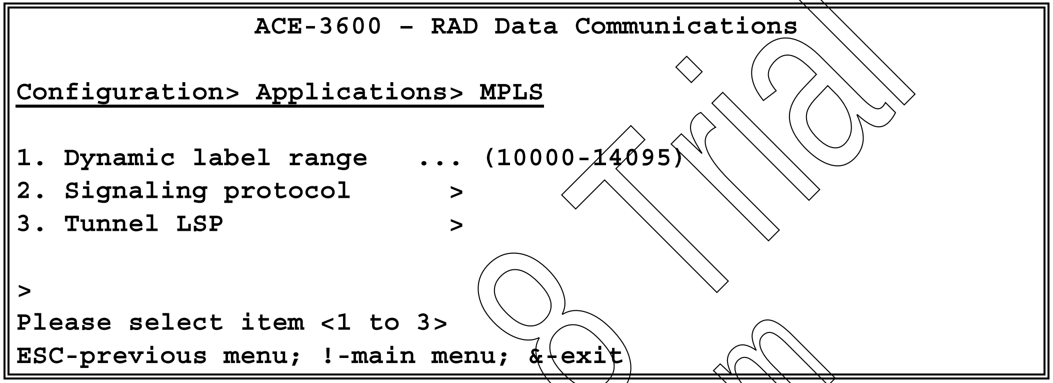
Configuring MPLS Parameters

To allow ACE-3600 to deliver traffic over MPLS networks, the MPLS parameters should be defined.

➤ To access the MPLS configuration parameters:

- From the Applications menu (see *Figure 4-45*), select **MPLS**.

  The MPLS menu is displayed.



```
                 ACE-3600 - RAD Data Communications

Configuration> Applications> MPLS

1. Dynamic label range    ... (10000-14095)
2. Signaling protocol       >
3. Tunnel LSP               >

>
Please select item <1 to 3>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-56. MPLS Menu

Table 4-49. MPLS Parameters

Parameter Description		Possible Values
Dynamic label range	Range of the MPLS dynamic label. Relevant only for the incoming direction and has no effect on the outgoing direction. *Note:* • *Cannot be changed when the LDP signaling protocol is enabled.* • *The range setting is rejected if there are static PW connections or tunnels configured with labels that are included in the dynamic range.* • *The range is relevant to both tunnel and PW labels.* • *ACE-3600 supports a single dynamic label range of up to 4094 labels. In such a case, the range is 16–65534.* • *The static range is automatically determined according to the dynamic range selection, yet it cannot be included in the 16–65534 range which is allocated only for dynamic labels.* • *When LDP is not in use, the range can be set to 0–0.*	10000–14095 16–65534 for dynamic labels only 0–0 when the dynamic range is not set Default: 10000–14095

Parameter	Description	Possible Values
Signaling protocol	Access the LDP options	See *Configuring the LDP Signaling Protocol* below
Tunnel LSP	Access the Tunnel LSP options	See *Configuring the Tunnel LSP Parameters*

Configuring the LDP Signaling Protocol

ACE-3600 uses the MPLS label distribution protocol (LDP) to automatically assign and distribute pseudowires and tunnel labels between MPLS peers.

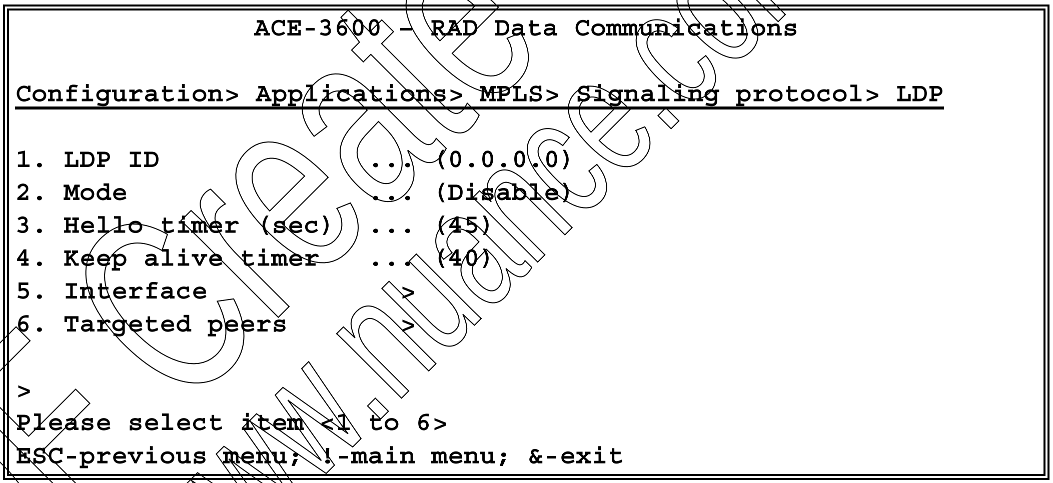
➤ To access the LDP parameters:

1. From the MPLS menu (see *Figure 4-56*), select Signaling Protocol.

   The Signaling Protocol menu is displayed.

2. Select LDP.

   The LDP menu is displayed.



```
                 ACE-3600 - RAD Data Communications

Configuration> Applications> MPLS> Signaling protocol> LDP

1. LDP ID              ... (0.0.0.0)
2. Mode                ... (Disable)
3. Hello timer (sec)   ... (45)
4. Keep alive timer    ... (40)
5. Interface               >
6. Targeted peers          >

>
Please select item <1 to 6>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-57. LDP Menu

Table 4-50. LDP Parameters

Parameter	Description	Possible Values
LDP ID	The LDP identifier to be used in all LDP sessions established with the unit. *Note:* • *The IP must be identical to one of the interface IP address or system address (see Table 4-45).* • *Cannot be changed when LDP is enabled.* • *If the LDP ID is not yet configured and a system address is defined, the system address is automatically displayed by default, and you only need to save this setting (press* ***S****).*	0.0.0.0 – 255.255.255.255 Default: 0.0.0.0
Mode	Indicates whether all LDP operations performed by the unit are enabled or disabled. 'Enable' can be selected only if an LDP ID is defined.	Enable Disable Default: Enable
Hello timer (sec)	The required interval in seconds between two consecutive Hello messages. LDP Hello messages enable LDP nodes to discover one another and to detect the failure of a neighbor or of the link to the neighbor. Hello messages are sent periodically on all interfaces where LDP is enabled. The Hello timer cannot be modified when LDP mode is enabled.	1–65534 Default: 45
Keep alive timer (sec)	For cases of inactivity, define the time in seconds after which a Keep Alive message is sent. Cannot be modified when LDP mode is enabled.	1–65534 Default: 40
Interface	Access the LDP interface configuration	See *Configuring the LDP Interface Parameters* below
Targeted peers	Access the targeted peers configuration	See *Setting the LDP Targeted Peers*

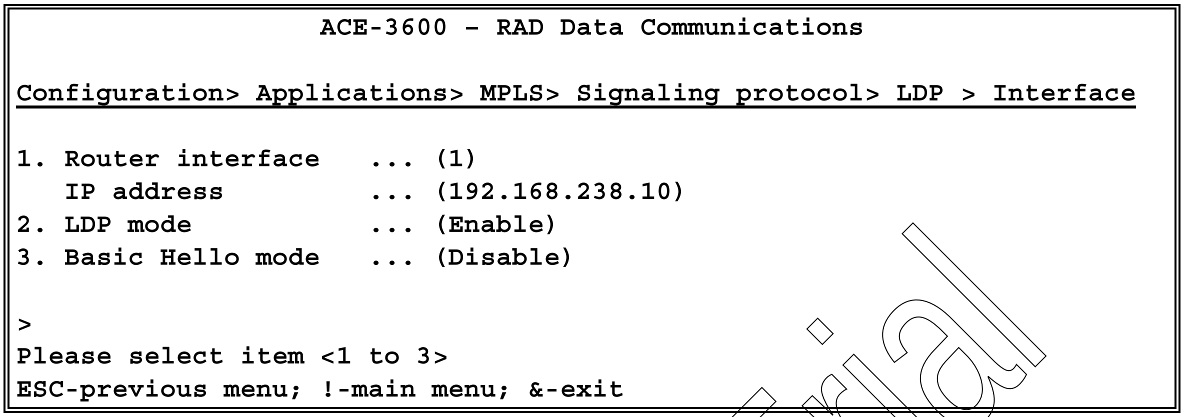
Configuring the LDP Interface Parameters

The LDP interface can be referenced to one of the existing router interfaces.

➤ **To access the LDP interface parameters:**

- From the LDP menu, select Interface.

The Interface menu is displayed.



```
                    ACE-3600 - RAD Data Communications

Configuration> Applications> MPLS> Signaling protocol> LDP > Interface

1. Router interface   ... (1)
   IP address         ... (192.168.238.10)
2. LDP mode           ... (Enable)
3. Basic Hello mode   ... (Disable)

>
Please select item <1 to 3>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-58. LDP Interface Menu

Table 4-51. LDP Interface Parameters

Parameter	Description	Possible Values
Router interface	ID number of a previously defined router interface on which the LDP basic Hello should be activated. You can enter a different number to display another interface's details.	1–512
IP address	Displays (read-only) the IP address of the router interface selected above.	0.0.0.0 – 255.255.255.255 (must match the IP of the router interface)
LDP mode	When enabled, LDP is activated on the selected router interface. Can be enabled only for Ethernet interfaces. Cannot be changed when the general LDP mode (see *Table 4-50*) is enabled.	Enable Disable Default: Disable
Basic Hello mode	Select whether basic Hello should be activated on the router interface. Visible only when LDP mode is enabled (see above). *Note:* • *Should be enabled for every router interface on which LDP basic discovery is enabled.* • *There can be only one router interface supporting basic Hello over a single physical port.* • *Cannot be changed when the general LDP mode (see Table 4-50) is enabled.*	Enable Disable Default: Disable

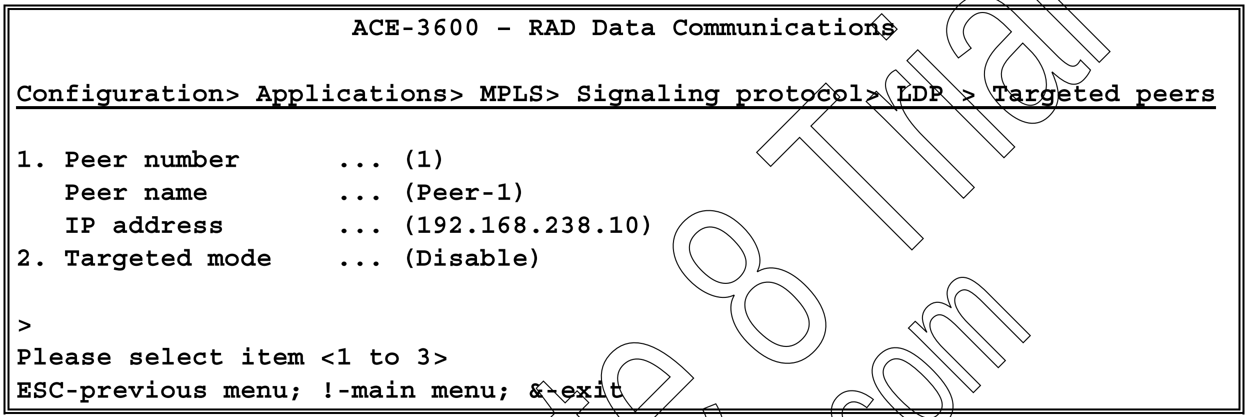
Setting the LDP Targeted Peers

You can define targeted remote peers with which ACE-3600 should attempt establishing LDP sessions.

➤ To set the targeted peers:

- From the LDP menu, select Targeted Peers.

  The Targeted Peers menu is displayed.



```
                    ACE-3600 - RAD Data Communications

Configuration> Applications> MPLS> Signaling protocol> LDP > Targeted peers

1. Peer number      ... (1)
   Peer name        ... (Peer-1)
   IP address       ... (192.168.238.10)
2. Targeted mode    ... (Disable)

>
Please select item <1 to 3>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-59. Targeted Peers Menu

Table 4-52. Targeted Peers Parameters

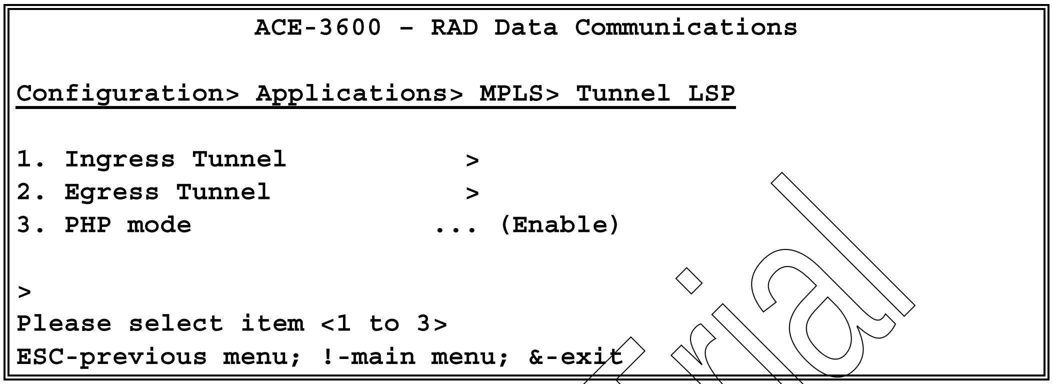
Parameter	Description	Possible Values
Peer number	ID number of an existing (previously defined) remote targeted peer. You can enter a different number to display another peer's details.	1–1024
Peer name	Displays (read-only) the name of the remote targeted peer selected above	
IP address	Displays (read-only) the IP address of the remote targeted peer selected above	0.0.0.0 – 255.255.255.255 (must match the IP of the remote peer)
Targeted mode	Enable or disable the targeted peers functionality. When enabled, ACE-3600 attempts to create a targeted LDP session with the peer.	Enable Disable Default: Disable

Configuring the Tunnel LSP Parameters

This section explains how to configure the PHP (penultimate pop-hopping) mode and the LSP tunnels. LSP tunnels are configured separately in the ingress and egress directions.

➤ To configure the PHP mode:

1. Navigate to the Tunnel LSP menu (*Figure 4-60*)



```
                 ACE-3600 - RAD Data Communications

Configuration> Applications> MPLS> Tunnel LSP

1. Ingress Tunnel           >
2. Egress Tunnel            >
3. PHP mode               ... (Enable)

>
Please select item <1 to 3>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-60. Tunnel LSP Menu

2. To enable or disable the PHP mode, select PHP Mode from the MPLS menu.

   The PHP mode is enabled/disabled.

   - When enabled: ACE-3600 advertises an implicit null label (a reserved label value of 3) for routes that are directly connected. This causes the previous hop (penultimate) router to pop the most outer label before transmitting the packet to the LER. The packet arriving at the device through this port does not carry a tunnel label.
   - When disabled: ACE-3600 advertises an actual label value to the previous hop. After the tunnel label is established, all traffic arriving at the device from the previous hop through this port, arrives above the tunnel label. This includes IP control traffic (such as LDP, PING) that is transmitted over a tunnel label and not as a raw IP address. The PHP mode cannot be disabled when there are PWs configured without tunnel label.

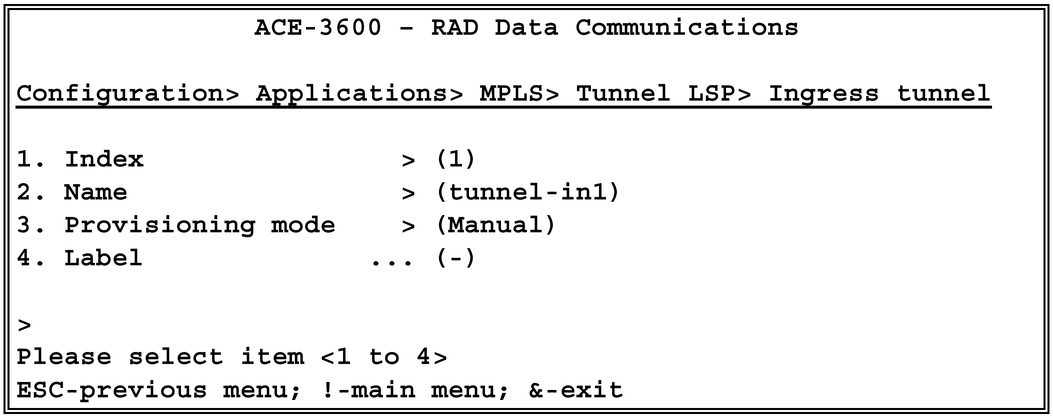
➤ To configure the ingress tunnel:

1. From the MPLS menu (see *Figure 4-56*), select Tunnel LSP.

   The Tunnel LSP menu is displayed.

2. Select Ingress Tunnel.

   The Ingress Tunnel menu is displayed.



```
                 ACE-3600 - RAD Data Communications

Configuration> Applications> MPLS> Tunnel LSP> Ingress tunnel

1. Index                  > (1)
2. Name                   > (tunnel-in1)
3. Provisioning mode      > (Manual)
4. Label                ... (-)

>
Please select item <1 to 4>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-61. Ingress Tunnel Menu

Table 4-53. Ingress Tunnel Parameters

Parameter Description		Possible Values
Index	ID number of the ingress tunnel	1–512
Name	Name of the ingress tunnel	Up to 32 characters Default: Tunnel-in
Provisioning mode	Indicates whether the tunnel assignment method is manual or LDP assigned. The provisioning mode cannot be changed dynamically (on-the-fly).	Manual LDP Default: Manual
Label	ID of the label. Visible only if the provisioning mode is set to Manual.	A value within the static label range (16–65534; see *Table 4-49*)

Note

- *When the provisioning mode is set to LDP, a label-blinding message with the LDP address (see Table 4-45) is published towards all LDP sessions created locally.*
- *The label binding message is not published over an LDP session created with targeted peers, meaning that tunnel labels are never created with targeted peers.*
- *Only one ingress tunnel created by LDP (not manual) is possible.*

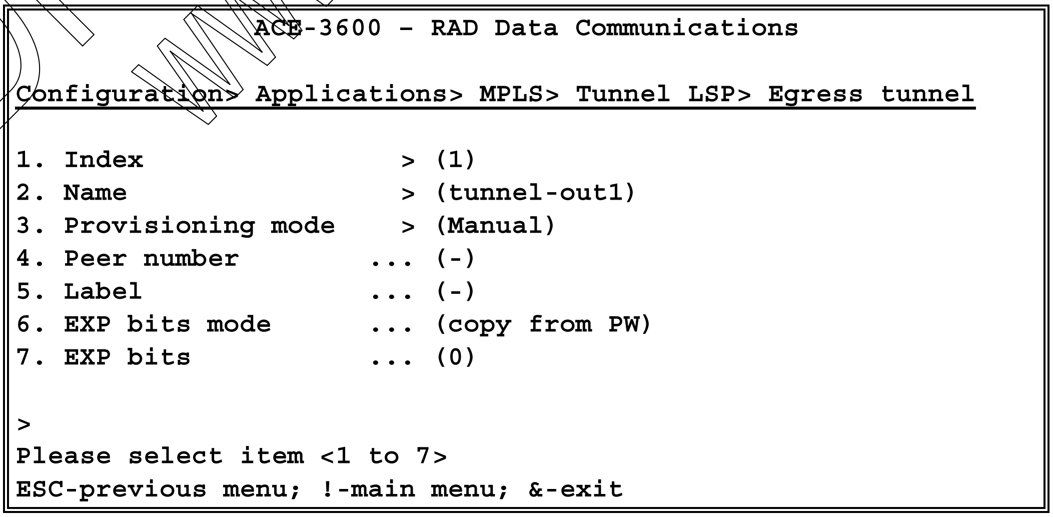
➤ To configure the egress tunnel:

1. From the MPLS menu (see *Figure 4-56*), select **Tunnel LSP**.

   The Tunnel LSP menu is displayed.

2. Select Egress Tunnel.

   The Egress Tunnel menu is displayed.



```
               ACE-3600 - RAD Data Communications

Configuration> Applications> MPLS> Tunnel LSP> Egress tunnel

1. Index                    > (1)
2. Name                     > (tunnel-out1)
3. Provisioning mode        > (Manual)
4. Peer number            ... (-)
5. Label                  ... (-)
6. EXP bits mode          ... (copy from PW)
7. EXP bits               ... (0)

>
Please select item <1 to 7>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-62. Egress Tunnel Menu

Table 4-54. Egress Tunnel Parameters

Parameter	Description	Possible Values
Index	ID number of the egress tunnel	1–512
Name	Name of the egress tunnel	Up to 32 characters Default: Tunnel-out
Provisioning mode	Indicates whether the tunnel assignment method is manual or LDP-assigned. The provisioning mode cannot be changed dynamically (on-the-fly).	Manual LDP Default: Manual
Peer number	ID number of the remote peer for which this egress tunnel is created. The peer numbers are defined on the *Targeted Peers Menu*. Visible only if the provisioning mode is LDP.	An existing peer number
Label	ID of the label. Visible only if the provisioning mode is set to Manual.	A value within the static label range (16–65534; see *Table 4-49*)
EXP bits mode	Indicates how the EXP bits of the tunnel label are set. If copied from the PW connection, the EXP bits are copied from the PSN parameters of the specific PW. If set as static, the EXP value is set manually below. The EXP bits mode cannot be changed dynamically.	Copy from PW Static Default: Copy from PW
EXP bits	The required value for the EXP bits. Visible only if the EXP bits mode is set to Static.	0–7

Configuring Multiservice over PSN Parameters

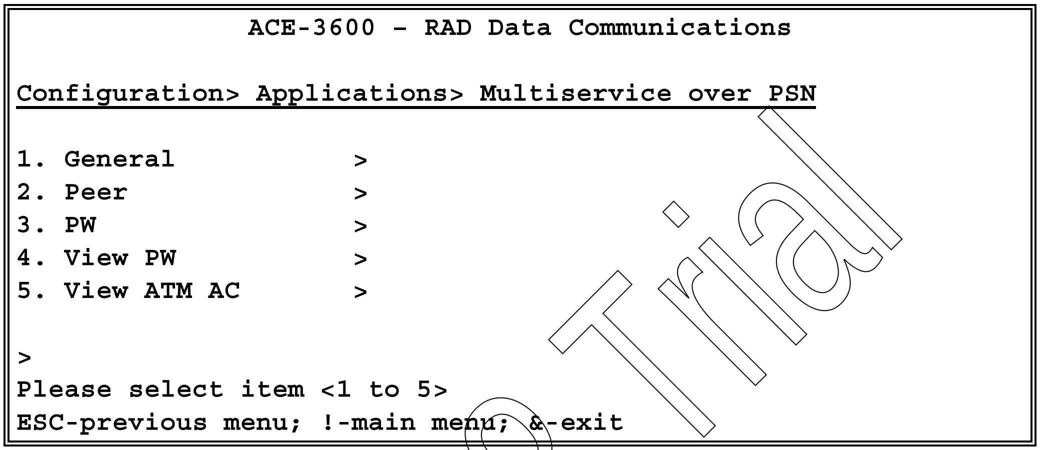
As explained in *Chapter 1*, ACE-3600 are equipped with Gigabit Ethernet interface for ATM over PSN traffic concentration. Ethernet tunneling parameters are configured via the Multiservice over PSN menu, which provides access to the following tasks:

- *Configuring General Multiservice over PSN Parameters*
- *Defining PSN Peers*
- *Creating Pseudowire (PW) Connections*
- *Viewing Existing PW Connections and Attachment Circuits*.

➤ To access the Multiservice over PSN options:

- From the Logical Layer menu (see *Figure 4-45*), select Multiservice over PSN.

  The Multiservice over PSN menu is displayed.



```
                    ACE-3600 - RAD Data Communications

Configuration> Applications> Multiservice over PSN

1. General            >
2. Peer               >
3. PW                 >
4. View PW            >
5. View ATM AC        >

>
Please select item <1 to 5>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-63. Multiservice over PSN Menu

Table 4-55. Multiservice over PSN Menu Options

Parameter	Description	Possible Values
General	Access the general multiservice over PSN parameters configuration	Refer to *Figure 4-64*
Peer	Access to the peer configuration	Refer to *Figure 4-65*
Pseudo wire (PW)	Access the PW configuration	Refer to *Figure 4-67*
View PW / View ATM AC	View the details of existing PW connections / attachment circuits	Refer to *Figure 4-71* and *Figure 4-72*

Configuring General Multiservice over PSN Parameters

The general parameters include packet misordering and reordering instructions for ATM over PSN traffic.

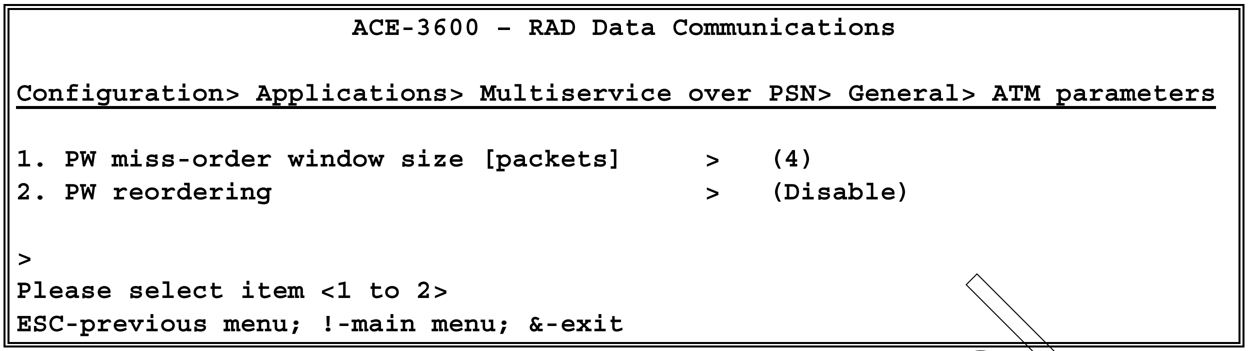
➤ To access the ATM parameters:

1. From the Multiservice over PSN menu, select General.

   The General menu is displayed.

2. Select ATM Parameters.

   The ATM Parameters menu is displayed.



```
                    ACE-3600 - RAD Data Communications

Configuration> Applications> Multiservice over PSN> General> ATM parameters

1. PW miss-order window size [packets]      >   (4)
2. PW reordering                            >   (Disable)

>
Please select item <1 to 2>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-64. ATM Parameters Menu

Table 4-56. ATM Parameters

Parameter Description		Possible Values
PW miss-order window size	In packet-switched traffic, some packets are not received according to their predefined sequence number. This condition is defined as misorder. Accordingly, this parameter defines the number of packets window, in which ACE-3600 tries to fix the packet sequence misorder errors. Cannot be changed when PWs exist.	0, 1, 2, 4, 8, 16, 32 Default: 4
PW reordering	To allow proper de-capsulation of ATM traffic, ACE-3600 has a mechanism that fixes misorders by re-ordering the received packets correctly. You can enable or disable the reordering mechanism. Cannot be changed when PWs exist.	Enable Disable Default: Disable

Defining PSN Peers

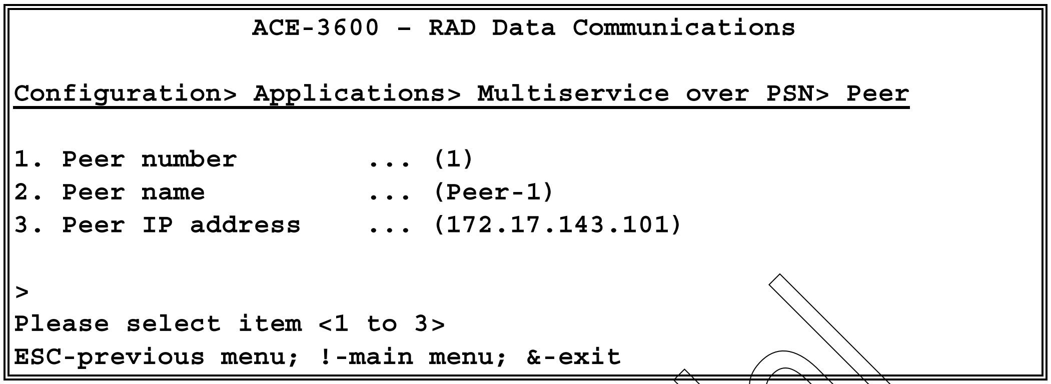
In a packet-switched network application, ACE-3600 operates opposite remote peer devices that each must be defined individually on the Peer menu.

Note *An Ethernet router interface and a default gateway must be configured prior to configuring PSN peers.*

➤ To access the Peer menu:

- From the Multiservice over PSN menu (see *Figure 4-63*), select **Peer**.

  The Peer menu is displayed.



```
                    ACE-3600 - RAD Data Communications

Configuration> Applications> Multiservice over PSN> Peer

1. Peer number         ... (1)
2. Peer name           ... (Peer-1)
3. Peer IP address     ... (172.17.143.101)

>
Please select item <1 to 3>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-65. Peer Menu

Table 4-57. Peer Parameters

Parameter Description		Possible Values
Peer number	A logical number representing a peer device	1–1024 Default: Next available peer number
Peer name	Name of the peer	Up to 32 characters Default: Peer-1
IP address	IP address of the peer device. *Note:* • *All routing definitions (IP and static routes) must be configured in advance before entering the IP address of the peer device. For more information, refer to Configuring the Router Interface.* • *Peer IP address cannot be the same as the router IP address.* • *The address part that is not the subnet cannot be all zeros or all ones.* • *Broadcast, all one- and all zero-IP addresses are not allowed.* • *Multicast IP addresses, ranging from 224.0.0.0 to 239.255.255.255 are allowed.* • *If the Peer IP address is changed dynamically (on-the-fly), the unit resets upon saving the modified peer.*	0.0.0.0 – 255.255.255.255

Note *The remote peer device cannot be removed if a PW is configured for this peer device.*

Creating Pseudowire (PW) Connections

In a packet-switched network application, ACE-3600 communicates with peer devices via pseudowire (PW) connections that are established over the PSN and are configured via the Pseudowire menu.

Each pseudowire configuration consists of:

a. General PW parameters

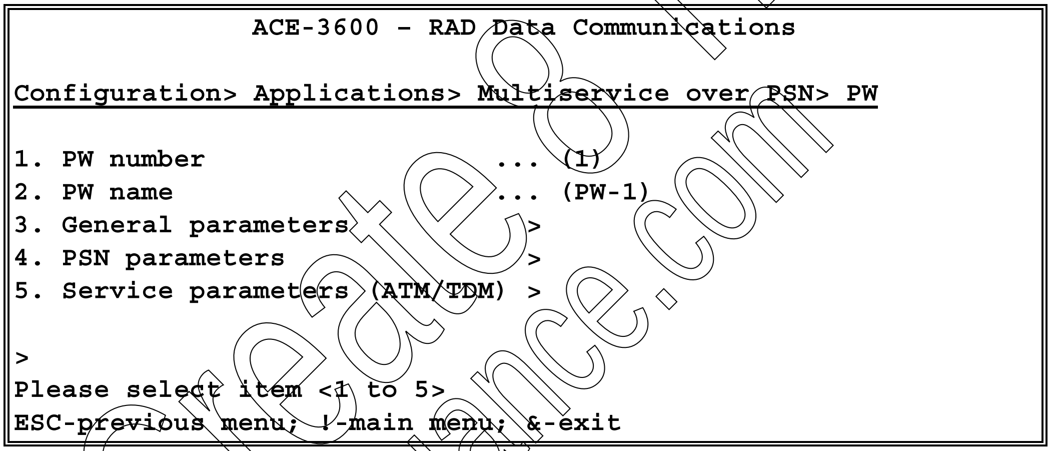
b. PSN parameters

c. Service parameters.

➤ To access the pseudowire configuration menu:

- From the Multiservice over PSN menu (see *Figure 4-63*), select PW.

  The Pseudowire menu is displayed.



```
                  ACE-3600 - RAD Data Communications

Configuration> Applications> Multiservice over PSN> PW

1. PW number                     ...  (1)
2. PW name                       ...  (PW-1)
3. General parameters              >
4. PSN parameters                  >
5. Service parameters (ATM/TDM)    >

>
Please select item <1 to 5>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-66. Pseudowire (PW) Menu

Table 4-58. Pseudowire (PW) Parameters

Parameter	Description	Possible Values
PW number	A logical number representing a PW connection	1–1536 **Default:** Next available PW number
PW name	Name of the PW connection	Up to 32 characters **Default:** A combination of the word PW with the next available PW number, for example **PW-1**.
General parameters	Access the general parameters of this PW	Refer to *Configuring the General PW Parameters*.
PSN parameters	Access the PSN parameters of this PW	Refer to *Configuring the PSN Parameters for the PW Connection*.

Parameter	Description	Possible Values
Service parameters	Access the ATM/TDM service parameters of this PW	Refer to *Configuring the ATM Service Parameters for the PW*.

Note

- *The **Save** command on this menu affects all the parameters that are set in the submenus.*
- *To remove (delete) a PW, press <**R**>.*

➤ To configure a PW link:

1. On the PW menu (Configuration > Applications > Multiservice over PSN > **PW**), set the PW number.
2. On the General Parameters submenu (Configuration > Applications > Multiservice over PSN > PW > **General parameters**), set the general PW parameters for the PW.
3. On the PSN Parameters submenu (Configuration > Applications > Multiservice over PSN > PW > **PSN parameters**), set the PSN parameters for the PW.
4. On the Service Parameters submenu (Configuration > Applications > Multiservice over PSN > PW > **Service parameters**), set the service parameters for the PW.
5. Save the PW link parameters.

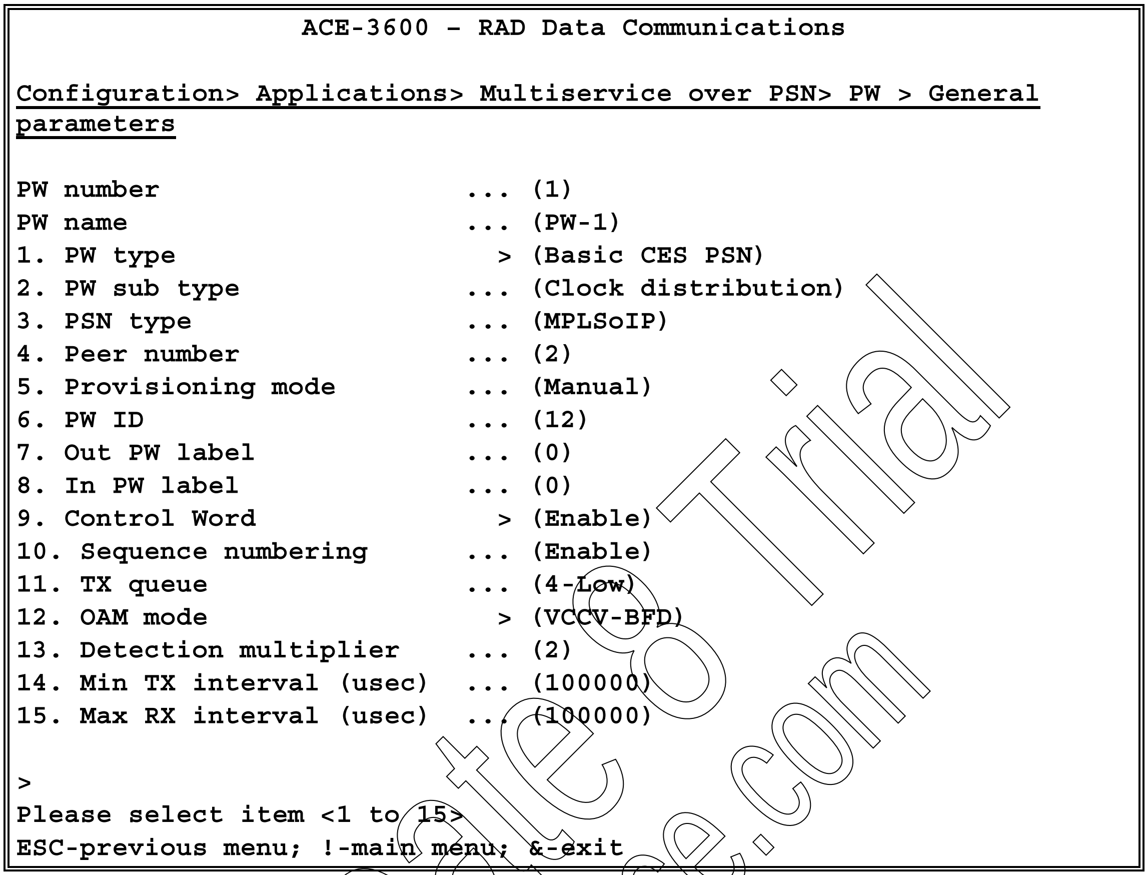
Configuring the General PW Parameters

Each individual pseudowire connection has general parameters that must be defined separately.

➤ To access the general pseudowire parameters:

- From the PW menu, select General Parameters.

The PW General Parameters menu is displayed.



```
                  ACE-3600 - RAD Data Communications

Configuration> Applications> Multiservice over PSN> PW > General
parameters

PW number                     ... (1)
PW name                       ... (PW-1)
1. PW type                      > (Basic CES PSN)
2. PW sub type                ... (Clock distribution)
3. PSN type                   ... (MPLSoIP)
4. Peer number                ... (2)
5. Provisioning mode          ... (Manual)
6. PW ID                      ... (12)
7. Out PW label               ... (0)
8. In PW label                ... (0)
9. Control Word                 > (Enable)
10. Sequence numbering        ... (Enable)
11. TX queue                  ... (4-Low)
12. OAM mode                    > (VCCV-BFD)
13. Detection multiplier      ... (2)
14. Min TX interval (usec)    ... (100000)
15. Max RX interval (usec)    ... (100000)

>
Please select item <1 to 15>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-67. Pseudowire General Parameters Menu

Table 4-59. Pseudowire General Parameters

Parameter Description		**Possible Values**
PW number	Displays the PW number as defined in the PW menu (read-only)	See *Table 4-58*
PW name	Displays the PW name as defined in the PW menu (read-only)	See *Table 4-58*
PW type	Defines the PW type and the type of data it carries. For more information about the different encapsulation types, refer to *Appendix E*.	ATM VP 1 to 1 ATM VC 1 to 1 ATM VP N to 1 ATM VC N to 1 AAL5-SDU Basic CES PSN Default: ATM VC N to 1
PW subtype	When the PW type is Basic CES PSN, the subtype indicates whether the PW is used for clock distribution or data. ***Note:*** *In order to configure IP multicast clock distribution, the relevant PW should be created using an IP multicast peer.*	Clock distribution Data
PSN type	The type of packet-switched network on which this PW is established. "o" stands for over. ***Note:*** • *UDPoIP is valid only for Basic CES PSN pseudowire types.* • *MPLSoIP cannot be selected when the PW subtype is clock distribution.*	MPLS UDPoIP MPLSoIP MPLSoGRE Default: MPLSoIP
Peer number	Number of an existing PSN peer device (see *Defining PSN Peers*) to which the current PW is assigned. The PW terminates on this peer. ***Note:*** • *When the provisioning mode is LDP PW ID (see below), the peer must be configured as a targeted peer.* • *A peer with a multicast IP address can be set only for a clock distribution PW.* • *The peer number cannot be changed dynamicaly (on-the-fly).*	1–1024
Provisioning mode	Determines whether the PW is established manually or by LDP signaling	Manual LDP PW ID Default: Manual

Parameter	Description	Possible Values
PW ID	A unique ID number that must be defined identically on both the local and remote unit. This ID is used to identify the PW connection when labels are exchanged with LDP.	1–4294967295
Out PW label	The PW label that is used in the outbound direction. Relevant only if the provisioning mode (see above) is set to Manual. The out label's value range depends on the selected PSN type.	1–4095 if the PSN type is UDPoIP 16–1048575 for any other PSN type
In PW label	The PW label that is used in the inbound direction. Not relevant for clock distribution. If the PW is defined manually and the PSN type is MPLS, MPLSoIP or MPLSoGRE, the PW value range must be within the static label range.	1–4095 if the PSN type is UDPoIP 16–65534 for any other PSN type
Control word	Determines whether a control word is used on this PW. The control word can be disabled only in the following PW types (see above): • ATM VP 1 to 1 • ATM VC 1 to 1 • ATM VP N to 1 • ATM VC N to 1. For detailed information about the control word structure, refer to *Appendix E*.	Enable Disable Default: Enable
Sequence numbering	When disabled, the Sequence bit in the control word equals zero (0). Relevant only if the control word is enabled (see above). Sequence numbering can be disabled only in the following PW types: • ATM VP 1 to 1 • ATM VC 1 to 1 • ATM VP N to 1 • ATM VC N to 1. In addition, the AAL5-SDU PW type does not support sequence numbering (set to Disable).	Enable Disable Default: Enable

Parameter	Description	Possible Values
TX queue	The priority of the PW in the outbound direction via the Ethernet port. ***Note:*** *Clock distribution PWs are automatically assigned with the priority level of 1 (above 2), which cannot be changed.*	2 (highest priority) 3 4 (lowest priority) Default: 4 for ATM VP 1 to 1, ATM VC 1 to 1, ATM VP N to 1, ATM VC N to 1 and AAL5-SDU 2 for Basic CES PSN
OAM mode	Determines whether the OAM feature (using VCCV-BFD messages) is enabled for this PW. Not relevant if the PW type is Basic CES PSN or AAL5-SDU. For more information about the VCCV-BFD functionality, refer to *Appendix F*.	Disable VCCV-BFD Default: Disabled
Detection multiplier	The negotiated transmit interval, multiplied by this value, provides the detection time for the transmitting system. Relevant only if the OAM mode (see above) is set to VCCV-BFD.	2–60 Default: **5**
Min TX interval (µsec)	The minimum time interval in microseconds that the system uses between transmitted BFD control packets. Relevant only if the OAM mode (see above) is set to VCCV-BFD.	1000000–4294967295 Default: 1000000
Mix RX interval (µsec)	The minimum time interval in microseconds that the system uses between received BFD control packets. Relevant only if the OAM mode (see above) is set to VCCV-BFD.	1000000–4294967295 Default: 1000000

Note *The general PW parameters cannot be changed dynamically (on-the-fly), except the OAM mode.*

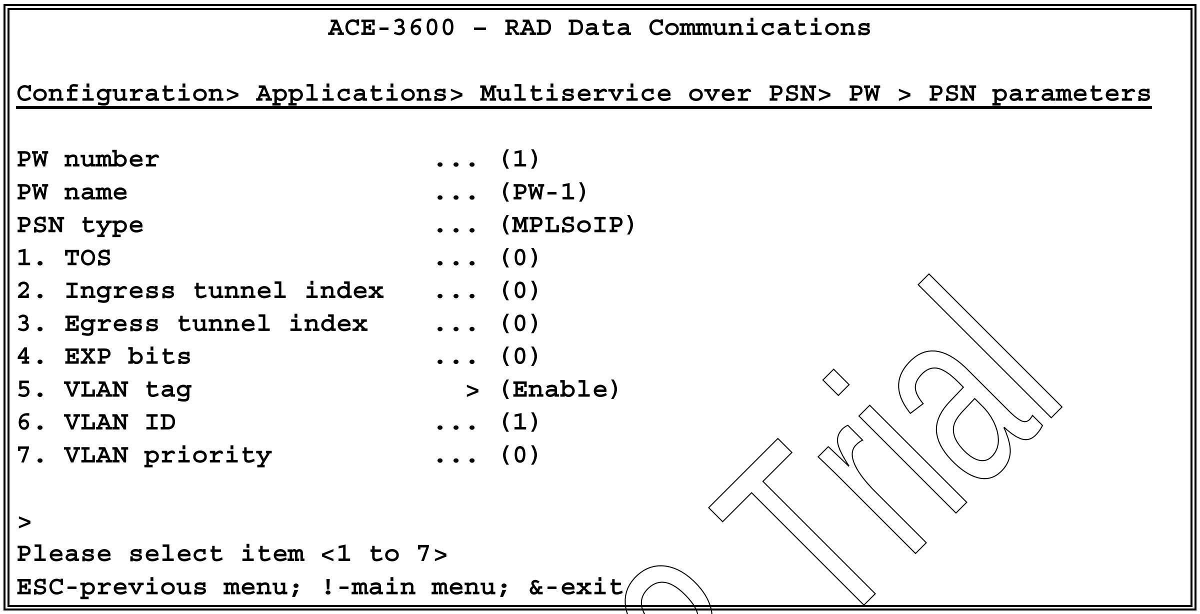
Configuring the PSN Parameters for the PW Connection

Each configured PW connection requires specific definitions for the selected packet-switched network on which it is configured.

➤ **To access the PW PSN parameters:**

- From the PW menu (see *Figure 4-66*), select **PSN Parameters**.

  The PSN Parameters menu is displayed.



```
                    ACE-3600 - RAD Data Communications

Configuration> Applications> Multiservice over PSN> PW > PSN parameters

PW number                 ... (1)
PW name                   ... (PW-1)
PSN type                  ... (MPLSoIP)
1. TOS                    ... (0)
2. Ingress tunnel index   ... (0)
3. Egress tunnel index    ... (0)
4. EXP bits               ... (0)
5. VLAN tag                 > (Enable)
6. VLAN ID                ... (1)
7. VLAN priority          ... (0)

>
Please select item <1 to 7>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-68. Pseudowire PSN Parameters Menu

Table 4-60. Pseudowire PSN Parameters

Parameter	Description	Possible Values
PW number	Displays the PW number as defined in the PW menu (read-only)	See *Table 4-58*
PW name	Displays the PW name as defined in the PW menu (read-only)	See *Table 4-58*
PSN type	Displays the selected PSN type for this PW (read-only)	See *Table 4-59*
TOS	Value of the TOS byte that is used on outbound traffic. ***Note****: Relevant if the PSN type is UDP over IP, MPLS over IP or MPLS over GRE.*	0–255 Default: 0
Ingress tunnel index	Index of the ingress tunnel definition for this PW. A value of 0 means that the tunnel label is not used. . ***Note:*** • *Relevant only for MPLS-based PSNs, not displayed for clock distribution.* • *Cannot be modified dynamically (on the fly).* • *The ingress tunnel's traffic descriptor must be configured in advance.* • *The ingress tunnel provisioning mode (manual or LDP-driven; see Figure 4-61) must be the same as the egress tunnel provisioning mode.*	0 or a configurable ingress tunnel index Default: 0
Egress tunnel index	Index of the egress tunnel definition for this PW. A value of 0 means that the tunnel label is not used.	0 or a configurable egress tunnel index Default: 0

Parameter	Description	Possible Values
	Note: • *Relevant only for MPLS-based PSNs and only if the PW subtype is data or clock distribution* • *Cannot be modified dynamically (on the fly).* • *The egress tunnel's traffic descriptor must be configured in advance.* • *The egress tunnel provisioning mode (manual or LDP-driven) must be the same as the ingress tunnel provisioning mode.* • *If the provisioning mode is LDP-driven, the* ***peer number*** *of the Egress Tunnel menu (see Figure 4-62) must be the same as the peer number in the PW General Parameters menu (see Figure 4-67).*	
EXP bits	The required value for the EXP bits to be used on the PW label and the tunnel label. ***Note****: Visible only for MPLS-based PSNs (MPLS, MPLSoIP, MPLSoGRE) and only if the PW subtype is data or clock distribution.*	0–7
VLAN tag	Enable or disable VLAN tagging on every transmitted packet. ***Note****: Cannot be modified dynamically (on the fly).*	Enable Disable Default: as configured for the matching router interface
VLAN ID	The VLAN ID that is carried on every transmitted packet of this PW. ***Note****: Visible only if VLAN tagging is enabled.*	0–4094 Default: as configured for the matching router interface
VLAN priority	The VLAN priority that is attached to every transmitted packet of this PW. ***Note****: Visible only if VLAN tagging is enabled.*	0–7 Default: 0

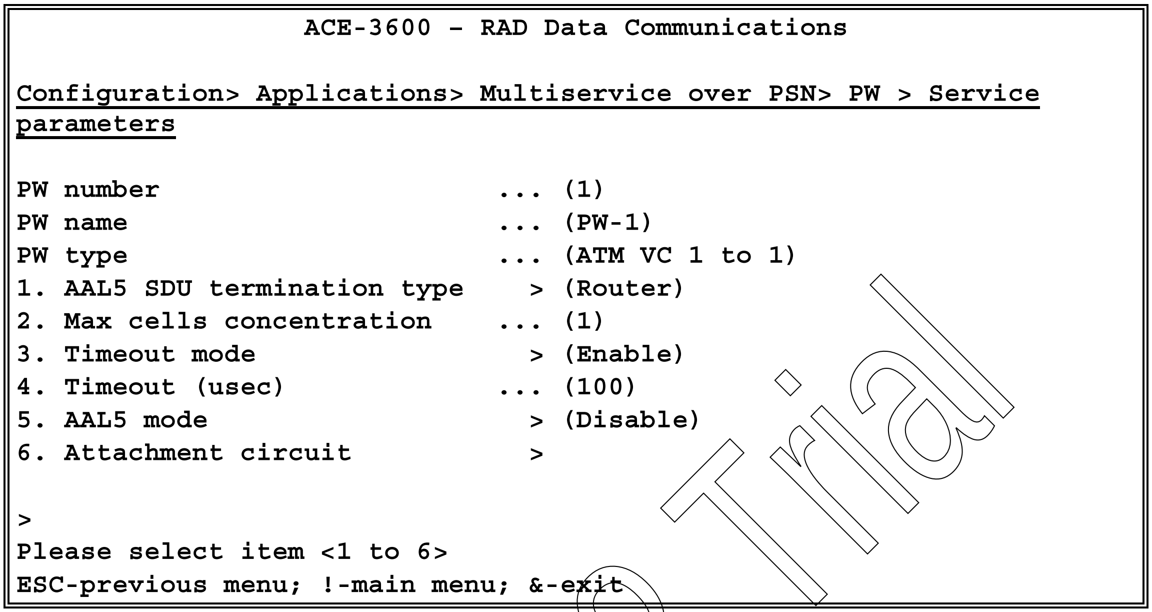
Configuring the ATM Service Parameters for the PW

ATM traffic that is carried over the pseudowire connection is defined as the connection's service. The service parameters are displayed and configured according to the previously selected PW type.

➤ To access the ATM service parameters:

- From the PW menu (see *Figure 4-66*), select **Service Parameters**.

  The Service Parameters appears and displays ATM (*Figure 4-69*) service parameters, depending on the PW type.



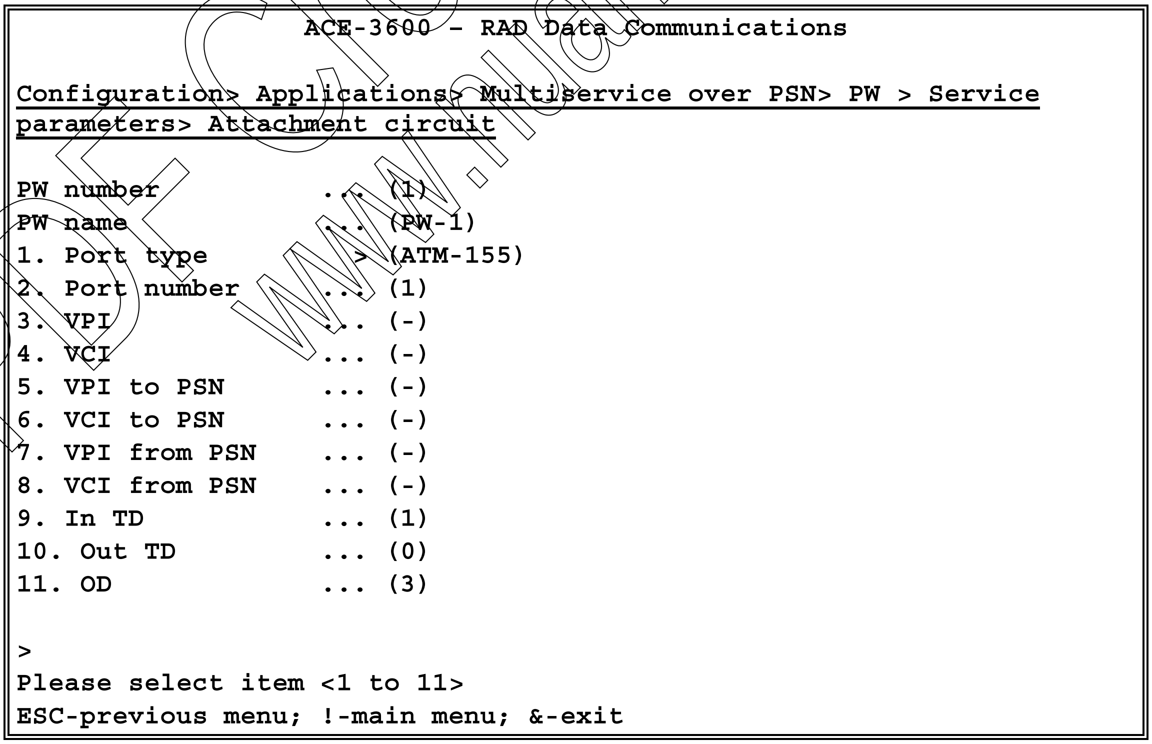
```
                    ACE-3600 - RAD Data Communications

Configuration> Applications> Multiservice over PSN> PW > Service
parameters

PW number                          ... (1)
PW name                            ... (PW-1)
PW type                            ... (ATM VC 1 to 1)
1. AAL5 SDU termination type         > (Router)
2. Max cells concentration         ... (1)
3. Timeout mode                      > (Enable)
4. Timeout (usec)                  ... (100)
5. AAL5 mode                         > (Disable)
6. Attachment circuit                >

>
Please select item <1 to 6>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-69. ATM Pseudowire Service Parameters Menu

Table 4-61. ATM Pseudowire Service Parameters – TBD

Parameter Description		Possible Values
PW number	Displays the PW number as defined in the PW menu (read-only)	See *Table 4-58*
PW name	Displays the PW name as defined in the PW menu (read-only)	See *Table 4-58*
PW type	Displays the PW type as defined in the PW General Parameters menu (read-only)	See *Table 4-59*
AAL5 SDU termination type	Determines whether an AAL5-SDU frames that are received from the PSN should be forwarded to the router or forwarded to an ATM VCC. Relevant only if the selected PW type (see *Table 4-59*) is AAL5-SDU. Cannot be changed dynamically (on-the-fly).	ATM Router Default: Router
Max cells concentration	Maximum number of ATM cells that are concentrated in a single Ethernet frame for this PW. An Ethernet frame is sent only in the following cases: • The maximum number of cells has been reached • An ATM cell indicating the end of the AAL5 PDU has been received (LBS in PTI field is 1) • The timeout for this PW has expired. ***Note:*** *This parameter can be changed dynamically (on-the-fly) only if the provisioning mode is manual. A change will cause a momentary traffic interruption.*	1–29 Default: 1

Parameter	Description	Possible Values
Timeout mode	Enable or disable the timeout mechanism for this PW. Not relevant for the AAL5-SDU PW type. *Note: This parameter can be changed dynamically and a change will cause a momentary traffic interruption.* For more information about the timeout mechanism, see *Frequently Asked Questions* in Chapter 6.	Enable Disable Default: Enable
Timeout (μsec)	The duration of the timeout in microseconds, used in ATM 1:1 or N:1 encapsulation when the timeout mode is enabled. The timer's granularity is 500 microseconds. Can be changed dynamically.	100–5000000 Default: 100
AAL5 mode	Enable or disable AAL5 mode for this PW. When enabled, receiving a cell with PTI=1 triggers a frame transmission. Not relevant for the AAL5-SDU PW type. Cannot be changed dynamically.	Enable Disable Default: Disable
Attachment circuit	Access the circuit parameters for the ATM PW connection (see *Figure 4-70*).	See *Table 4-62*



```
                     ACE-3600 - RAD Data Communications

Configuration> Applications> Multiservice over PSN> PW > Service
parameters> Attachment circuit

PW number           ...  (1)
PW name             ...  (PW-1)
1. Port type          >  (ATM-155)
2. Port number      ...  (1)
3. VPI              ...  (-)
4. VCI              ...  (-)
5. VPI to PSN       ...  (-)
6. VCI to PSN       ...  (-)
7. VPI from PSN     ...  (-)
8. VCI from PSN     ...  (-)
9. In TD            ...  (1)
10. Out TD          ...  (0)
11. OD              ...  (3)

>
Please select item <1 to 11>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-70. Attachment Circuit Menu for ATM PW

Table 4-62. Attachment Circuit Parameters for ATM PW

Parameter Description		Possible Values
PW number	Displays the PW number as defined in the PW menu (read-only)	See *Table 4-58*
PW name	Displays the PW name as defined in the PW menu (read-only)	See *Table 4-58*
Port type	Type of the port from which the PW traffic originated	ATM-155
Port number	Number of the port from which the PW traffic originated	1–8 for ATM-155
VPI	The virtual path identifier of the originating traffic. The VPI parameter cannot be used here if it is in use by another VP XC, or if the VPI/VCI is in use by another ATM PW or ATM VC.	0–4095
VCI	The virtual channel identifier of the originating traffic. Visible only if the PW type is VC 1:1 or VC N:1. The VPI parameter cannot be used here if it is in use by another VP XC, or if the VPI/VCI is in use by another VC XC.	32–65535
VPI to PSN	The virtual path identifier that should be carried toward the PSN by this N:1 PW. Visible only for the N:1 VC and N:1 VP PW types. This parameter is automatically filled according to the VPI value (see above).	0–4095
VCI to PSN	The virtual channel identifier that should be carried over the PSN by this N:1 PW. Visible only for the N:1 VC PW type. This parameter is automatically filled according to the VPI value (see above).	32–65535
VPI from PSN	The virtual path identifier that is expected from the PSN side on this N:1 PW. Visible only for the N:1 VC and N:1 VP PW types. This parameter is automatically filled according to the VPI value (see above). You can set another value as long as it is unique for this PW.	0–4095

Parameter	Description	Possible Values
VCI from PSN	The virtual channel identifier that is expected from the PSN on this N:1 PW. Visible only for the N:1 VC PW type. This parameter is automatically filled according to the VPI value (see above). You can set another value as long as it is unique for this PW.	32–65535
In TD	ID number of a previously defined policing traffic descriptor (In direction), relevant for this PW. For N:1 encapsulation, the TD setting is applied on all the VCs/VPCs connected to the PW (policing is performed at the PW level). *Note:* • *The traffic descriptor of all the VCs attached to the same N:1 PW must be the same.* • *When the TD is set to 0, the policing for the selected ATM channel is stopped.* • *Can be changed dynamically (on-the-fly) as long as it has the same service category and mode.*	0–99999 Default: 0
Out TD	ID number of a previously defined traffic descriptor (Out direction), relevant for this PW. For N:1 encapsulation, the TD setting is applied on all the VCs/VPCs connected to the PW (shaping is performed at the PW level). *Note:* • *The traffic descriptor of all the VCs attached to the same N:1 PW must be the same.* • *A TD that is automatically created for a CES connection cannot be used.* • *Can be changed dynamically (on-the-fly) as long as it has the same service category and mode.*	1–99999 Default: 1
OD	ID number of a previously defined OAM descriptor that is relevant to this PW. The OAM descriptor type must be Intermediate.	1–256 Default: 1

Note

- *All attachment circuit parameters except TD cannot be changed dynamically (on-the-fly).*
- *The Save (**S**) and Remove (**R**) menu functions appear on this submenu to allow addition/removal of any VCC/VPC connected to the N:1 PW.*

Viewing Existing PW Connections and Attachment Circuits

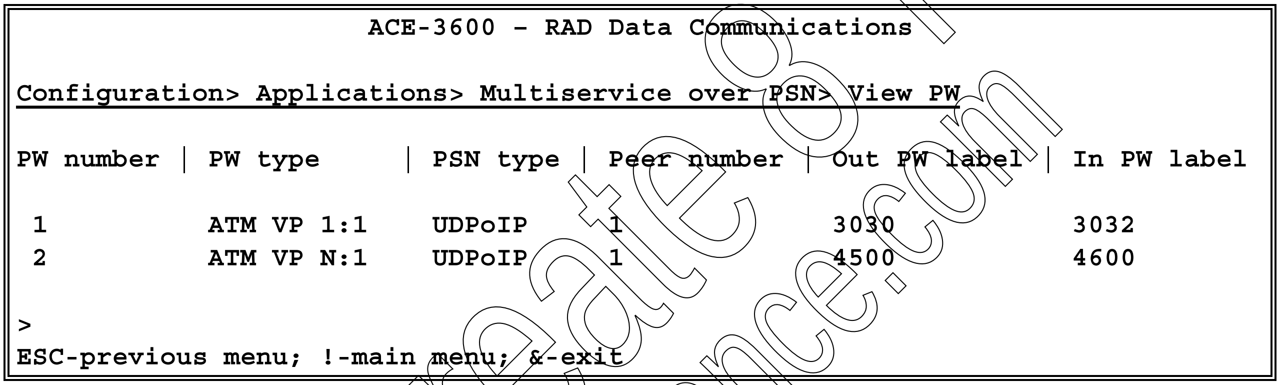
You can view the list of all pseudowire connections that were defined for ACE-3600. The list provides the following details:

- ID number of each PW connection
- Type of the PW (encapsulation type) or PW subtype in case of CESoPSN
- The type of the PSN on which the PW established
- ID number of the remote peer on which the PW terminates
- The Out Label and In Label of the PW.

➤ To view the currently defined pseudowire connections:

- From the Multiservice over PSN menu (see *Figure 4-63*), select View PW.

  The pseudowire connections list is displayed.



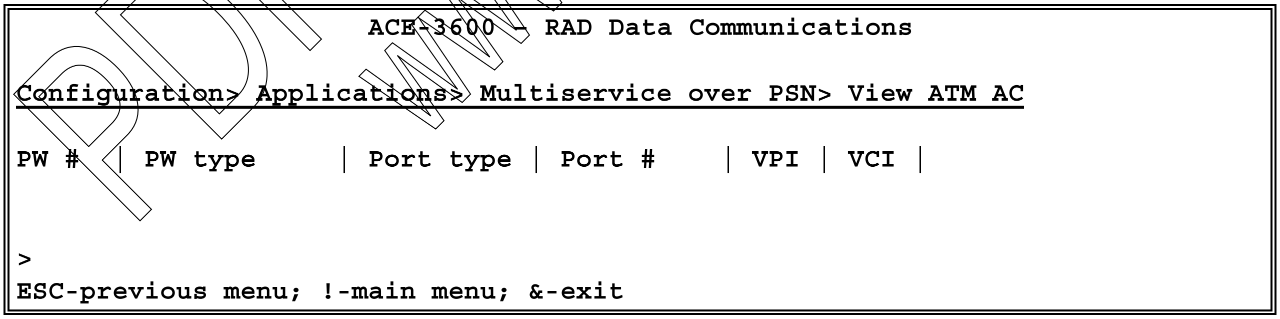
```
                    ACE-3600 - RAD Data Communications

Configuration> Applications> Multiservice over PSN> View PW

PW number | PW type      | PSN type | Peer number | Out PW label | In PW label

 1          ATM VP 1:1    UDPoIP      1             3030           3032
 2          ATM VP N:1    UDPoIP      1             4500           4600

>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-71. Pseudowire Connections List

➤ To view the currently defined ATM attachment circuits:

- From Multiservice over PSN menu, select View ATM AC.

  The ATM ACs are displayed.



```
                    ACE-3600 - RAD Data Communications

Configuration> Applications> Multiservice over PSN> View ATM AC

PW #   | PW type      | Port type | Port #     | VPI | VCI |


>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-72. ATM Attachment Circuits List

4.4 Additional Tasks

You can perform additional tasks as may be necessary or helpful from time to time:

- *Displaying the Inventory*
- *Viewing the License Information*
- *Changing the Password*
- *Managing the File System* – which includes:
  - *Updating the Main Module (Main Card) Software*
  - *Loading a Preset Configuration*
  - *Displaying the Application File Details*
  - *Swapping Application Files*
  - *Transferring Files via TFTP*
  - *Transferring Files via XMODEM*
- *Restarting/Resetting ACE-3600*.

Displaying the Inventory

The inventory screen displays all physical entities that compose the ACE-3600 unit, according to the RFC2737 Entity MIB. For each entity, you can display an inventory table, which provides miscellaneous info regarding the entity. The following parameters are displayed as info columns in the inventory table of each entity (depending on whether the parameters are relevant to the entity):

Index	The physical entity's unique index number
Description	Text description of the physical entity, with dots between words (see *Figure 4-73*)
Name	The physical entity's name
SW version	The physical entity's software version. For a chassis entity, this field contains the running device's software revision and the boot revision
HW version	The physical entity's hardware version
FW version	The physical entity's firmware version
Serial number	The physical entity's serial number
Asset ID	This string is provided to store a user-specific asset identifier for removable physical components. Applicable only to a chassis component

Alias — User-assigned alias name for the physical entity, as specified by a network manager.

FRU — Field Replaceable Unit. Two FRU values are possible:

'True' – the corresponding entity (component) can be replaced in the field.

'False' – the corresponding entity cannot replaced in the field.

Vendor type — The physical entity’s vendor type

Class — The physical entity’s hardware type: chassis, container, power supply, container, fan or port

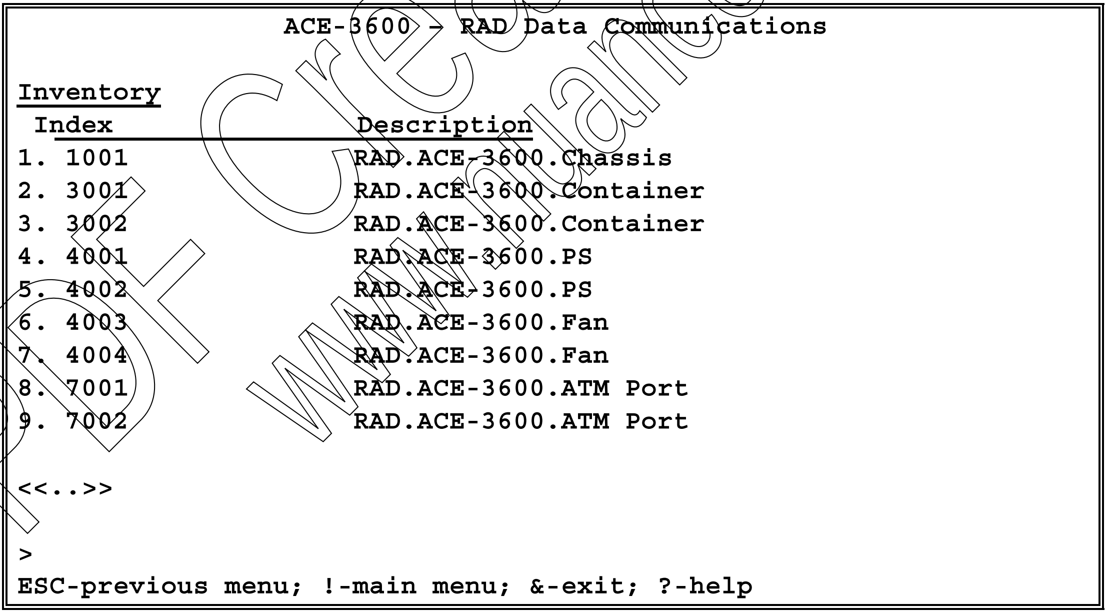
Model name — The physical entity's model name/type

To view the additional columns that are not visible on the initial table, scroll to the right using the right-scroll key (CTRL-D).

➤ To display the inventory:

- From the Main menu, select Inventory.

  The Inventory details are displayed.



```
                    ACE-3600 - RAD Data Communications

Inventory
 Index                Description
1. 1001              RAD.ACE-3600.Chassis
2. 3001              RAD.ACE-3600.Container
3. 3002              RAD.ACE-3600.Container
4. 4001              RAD.ACE-3600.PS
5. 4002              RAD.ACE-3600.PS
6. 4003              RAD.ACE-3600.Fan
7. 4004              RAD.ACE-3600.Fan
8. 7001              RAD.ACE-3600.ATM Port
9. 7002              RAD.ACE-3600.ATM Port

<<..>>


>
ESC-previous menu; !-main menu; &-exit; ?-help
```

Figure 4-73. Inventory Table Screen

You can scroll the page forward (>>) and backward (<<) by pressing CTRL-D or CTRL-R, and up or down by pressing CTRL-U or CTRL-D.

Viewing the License Information

ACE-3600 is delivered with a prefixed **software license pack**, which defines which functional features are available for use. The software license pack is ordered at the purchase stage, and you can view which features are defined in the unit's license file.

➤ To view the license information:

1. From the Main Menu, select **Utilities**.

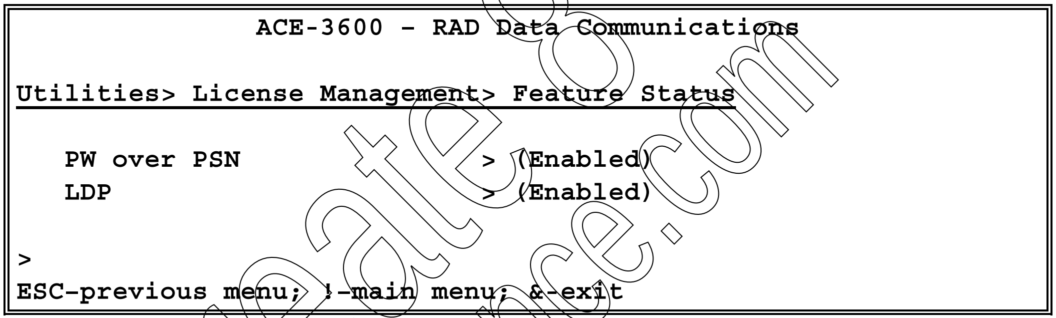
   The Utilities menu is displayed.

2. From the Utilities menu, select **License Management**.

   The License Management menu is displayed.

3. From the License Management menu, select **Feature Status**.

   The Feature Status information is displayed.



```
                ACE-3600 - RAD Data Communications

Utilities> License Management> Feature Status

   PW over PSN            >  (Enabled)
   LDP                    >  (Enabled)

>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-74. Feature Status Menu

Table 4-63. Feature Status Menu Parameters

Parameter	Description	Possible Values (Read-only)
PSN	Availability of the pseudowire over PSN features	Enabled Disabled
LDP	Availability of the LDP features	Enabled Disabled

Changing the Password

For security reasons, it is recommended that you change your user password periodically, and upon configuring the device for the first time. Passwords can be changed in the Change Password menu.

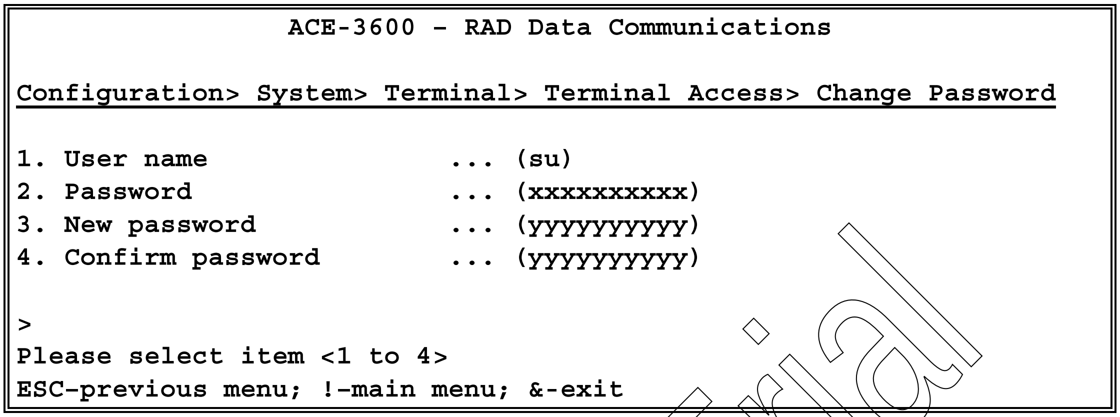
➤ To access the Change Password menu:

1. From the Terminal menu (see *Figure 4-4*), select Terminal Access.

   The Terminal Access menu (see *Figure 4-5*) is displayed.

2. Select Change Password.

The Change Password menu is displayed.



```
                  ACE-3600 - RAD Data Communications

Configuration> System> Terminal> Terminal Access> Change Password

1. User name                 ... (su)
2. Password                  ... (xxxxxxxxxx)
3. New password              ... (yyyyyyyyyy)
4. Confirm password          ... (yyyyyyyyyy)

>
Please select item <1 to 4>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-75. Change Password Menu

Table 4-64. Change Password Menu Parameters

Parameter	Description	Possible Values
User name	Enter the user name for whom the password should be changed.	"**su**" can change password for all access levels. "**tech**" and "**user**" can change the passwords only for themselves.
Password	Enter the current user's password.	Up to 10 alphanumeric characters, case-sensitive Default: "xxxxxxxxxx" and "1234"
New password	Enter the new user's password. ***Note**: Appears only if the password (item no. 2) is correct.*	Up to 10 alphanumeric characters, case-sensitive
Confirm password	Re-enter the new password to confirm it. ***Note:** Appears only if the password (item no. 2) is correct.*	Up to 10 alphanumeric characters, case-sensitive

Managing the File System

The file system management options allow you to:

- Update the main module (main card) software
- Load a preset configuration (see *Loading a Preset Configuration*)
- Display the details of the application files currently stored in the unit (see *Displaying the Application File Details*)
- Swap the active and backup application files (see *Swapping Application Files*)
- Download/upload software or configuration files using the TFTP or XMODEM protocols (see *Transferring Files via TFTP* and *Transferring Files via XMODEM*)

- Save/delete the default configuration file (see *Saving/Deleting the Default Configuration File*).

Updating the Main Module (Main Card) Software

Unlike a standalone unit that does not have two main processor modules, ACE-3600 requires a special procedure for updating the software files of its two main modules that work in redundancy mode. The software can be downloaded to the main modules using one of the following procedures:

- Single traffic switch – the active main module is reset only once and traffic is affected only once
- Double traffic switch – the active main module is reset twice and the traffic is affected twice.

➤ To perform a single traffic switch procedure:

1. Initiate the Software Download command using a TFTP server, as explained in *Transferring Files via TFTP* (Utilities › File Utilities › File Transfer › TFTP › Software download).
2. Perform an update of the downloaded files on Main Card B, as explained in *Setting the Main Module Redundancy* (Configuration › Protection › Main Card Redundancy › Software update to other card).
   - ▪ During the software update procedure, the “Software Update operation is in progress” message is displayed at the bottom of the Main Card Redundancy window.
   - ▪ When the update procedure completes, the “Ready” message is displayed at the bottom of the window.
3. Perform a reset to Main Card B (Configuration › Protection › Main Card Redundancy › Reset other card).

   During the reset:

   - □ Redundancy Status shows a "Communication loss"
   - □ Main Card B starts with the updated software version
   - □ Redundancy Status shows "Software Mismatch".
4. Perform a reset (Utilities › Device Reset) to the active main module (Main Card A).

   During the reset:

   - □ Main Card B becomes the active main module, causing the traffic to switch to it.
   - □ Redundancy Status shows "Communication loss".
   - □ Main Card A is updated with the new software version.
   - □ Redundancy Status shows "OK" indication when the process finishes.

Note *You can switch back to Main Card A manually, using 'Switch to other card', yet this would affect the traffic again.*

➤ To perform a double traffic switch procedure:

1. Initiate the **Software Download** command using TFTP or XMODEM (see *Transferring Files via TFTP* or *Transferring Files via XMODEM*).
2. Reset the active main module (**Utilities > Device Reset**).

   During the reset:

   - Main Card B becomes the active main module, causing the traffic to switch to it.
   - Redundancy Status shows "Communication loss".
   - Main Card A is updated with the new software version.
   - Redundancy Status shows "Software Mismatch".
3. Repeat the software download procedure for Main Card B, which is the active main module.
4. Reset the active main card (Utilities > Device Reset).

   During the reset, Main Card B becomes the active main module, causing the traffic to switch back to it.

Loading a Preset Configuration

The timesaving alternative to the manual menu-driven configuration is loading a preset configuration file, provided that such configuration is available.

➤ To load a preset configuration to ACE-3600:

1. Initiate the Configuration Download command from the TFTP menu, as explained in *Transferring Files via TFTP* (Utilities > File Utilities > File Transfer > TFTP > Configuration download).

   The download is performed on the active main module (Main Card A). During the download, the following messages are displayed: Connected, Transferring data, File transferred.

   Once the download is complete, the unit automatically reboots itself. During the reboot:

   - Main Card B becomes the active main module, causing the traffic to switch to it.
   - Redundancy Status shows "Communication loss" and then "Configuration mismatch" at the end of the process.
2. Repeat the Configuration Download command for Main Card B, which is the currently active main module.

   Once the download is complete, the unit automatically reboots itself. During the reboot:

   - Main Card A becomes the active main module again, causing the traffic to switch back to it.
   - Redundancy Status shows "Communication loss" and then "OK" at the end of the process.

Displaying the Application File Details

➤ To display the ACE-3600 application files:

1. From the Utilities menu, select **File Utilities**.

   The File Utilities menu is displayed.

2. Select **File System**.

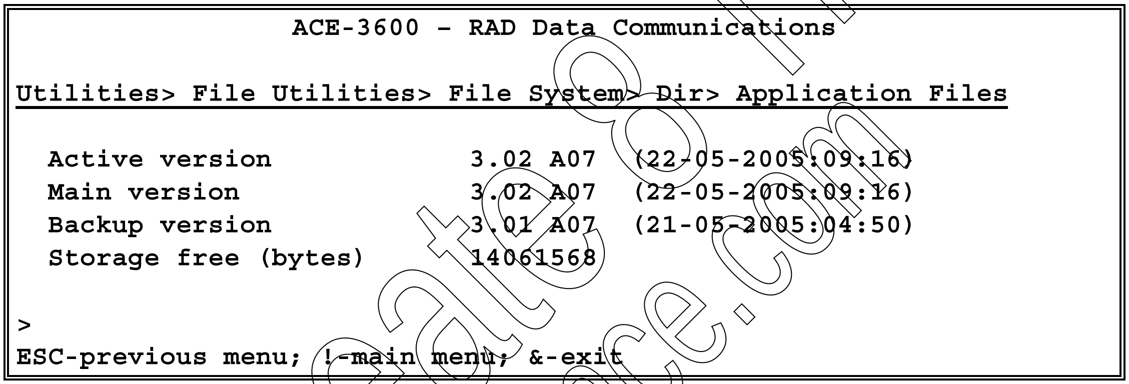
   The File System menu is displayed.

3. Select **Dir**.

   The Dir menu is displayed.

4. Select **Application Files**.

   The Application Files menu is displayed.



```
                    ACE-3600 - RAD Data Communications

Utilities> File Utilities> File System> Dir> Application Files

  Active version             3.02 A07  (22-05-2005:09:16)
  Main version               3.02 A07  (22-05-2005:09:16)
  Backup version             3.01 A07  (21-05-2005:04:50)
  Storage free (bytes)       14061568

>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-76. Application Files Menu

Table 4-65. Application Files Menu Parameters

Parameter	Description	Possible Values
Active version	The active version of the running application. ***Note:*** *The active version is read at power-up from the DiskOnChip main version header file.*	Alphanumeric version number with the version's date and time (read-only)
Main version	The main application version, which may not necessarily be the currently active one. ***Note:*** *The main version is read at power-up from the DiskOnChip main version header file and after software download to main version.*	Alphanumeric version number with the version's date and time (read-only)
Backup version	The backup application version, for rare cases when the main version is corrupted. *Note: The backup version is read at power-up from the DiskOnChip main version header file, or after downloading the backup software version.*	Alphanumeric version number with the version's date and time (read-only)
Storage free (bytes)	Free space left on the ACE-3600 internal flash disk	0–99999999

Swapping Application Files

The current application files can be swapped with the backup files when necessary.

➤ **To swap between the main and backup application files:**

1. From the Dir menu (**Utilities > File Utilities > File System > Dir**), select **Swap application files.**

   A confirmation message is displayed: **`Are you sure (Y/N)?`**

2. Type **Y** to confirm the files swap.

   ACE-3600 continues to run with the previous files version until you manually reset the unit (see *Restarting/Resetting ACE-3600*).

Requirements for TFTP/XMODEM File Transfer Operations

Note *The following information applies to XMODEM and TFTP file transfer operations that are available/selectable from either the boot menu or the standard management menus. For more information about the boot operations, refer to Appendix B.*

From time to time, various file transferring operations, such as preset configuration download/upload, license or user file download/upload may be necessary. You may want to share the unit's configuration with other units, download new software into the unit, obtain a new boot code, or use file transferring for other purposes.

All file transfer operations are performed via the XMODEM or TFTP protocols, and require a protocol-compatible application that must be installed on the computer/server with which ACE-3600 communicates. For example, if you connect ACE-3600 to a laptop, the laptop requires an application that allows communication and file transfers via the selected protocol.

Accordingly:

- For file transfers via XMODEM – a standard terminal application, such as Windows HyperTerminal, must be installed on the local computer. HyperTerminal is bundled with Windows XP by default, and can be accessed via Start > All Programs > Accessories > Communications > HyperTerminal. For more information, refer to *Chapter 3*.
- For file transfers via TFTP – a TFTP server application must be installed on the local or remote computer. As it runs in the background, the TFTP server waits for any TFTP file transfer request originating from the ACE-3600 unit, and carries out the received request automatically.

  A variety of third-party applications, such as 3Cdaemon (available from www.3com.com) or PumpKIN (available from http://kin.klever.net/pumpkin/), allow the instant creation of a TFTP server on a computer. For more information, refer to the documentation of these applications.

When using the RADview-EMS management package, a dedicated TFTP application is installed on the network management station (NMS), allowing TFTP protocol operations to be initiated to/from it. For more information, refer to the RADview-EMS user's manual.

Transferring Files via TFTP

The TFTP protocol is typically used for remote IP-to-IP file transfers via the product unit's Ethernet interface. It can be used, however, for local file transfer as well, as the transfer rate of the Ethernet interface is much faster than that of the RS-232 interface.

Setting-up a TFTP Server

If you use a local laptop and TFTP is the preferred transfer method, a TFTP server application must be installed on it.

As previously mentioned in *Requirements for TFTP/XMODEM File Transfer Operations*, third-party applications are available and you should refer to their setup documentation.

Checking the Firewall Settings

TFTP file transfers are carried out through Port 69. You should check that the firewall you are using on the server computer allows communication through this port.

➤ To allow communication through Port 69 in Windows XP:

1. Double-click the My Network Places icon, located on the desktop.

   The My Network Place window appears.

2. On the Network Tasks sidebar, click View network connections.

   The available network connections are displayed.

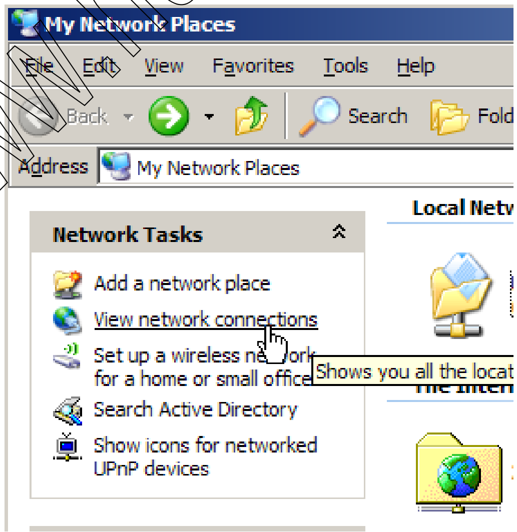


Figure 4-77. View Network Connections

3. On the Network Tasks sidebar, click Change Windows Firewall settings.

   The Windows Firewall dialog box appears.

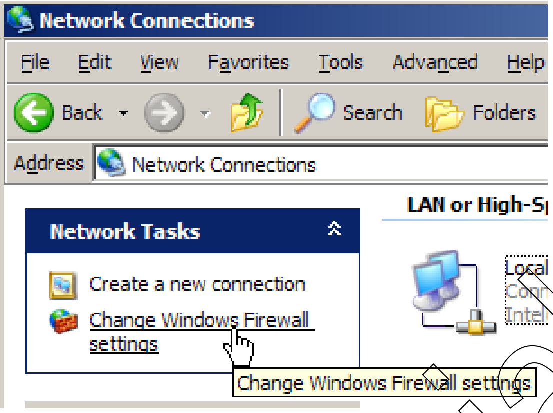
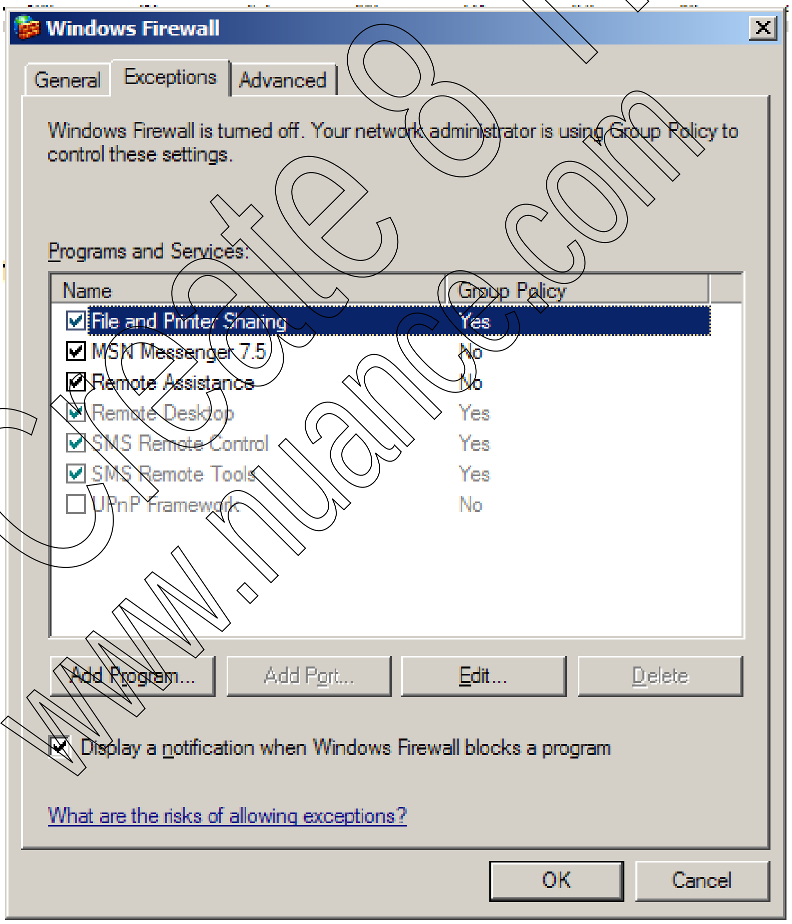

Network Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders
Address Network Connections
Network Tasks
Create a new connection
Change Windows Firewall settings
LAN or High-S
Local
Conr
Intel
Change Windows Firewall settings

Figure 4-78. Change Firewall Settings

4. Click the Exceptions tab.


Windows Firewall
General Exceptions Advanced

Windows Firewall is turned off. Your network administrator is using Group Policy to control these settings.

Programs and Services:

Name	Group Policy
☑ File and Printer Sharing	Yes
☑ MSN Messenger 7.5	No
☑ Remote Assistance	No
☑ Remote Desktop	Yes
☑ SMS Remote Control	Yes
☑ SMS Remote Tools	Yes
□ UPnP Framework	No

Add Program... Add Port... Edit... Delete

☑ Display a notification when Windows Firewall blocks a program

What are the risks of allowing exceptions?

Figure 4-79. Windows Firewall Dialog Box – Exceptions Tab

5. Check whether Port 69 appears on the exceptions list. If it does not, click Add Port and add it to the list of exceptions.

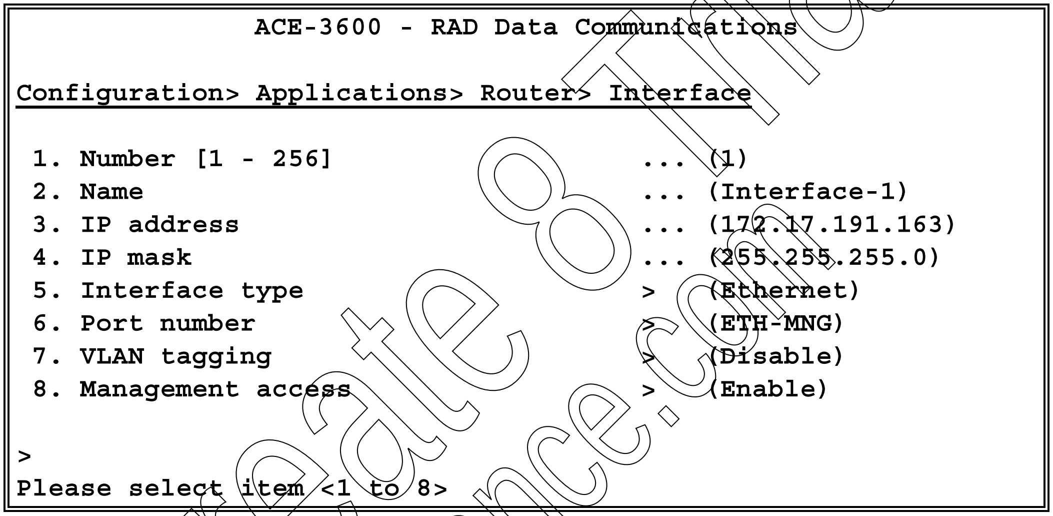
Note *Different firewall types require different configuration. Refer to your firewall's documentation to check how TFTP file transfers can be allowed to pass through it using a UDP-type port.*

Setting the Unit's IP Address

Before a TFTP file transfer can take place, you must assign an IP address to the ACE-3600 unit.

➤ To set the IP address for the ACE-3600 unit:

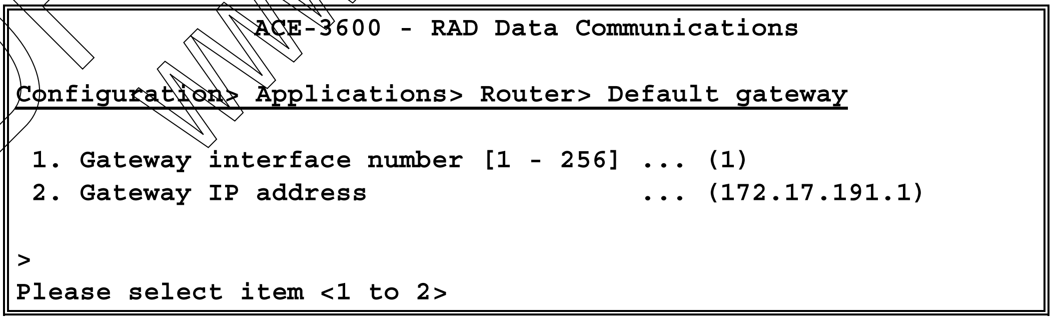
1. When logged into the product via HyperTerminal (for more information, refer to Chapter 3 of the product manual), select Configuration > Applications > Router > Interface.
2. Enter the router interface's IP address and IP mask. For more information about the parameters on this menu, refer to the product manual.



```
                ACE-3600 - RAD Data Communications

Configuration> Applications> Router> Interface

 1. Number [1 - 256]                ...  (1)
 2. Name                            ...  (Interface-1)
 3. IP address                      ...  (172.17.191.163)
 4. IP mask                         ...  (255.255.255.0)
 5. Interface type                  >    (Ethernet)
 6. Port number                     >    (ETH-MNG)
 7. VLAN tagging                    >    (Disable)
 8. Management access               >    (Enable)

>
Please select item <1 to 8>
```

Figure 4-80. Router Interface Menu

3. Press S to save.
4. Select Configuration > Applications > Router > Default gateway.
5. Enter the default gateway's IP address.



```
                ACE-3600 - RAD Data Communications

Configuration> Applications> Router> Default gateway

 1. Gateway interface number [1 - 256] ... (1)
 2. Gateway IP address                 ... (172.17.191.1)

>
Please select item <1 to 2>
```

Figure 4-81. Default Gateway Menu

The unit's gateway address is set.

Note *Other RAD products may require a different procedure for setting the unit's IP address. Refer to the relevant product's Installation and Operation Manual for more information.*

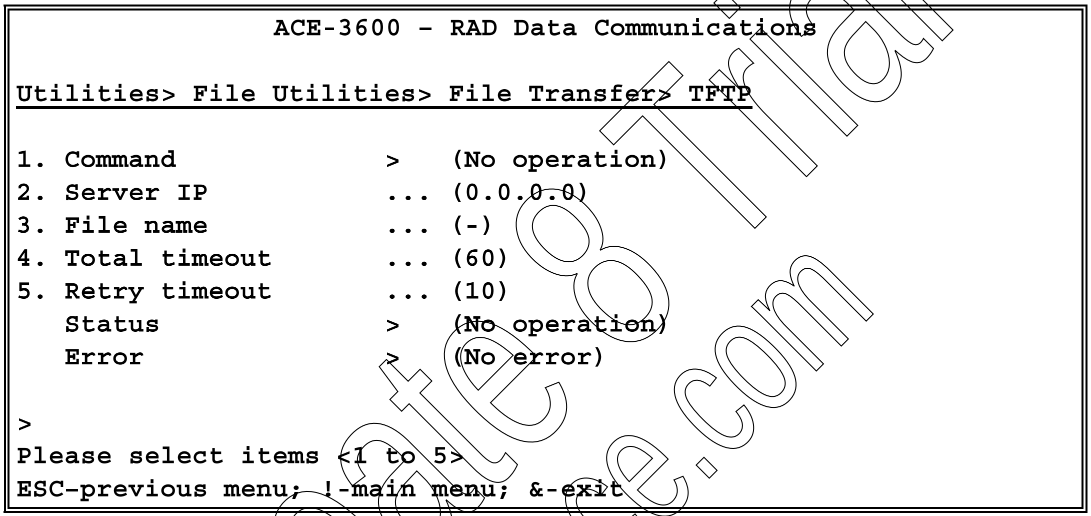
Selecting and Performing a TFTP Operation

The TFTP file transfer options differ from one product family to another.
The ACE-3600 product family has 10 different TFTP file transfer options, including license and default configuration download (for more information, refer to *Saving/Deleting the Default Configuration File*).

➤ To select and carry out a TFTP file transfer option:

1. Select Utilities > File Utilities > File Transfer > TFTP.

   The TFTP menu is displayed.



```
                 ACE-3600 - RAD Data Communications

Utilities> File Utilities> File Transfer> TFTP

1. Command               >    (No operation)
2. Server IP             ...  (0.0.0.0)
3. File name             ...  (-)
4. Total timeout         ...  (60)
5. Retry timeout         ...  (10)
   Status                >    (No operation)
   Error                 >    (No error)

>
Please select items <1 to 5>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-82. TFTP Menu

2. On Server IP, enter the IP address of the TFTP server.
3. On File Name, enter the name of the file to be transferred.
4. On Command, select the required TFTP operation (see *Table 4-66*).
5. Press S to save the command request.

   The unit begins communicating with the TFTP server and performing the specified command. On the TFTP server side, the server application receives the command and carries it out automatically. Once the transfer is completed, the 'Ended OK' status is shown.

Table 4-66. TFTP Operations

Parameter Description		**Possible Values**
Command	Select the type of the file transfer command to be carried out: • No operation – no file transfer is performed. • Software download – download new application files to the unit, for replacing the currently running application files. • Configuration download – download a preset configuration to the unit. • Configuration upload – upload the unit's configuration. • Event log upload – upload the unit's event log. • Software download to backup – download files that will replace the backup application files (not the currently running application files).	No operation Software download Configuration download Configuration upload Event log upload Software download to backup Monitoring upload User file download User file upload
	• Monitoring upload – upload the monitoring statistics • User file download – download any type of file to the unit (within the flash memory limits). • User file upload – upload any type of file. • Default configuration download – download a default configuration file. • License download – download a license file to the unit.	Default configuration download License download Default: No operation
Server IP	The IP address of the server from/to which the files are transferred.	0.0.0.0 – 255.255.255.255
File name	The name of the remote file to be downloaded/uploaded It is a string.	8 alphanumeric characters; not case-sensitive
Total timeout	Total timeout period (in seconds), which is the maximum time period allowed for the attempted transmission	1–1000 Default: 60
Retry timeout	The retry timeout period (in seconds), which is the time period allowed to retry the transmission session.	10 (read-only)

Parameter	Description	Possible Values
Status	TFTP file transfer status. The status display is refreshed every one second.	No Operation Connecting Transferring data Ended on Time out Ended OK Error
Error	TFTP file transfer error status (if an error has occurred). The error status display is refreshed every one second.	Unavailable (no router interface IP) No error File not found Illegal TFTP operation Unknown transfer ID Illegal PDU size Illegal file mode No empty XC No empty UDP port Server overflow

Note *Once a **configuration download** is complete, ACE-3600 automatically resets itself.*

Transferring Files via XMODEM

The XMODEM protocol is typically used for local file transfers via the product unit's RS-232 serial interface. The file transfer is performed directly via the RS-232 cable and does not involve IP-based connectivity, nor firewall concerns.

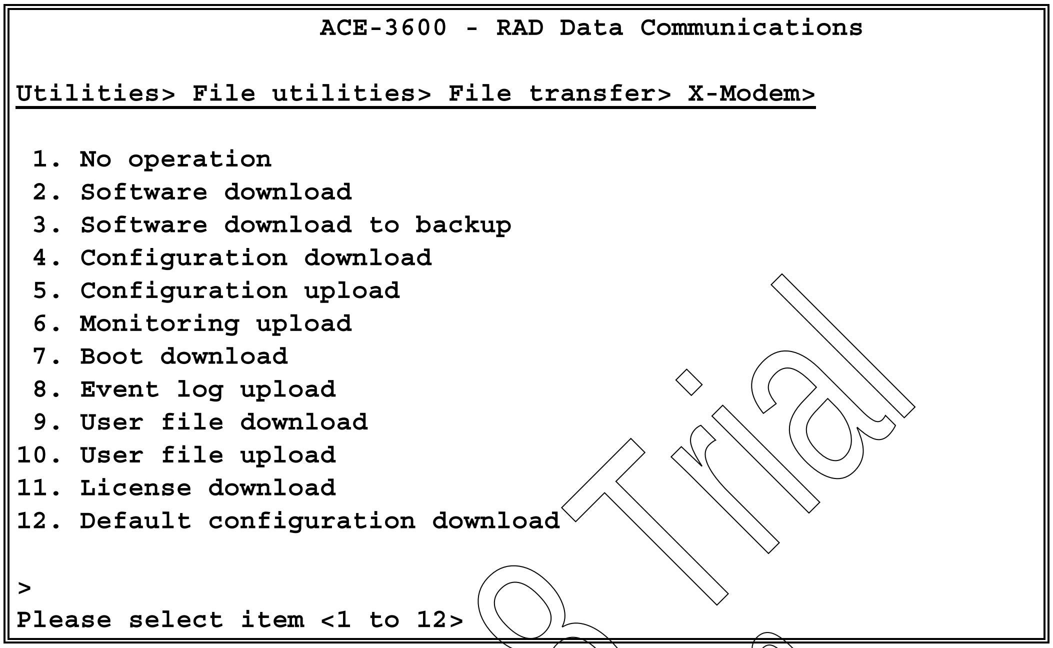
Selecting an Operation

The XMODEM file transfer options differ from one product family to another. The ACE-3600 product family has 11 different XMODEM file transfer options, including license and default configuration download.

➤ To select an XMODEM file transfer option:

1. When logged into the product via HyperTerminal (for more information, refer to *Chapter 3*), select Utilities > File utilities > File transfer > X-Modem.

   The XMODEM file transfer options are displayed.



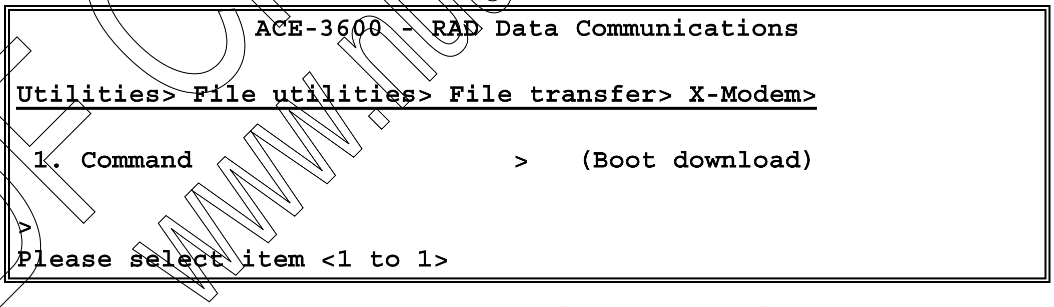
```
                   ACE-3600 - RAD Data Communications

Utilities> File utilities> File transfer> X-Modem>

 1. No operation
 2. Software download
 3. Software download to backup
 4. Configuration download
 5. Configuration upload
 6. Monitoring upload
 7. Boot download
 8. Event log upload
 9. User file download
10. User file upload
11. License download
12. Default configuration download

>
Please select item <1 to 12>
```

Figure 4-83. XMODEM File Transfer Options

2. Select the required transfer operation. For more information about each option, refer to *Table 4-67*.

Note

- *A **download** option means that a file is to be sent from the local computer to the product unit.*
- *An **upload** option means that a file is to be sent from the product unit to the local computer.*



```
               ACE-3600 - RAD Data Communications

Utilities> File utilities> File transfer> X-Modem>

 1. Command                    >   (Boot download)

>
Please select item <1 to 1>
```

Figure 4-84. A Transfer Option (Boot Download) is Selected

3. Press S to save the selection.

   Depending on the selected operation, the unit waits for a manual file transfer operation (see *Sending a File to the Unit* or *Receiving Files from the Unit*).

Table 4-67. XMODEM Operations

Parameter Description		Possible Values
Command	The file transfer command to be carried out; see explanation of each in *Table 4-66*. Boot download is explained in *Appendix B*.	No operation Software download Configuration download Configuration upload Event log upload Software download to backup Boot download Monitoring upload User file download User file upload Default: No operation

Note *Once a* ***configuration download*** *is complete, ACE-3600 automatically resets itself.*

Sending a File to the Unit

The actual XMODEM file transfer is invoked manually from the HyperTerminal Transfer menu.

➤ To send a file from the local computer to the product unit:

1. From the **Transfer** menu, select **Send File**.

   The Send File dialog box appears.

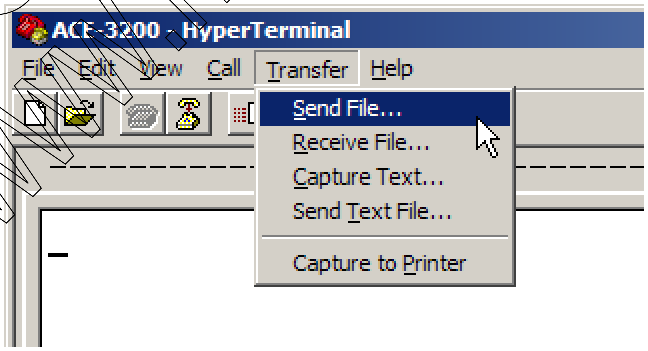
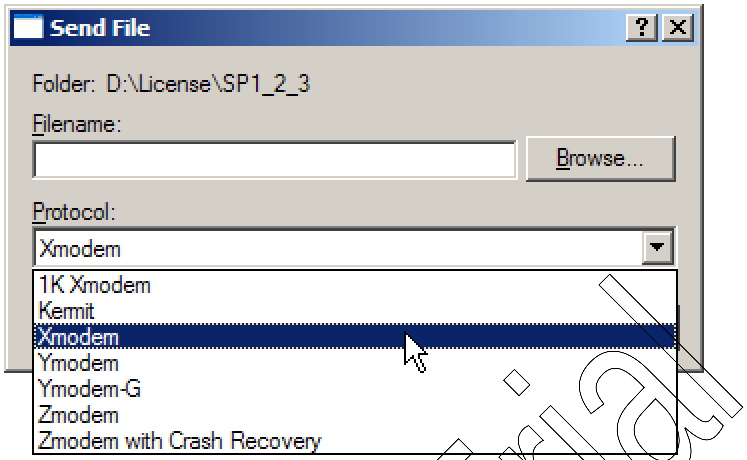


Figure 4-85. HyperTerminal Transfer Menu – Send File

2. From the Protocol drop-down list, select Xmodem.



Send File

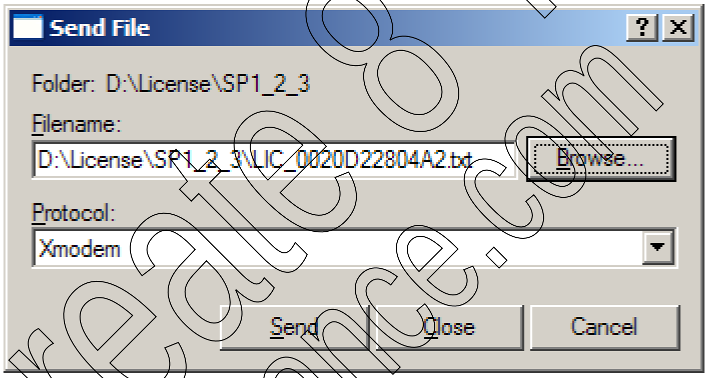
Folder: D:\License\SP1_2_3

Filename:

Protocol: Xmodem

Figure 4-86. Send File Dialog Box – Selecting Xmodem

3. Click Browse and locate the path of the file that should be transferred.



Send File

Folder: D:\License\SP1_2_3

Filename: D:\License\SP1_2_3\LIC_0020D22804A2.txt

Protocol: Xmodem

Figure 4-87. Send File Dialog Box – File Specified

4. Click Send.

   The specified file is sent to the product unit.

Receiving Files from the Unit

Vice-versa, the actual receive operation is also invoked manually.

➤ To receive a file from the product unit to the local computer:

1. From the Transfer menu, select Receive File.

   The Receive File dialog box appears.

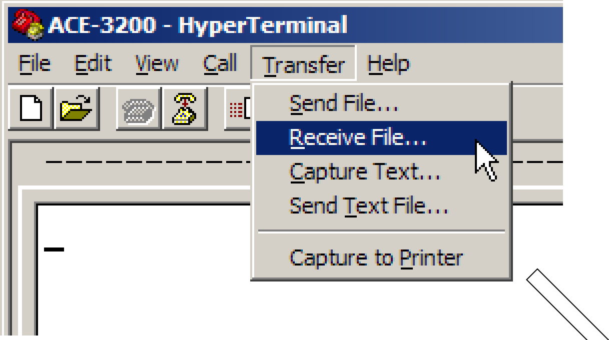
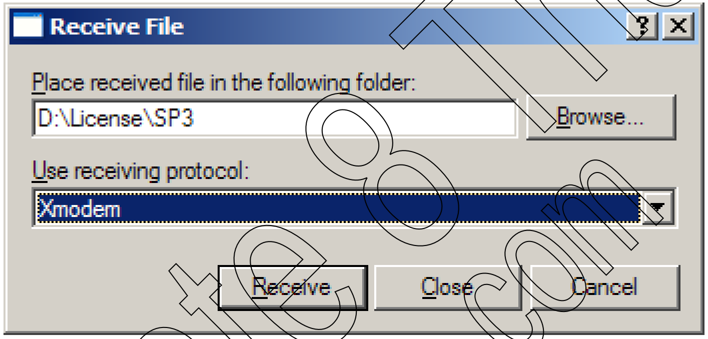


Figure 4-88. Receive File Dialog Box

2. From the Protocol drop-down list, select Xmodem.



Place received file in the following folder: D:\License\SP3

Use receiving protocol: Xmodem

Figure 4-89. Receive File Dialog Box

3. Click Browse to define the local directory into which the file should be transferred.
4. Click Receive.

   The specified file is received from the product unit to the local computer.

Saving/Deleting the Default Configuration File

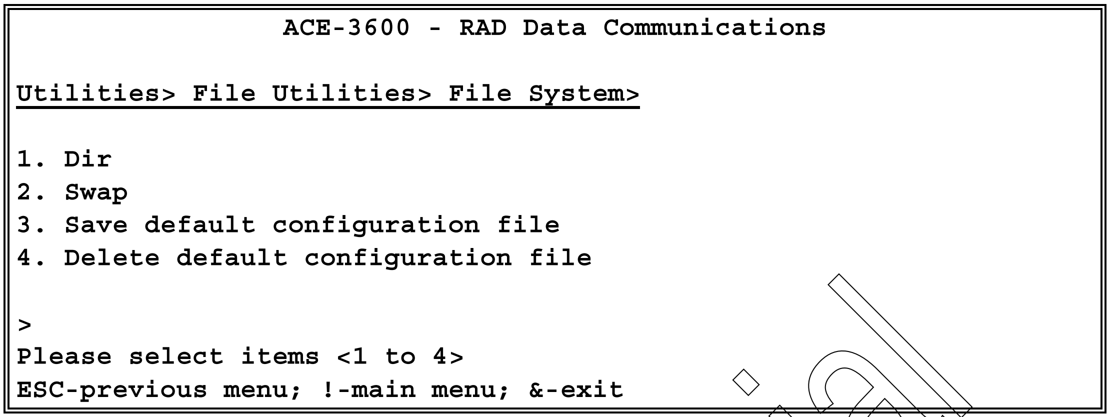
The current configuration of ACE-3600, including the entire set of parameters defined through the management menus, can be saved as the default configuration, meaning that any configuration reset operation (see *Resetting the Unit to Configuration Defaults*) returns the unit to that saved default configuration. If there is no configuration saved as default, the factory-default settings are used on the reset operation.

➤ To save the current configuration as default:

1. From the Utilities menu, select File Utilities.

   The File Utilities menu is displayed.
2. Select File System.

   The File System menu is displayed.



```
                     ACE-3600 - RAD Data Communications

Utilities> File Utilities> File System>

1. Dir
2. Swap
3. Save default configuration file
4. Delete default configuration file

>
Please select items <1 to 4>
ESC-previous menu; !-main menu; &-exit
```

Figure 4-90. File System Menu

3. Select Save default configuration file.

   The current device configuration is saved internally as the default configuration using the *.cfg file extension.

➤ To delete the default configuration file:

- From the File System menu, select Delete default configuration file.

  The default configuration file is deleted and the factory-default configuration is used instead.

Restarting/Resetting ACE-3600

ACE-3600 supports two types of initialization operations:

- *Restarting the Unit*
- *Resetting the Unit to Configuration Defaults.*

Restarting the Unit

When necessary, you can restart the ACE-3600 unit. Restarting ceases any current operation, reloads the application file and initiates a device self test.

Note

- *Restarting the unit does not affect configuration settings.*
- *Only the **active main module** is reset. When the reset starts, the standby module immediately becomes the active main module.*

➤ To restart ACE-3600:

1. From the Utilities Menu (Main Menu > Utilities), select Device reset.

   A confirmation message appears: **`Are you sure? (Y/N)`**.

2. Type Y to confirm the device reset (restart).

   The unit's active main module of restarts by reloading its software and performing a self test.

Resetting the Unit to Configuration Defaults

You can reset ACE-3600 to its factory-default configuration or to a saved configuration (see *Saving/Deleting the Default Configuration File*), discarding the current configuration.

Note *This operation is irreversible unless the current configuration can be restored from downloadable files.*

➤ To reset ACE-3600 to factory defaults:

1. From the System menu (see *Figure 4-3*), select Factory Default.

   A confirmation message appears: `Are you sure (Y/N)?`

2. Type Y to confirm the resetting of the unit to the factory defaults.

   ACE-3600 resets all parameters to their default values and then reboots itself.

Chapter 5

Configuring a Typical Application

This chapter describes the configuration of ACE-3600 in a typical application, and provides practical configuration examples for implementing it.

Figure 5-1 illustrates a typical application, in which:

1. Two 3G Node B units are connected to the ACE-3100 and ACE-3200 units, which serve as the remote gateways.
2. Node B (1) is connected to ACE-3100 via an STM-1/OC-3 link, and Node B (2) is connected to ACE-3200 via an E1/T1/J1 IMA link.
3. On the central site side, a 3G RNC is connected to ACE-3600, which serves as the central gateway. The RNC is connected to ACE-3600 via multiple STM-1/OC-3 links, using automatic protection switching (APS; optional).
4. On the ACE-3600 side, one VP connection and one VC connection are configured for each remote gateway unit that interconnects with a 3G Node B unit.

The 3G RNC provides the timing reference to ACE-3600, and the clock/timing is then distributed by ACE-3600 over the PSN towards ACE-3100 and ACE-3200 (that are able to recover the clock).

A network management station connected to the PSN can manage all units over an IP-based format.

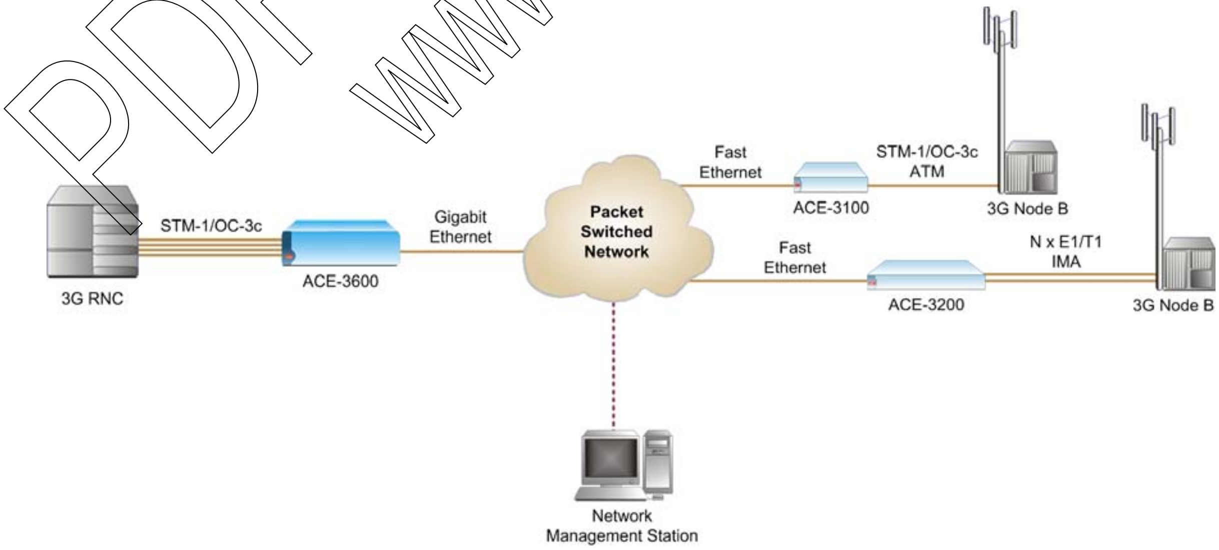


Figure 5-1. Emulated ATM Services over PSN

5.1 Configuring the ACE-3600 Unit

The ACE-3600 configuration stages are:

a. *Configuring the Physical Layer Parameters* – which includes:
   - *Configuring the ATM-155 Ports*
   - *Configuring the GbE Ports*

b. *Setting the Protection Parameters* – which includes:
   - *Setting System Redundancy*
   - *Setting Ethernet Redundancy*
   - *Setting ATM-155 Port Protection*

c. *Configuring the Application Parameters* – which includes:
   - *Configuring the Router Parameters*
   - *Configuring the General Multiservice PW over PSN Parameters*
   - *Configuring the Remote Peer Parameters*
   - *Configuring the Pseudowire Parameters*

d. *Setting the Clock Source*

e. *Defining the Manager IP Address.*

Instructions regarding the ACE-3100 and ACE-3200 unit in this typical application can be found in the ACE-3100, ACE-3200 Installation and Operation Manual.

Note *The IP addresses and IP masks presented in this chapter are only an example. You should set the IP and mask addresses according to the actual network parameters.*

Configuring the Physical Layer Parameters

Configuring the ATM-155 Ports

➤ To configure the ATM-155 port(s):

- In the ATM-155 menu (Configuration > Physical layer > Port > **ATM-155**), set the following parameters for each of the four ports of interface module 1:

Parameter	Value
Port number	1, 2, 3, 4 (define separately for each port)
Port activation	Enable
Transmit clock source	System

Parameter	Value
Frame type	SDH
Output rate (cps)	353208
OAM cell generation	Disable

Note *For APS, the same parameters should be defined for the corresponding ports on interface module 2 (ports 5–8).*

Configuring the GbE Ports

➤ To configure the Gigabit Ethernet parameters:

- On the Ethernet menu (Configuration › Physical layer › Port › **Ethernet**), set the following parameters for each Ethernet port:

Parameter	Value
Port number	GbE-1
Port activation	Enable
Auto negotiation	Enable
Default type	1000Mbps full duplex
Rate limiter	Disable

Note *For redundancy protection (if required), configure the same parameters for GbE Port 2.*

Setting the Protection Parameters

Setting System Redundancy

You can set the two main modules (if two are installed) to work in redundancy protection mode (optional).

➤ To set the system redundancy parameters:

- On the Main Card Redundancy menu (Configuration › System › Protection › **Main Card redundancy**), set the following parameters:

Parameter	Value
Card redundancy	On
Default main card	Card A
WTR time (sec)	5

Setting Ethernet Redundancy

You can set a redundancy mode for the Gigabit Ethernet link between ACE-3600 and the PSN equipment (optional).

➤ To configure the Ethernet redundancy:

- On the Ethernet Redundancy menu (Configuration > System > Protection > Ethernet redundancy), set the following parameters:

Parameter	Value
Group ID	1
Primary port	Gbe-1
Secondary port	GbE-2
Mode	1:1
Revertive	No

Setting ATM-155 Port Protection

You can set a protection mode for the STM-1/OC-3c link between ACE-3600 and the RNC (optional).

➤ To configure the APS parameters:

- On the APS menu (Configuration > System > Protection > APS), set the following parameters:

Parameter Value	
Group ID	APS-1
Port type	ATM-155
Working port #1	1, 2, 3, 4
Working port #2	5, 6, 7, 8 (in correspondence to port #1)
Mode	1+1 optimized bi-directional
WTR time (sec)	300

Configuring the Application Parameters

The ACE-3600 application configuration includes:

- Router parameters
- General multiservice over PSN parameters
- Remote peer parameters
- Pseudowire parameters.

Configuring the Router Parameters

➤ To configure the router parameters:

1. On the router Interface menu (Configuration › Applications › Router › Interface), set the following parameters:

Parameter Value	
Number	1
Name	Interface-1
IP address	172.17.143.100
IP mask	255.255.255.0
Interface type	Ethernet RDN group
Group number	1
VLAN tagging	Disable

2. On the Default Gateway menu (Configuration › Applications › Router › Default gateway), set the following parameters:

Parameter	Value
Gateway interface number	1
Gateway IP address	172.17.143.1

Configuring the Traffic Descriptors

➤ To configure the traffic descriptors:

1. On the Traffic Descriptor menu (Configuration › Applications › ATM › Traffic descriptor), set the following VPoPSN parameters:

Parameter Value	
Traffic descriptor number	2
Service category	CBR
Shaping mode	Shaped
PCR	3000
CDVT (μsec)	1

2. After saving the TD parameters above, set another TD with the following VCoPSN parameters:

Parameter	Value
Traffic descriptor number	3
Service category	CBR
Shaping mode	Shaped

Parameter	Value
PCR	6000
CDVT (μsec)	1

Configuring the General Multiservice PW over PSN Parameters

➤ To configure the general multiservice over PSN parameters:

- On the General menu (Configuration > Applications > Multiservice over PSN > General > **TDM parameters**), set the following parameters:

Parameter	Value
Miss-order window size	8
Reordering	Enable

Configuring the Remote Peer Parameters

➤ To configure the remote peer parameters:

- On the Peer menu (Configuration > Applications > Multiservice over PSN > **Peer**), set the following parameters for the three peers:

Table 5-1. ACE-3100 Peer Parameters

Parameter Value	
Peer number	1
Peer name	Peer-1
Peer IP address	172.17.143.200

Table 5-2. ACE-3200 Peer Parameters

Parameter Value	
Peer number	2
Peer name	Peer-2
Peer IP address	172.17.143.201

Configuring the Pseudowire Parameters

In this application, ACE-3600 requires four pseudowire links for ATM traffic over PSN, and two pseudowire links for the clock distribution channels towards the three remote peers. In total, six different pseudowire configurations are required.

Each pseudowire configuration consists of:

a. General PW parameters

b. PSN parameters

c. Service parameters (not relevant for the clock distribution PW).

➤ **To configure a PW link:**

1. On the PW menu (Configuration > Applications > Multiservice over PSN > **PW**), set the PW number and name.
2. On the General Parameters submenu (Configuration > Applications > Multiservice over PSN > PW > **General parameters**), set the general PW parameters for the PW.
3. On the PSN Parameters submenu (Configuration > Applications > Multiservice over PSN > PW > **PSN parameters**), set the PSN parameters for the PW.
4. On the Service Parameters submenu (Configuration > Applications > Multiservice over PSN > PW > **Service parameters**), set the service parameters for the PW.

Note *For an ATM PW, **save the parameters before** entering the attachment circuit parameters (Configuration > Applications > Multiservice over PSN > PW > Service parameters > **Attachment circuit**). The attachment circuit parameters can then be saved separately.*

5. Save the PW link parameters.

The following tables detail the required parameters of each PW link:

Table 5-3. Clock Distribution PW Towards ACE-3100

PW Submenu	Parameter	Value
–	PW number	1
–	PW name	PW-1
General	PW type	Basic CES PSN
	PW subtype	Clock distribution
	PSN type	UDPoIP
	Peer number	1
	Provisioning mode	Manual
	Out PW label	100
	Control word	Enable
PSN	TOS	0
	VLAN tag	Disable

Table 5-4. Data PW for VP (100)

PW Submenu	Parameter	Value
–	PW number	2
–	PW name	PW-2
General	PW type	ATM VP N to 1

PW Submenu	Parameter	Value
	PSN type	MPLSoIP
	Peer number	1
	Provisioning mode	Manual
	Out PW label	101
	In PW label	101
	Control word	Enable
	Sequence number	Enable
	TX queue	4- Low
	OAM mode	Enable
PSN	TOS	0
	EXP bits	0
	VLAN tag	Disable
Service	Max cells concatenation	5
	Timeout mode	Enable
	PW timeout (µsec)	100
	AAL5 mode	Disable
Attachment circuit	Port type	ATM-155
	Port number	1
	VPI	100
	VPI to PSN	100
	VPI from PSN	100
	TD	2
	OD	3

Table 5-5. Data PW for VC (0/100)

PW Submenu	Parameter	Value
–	PW number	3
–	PW name	PW-3
General	PW type	ATM VC N to 1
	PSN type	MPLSoIP
	Peer number	1
	Provisioning mode	Manual

PW Submenu	Parameter	Value
	Out PW label	102
	In PW label	102
	Control word	Enable
	Sequence number	Enable
	TX queue	4- Low
	OAM mode	Enable
PSN	TOS	0
	EXP bits	0
	VLAN tag	Disable
Service	Max cells concatenation	5
	Timeout mode	Enable
	PW timeout (μsec)	100
	AAL5 mode	Disable
Attachment circuit	Port type	ATM-155
	Port number	1
	VPI	0
	VCI	100
	VPI to PSN	0
	VCI to PSN	100
	VPI from PSN	0
	VCI from PSN	100
	TD	3
	OD	3

Table 5-6. Clock Distribution PW Towards ACE-3200

PW Submenu	Parameter	Value
–	PW number	4
–	PW name	PW-4
General	PW type	Basic CES PSN
	PW subtype	Clock distribution
	PSN type	UDPoIP
	Peer number	2

PW Submenu	Parameter	Value
	Provisioning mode	Manual
	Out PW label	100
	Control word	Enable
PSN	TOS	0
	VLAN tag	Disable

Table 5-7. Data PW for VP (200)

PW Submenu	Parameter	Value
–	PW number	5
–	PW name	PW-5
General	PW type	ATM VP N to 1
	PSN type	MPLSoIP
	Peer number	2
	Provisioning mode	Manual
	Out PW label	201
	In PW label	201
	Control word	Enable
	Sequence number	Enable
	TX queue	4- Low
	OAM mode	Enable
PSN	TOS	0
	EXP bits	0
	VLAN tag	Disable
Service	Max cells concatenation	5
	Timeout mode	Enable
	PW timeout (µsec)	100
	AAL5 mode	Disable
Attachment circuit	Port type	ATM-155
	Port number	1
	VPI	200
	VPI to PSN	200
	VPI from PSN	200

PW Submenu	Parameter	Value
	TD	2
	OD	3

Table 5-8. Data PW for VC (0/200)

PW Submenu	Parameter	Value
–	PW number	6
–	PW name	PW-6
General	PW type	ATM VC N to 1
	PSN type	MPLSoIP
	Peer number	2
	Provisioning mode	Manual
	Out PW label	202
	In PW label	202
	Control word	Enable
	Sequence number	Enable
	TX queue	4- Low
	OAM mode	Enable
PSN	TOS	0
	EXP bits	0
	VLAN tag	Disable
Service	Max cells concatenation	5
	Timeout mode	Enable
	Timeout (µsec)	100
	AAL5 mode	Disable
Attachment circuit	Port type	ATM-155
	Port number	1
	VPI	0
	VCI	200
	VPI to PSN	0
	VCI to PSN	200
	VPI from PSN	0
	VCI from PSN	200

PW Submenu	Parameter	Value
	TD	3
	OD	3

Setting the Clock Source

➤ **To set the clock source for ACE-3600:**

1. On the Master Clock menu (Configuration > System > Clock > **Master clock**), set the following parameters:

Parameter	Value
Source	RX clock
Port type	ATM-155
Port number	1

2. On the Fallback Clock menu (Configuration > System > Clock > **Fallback clock**), set the following parameters:

Parameter	Value
Source	RX clock
Port type	ATM-155
Port number	5

Defining the Manager IP Address

➤ **To define the manager IP address:**

- On the Manager List menu (Configuration > System > Management > **Manager List**), set the following parameters:

Parameter	Value
IP address	172.17.143.50
Trap mask	Manual

5.2 Configuring the Remote ACE-3100 Unit

This section describes the configuration of the ACE-3100 unit that appears in *Figure 5-1*. The configuration stages are:

- *Configuring the Physical Layer Parameters* – which includes:
  - *Configuring the ATM-155 Ports*
  - *Configuring the Ethernet Ports*
- *Configuring the Application Parameters* – which includes:
  - *Configuring the Router Parameters*
  - *Configuring the Traffic Descriptors*
  - *Configuring the General Multiservice PW over PSN Parameters*
  - *Configuring the Remote Peer Parameters*
  - *Configuring the Pseudowire Parameters*
- *Setting the ACE-3100 Clock Source*
- *Defining the Manager IP Address*.

Configuring the Physical Layer Parameters

Configuring the ATM-155 Ports

➤ To configure the ATM-155 port(s):

- On the ATM-155 menu (Configuration > Physical layer > Port > ATM-155), set the following parameters:

Parameter Value	
Port number	1
Port activation	Enable
Transmit clock source	System
Frame type	SDH
Output rate (cps)	12000
OAM cell generation	Disable

Note *For APS functionality (if required), configure the same parameters for Port 2.*

Configuring the Ethernet Ports

➤ To configure the Ethernet parameters:

- On the Ethernet menu (Configuration › Physical layer › Port › **Ethernet**), set the following parameters for each Ethernet port:

Parameter	Value
Port number	1
Port activation	Enable
Auto negotiation	Enable
Max. capability advertised	100BaseT Full Duplex
Rate limiter	Disable

Configuring the Application Parameters

The ACE-3100 application configuration includes:

- Router parameters
- Traffic descriptor parameters
- General multiservice over PSN parameters
- Remote peer parameters
- Pseudowire parameters (clock recovery, ATM VP and ATM VC over PSN).

Configuring the Router Parameters

➤ To configure the router parameters:

1. On the router Interface menu (Configuration › Applications › Router › Interface), set the following parameters:

Parameter Value	
Number	1
Name	Interface-1
IP address	172.17.143.200
IP mask	255.255.255.0
Interface type	Ethernet
Port number	1
VLAN tagging	Disable

2. On the Default Gateway menu (Configuration › Applications › Router › **Default gateway**), set the following parameters:

Parameter	Value
Gateway interface number	1

Parameter	Value
Gateway IP address	172.17.143.1

Configuring the Traffic Descriptors

➤ To configure the traffic descriptors:

1. On the Traffic Descriptor menu (Configuration > Applications > ATM > **Traffic descriptor**), set the following VPoPSN parameters:

Parameter	Value
Traffic descriptor number	2
Service category	CBR
Shaping mode	Shaped
PCR	3000
CDVT (μsec)	1

2. After saving the TD parameters above, set another TD with the following VCoPSN parameters:

Parameter	Value
Traffic descriptor number	3
Service category	CBR
Shaping mode	Shaped
PCR	6000
CDVT (μsec)	1

Configuring the General Multiservice PW over PSN Parameters

➤ To configure the general multiservice over PSN parameters:

- On the General menu (Configuration > Applications > Multiservice over PSN > General > ATM parameters), set the following parameters:

Parameter Value	
Miss-order window size	8
Reordering	Enable

Configuring the Remote Peer Parameters

➤ To configure the peer parameters for the remote ACE-3600:

- On the Peer menu (Configuration > Applications > Multiservice over PSN > **Peer**), set the following parameters:

Parameter	Value

Peer number	1
Peer name	Peer-1
Peer IP address	172.17.143.100

Configuring the Pseudowire Parameters

In this application, ACE-3100 requires two pseudowire links for ATM VC/VP over PSN, and one pseudowire link for the clock recovery channel. In total, three different pseudowire configurations are required.

Each pseudowire configuration consists of:

a. General PW parameters

b. PSN parameters

c. Service parameters (not relevant for the clock recovery PW).

➤ **To configure a PW link:**

1. On the PW menu (Configuration › Applications › Multiservice over PSN › **PW**), set the PW number and name.
2. On the General Parameters submenu (Configuration › Applications › Multiservice over PSN › PW › **General parameters**), set the general PW parameters for the PW.
3. On the PSN Parameters submenu (Configuration › Applications › Multiservice over PSN › PW › **PSN parameters**), set the PSN parameters for the PW.
4. On the Service Parameters submenu (Configuration › Applications › Multiservice over PSN › PW › **Service parameters**), set the service parameters for the PW.

Note *For an ATM PW,* ***save the parameters before*** *entering the attachment circuit parameters (Configuration › Applications › Multiservice over PSN › PW › Service parameters ›* ***Attachment circuit****). The attachment circuit parameters can then be saved separately.*

5. Save the PW link parameters.

The following tables detail the required parameters of each PW link:

Table 5-9. ACE-3100 – Clock Recovery PW

PW Submenu	Parameter	Value
–	PW number	1
–	PW name	PW-1
General	PW type	Basic CES PSN
	PW subtype	Clock recovery
	PSN type	UDPoIP

PW Submenu	Parameter	Value
	Peer number	1
	Provisioning mode	Manual
	In PW label	100
	Control word	Enable
PSN	TOS	0
	VLAN tag	Disable

Table 5-10. ACE-3100 – Data PW for VP (100)

PW Submenu	Parameter	Value
–	PW number	2
–	PW name	PW-2
General	PW type	ATM VP N to 1
	PSN type	MPLSoIP
	Peer number	1
	Provisioning mode	Manual
	Out PW label	101
	In PW label	101
	Control word	Enable
	Sequence number	Enable
	TX queue	4- Low
	OAM mode	Enable
PSN	TOS	0
	EXP bits	0
	VLAN tag	Disable
Service	Max cells concatenation	5
	Timeout mode	Enable
	PW timeout (μsec)	100
	AAL5 mode	Disable
Attachment circuit	Port type	ATM-155
	Port number	1
	VPI	100
	VPI to PSN	100

PW Submenu	Parameter	Value
	VPI from PSN	100
	TD	2
	OD	3

Table 5-11. ACE-3100 – Data PW for VP (0/100)

PW Submenu	Parameter	Value
–	PW number	3
–	PW name	PW-3
General	PW type	ATM VC N to 1
	PSN type	MPLSoIP
	Peer number	1
	Provisioning mode	Manual
	Out PW label	102
	In PW label	102
	Control word	Enable
	Sequence number	Enable
	TX queue	4- Low
	OAM mode	Enable
PSN	TOS	0
	EXP bits	0
	VLAN tag	Disable
Service	Max cells concatenation	5
	Timeout mode	Enable
	PW timeout (µsec) 100	
	AAL5 mode	Disable
Attachment circuit	Port type	ATM-155
	Port number	1
	VPI	0
	VCI	100
	VPI to PSN	0
	VCI to PSN	100
	VPI from PSN	0

PW Submenu	Parameter	Value
	VCI from PSN	100
	TD	3
	OD	3

Setting the ACE-3100 Clock Source

➤ **To configure the clock source for ACE-3100:**

1. On the Recovered Clock menu (Configuration > System > Clock > Recovered clock), set the following parameters:

Parameter	Value
ID	1
Activity	Enable
Type	Adaptive
PW number	1
Source quality	Stratum 1
Network type	Type B

2. On the Master Clock menu (Configuration > System > Clock > Recovered clock), set the following parameters:

Parameter	Value
Source	Recovered
Recovered ID	1

Defining the Manager IP Address

➤ **To define the manager IP address:**

- On the Manager List menu (Configuration > System > Management > Manager List), set the following parameters:

Parameter	Value
IP address	172.17.143.50
Trap mask	Manual

5.3 Configuring the Remote ACE-3200 Unit

This section describes the configuration of the ACE-3200 unit that appears in *Figure 5-1*. The configuration stages are:

- *Configuring the Physical Layer Parameters* – which includes:
  - *Configuring the E1 Ports to IMA Mode*
  - *Configuring the Ethernet Ports*
- *Configuring the Application Parameters* – which includes:
  - *Defining an IMA Group*
  - *Configuring the Router Parameters*
  - *Configuring the Traffic Descriptors*
  - *Configuring the General Multiservice PW over PSN Parameters*
  - *Configuring the Remote Peer Parameters*
  - *Configuring the Pseudowire Parameters*
- *Setting the ACE-3200 Clock Source*.
- *Defining the Manager IP Address*.

Configuring the Physical Layer Parameters

Configuring the E1 Ports to IMA Mode

➤ To configure an E1 port:

- From the E1 menu (Configuration > Physical layer > Port > E1), set the following parameters:

Parameter Value	
Port number	1
Port activation	Enable
Transmit clock source	System
RX sensitivity	Low
Line type	CRC enabled
Idle code	7E
Mode	E1-IMA

Note *The same parameters should be defined for all E1 ports in the required IMA group (ports 1–8).*

Configuring the Ethernet Ports

➤ To configure the Ethernet parameters:

- On the Ethernet menu (Configuration > Physical layer > Port > Ethernet), set the following parameters for each Ethernet port:

Parameter Value	
Port number	1
Port activation	Enable
Auto negotiation	Enable
Max. capability advertised	100BaseT Full Duplex
Rate limiter	Disable

Configuring the Application Parameters

The ACE-3200 application configuration includes:

- IMA group parameters
- Router parameters
- Traffic descriptor parameters
- General multiservice over PSN parameters
- Remote peer parameters
- Pseudowire parameters (clock recovery, ATM VP and ATM VC over PSN).

Defining an IMA Group

➤ To define an IMA group:

- On the IMA menu (Configuration > Applications > ATM > IMA), set the following parameters:

Parameter Value	
Group number	1
Min RX/TX links	1
Group ID	0
TX frame length (cells)	128
Max differential delay (ms)	25
Blocking	Unblock
IMA version	1.1
Common TX clock source	System
Links in group	1–8

Configuring the Router Parameters

➤ To configure the router parameters:

1. On the router Interface menu (Configuration > Applications > Router > Interface), set the following parameters:

Parameter	Value
Number	1
Name	Interface-1
IP address	172.17.143.201
IP mask	255.255.255.0
Interface type	Ethernet
Port number	1
VLAN tagging	Disable

2. On the Default Gateway menu (Configuration > Applications > Router > Default gateway), set the following parameters:

Parameter	Value
Gateway interface number	1
Gateway IP address	172.17.143.1

Configuring the Traffic Descriptors

➤ To configure the traffic descriptors:

1. On the Traffic Descriptor menu (Configuration > Applications > ATM > Traffic descriptor), set the following VPoPSN parameters:

Parameter Value	
Traffic descriptor number	2
Service category	CBR
Shaping mode	Shaped
PCR	3000
CDVT	1

2. After saving the TD parameters above, set another TD with the following VCoPSN parameters:

Parameter	Value
Traffic descriptor number	3
Service category	CBR
Shaping mode	Shaped

Parameter	Value
PCR	6000
CDVT	1

Configuring the General Multiservice PW over PSN Parameters

➤ To configure the general multiservice over PSN parameters:

- On the General menu (Configuration > Applications > Multiservice over PSN > General > **ATM parameters**), set the following parameters:

Parameter	Value
Miss-order window size	8
Reordering	Enable

Configuring the Remote Peer Parameters

➤ To configure the peer parameters for the remote ACE-3600:

- On the Peer menu (Configuration > Applications > Multiservice over PSN > **Peer**), set the following parameters:

Parameter	Value
Peer number	1
Peer name	Peer-1
Peer IP address	172.17.143.100

Configuring the Pseudowire Parameters

In this application, ACE-3200 (1) requires two pseudowire links for ATM VC, ATM VP, and one pseudowire link for the clock recovery channel. In total, three different pseudowire configurations are required.

Each pseudowire configuration consists of:

a. General PW parameters

b. PSN parameters

c. Service parameters (not relevant for the clock recovery PW).

Refer to the PW link creation steps on page *5-16*.

The following tables detail the required parameters of each PW link:

Table 5-12. ACE-3200 (1) – Clock Recovery PW

PW Submenu	Parameter	Value
— PW	number	1

PW Submenu	Parameter	Value
–	PW name	PW-1
General	PW type	Basic CES PSN
	PW subtype	Clock recovery
	PSN type	UDPoIP
	Peer number	1
	Provisioning mode	Manual
	In PW label	100
	Control word	Enable
PSN	TOS	0
	VLAN tag	Disable

Table 5-13. ACE-3200 (1) – Data PW for VP (200)

PW Submenu	Parameter	Value
–	PW number	2
–	PW name	PW-2
General	PW type	ATM VP N to 1
	PSN type	MPLSoIP
	Peer number	1
	Provisioning mode	Manual
	Out PW label	201
	In PW label	201
	Control word	Enable
	Sequence number	Enable
	TX queue	4- Low
	OAM mode	Enable
PSN	TOS	0
	EXP bits	0
	VLAN tag	Disable
Service	Max cells concatenation	5
	Timeout mode	Enable
	PW timeout (μsec)	100
	AAL5 mode	Disable

PW Submenu	Parameter	Value
Attachment circuit	Port type	IMA-Group
	Port number	1
	VPI	200
	VPI to PSN	200
	VPI from PSN	200
	TD	2
	OD	3

Table 5-14. ACE-3200 (1) – Data PW for VC (0/200)

PW Submenu	Parameter	Value
–	PW number	3
–	PW name	PW-3
General	PW type	ATM VC N to 1
	PSN type	MPLSoIP
	Peer number	1
	Provisioning mode	Manual
	Out PW label	202
	In PW label	202
	Control word	Enable
	Sequence number	Enable
	TX queue	4- Low
	OAM mode	Enable
PSN	TOS	0
	EXP bits	0
	VLAN tag	Disable
Service	Max cells concatenation	5
	Timeout mode	Enable
	Timeout (µsec)	100
	AAL5 mode	Disable
Attachment circuit	Port type	IMA-Group
	Port number	1
	VPI	0

PW Submenu	Parameter	Value
	VCI	200
	VPI to PSN	0
	VCI to PSN	200
	VPI from PSN	0
	VCI from PSN	200
	TD	3
	OD	3

Setting the ACE-3200 Clock Source

➤ **To configure the clock source for ACE-3200 (1):**

1. On the Recovered Clock menu (Configuration > System > Clock > Recovered clock), set the following parameters:

Parameter Value	
ID	1
Activity	Enable
Type	Adaptive
PW number	1
Source quality	Stratum 1
Network type	Type B

2. On the Master Clock menu (Configuration > System > Clock > **Recovered clock**), set the following parameters:

Parameter Value	
Source	Recovered
Recovered ID	1

Defining the Manager IP Address

➤ **To define the manager IP address:**

- On the Manager List menu (Configuration > System > Management > **Manager List**), set the following parameters:

Parameter	Value
IP address	172.17.143.50
Trap mask	Manual

Chapter 6

Monitoring and Diagnostics

This chapter covers the following topics:

- *Monitoring Performance* – Monitoring the ACE-3600 unit's performance statistics during operation; see *Section 6.1*.
- *Detecting Errors* – Error detection options and the complete list of possible log events; see *Section 6.2*.
- *Handling Alarms* – Interpreting alarm traps; see *Section 6.3*.
- *Testing the Unit* – Displaying self-test results and performing connectivity, physical loopback and ATM cell tests using the diagnostics options; see *Section 6.4*.
- *Troubleshooting* – Troubleshooting chart; see *Section 6.5.*
- *Recovering ACE Units* – Instructions on recovering the unit; see *Section 6.6*
- *Frequently Asked Questions* – see *Section 6.7*.

6.1 Monitoring Performance

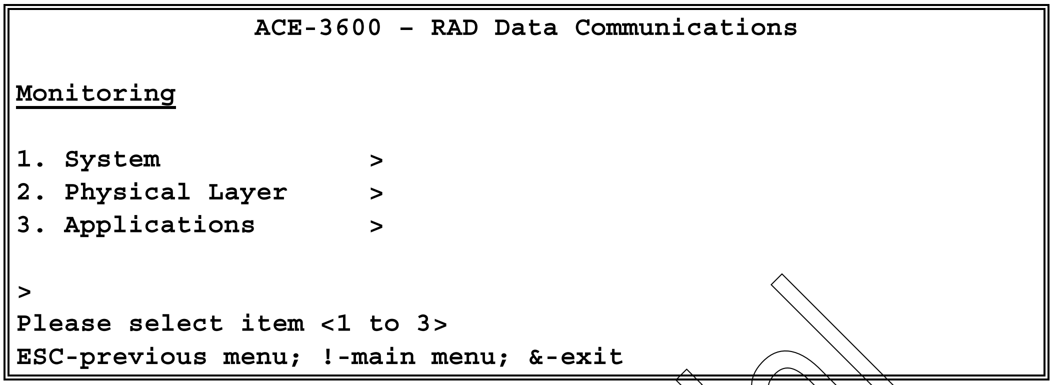
The performance of ACE-3600 can be monitored during operation to verify that the unit is delivering service as expected. The monitoring options consist of the following categories:

- *Monitoring the System*
- *Monitoring the Physical Layer*
- *Monitoring the Application Performance*

➤ To access the unit's monitoring options:

- From the Main menu, select Monitoring.

  The Monitoring menu appears.



```
                   ACE-3600 - RAD Data Communications

Monitoring

1. System              >
2. Physical Layer      >
3. Applications        >

>
Please select item <1 to 3>
ESC-previous menu; !-main menu; &-exit
```

Figure 6-1. Monitoring Menu

Monitoring the System

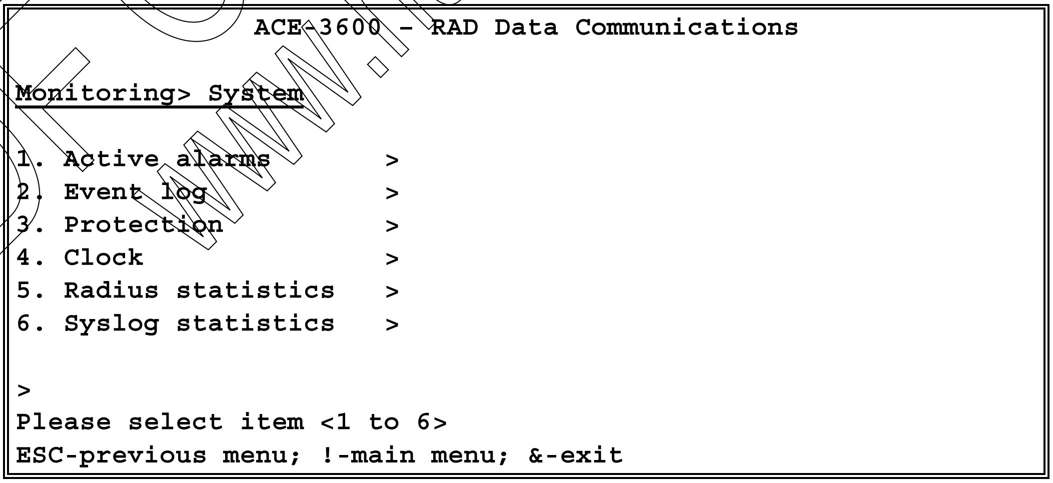
The system monitoring options include the following activities:

- *Viewing the Active Alarms*
- *Viewing the Event Log*
- *Viewing the Protection Status*
- *Monitoring the Clock*
- *Viewing the RADIUS Statistics*
- *Viewing the Syslog Statistics*

➤ To access the System menu:

- From the Monitoring menu (see *Figure 6-1*), select System.

The System menu is displayed.



```
                   ACE-3600 - RAD Data Communications

Monitoring> System

1. Active alarms        >
2. Event log            >
3. Protection           >
4. Clock                >
5. Radius statistics    >
6. Syslog statistics    >

>
Please select item <1 to 6>
ESC-previous menu; !-main menu; &-exit
```

Figure 6-2. System Menu

Table 6-1. System Monitoring Options

Parameter Description		Possible Values
Active alarms	View the currently active alarms	Refer to *Figure 6-3*
Event log	View the event log	Refer to *Figure 6-4*
Protection	View the current protection information	Refer to *Figure 6-6*
Clock	Access the clock monitoring options	Refer to *Figure 6-12*
Radius statistics	View the current Radius statistics	Refer to *Figure 6-14*
Syslog statistics	View the current Syslog statistics	Refer to *Figure 6-15*

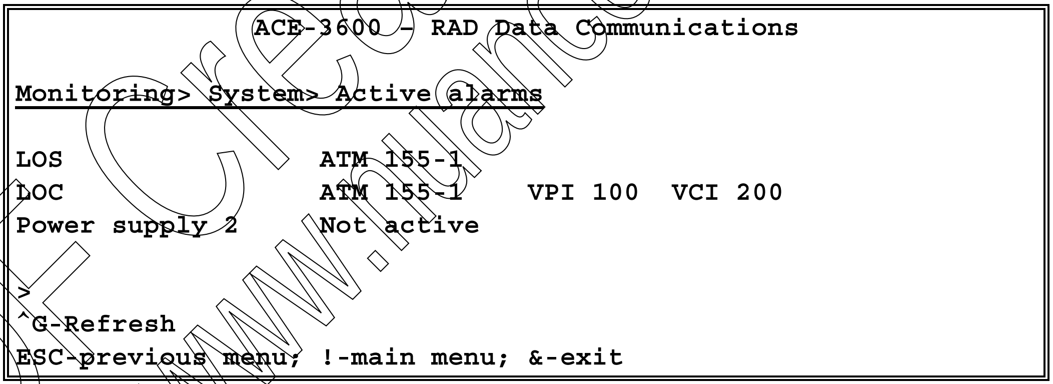
Viewing the Active Alarms

The Active Alarms information indicates any current alarm that requires your attention.

➤ To view the active alarms:

- From the System menu (see *Figure 6-2*), select Active Alarms.

The currently active alarms are displayed in a list.



```
               ACE-3600 - RAD Data Communications

Monitoring> System> Active alarms

LOS                ATM 155-1
LOC                ATM 155-1    VPI 100  VCI 200
Power supply 2     Not active


>
^G-Refresh
ESC-previous menu; !-main menu; &-exit
```

Figure 6-3. Active Alarms are displayed

Table 6-2. Active Alarms Menu Parameters

Parameter Description		Possible Values
Alarm type/name	The active alarm type/name is listed on the left column of the screen.	System alarms, physical layer alarms, ATM layer alarms (LOS, LOC, PS, etc.)

Parameter	Description	Possible Values
Alarm parameters	The alarm parameters appear in the corresponding row	• Port type, port number for physical layer alarms. • Port type, port number, IMA group number, VPI and VCI for ATM layer alarms. • Power supply / fan status

Note *For more information about alarm traps, see Handling Alarms.*

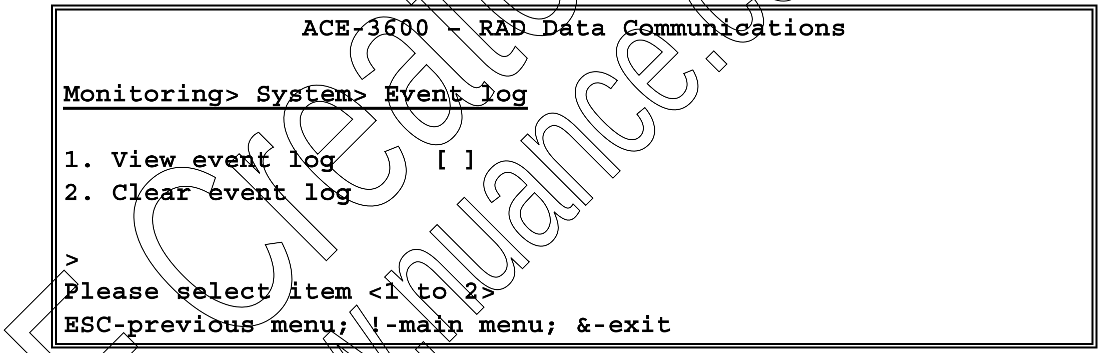
Viewing the Event Log

The event log displays information regarding all events that occurred up to this point.

➤ To view the event log:

1. From the System menu (see *Figure 6-2*), select Event Log.

   The Event Log menu is displayed.

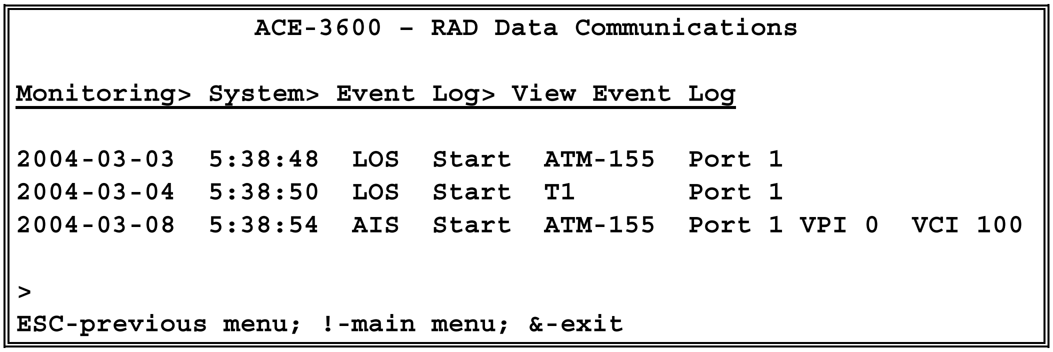


```
                 ACE-3600 - RAD Data Communications

Monitoring> System> Event log

1. View event log       [ ]
2. Clear event log

>
Please select item <1 to 2>
ESC-previous menu; !-main menu; &-exit
```

Figure 6-4. Event Log Menu

2. From the Event Log menu, select View Event Log.

   The View Event Log screen appears and displays information regarding all recorded events.



```
                 ACE-3600 - RAD Data Communications

Monitoring> System> Event Log> View Event Log

2004-03-03  5:38:48  LOS  Start  ATM-155  Port 1
2004-03-04  5:38:50  LOS  Start  T1       Port 1
2004-03-08  5:38:54  AIS  Start  ATM-155  Port 1 VPI 0  VCI 100

>
ESC-previous menu; !-main menu; &-exit
```

Figure 6-5. View Event Log

Table 6-3. View Event Log Parameters

Parameter Description		Possible Values
Date	Date of the event, in the format of: [YYYY-MM-DD]	[2000-01-01] to [2099-12-31]
Time	Time of the event, in the format of: [HH-MM-SS]	[00-00-00] to [23-59-59]
Event	Name of the event	String describing type of event
Event state	State of the event	Start End
Event specific parameters	Specific parameter for each event	A list of strings describing event parameters

Note *For the complete list of possible events, see the List of Log Events.*

➤ To clear all records in the event log:

- From the Event Log menu (see *Figure 6-4*), select Clear Event Log.

Viewing the Protection Status

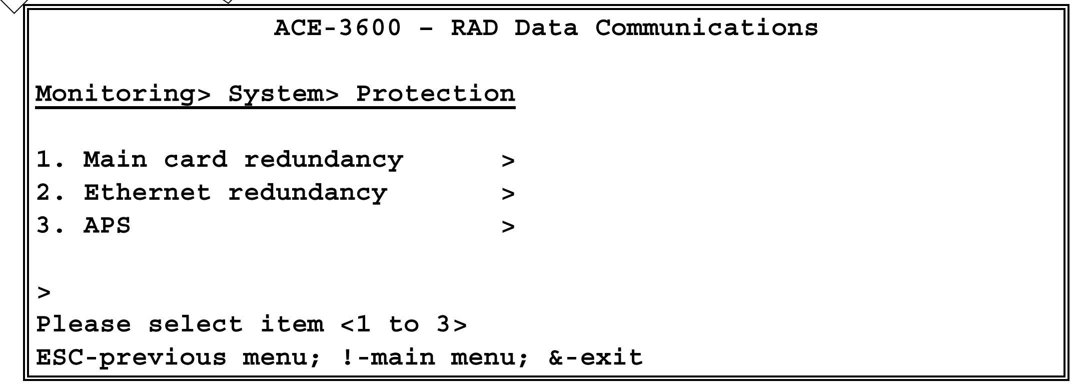
The protection monitoring options allow you to view the current status of all protected hardware components, depending on your specific hardware unit. This includes:

- *Viewing the Main Module Protection Status*
- *Viewing the Ethernet Redundancy*
- *Viewing the APS Status*

➤ To access the protection monitoring options:

- From the System menu (see *Figure 6-2*), select Protection.

  The Protection menu is displayed.



```
                    ACE-3600 - RAD Data Communications

Monitoring> System> Protection

1. Main card redundancy       >
2. Ethernet redundancy        >
3. APS                        >

>
Please select item <1 to 3>
ESC-previous menu; !-main menu; &-exit
```

Figure 6-6. Protection Menu

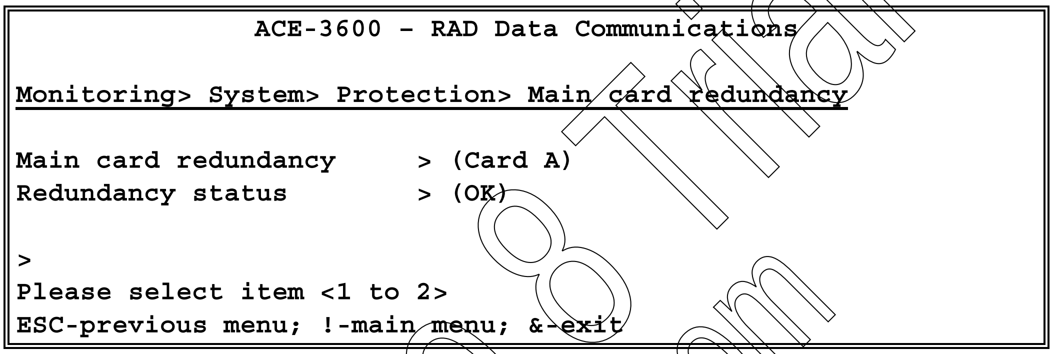
Viewing the Main Module Protection Status

If two main modules (main cards) are installed in ACE-3600 and the main module protection feature is enabled, you can check whether the redundancy protection is functioning properly, and check which of the main modules is currently the active one.

➤ To view the main module redundancy information:

- From the Protection menu, select **Main Card Redundancy**.

  The Main Card Redundancy menu is displayed.



```
                ACE-3600 - RAD Data Communications

Monitoring> System> Protection> Main card redundancy

Main card redundancy     > (Card A)
Redundancy status        > (OK)

>
Please select item <1 to 2>
ESC-previous menu; !-main menu; &-exit
```

Figure 6-7. Main Card Redundancy Menu

Table 6-4. Main Card Redundancy Monitoring Parameters

Parameter Description		Possible Values
Active main card	Displays which is the currently active main module. Card A is the main module located **above** Card B. For more information about the active module principle, refer to *Chapter 1*.	Card A Card B **Default: Card A**
Redundancy status	Displays the current redundancy status. There are four status types: • OK – redundancy is up and running fine • Card A/B absent – the specified module is physically missing. • Communication loss – the two main modules are not communicating. • Mismatch – the two modules differ in their hardware, software or configuration.	OK Card A absent Card B absent Communication loss Hardware mismatch Software mismatch Configuration mismatch Default: OK

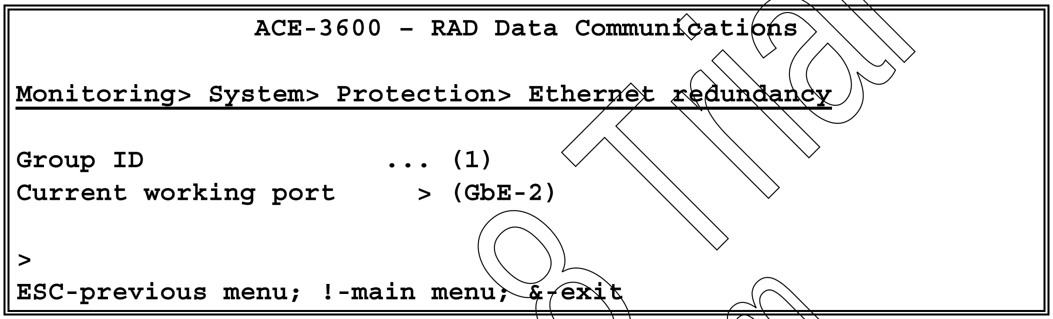
Viewing the Ethernet Redundancy Details

If the Gigabit Ethernet ports of ACE-3600 are set to work in redundancy mode, you can check their group ID and which of them is the currently working port.

➤ To view the Ethernet port redundancy details:

- From the Protection menu, select **Ethernet Redundancy**.

  The Ethernet Redundancy menu is displayed.



```
                 ACE-3600 - RAD Data Communications

Monitoring> System> Protection> Ethernet redundancy

Group ID                ... (1)
Current working port      > (GbE-2)

>
ESC-previous menu; !-main menu; &-exit
```

Figure 6-8. Ethernet Redundancy Menu

Table 6-5. Ethernet Redundancy Details

Parameter Description		Possible Values
Group ID	Read-only ID of the redundancy group to which the Gigabit Ethernet ports belong, as was previously defined (for more information, see *Setting the Ethernet Redundancy* in Chapter 4). If no group exists, the field is displayed blank.	As previously defined or blank.
Current working port	The currently active GbE port. In 1+1 protection mode it can be only the transmitting port, and in 1:1 protection mode it can be either the transmitting or the receiving port.	GbE-1 GbE-2

Viewing the APS Status

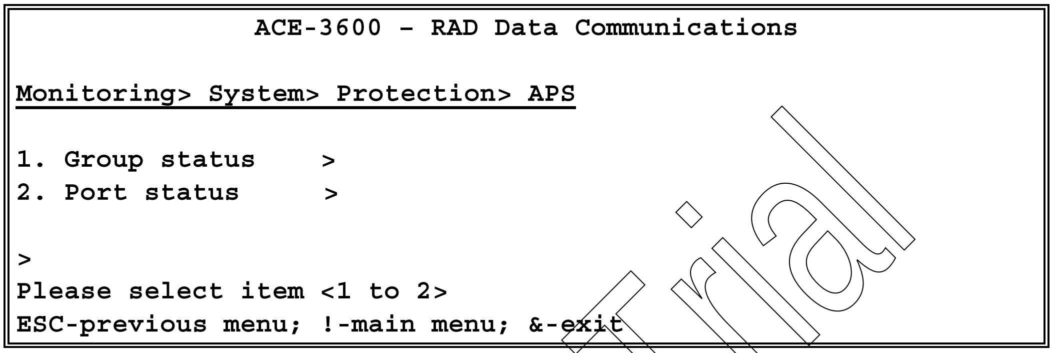
If enabled, the APS mode applied on ATM-155 ports can be monitored at the group level or the port level:

- **Group status** – current information regarding the performance of all ports that belong to the APS group, in terms of group ID, current working port and Tx/Rx bytes transmitted/received through the APS ports.
- **Port Status** – current information regarding the performance of a specific port, in terms of the port's signal failures or signal quality degrading.

➤ To access the APS monitoring options:

- From the Protection menu (see *Figure 6-6*), select APS.

The APS menu is displayed.



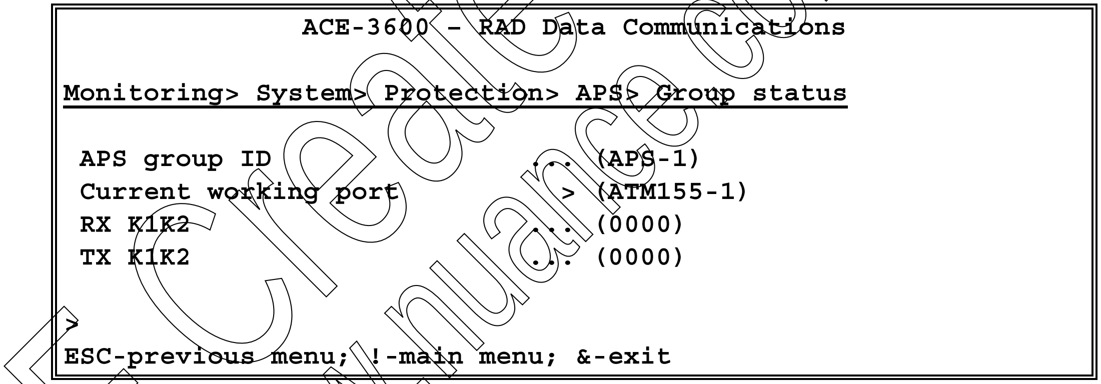
```
                    ACE-3600 - RAD Data Communications

Monitoring> System> Protection> APS

1. Group status    >
2. Port status     >

>
Please select item <1 to 2>
ESC-previous menu; !-main menu; &-exit
```

Figure 6-9. APS Monitoring Menu

➤ To view the APS group status:

- From the APS menu, select Group Status.

The APS group status is displayed.



```
                    ACE-3600 - RAD Data Communications

Monitoring> System> Protection> APS> Group status

 APS group ID                  ... (APS-1)
 Current working port            > (ATM155-1)
 RX K1K2                       ... (0000)
 TX K1K2                       ... (0000)

>
ESC-previous menu; !-main menu; &-exit
```

Figure 6-10. APS Group Status

Table 6-6. APS Group Status Parameters

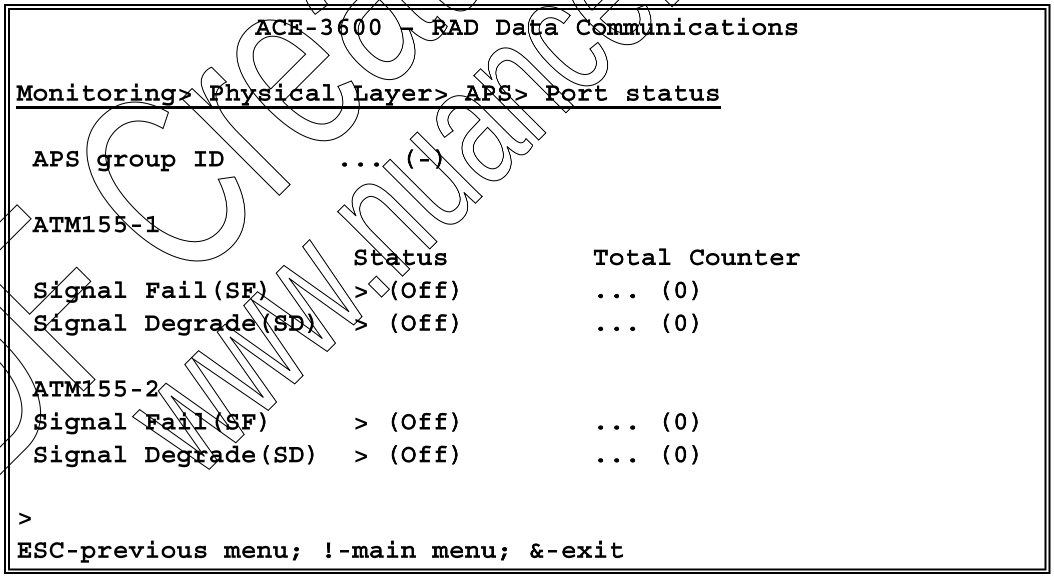
Parameter	Description	Possible Values
APS group ID	Read-only identification of the configured APS group (if any). If no APS group was defined, an empty string is displayed.	The ID that was previously defined for the APS group (for more information, see *Configuring the Protection Parameters* in Chapter 4).

Parameter	Description	Possible Values
Current working port	The port from which the traffic is received.	ATM155-1 ATM155-2 ATM155-3 ATM155-4 ATM155-5 ATM155-6 ATM155-7 ATM155-8
RX K1K2	The content of the received K1K2 bytes, which are exchanged through the APS ports.	The bytes content (read-only)
TX K1K2	The content of the transmitted K1K2 bytes, which are exchanged through the APS ports.	The bytes content (read-only)

➤ To view the APS port status:

- From the APS menu, select Port Status.

  The APS port status list is displayed.



```
               ACE-3600 - RAD Data Communications

Monitoring> Physical Layer> APS> Port status

 APS group ID       ...  (-)

 ATM155-1
                     Status          Total Counter
 Signal Fail(SF)     > (Off)         ... (0)
 Signal Degrade(SD)  > (Off)         ... (0)

 ATM155-2
 Signal Fail(SF)     > (Off)         ... (0)
 Signal Degrade(SD)  > (Off)         ... (0)

>
ESC-previous menu; !-main menu; &-exit
```

Figure 6-11. APS Port Status List

Table 6-7. APS Port Status Parameters

Parameter Description		Possible Values
APS group ID	Read-only identification of the configured APS group to which the port belongs. If no APS group was defined, an empty string is displayed.	The ID that was previously defined for the APS group (for more information, see *Setting Automatic Protection Switching* in Chapter 4).
Status (column)	Indicates whether a defect exists for the corresponding parameter (for either SF or SD; see description below). When On, a defect exists.	On Off
Total Counter (column)	Total number of defects that were counted for the corresponding parameter since the APS mode was last activated.	Numerical
SF	Indicates whether a signal failure has occurred. A signal failure (SF) is a severe failure caused by LOS, LOF Line AIS or Line BER that exceeds a specified threshold (10^{-3}). When On, a signal failure has occurred.	On Off
SD	Indicates whether a signal quality degrading has occurred. A signal degrading (SD) is a minor failure condition caused by Line BER (bit error rate) that exceeds a specified threshold (10^{-6}). When On, a quality degrading has occurred.	On Off

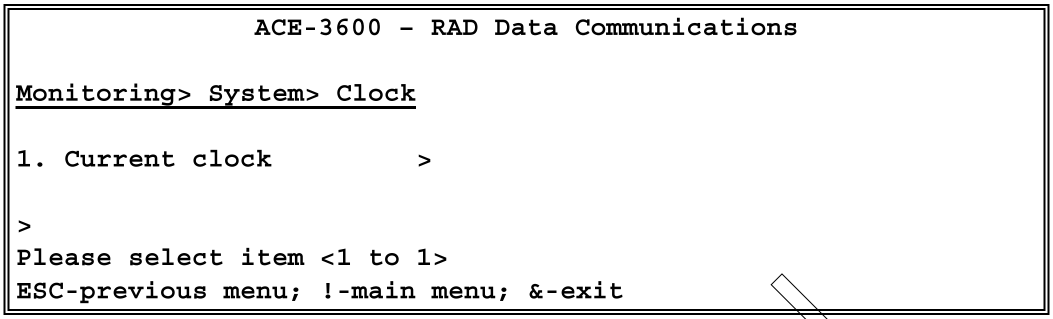
Monitoring the Clock

The availability and performance of the unit's current clock source can be monitored when necessary.

➤ To access the clock monitoring options:

- From the System monitoring menu (see *Figure 6-2*), select Clock.

  The Clock menu is displayed.



```
                ACE-3600 - RAD Data Communications

Monitoring> System> Clock

1. Current clock          >

>
Please select item <1 to 1>
ESC-previous menu; !-main menu; &-exit
```

Figure 6-12. Clock Monitoring Menu

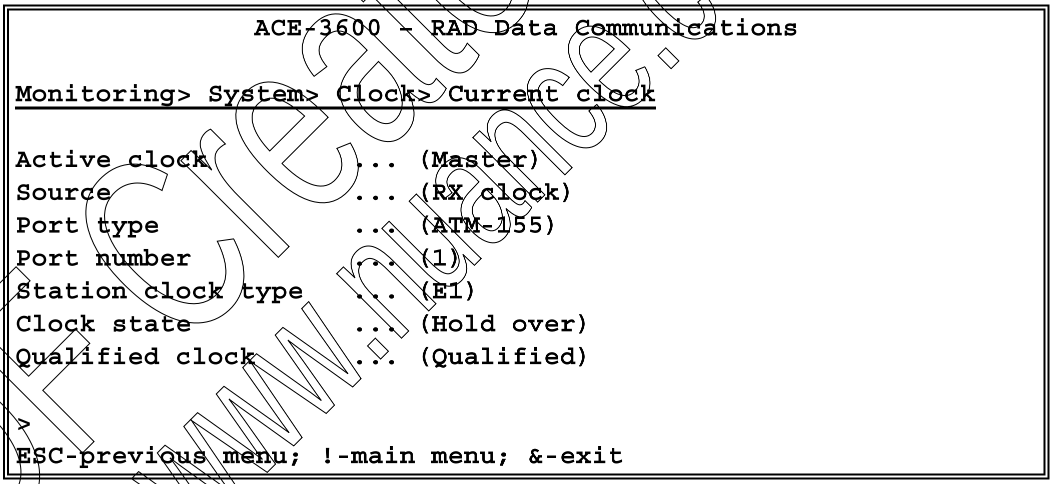
Viewing the Current Clock Source Details

You can display the details of the clock source (master or fallback) from which ACE-3600 currently recovers its timing reference. The master and fallback clock sources must be pre-configured prior to monitoring them (for more information, see *Setting the Clock Source* in Chapter 4).

➤ To view the details of the current clock source:

- From the Clock monitoring menu, select Current Clock.

  The details of the current clock source are displayed (read-only).



```
                ACE-3600 - RAD Data Communications

Monitoring> System> Clock> Current clock

Active clock          ...  (Master)
Source                ...  (RX clock)
Port type             ...  (ATM-155)
Port number           ...  (1)
Station clock type    ...  (E1)
Clock state           ...  (Hold over)
Qualified clock       ...  (Qualified)


>
ESC-previous menu; !-main menu; &-exit
```

Figure 6-13. Current Clock Source Details

Table 6-8. Current Clock Source Parameters

Parameter Description		Possible Values (Read-only)
Active clock	Displays the currently active clock source: • Master – Timing is derived from the master (primary) clock source. • Fallback – Timing is derived from the fallback (secondary) clock source. • None – No clock source id currently defined/available.	Master Fallback None

Parameter	Description	Possible Values (Read-only)
Source	Displays the type of the clock source: • Internal – the clock is provided by an internal oscillator. • RX clock – the clock is derived from the incoming traffic of one of the unit's ports. • Station – the clock is provided via the station clock port	Internal RX clock Station
Port type	Type of the port that is used by the clock source. Relevant only if the clock source type is RX clock; read-only.	ATM-155
Port number	Number of the port that is used by the clock source. Relevant only if the clock source type is RX clock.	1–8 for ATM-155 1 for Station Clock
Station clock type	Type of the station clock interface (if used)	E1 T1
Clock state	The current state of the clock source: • Free run – the clock is not locked and taked from the internal SEC chip • Fine locked – the clock is locked on the clock source • Rapid locked – the clock is locking on the clock source • Holdover – the clock is in holdover mode due to a source loss event For more information about clock states, refer to *Appendix D*.	Free run Fine locked Rapid locked Holdover
Qualified clock	Indicates whether the clock source qualifies the Stratum requirements: • Qualified – the clock locks fast and its frequancy meets the Stratum standards. • Disqualified – it takes more than 100 seconds to lock on the clock source and the frequency is not in the Stratum acceptable range.	Qualified Disqualified

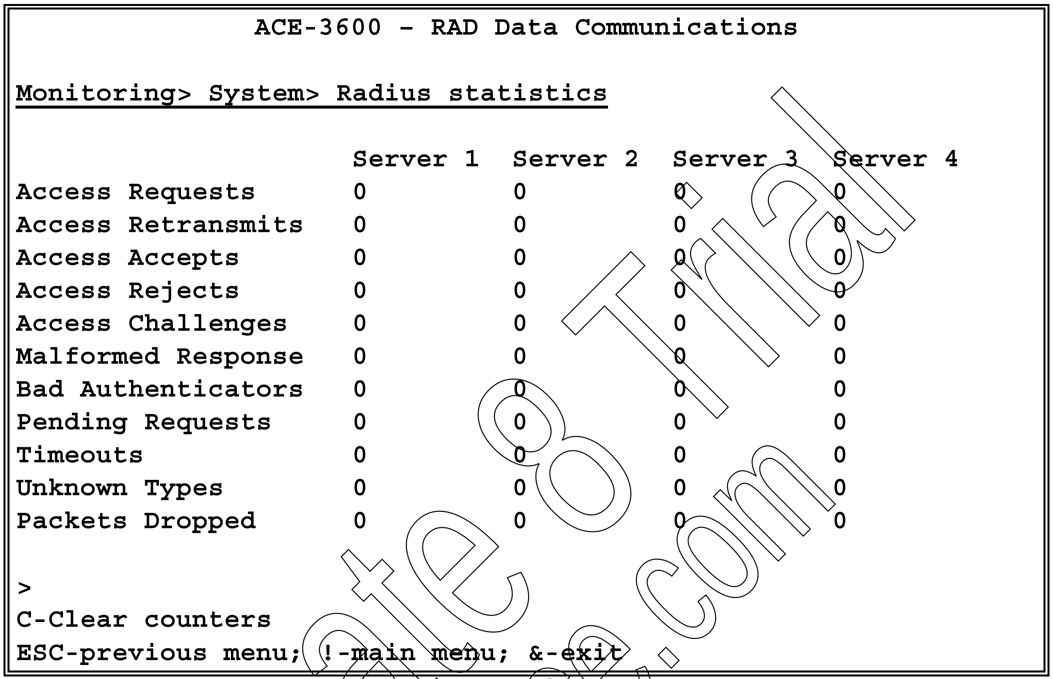
Viewing the RADIUS Statistics

ACE-3600 records the occurrence of all events that relate to communication with the Radius servers, if such were defined for the unit. You can view the statistics of these events per server.

➤ To display the Radius statistics:

- From the System menu, select **Radius Statistics**.

  The Radius statistics are displayed in columns, while each column displays the statistics of a specific server.



```
                    ACE-3600 - RAD Data Communications

Monitoring> System> Radius statistics

                     Server 1  Server 2  Server 3  Server 4
Access Requests      0         0         0         0
Access Retransmits   0         0         0         0
Access Accepts       0         0         0         0
Access Rejects       0         0         0         0
Access Challenges    0         0         0         0
Malformed Response   0         0         0         0
Bad Authenticators   0         0         0         0
Pending Requests     0         0         0         0
Timeouts             0         0         0         0
Unknown Types        0         0         0         0
Packets Dropped      0         0         0         0

>
C-Clear counters
ESC-previous menu; !-main menu; &-exit
```

Figure 6-14. Radius Statistics

Table 6-9. Radius Statistics Parameters

Parameter Description		Possible Values
Access Requests	Number of access request packets that were sent to this server, not including re-transmissions.	$1–2^{32-1}$ Default: 0
Access Retransmits	Number of re-transmission request packets that were sent to this server	$1–2^{32-1}$ Default: 0
Access Accepts	Number of access accept packets (valid or invalid) that were received from this server	Numerical
Access Rejects	Number of access rejection packets (valid or invalid) that were received from the this server	Numerical
Access Challenges	Number of access challenge packets (valid or invalid) that were received from this server	Numerical

Parameter	Description	Possible Values
Malformed Response	Number of malformed access response packets that were received from this server. Malformed packets include packets with an invalid **length**. Bad authenticators (see below), signature attributes or unknown types are not included in this count.	Numerical
Bad Authenticators	Number of access response packets containing invalid authenticators or invalid signature attributes received from this server.	Numerical
Pending Requests	Number of access request packets that are destined to this server but have not yet timed-out or received any response (access accept, access reject, access challenge or access re-transmission) from the server.	Numerical
Timeouts	Number of timeouts received from this server. When a timeout is received, ACE-3600 may try to resend the access request to the same server or to a different server. A resend to the same server counts as a re-transmit, and a resend to a different server counts as an access request.	Numerical
Unknown Types	Number of unrecognized packets that were received from this server on the authentication port.	Numerical
Packets Dropped	Number of packets that were received from this server but were dropped (for any reason) after passing through the authentication port.	Numerical

Note *The* ***Clear (C)*** *command clears and resets all counters to 0.*

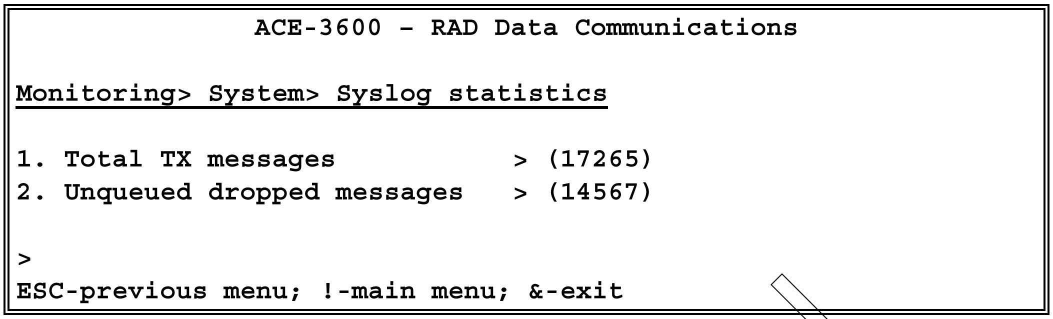
Viewing the Syslog Statistics

If ACE-3600 was set to log events on a Syslog server (see *Setting the Syslog Parameters* in Chapter 4), you can display the statistics of these events.

➤ **To display the Syslog statistics:**

- From the System menu (see *Figure 6-2*), select **Syslog statistics**.

  The Syslog statistics are displayed.



```
                ACE-3600 - RAD Data Communications

Monitoring> System> Syslog statistics

1. Total TX messages           > (17265)
2. Unqueued dropped messages   > (14567)

>
ESC-previous menu; !-main menu; &-exit
```

Figure 6-15. Syslog Statistics

Table 6-10. Syslog Statistics Parameters

Parameter	Description	Possible Values
Total TX messages	Number of messages transmitted by the Syslog server	Numerical integer
Unqueued dropped messages	Number of messages that could not be queued for transmission by the Syslog server	Numerical integer

Monitoring the Physical Layer

The physical layer includes options for monitoring the ACE-3600 physical ports, and allows the following activities:

- *Viewing the Ethernet Port Information*
- *Viewing the ATM-155 Port Statistics*.

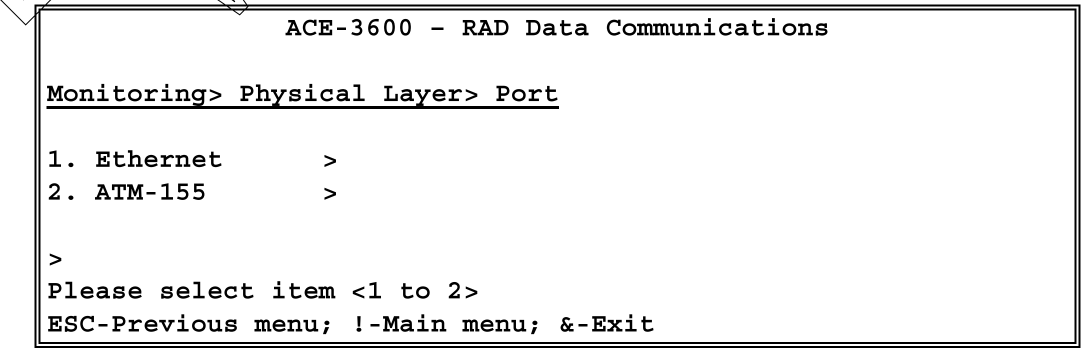
➤ To access the port monitoring options:

1. From the Monitoring menu, select Physical Layer.

   The Physical Layer is displayed.

2. Select Port.

   The Port menu is displayed.



```
                ACE-3600 - RAD Data Communications

Monitoring> Physical Layer> Port

1. Ethernet      >
2. ATM-155       >

>
Please select item <1 to 2>
ESC-Previous menu; !-Main menu; &-Exit
```

Figure 6-16. Port Menu

Table 6-11. Port Monitoring Options

Parameter	Description	Possible values
Ethernet	Ethernet monitoring menu	Refer to *Figure 6-17* below
ATM-155	ATM-155 monitoring menu	Refer to *Figure 6-19*

Viewing the Ethernet Port Information

The Ethernet port information is presented in two categories:

- Port status – the port's MAC address, duplex mode, bit rate and connection status
- Port statistics – statistics regarding the port's performance.

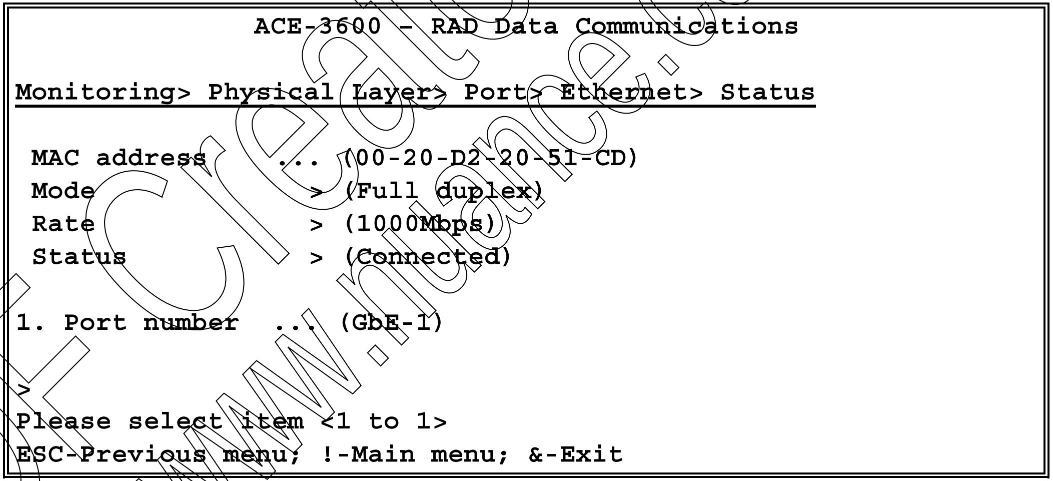
➤ To view the Ethernet port status:

1. From the Port menu (see *Figure 6-16*), select Ethernet.

   The Ethernet menu appears.

2. From the Ethernet menu, select Status.

   The port status details are displayed.



```
                  ACE-3600 - RAD Data Communications

Monitoring> Physical Layer> Port> Ethernet> Status

 MAC address      ...  (00-20-D2-20-51-CD)
 Mode               >  (Full duplex)
 Rate               >  (1000Mbps)
 Status             >  (Connected)

1. Port number    ... (GbE-1)

>
Please select item <1 to 1>
ESC-Previous menu; !-Main menu; &-Exit
```

Figure 6-17. Ethernet Port Status Information

Table 6-12. Ethernet Port Status Parameters

Parameter	Description	Possible Values
MAC address	MAC address of the Ethernet port	XX-XX-XX-XX-XX-XX (hexadecimal)
Mode	The port mode is either the default mode set by the user, or the mode selected based on the autonegotiation results.	Half duplex Full duplex

Parameter	Description	Possible Values
Rate	The port rate is either the default rate set by the user, or the rate based on the autonegotiation results.	10 Mbps 100 Mbps 1000 Mbps
Status	The Ethernet link status. Not connected status indicates no link. Connected status indicates that link is normal	Connected Not connected
Port number	The Ethernet port for which the statistics is displayed	GbE-1 ETH-MNG Default: ETH-MNG

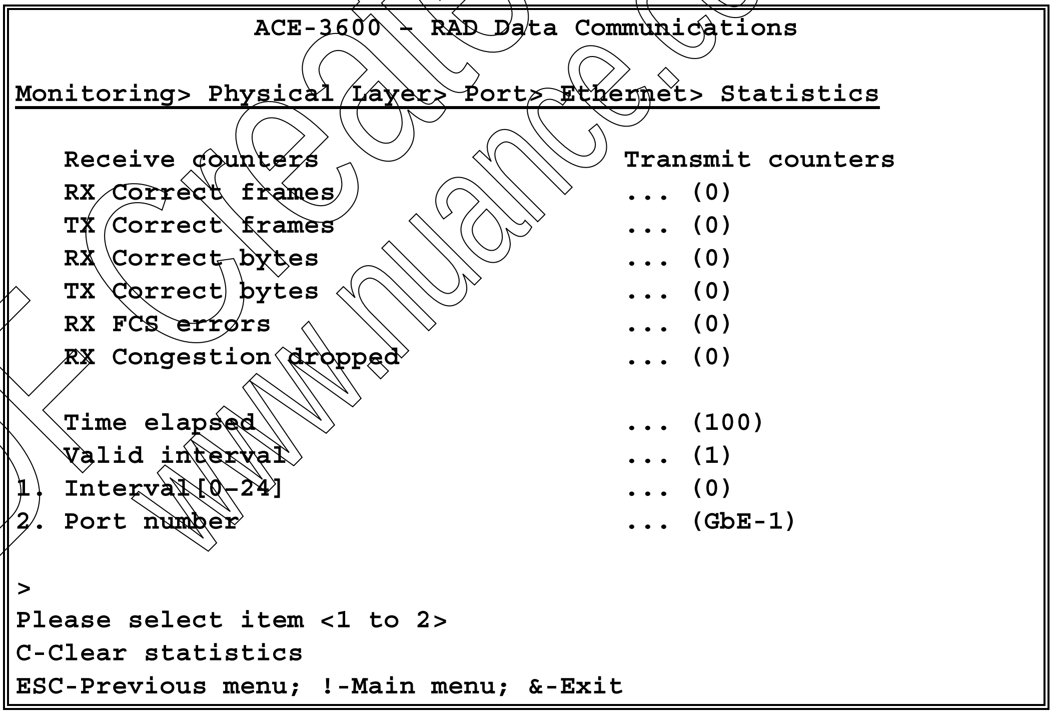
➤ To view the Ethernet port statistics:

1. From the Port menu (see *Figure 6-16*), select Ethernet.

   The Ethernet menu appears.

2. From the Ethernet menu, select Statistics.

   The port statistics are displayed.



```
                 ACE-3600 - RAD Data Communications

Monitoring> Physical Layer> Port> Ethernet> Statistics

   Receive counters                  Transmit counters
   RX Correct frames                 ... (0)
   TX Correct frames                 ... (0)
   RX Correct bytes                  ... (0)
   TX Correct bytes                  ... (0)
   RX FCS errors                     ... (0)
   RX Congestion dropped             ... (0)

   Time elapsed                      ... (100)
   Valid interval                    ... (1)
1. Interval[0-24]                    ... (0)
2. Port number                       ... (GbE-1)

>
Please select item <1 to 2>
C-Clear statistics
ESC-Previous menu; !-Main menu; &-Exit
```

Figure 6-18. Ethernet Port Statistics and Menu

Table 6-13. Ethernet Statistics Parameters

Parameter Description		Possible Values
RX correct frames	Number of successfully received frames	Numerical
RX correct bytes	Number of successfully received bytes	Numerical

Parameter	Description	Possible Values
RX alignment errors	Number of received frames that do not have an integral number of octets, valid only for Ethernet ports.	Numerical
RX FCS errors	Number of received frames that did not pass the FCS check	Numerical
RX congestion dropped	Number of frames that were dropped due to lack of buffers. This may be caused by attempting to send traffic towards the Ethernet connection at a rate higher than the ATM transmission rate.	Numerical
TX correct frames	Number of successfully transmitted frames	Numerical
TX correct bytes	Number of successfully transmitted bytes	Numerical
TX single collisions	Number of successfully transmitted frames for which transmission was inhibited by **one** collision exactly. Valid only in full-duplex mode.	Numerical
TX multiple collisions	Number of successfully transmitted frames for which transmission was inhibited by **more than one** collision. Valid only in half-duplex mode. Valid only in full-duplex mode.	Numerical
TX deferred transmit	Number of frames for which the first transmission attempt is delayed, due to a busy line. Valid only in half-duplex mode. Valid only in full-duplex mode.	Numerical
Port number	The Ethernet port for which the statistics is displayed. You can select a different Ethernet port.	GbE-1 ETH-MNG Default: ETH-MNG

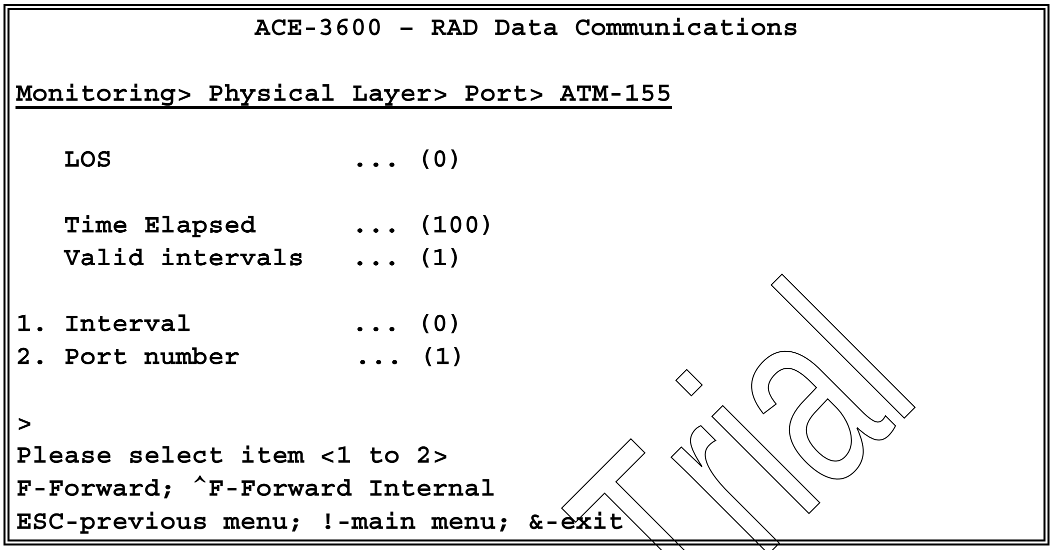
Viewing the ATM-155 Port Statistics

The ATM-155 port statistics refer to the LOS duration (seconds) with regard to a specific port and a specific time interval.

➤ To view the ATM-155 port statistics:

- From the Port monitoring menu (see *Figure 6-16*), select ATM-155.

  The connection statistics of Port 1 is displayed by default. *Table 6-14* explains the different statistic parameters.



```
                    ACE-3600 - RAD Data Communications

Monitoring> Physical Layer> Port> ATM-155

   LOS                ... (0)

   Time Elapsed       ... (100)
   Valid intervals    ... (1)

1. Interval           ... (0)
2. Port number        ... (1)

>
Please select item <1 to 2>
F-Forward; ^F-Forward Internal
ESC-previous menu; !-main menu; &-exit
```

Figure 6-19. ATM-155 Port Statistics and Menu

Table 6-14. ATM-155 Port Statistics Parameters

Parameter Description		Possible Values
LOS	The number of seconds during which LOS was detected	Numerical
Time elapsed / Start time	Elapsed time (in seconds) since the beginning of the current interval. Start time is for the chosen interval.	0–899
Valid interval	Valid intervals is the number of intervals that are saved	0–24
Interval	The interval number to be displayed	0–24 if Interval 24 exists, or 0 to last existing interval if not Default: 0
Port number	The ATM-155 port number for which the statistics are displayed. You can select another port to view its statistics.	1–8 Default: 1

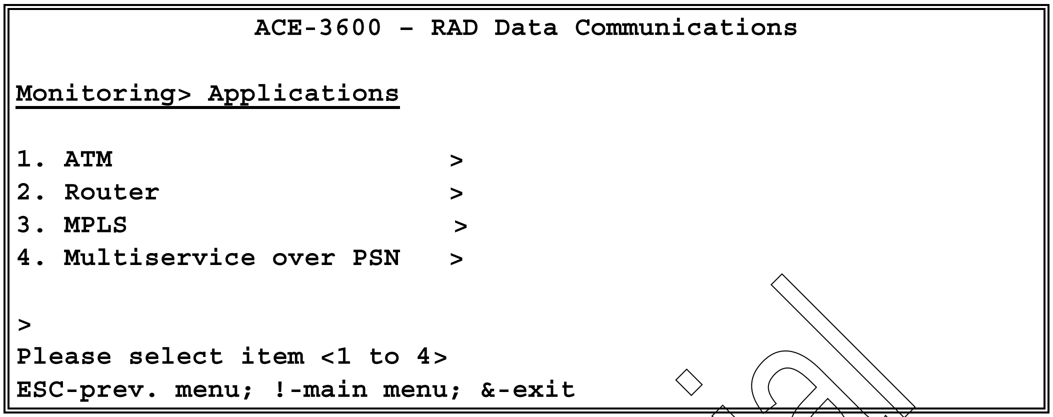
Monitoring the Application Performance

The application monitoring options allow you to review the actual performance of the unit with regards to the application parameters set under the Configuration menu (see *Configuring the Application Parameters* in Chapter 4).

➤ To access the application monitoring options:

- From the Monitoring menu (see *Figure 6-1*), select Applications.

  The Applications monitoring menu is displayed.



```
                    ACE-3600 - RAD Data Communications

Monitoring> Applications

1. ATM                      >
2. Router                   >
3. MPLS                     >
4. Multiservice over PSN    >

>
Please select item <1 to 4>
ESC-prev. menu; !-main menu; &-exit
```

Figure 6-20. Applications Menu

Table 6-15. Application Monitoring Options

Parameter	Description	Possible Values
ATM	ATM traffic monitoring options	Refer to *Figure 6-21*
Router	Router monitoring options	Refer to *Figure 6-27*
MPLS	MPLS traffic monitoring options	Refer to *Figure 6-30*
Multiservice over PSN	Multiservice over PSN monitoring options	Refer to *Figure 6-35*

Viewing the ATM Traffic Statistics

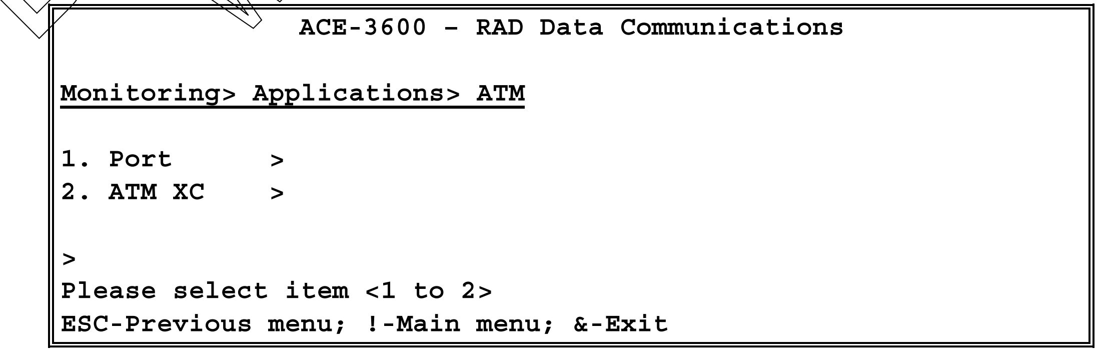
The ATM traffic statistics is available in the following categories:

- *Displaying ATM Port Statistics*
- *Displaying ATM XC Statistics*

➤ To access the ATM operation statistics categories:

- On the Applications monitoring menu, select ATM.

The ATM monitoring menu appears.



```
                    ACE-3600 - RAD Data Communications

Monitoring> Applications> ATM

1. Port      >
2. ATM XC    >

>
Please select item <1 to 2>
ESC-Previous menu; !-Main menu; &-Exit
```

Figure 6-21. ATM Monitoring Menu

Table 6-16. ATM Menu Parameters

Parameter	Description	Possible Values
Port	ATM port level monitoring menu	Refer to *Figure 6-22* below
ATM XC	ATM XC monitoring menu	Refer to *Figure 6-23*

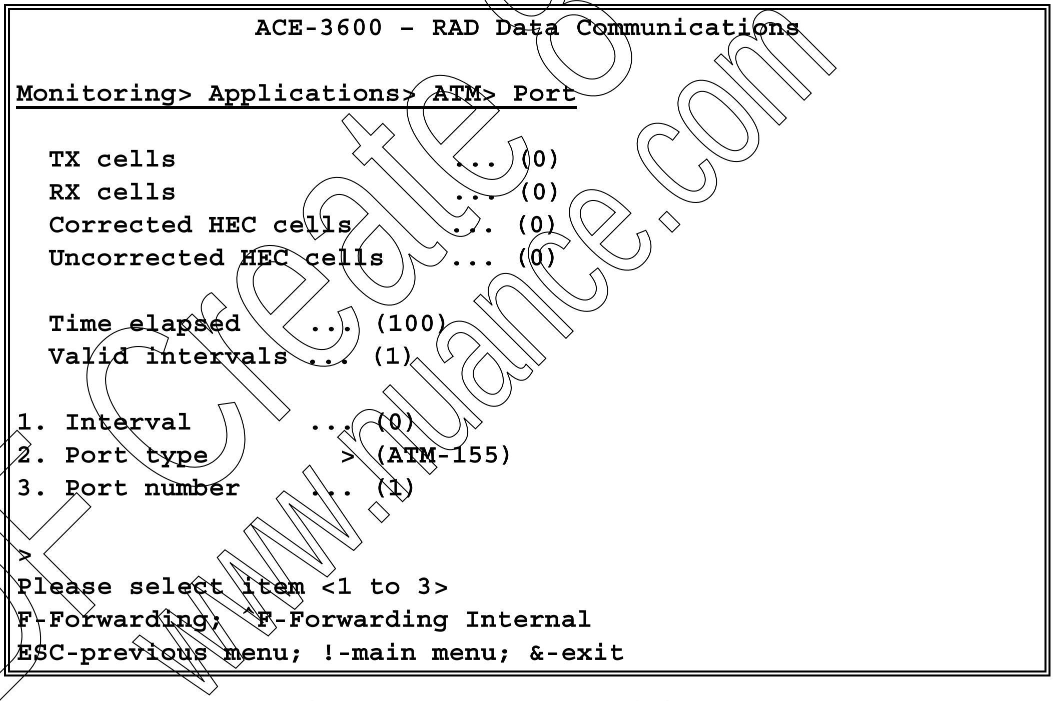
Displaying ATM Port Statistics

The ATM port operation statistics includes details regarding the recorded traffic of TX cells, RX cells, corrected HEC cells and uncorrected HEC cells.

➤ To view the port statistics:

- From the ATM monitoring menu, select Port.

  The operation statistics of Port are displayed by default. *Table 6-17* explains the different statistic parameters.



```
                    ACE-3600 - RAD Data Communications

Monitoring> Applications> ATM> Port

  TX cells                  ...  (0)
  RX cells                  ...  (0)
  Corrected HEC cells       ...  (0)
  Uncorrected HEC cells     ...  (0)

  Time elapsed     ...  (100)
  Valid intervals  ...  (1)

1. Interval        ...  (0)
2. Port type         >  (ATM-155)
3. Port number     ...  (1)

>
Please select item <1 to 3>
F-Forwarding; ^F-Forwarding Internal
ESC-previous menu; !-main menu; &-exit
```

Figure 6-22. ATM Port Statistics Menu

Table 6-17. ATM Port Statistics Parameters

Parameter	Description	Possible Values
TX cells	Number of cells transmitted on that port	Numerical
RX cells	Number of cells received without HEC error	Numerical

Parameter	Description	Possible Values
Corrected HEC cells	The number of frames received with an errored HEC, corrected (single error) and passed on into the device. This parameter is visible for ATM-155 ports only.	Numerical
Uncorrected HEC cells	The number of frames received with an uncorrected HEC error (two or more errors) and were therefore dropped. .	Numerical
Time elapsed / Start time	The elapsed time period in seconds since the beginning of the current interval. Start time is for the chosen interval.	0–899
Valid intervals	The number of intervals that are saved	0–24
Interval	The interval number to be displayed	0–24 if Interval 24 exists, or 0 to last existing interval if not Default: 0
Port type	The port type for which the statistics are displayed above	ATM-155 Default: ATM-155
Port number	Number of the port for which the statistics are displayed above	1–8 for ATM-155 Default: 1

➤ **To view the statistics of a different port:**

- From the Port menu (displayed below the current statistics data), select **Port Number** and then type the port number.

➤ To view the statistics of a previous time interval:

- From the Port menu, select Interval and then type the number of the 15-minute interval, which statistics you want to display.

  For more information about the displayed parameters, see *Table 6-17*.

➤ To view the connection parameters of a different type:

- From the Port menu, select Port Type and then select the required port type.

Displaying ATM XC Statistics

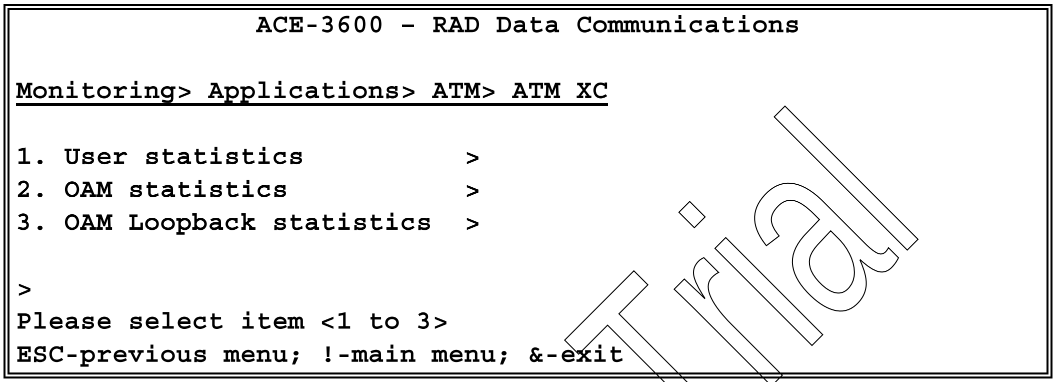
The ATM XC operation statistics consist of three information categories:

- User statistics
- OAM statistics
- OAM loopback statistics.

➤ To access the ATM XC statistics:

- From the ATM monitoring menu, select XC.

  The ATM XC monitoring options are displayed.



```
                  ACE-3600 - RAD Data Communications

Monitoring> Applications> ATM> ATM XC

1. User statistics           >
2. OAM statistics            >
3. OAM Loopback statistics   >

>
Please select item <1 to 3>
ESC-previous menu; !-main menu; &-exit
```

Figure 6-23. ATM XC Statistics Menu

Table 6-18. ATM XC Menu Options

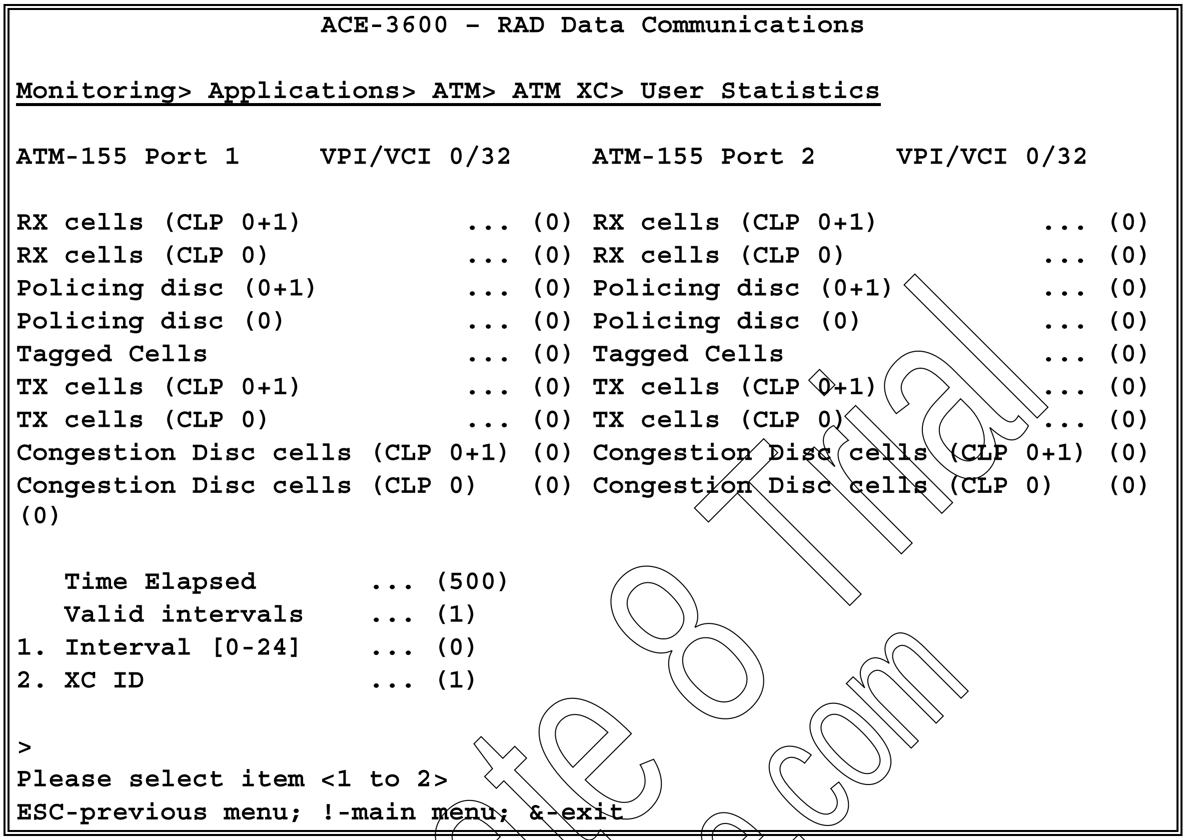
Parameter	Description	Possible Values
User statistics	Access the XC user statistics	Refer to *Figure 6-24*
OAM statistics	Access the XC OAM statistics	Refer to *Figure 6-25*
OAM Loopback statistics	Access the OAM loopback statistics	Refer to *Figure 6-26*

Displaying the ATM XC User Statistics

➤ To view the XC user statistics:

- From the ATM XC menu, select User Statistics.

  Table 6-19 explains the displayed user statistics parameters and other display options that are available.



```
                  ACE-3600 - RAD Data Communications

Monitoring> Applications> ATM> ATM XC> User Statistics

ATM-155 Port 1     VPI/VCI 0/32     ATM-155 Port 2     VPI/VCI 0/32

RX cells (CLP 0+1)          ... (0) RX cells (CLP 0+1)          ... (0)
RX cells (CLP 0)            ... (0) RX cells (CLP 0)            ... (0)
Policing disc (0+1)         ... (0) Policing disc (0+1)         ... (0)
Policing disc (0)           ... (0) Policing disc (0)           ... (0)
Tagged Cells                ... (0) Tagged Cells                ... (0)
TX cells (CLP 0+1)          ... (0) TX cells (CLP 0+1)          ... (0)
TX cells (CLP 0)            ... (0) TX cells (CLP 0)            ... (0)
Congestion Disc cells (CLP 0+1) (0) Congestion Disc cells (CLP 0+1) (0)
Congestion Disc cells (CLP 0)   (0) Congestion Disc cells (CLP 0)   (0)
(0)

   Time Elapsed       ... (500)
   Valid intervals    ... (1)
1. Interval [0-24]    ... (0)
2. XC ID              ... (1)

>
Please select item <1 to 2>
ESC-previous menu; !-main menu; &-exit
```

Figure 6-24. XC User Statistics Menu

Table 6-19. XC User Statistics Parameters

Parameter Description		Possible Values
RX cells (CLP 0+1)	Number of cells received on the ATM channel with CLP0 or CLP1	Numerical
RX cells (CLP 0)	Number of cells received on the ATM channel with CLP0	Numerical
Policing disc (CLP 0+1)	Number of cells discarded by the ATM policer on the ATM channel with CLP0 or CLP1	Numerical
Policing disc (CLP 0)	Number of cells discarded by the ATM policer on the ATM channel with CLP0	Numerical
Tagged Cells	Number of cells tagged by the ATM policer	Numerical
TX cells (CLP 0+1)	Number of cells transmitted on the ATM channel with CLP0 or CLP1	Numerical
TX cells (CLP 0)	Number of cells transmitted on the ATM channel with CLP0	Numerical
Congestion Disc cells (CLP 0+1)	Number of cells discarded on the ATM channel with CLP0 or CLP1	Numerical
Congestion Disc cells (CLP 0)	Number of cells discarded on the ATM channel with CLP0	Numerical
Time Elapsed /	The period in seconds since the beginning of the	0–899

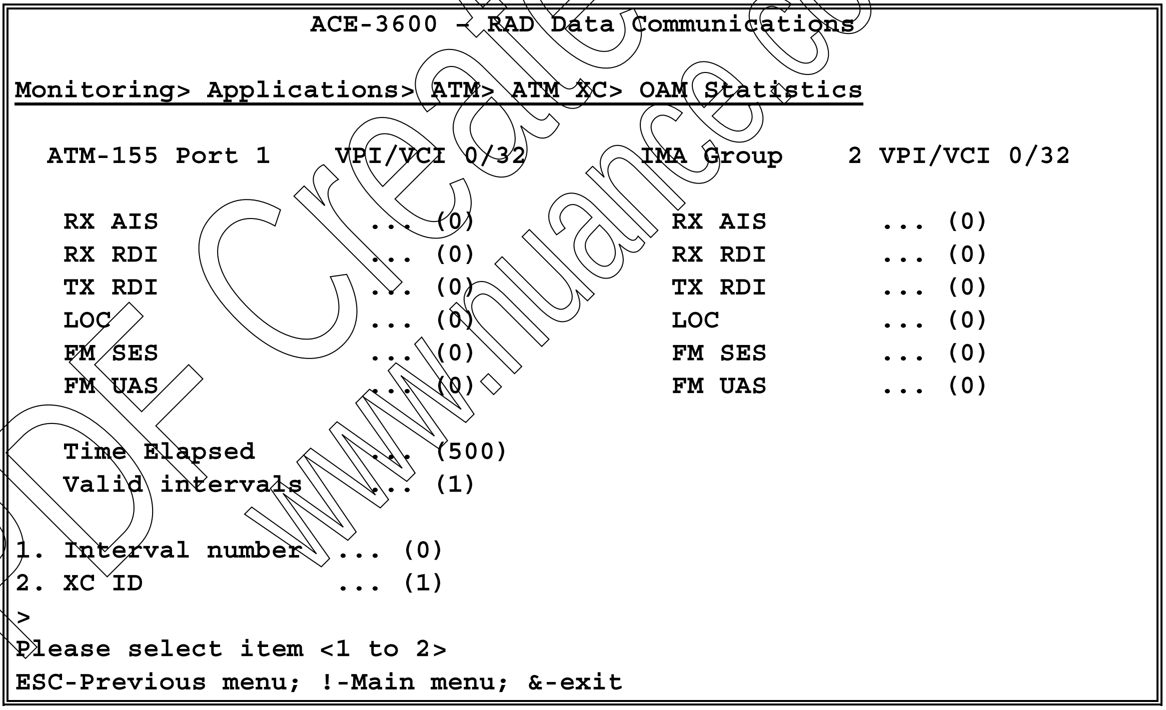
Parameter	Description	Possible Values
Start Time	current interval. Start Time is for intervals 1–24	
Interval	The interval number to be displayed	0–24 if Interval 24 exists, or 0 to last existing interval if not Default: 0
XC ID	ID of the XC for which the statistics above are displayed	XC number

Displaying the ATM XC OAM Statistics

➤ **To view the XC OAM statistics:**

- From the ATM XC monitoring menu (see *Figure 6-23*), select OAM Statistics.

  Table 6-20 explains the displayed OAM statistics parameters and other display options that are available.



```
                   ACE-3600 - RAD Data Communications

Monitoring> Applications> ATM> ATM XC> OAM Statistics

  ATM-155 Port 1    VPI/VCI 0/32       IMA Group    2 VPI/VCI 0/32

   RX AIS               ... (0)          RX AIS          ... (0)
   RX RDI               ... (0)          RX RDI          ... (0)
   TX RDI               ... (0)          TX RDI          ... (0)
   LOC                  ... (0)          LOC             ... (0)
   FM SES               ... (0)          FM SES          ... (0)
   FM UAS               ... (0)          FM UAS          ... (0)

   Time Elapsed         ... (500)
   Valid intervals      ... (1)

1. Interval number    ... (0)
2. XC ID              ... (1)
>
Please select item <1 to 2>
ESC-Previous menu; !-Main menu; &-exit
```

Figure 6-25. OAM Statistics Menu

Table 6-20. OAM Statistics Parameters and Menu

Parameter Description		Possible Values
RX AIS	The number of seconds during which AIS cells where received	Numerical
RX RDI	The number of seconds during which RDI cells where received	Numerical

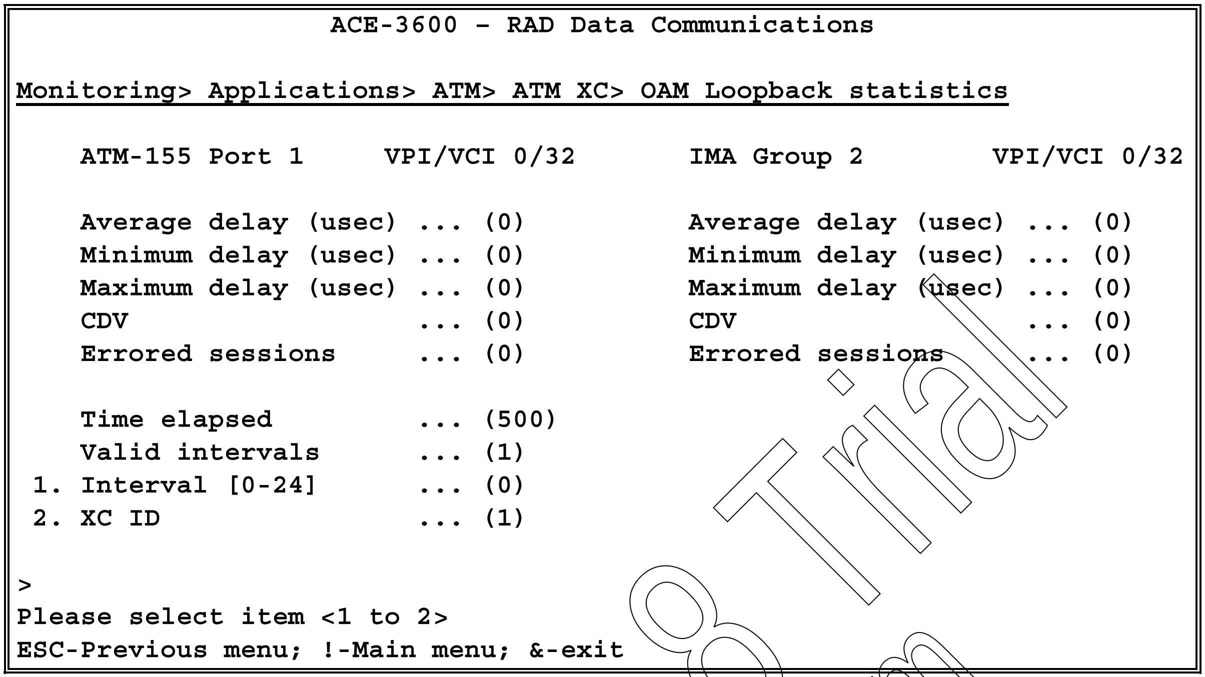
Parameter	Description	Possible Values
TX RDI	The number of seconds during which RDI cells where transmitted	Numerical
LOC	The number of seconds during which loss of continuity was declared (valid when CC is activated)	Numerical
FM SES	The time in seconds during which AIS cells where received or LOC state was declared	Numerical
FM UAS	Activated as a result of 10 consecutive SES's, and deactivated as a result of 10 consecutive seconds without SES.	Numerical
Time Elapsed / Start Time	The period in seconds since the beginning of the current interval. Start Time is for intervals 1–24.	0–899
Valid intervals	The number of intervals that are saved	0–24
Interval number	The interval number to be displayed	0–24 if Interval 24 exists, or 0 to last existing interval if not **Default: 0**
XC ID	ID of the XC for which the statistics above are displayed	XC number

Displaying the ATM XC OAM Loopback Statistics

➤ **To view the XC OAM loopback statistics:**

- From the ATM XC monitoring menu (see *Figure 6-23*), select **OAM Loopback Statistics.**

  Table 6-21 explains the displayed OAM loopback statistics parameters and other display options that are available.



```
                     ACE-3600 - RAD Data Communications

Monitoring> Applications> ATM> ATM XC> OAM Loopback statistics

    ATM-155 Port 1     VPI/VCI 0/32       IMA Group 2       VPI/VCI 0/32

    Average delay (usec) ... (0)        Average delay (usec) ... (0)
    Minimum delay (usec) ... (0)        Minimum delay (usec) ... (0)
    Maximum delay (usec) ... (0)        Maximum delay (usec) ... (0)
    CDV                  ... (0)        CDV                  ... (0)
    Errored sessions     ... (0)        Errored sessions     ... (0)

    Time elapsed         ... (500)
    Valid intervals      ... (1)
 1. Interval [0-24]      ... (0)
 2. XC ID                ... (1)

>
Please select item <1 to 2>
ESC-Previous menu; !-Main menu; &-exit
```

Figure 6-26. OAM Loopback Statistics Menu

Table 6-21. OAM Loopback Statistics Parameters

Parameter	Description	Possible Values
Average delay	The average delay measured for the OAM cells roundtrip, in microseconds.	Numerical
Minimum delay	The minimum delay measured for the OAM cells roundtrip, in microseconds.	Numerical
Maximum delay	The maximum delay measured for the OAM cells roundtrip, in microseconds.	Numerical
CDV	The cell delay variation measured for the connection. The CDV is calculated as the standard deviation of the delay measurements.	Numerical
Errored sessions	Number of failed loopback sessions. If a loopback cell is not received back within 5 seconds (if the cell does not complete the roundtrip within 5 seconds), the cell is considered as a failed cell (for more information, refer to *Appendix C*).	Numerical
Interval	The interval number to be displayed	0–24 if Interval 24 exists, or 0 to last existing interval if not Default: 0
XC ID	ID of the XC for which the statistics above are displayed	XC number

Note *The **Clear (C)** command clears all bridge port statistics.*

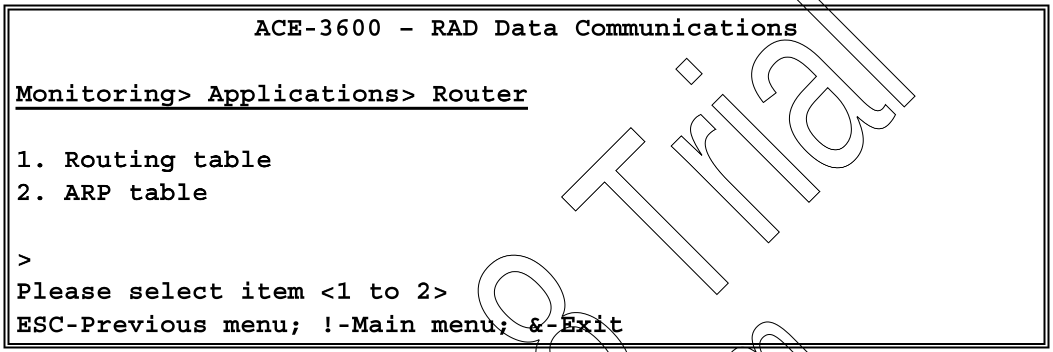
Monitoring the Routing Functionality

You can monitor the router definitions by viewing the current routing table and ARP (address resolution protocol) table.

➤ To access the router monitoring options:

- From the Applications monitoring menu (see *Figure 6-20*), select Router.

  The router monitoring options are displayed.

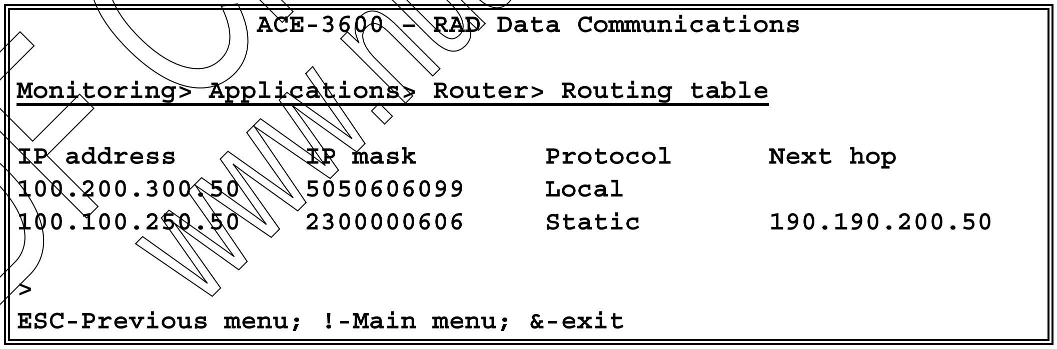


```
                ACE-3600 - RAD Data Communications

Monitoring> Applications> Router

1. Routing table
2. ARP table


>
Please select item <1 to 2>
ESC-Previous menu; !-Main menu; &-Exit
```

Figure 6-27. Router Menu

Table 6-22. Router Monitoring Options

Parameter	Description	Possible Values
Routing table	Display the routing table	See *Figure 6-28*
ARP table	Display the ARP table	See *Figure 6-29*

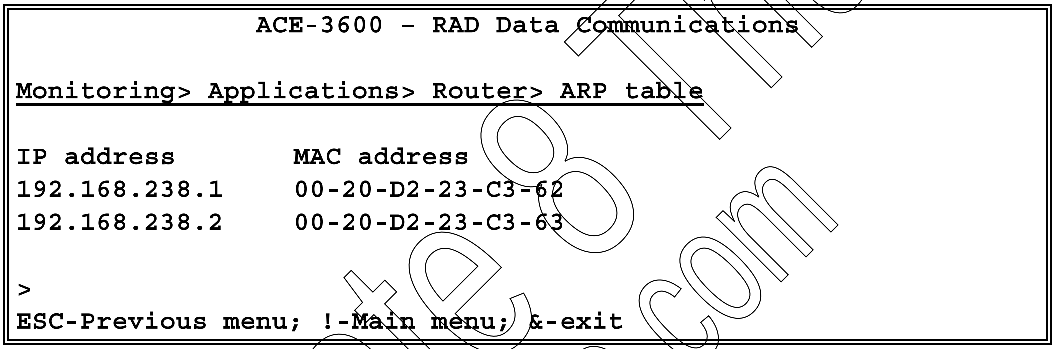


```
                ACE-3600 - RAD Data Communications

Monitoring> Applications> Router> Routing table

IP address        IP mask        Protocol      Next hop
100.200.300.50    5050606099     Local
100.100.250.50    2300000606     Static        190.190.200.50


>
ESC-Previous menu; !-Main menu; &-exit
```

Figure 6-28. Routing Table

Table 6-23. Routing Table Parameters

Parameter Description		Possible Values
IP address	IP address of each entry	A valid IP address
IP mask	IP mask of the each entry	Numerical
Protocol	Indicates whether the entry is local interfaces or static configuration	Local Static
Next hop	IP address of the entry's next hop. Relevant only for static entries.	A valid IP address



```
                     ACE-3600 - RAD Data Communications

Monitoring> Applications> Router> ARP table

IP address         MAC address
192.168.238.1      00-20-D2-23-C3-62
192.168.238.2      00-20-D2-23-C3-63

>
ESC-Previous menu; !-Main menu; &-exit
```

Figure 6-29. ARP Table

Table 6-24. ARP Table Parameters

Parameter Description		Possible Values
IP address	IP address used by the address resolution protocol	A valid IP address
MAC address	MAC address used by the address resolution protocol	A valid MAC address

Viewing the MPLS Traffic Statistics

The MPLS traffic monitoring includes the statistics of the LDP performance.

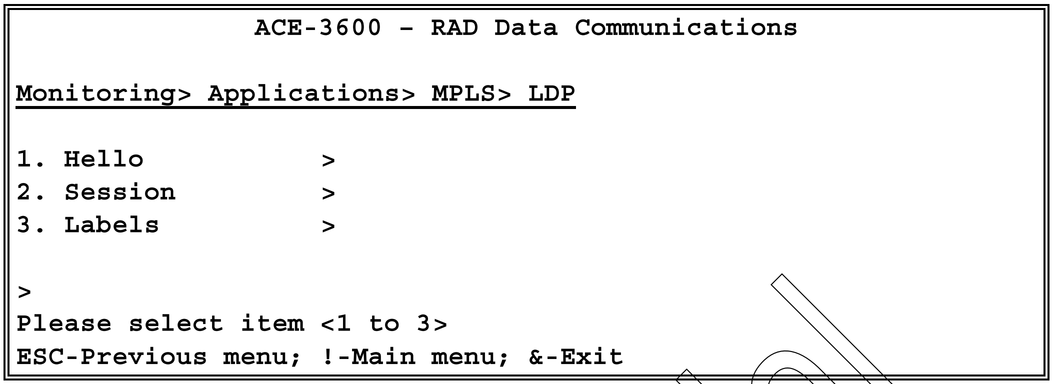
➤ To access the LDP monitoring options:

1. From the Applications monitoring menu (see *Figure 6-20*), select MPLS.

   The MPLS menu is displayed.

2. Select LDP.

   The LDP monitoring menu is displayed.

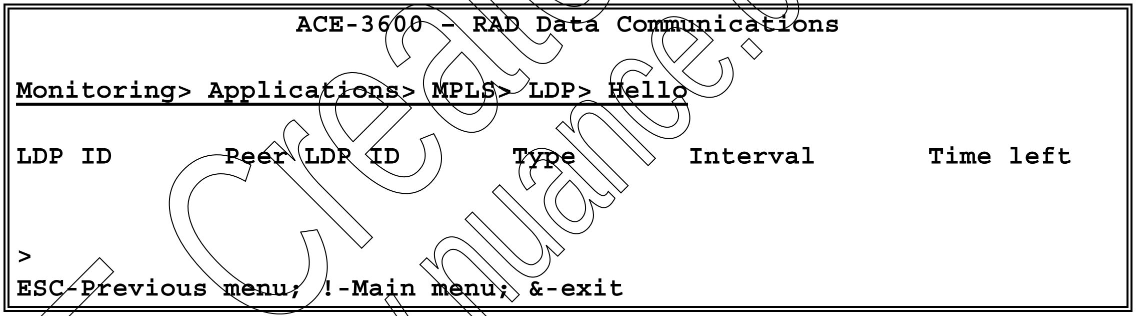


```
                ACE-3600 - RAD Data Communications

Monitoring> Applications> MPLS> LDP

1. Hello            >
2. Session          >
3. Labels           >

>
Please select item <1 to 3>
ESC-Previous menu; !-Main menu; &-Exit
```

Figure 6-30. LDP Monitoring Menu

Table 6-25. LDP Monitoring Options

Parameter Description		Possible Values
Hello	Display the Hello layer statistics	See *Figure 6-31*
Session	Display the LDP session statistics	See *Figure 6-32*
Labels	Display the LDP labels information	See *Figure 6-33*

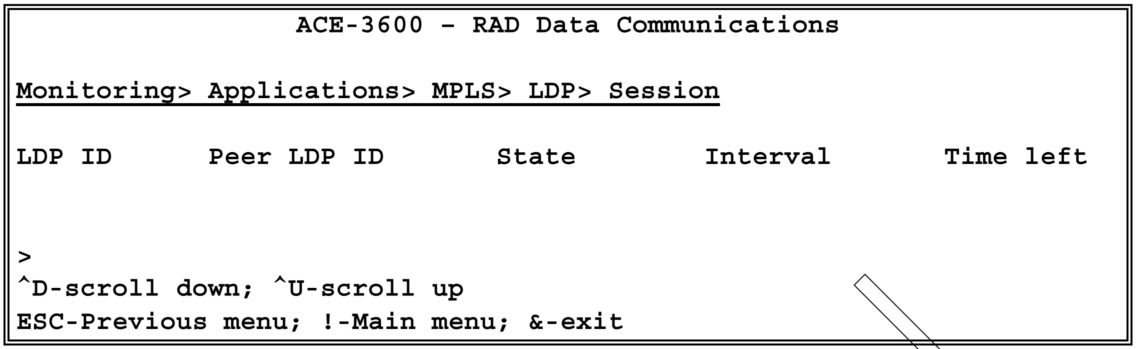


```
                ACE-3600 - RAD Data Communications

Monitoring> Applications> MPLS> LDP> Hello

LDP ID       Peer LDP ID      Type      Interval       Time left


>
ESC-Previous menu; !-Main menu; &-exit
```

Figure 6-31. Hello Statistics

Table 6-26. Hello Statistics Parameters

Parameter Description		Possible Values
LDP ID	LDP ID of the local unit	
Peer LDP ID	LDP ID of the remote peer	
Type	The type of Hello adjacency: • L (link) – the adjacencies are established with basic discovery • T (targeted) – the adjacencies are established with extended discovery	L T
Interval	The frequentness of sending Hello messages by the local unit	
Time left	The time in seconds during which the local unit waits for the peer to send a Hello message	

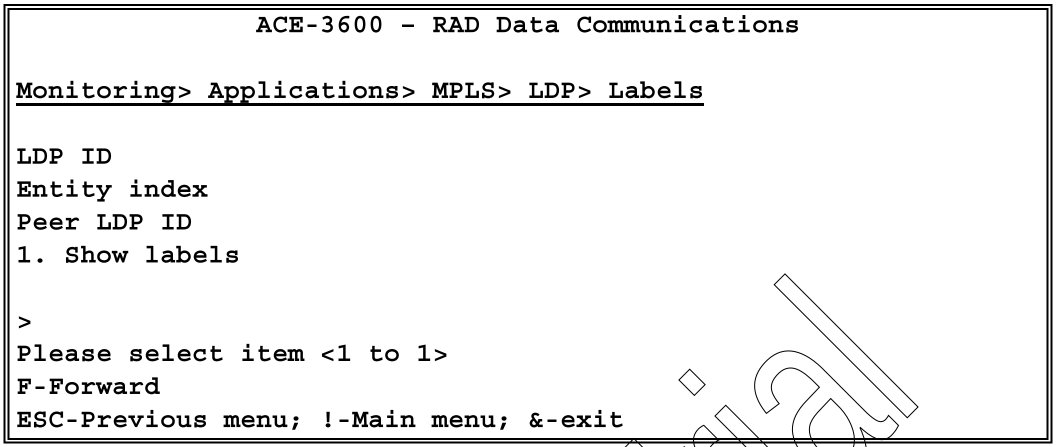


```
                   ACE-3600 - RAD Data Communications

Monitoring> Applications> MPLS> LDP> Session

LDP ID      Peer LDP ID      State       Interval      Time left



>
^D-scroll down; ^U-scroll up
ESC-Previous menu; !-Main menu; &-exit
```

Figure 6-32. LDP Session Statistics

Table 6-27. LDP Session Statistics Parameters

Parameter	Description	Possible Values
LDP ID	LDP ID of the local unit	
Peer LDP ID	LDP ID of the remote peer	
State	The current state of the LDP session: • Up – the session is active and for label exchange • None – the session's initial state before a TCP connection is established • Init – indicates that the TCP connection is initiated, or that the LDP session has started listening to the LDP port. The first option is when the session is in active role, and the second when it is in passive role. • Openrec – an initialization message has been received from the peer • Openset – the peer has transmitted an initialization message and is waiting for reply. Relevant only the LDP session is in active role.	Up None Init Openrec Openset
Interval	The negotiated Keep Alive time, which represents the number of seconds between Keep Alive messages	
Time left	The Keep Alive hold time remaining for this LDP session	

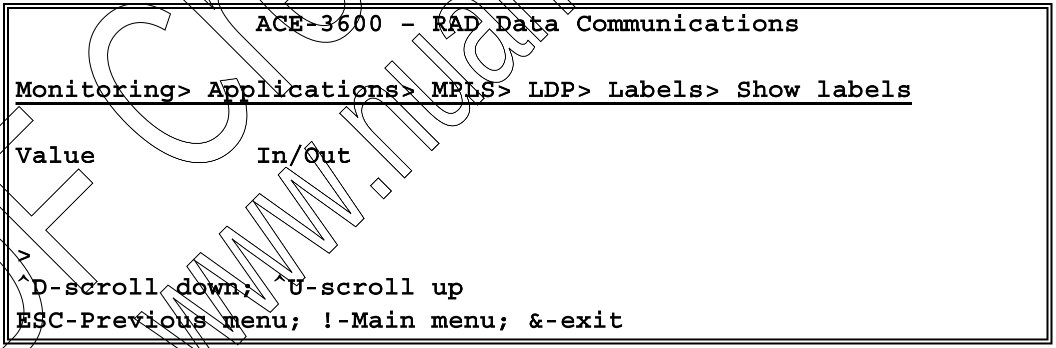


```
                 ACE-3600 - RAD Data Communications

Monitoring> Applications> MPLS> LDP> Labels

LDP ID
Entity index
Peer LDP ID
1. Show labels

>
Please select item <1 to 1>
F-Forward
ESC-Previous menu; !-Main menu; &-exit
```

Figure 6-33. LDP Label Information

Table 6-28. LDP Label Parameters

Parameter	Description	Possible Values
LDP ID	LDP ID of the local unit	
Entity index	The LDP entity's index number	
Peer LDP ID	LDP ID of the remote peer	
Show labels	Select this option to view the LDP labels that are exchanged on this session	See *Figure 6-34*



```
                 ACE-3600 - RAD Data Communications

Monitoring> Applications> MPLS> LDP> Labels> Show labels

Value        In/Out



>
^D-scroll down; ^U-scroll up
ESC-Previous menu; !-Main menu; &-exit
```

Figure 6-34. Show Labels

Table 6-29. Label Parameters

Parameter	Description	Possible Values
Value (column top)	Shows the value of each LDP label in the session	
In/Out (column top)	Specifies whether each label is an In or Out label	

Monitoring Multiservice over PSN Traffic

ACE-3600 provides detailed information regarding all pseudowire traffic from and to the unit. This includes:

- *Displaying Pseudowire Connection Status*
- *Displaying Pseudowire Connection Statistics*

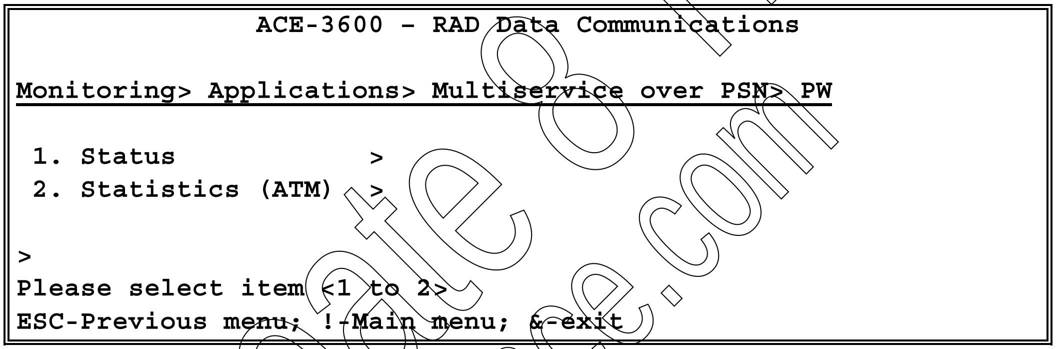
➤ To access the pseudowire monitoring options:

1. From the Applications monitoring menu (see *Figure 6-20*), select Multiservice over PSN.

   The Multiservice over PSN menu is displayed.

2. Select PW.

   The PW monitoring menu is displayed.



```
                ACE-3600 - RAD Data Communications

Monitoring> Applications> Multiservice over PSN> PW

 1. Status              >
 2. Statistics (ATM)    >

>
Please select item <1 to 2>
ESC-Previous menu; !-Main menu; &-exit
```

Figure 6-35. Pseudowire Monitoring Menu

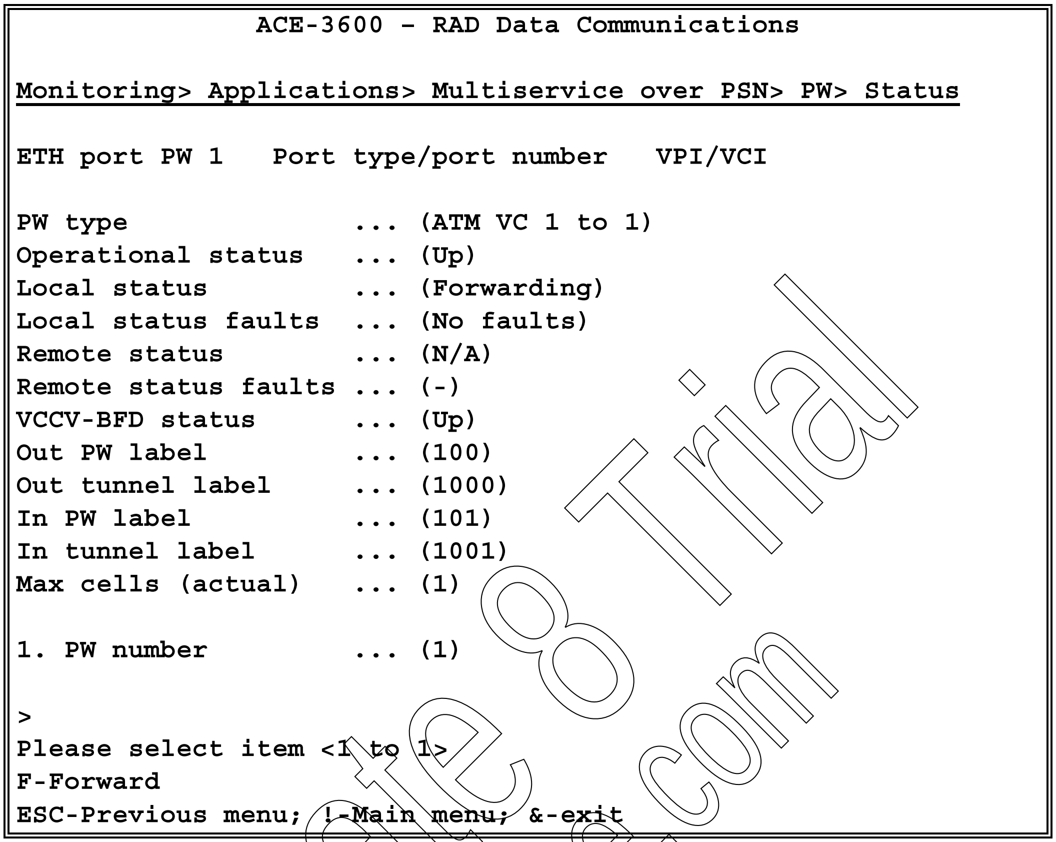
Displaying Pseudowire Connection Status

The pseudowire connection status includes the PW type, its operational status and its labels.

➤ To view the pseudowire connection status:

- From the PW monitoring menu, select Status.

  The status details of a PW connection are displayed. All status details are read-only.



```
                ACE-3600 - RAD Data Communications

Monitoring> Applications> Multiservice over PSN> PW> Status

ETH port PW 1   Port type/port number   VPI/VCI

PW type                ... (ATM VC 1 to 1)
Operational status     ... (Up)
Local status           ... (Forwarding)
Local status faults    ... (No faults)
Remote status          ... (N/A)
Remote status faults   ... (-)
VCCV-BFD status        ... (Up)
Out PW label           ... (100)
Out tunnel label       ... (1000)
In PW label            ... (101)
In tunnel label        ... (1001)
Max cells (actual)     ... (1)

1. PW number           ... (1)

>
Please select item <1 to 1>
F-Forward
ESC-Previous menu; !-Main menu; &-exit
```

Figure 6-36. Pseudowire Status Details

Table 6-30. Pseudowire Status Parameters

Parameter Description		Possible Values
PW type	Type of the pseudowire connection	ATM VP 1 to 1 ATM VC 1 to 1 ATM VP N to 1 ATM VC N to 1 AAL5-SDU SAToP Basic CES PSN
Operational status	Indicates the current status of the PW connection: • Up – the connection is up and running • Down – the connection is down • Not present – a configuration is missing • Lower layer down – the underlying layer (MAC, tunnel) is down	Up Down Not present Lower layer down
Local status	The status of the pseudowire at the local side ***Note:*** *There is no Local Status if PW Type is AAL5-SDU.*	Forwarding Local Faults

Parameter	Description	Possible Values
Local status faults	The faults at the local side of the pseudowire connection ***Note:*** *This field may display one or more faults.*	No faults NotFwding – PW cannot send packets AcRx – Errors on the receiving channel of the attachment circuit AcTx - Errors on the transmitting channel of the attachment circuit PsnRx - Errors on the receiving channel of the pseudowire towards the PSN. PsnTx - Errors on the transmitting channel of the pseudowire towards the PSN.
Remote status	The status of the pseudowire at the remote side *Note:The remote status is available only when using LDP.*	N/A – Remote status capability is not applicable Forwarding – No remote errors reported by the remote device Remote faults – Errors reported by the remote device

Parameter	Description	Possible Values
Remote status faults	The faults at the remote side of the pseudowire connection ***Note:*** *This field may display one or more faults.*	No faults NotFwding – PW cannot forward packets AcRx – Errors on the receiving channel of the attachment circuit AcTx - Errors on the transmitting channel of the Attachment circuit PsnRx - Errors on the receiving channel of the pseudowire towards the PSN. PsnTx - Errors on the transmitting channel of the pseudowire towards the PSN.
VCCV-BFD status	Current status of the VCCV-BFD verification mechanism: • Init – the mechanism in initializing • Up – the mechanism is working and detecting connection faults • Down / control-detection-time-expired – for a detailed explanation, see *Appendix F* • Down / neighbour-signaled-session-down – for a detailed explanation, see *Appendix F*	Init Up Down
Out PW label	The PW label that is used in the outbound direction. Relevant only if the PW subtype is clock recovery and if the provisioning mode is set to Manual (for more information, see *Creating Pseudowire Connections* in Chapter 4).	1–4095 if the PSN type is UDPoIP 16–1048575 for any other PSN type
Out tunnel label	Index of the egress tunnel definition for this PW. A value of 0 means that the tunnel label is not used.	
In PW label	The PW label that is used in the inbound direction.	
In tunnel label	Index of the ingress tunnel definition for this PW. A value of 0 means that the tunnel label is not used.	

Parameter	Description	Possible Values
Max cells (actual)	Displays the actual number of cells for an ATM PW	
PW number	ID number of an existing (previously defined) PW connection for which the details are displayed above. You can enter a different PW number to view its connection status.	1–1536

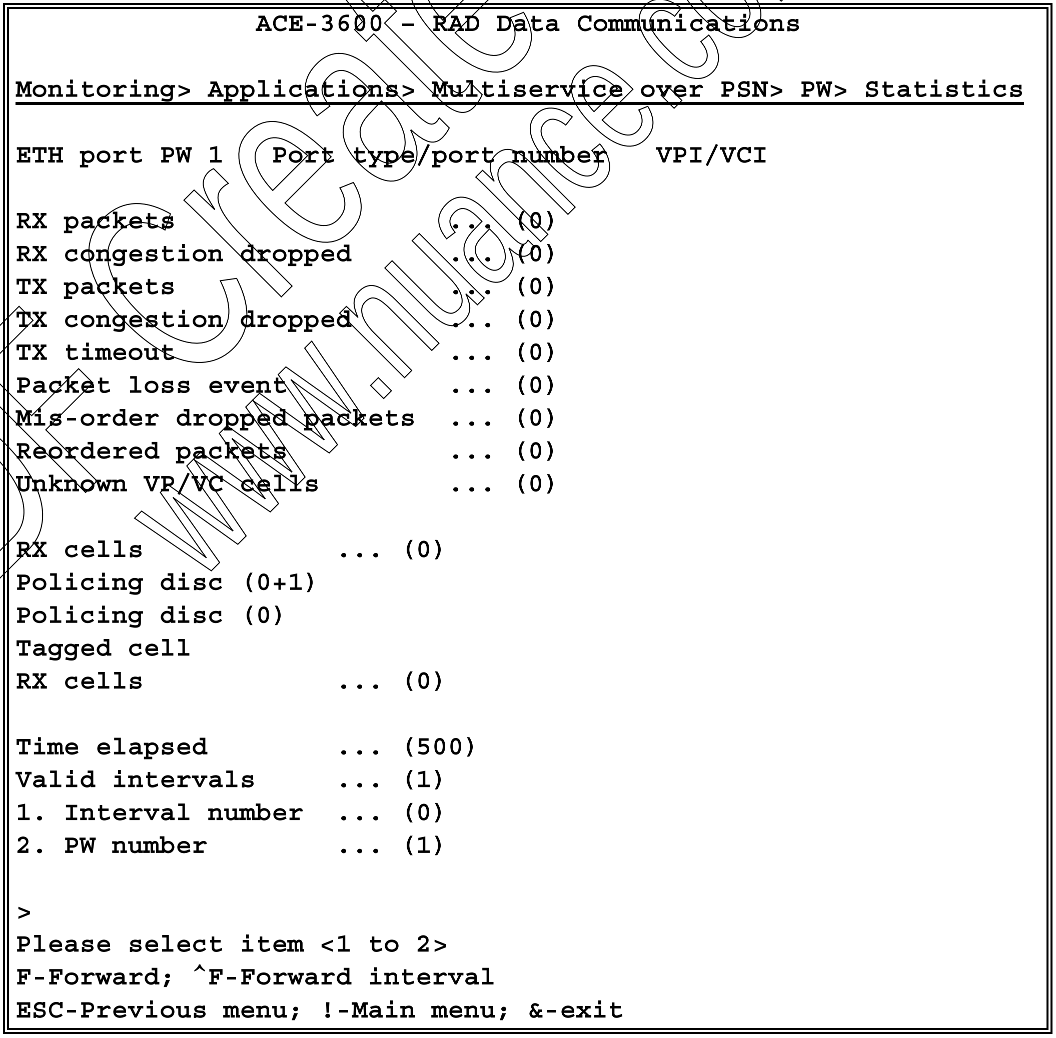
Displaying Pseudowire Connection Statistics

The pseudowire connection statistics include details regarding RX/TX packets, lost or recorded packets, and traffic encapsulated over the PW.

➤ To display the PW connection statistics:

- From the PW monitoring menu (see *Figure 6-35*), select **Statistics**.

  The performance statistics of a PW connection are displayed. The displayed details are read-only.



```
               ACE-3600 - RAD Data Communications

Monitoring> Applications> Multiservice over PSN> PW> Statistics

ETH port PW 1   Port type/port number   VPI/VCI

RX packets                 ... (0)
RX congestion dropped      ... (0)
TX packets                 ... (0)
TX congestion dropped      ... (0)
TX timeout                 ... (0)
Packet loss event          ... (0)
Mis-order dropped packets  ... (0)
Reordered packets          ... (0)
Unknown VP/VC cells        ... (0)

RX cells            ... (0)
Policing disc (0+1)
Policing disc (0)
Tagged cell
RX cells            ... (0)

Time elapsed        ... (500)
Valid intervals     ... (1)
1. Interval number  ... (0)
2. PW number        ... (1)

>
Please select item <1 to 2>
F-Forward; ^F-Forward interval
ESC-Previous menu; !-Main menu; &-exit
```

Figure 6-37. ATM Pseudowire Statistics

Table 6-31. ATM Pseudowire Statistics Parameters

Parameter Description		Possible Values
Top row	The top row displays: • Ethernet port type and port number • PW number (can be changed below) • ATM port type/number • VPI/VCI of the PW connection.	
RX packets	Number of packets received on this PW	Numerical
RX congestion dropped	Number of packets dropped due to congestion on the receive direction	Numerical
TX packets	Number of packets transmitted on this PW	Numerical
TX congestion dropped	Number of packets dropped due to congestion on the transmit direction (toward the PSN)	Numerical
TX timeout	Number of packets transmitted to the Ethernet port because of timeout expiration	Numerical
Packet loss event	Number of Losses of frame/frames, which was identified by a gap in the sequence number and not classified as a misorder	Numerical
Miss-order dropped packets	Number of packets that were dropped (not fixed) by the reordering mechanism.	Numerical
Reordered packets	Number of packets that were received later than expected and were fixed by the reordering mechanism	Numerical
Unknown VP/VC cells	Number of cells that were received from the PSN with an unknown VPI/VCI value. Relevant only for N:1 VC/VP PW types.	Numerical
RX cells	Number of complete cells received on the specified VC/VP from the ATM side	Numerical
RX congestion dropped	Number of packets dropped due to congestion on the receive direction	Numerical
TX packets	Number of packets transmitted on this PW	Numerical
TX congestion dropped	Number of packets dropped due to congestion on the transmit direction (toward the PSN)	Numerical
TX cells	Number of cells transmitted on the specified VC/VP toward the ATM side	Numerical
Time Elapsed / Start Time	Time Elapsed is the period in seconds since the beginning of the current interval. Start Time is for intervals 1–24.	0–899
Valid intervals	The number of intervals that are saved	0–24

Parameter	Description	Possible Values
Interval number	Number of the interval to be displayed. You can enter a different number of press ^F to view the next interval.	0–24 if Interval 24 exists, or 0 to last existing interval if not Default: 0
PW number	ID number of an existing (previously defined) PW connection for which the details are displayed above. You can enter a different PW number to view its connection status, or press F to view the next PW.	1–1536

6.2 Detecting Errors

Error Detection Options

ACE-3600 maintains a cyclic event log file that stores up to 2000 events. All stored events are time-stamped. The event log file contents may be viewed on the ASCII terminal or on a Network Management Station (NMS), and it may be cleared at any time (see *Figure 6-4*).

To detect and resolve faults/errors in ACE-3600, the following options are available:

- Check for active alarms –
  - For menu instructions, see *Viewing the Active Alarms.*
  - For handling alarms and their trap, see *Handling Alarms and Traps*.
- Review the events recorded in the event log:
  - For menu instructions, see *Viewing the Event Log*.
- For the complete list of possible events, see *List of Log Events* below.
- Perform external and internal loopback tests, such as ATM port timed external loop (towards the line) or ATM port timed internal loop (towards the ATM link).
- Perform cell tests, in which a predefined cell is sent towards the ATM link.
- Review the troubleshooting charts (see *Table 6-44*), based on LED indications or other inputs.

List of Log Events

Refer to the following tables for the full list of system, port and OAM events.

Table 6-32. System Events List

No.	Event string	Status/Entity Type/Entity #
1.	Cold start	
2.	Device reset	
3.	Software watchdog reset	
4.	Login	Valid/Invalid
5.	Authentication	Fail
6.	Power supply #n	Active/ Not Active
7.	Fan #n	OK/ Fail
8.	Software download	Ended OK/ Failed
9.	Configuration download	Ended OK/ Failed
10.	Configuration upload	Ended OK/ Failed
11.	Fatal error	File: ‹file name›, line: ‹line number›
12.	Exception	PC=‹0xXXXXXXXX›, CAUSE=‹0xYYYYYYYY›
13.	Master clock is active	
14.	Fallback clock is active	
15.	No reference clock is active	
16.	Internal clock source active	ATM155-1
17.	Reference clock source active	ATM155-1
18.	Loopback clock source active	ATM155-1
19.	Recovered clock	
20.	Start collection	
21.	PW up/down	PW #n Up/Down
22.	LDP session up/down	LDP #n Up/Down
23.	Statistics collection OK	#n files
24.	Ethernet port is active	ETH #n
25.	Station clock	OK/ Fail
26.	Recovered clock changed to Free run / Frequency acquisition / Rapid phase lock / Fine phase lock / Hold over -	#n

No.	Event string	Status/Entity Type/Entity #
27.	Card Inserted	Card type
28.	Card Absent	Slot-#n
29.	Fan drawer Inserted/Absent	
30.	Control card Inserted/Absent	
31.	Power supply #n Absent	
32.	Card mismatch	Slot #n\Fan drawer\Control
33.	Card A absent; Card B absent	Start/End
34.	Redundancy communication loss	Start/End
35.	Redundancy hardware mismatch	Start/End
36.	Redundancy application mismatch	Start/End
37.	Redundancy configuration mismatch	Start/End
38.	Redundancy switch to card A; Redundancy switch to card B	
39.	Statistic collection Ended OK -	#n files
40.	Eth Redundancy: GbE- #n is active APS: ATM-155-#n is active	

Table 6-33. ATM-155 Port Events List

No.	Event String	Status	Port Type/Port #
1.	SFP	Plugged/Unplugged	ATM155 #n
2.	LOS	Start/End	ATM155 #n
3.	LOF	Start/End	ATM155 #n
4.	LOP	Start/End	ATM155 #n
5.	LCD	Start/End	ATM155 #n
6.	SLM	Start/End	ATM155 #n
7.	Line AIS	Start/End	ATM155 #n
8.	Path AIS	Start/End	ATM155 #n
9.	Line RD	Start/End	ATM155 #n
10.	Path RD	Start/End	ATM155 #n
11.	Section BIP/ RS BIP	Start/End	ATM155 #n
12.	Line BIP/MS BIP	Start/End	ATM155 #n
13.	Path BIP/HP BIP	Start/End	ATM155 #n
14.	Line FEBE/MS FEBE	Start/End	ATM155 #n
15.	Path FEBE/HP FEBE	Start/End	ATM155 #n

No. Event	String	Status	Port Type/Port #
16.	APS: ATM port ATM-155# is active	Start/End ATM155	#n

Table 6-34 ETH Port Events List

No. Event	String	Status	Port Type/Port #
1.	Link	Up/Down	Ethernet - #n

Table 6-35. OAM Events List

No. Event	String	Status	Port Type/Port #	VPI/VCI
1.	Rx AIS	Start/End	ATM-155 #n	VPI #X, VCI #Y
2.	Rx RDI	Start/End	E1 #n	VPI #X, VCI #Y
3.	Tx RDI	Start/End	T1 #n	VPI #X, VCI #Y
4.	LOC	Start/End	J1 #n	VPI #X, VCI #Y
5.	Loopback	Active/Failed	E1 #n	VPI #X, VCI #Y

Table 6-36. BFD (PW Connectivity) Events List

No.	Event String	Status	PW #
1.	BFD Up	No diagnostic	PW #n
2.	BFD Down	No diagnostic	PW #n
3.	BFD Init	No diagnostic	PW #n
4.	BFD Down	Control detection time expired	PW #n
5.	BFD Down	Neighbor signaled session down	PW #n

6.3 Handling Alarms and Traps

ACE-3600 includes a configurable mechanism of detecting and reporting alarms. Upon the occurrence an alarm, ACE-3600 sends or does not send an alarm trap to the network manager location, depending on a pre-configured activation or masking of that specific alarm trap.

Even though masked traps are not sent, all alarms are recorded in the system event log upon their occurrence.

Viewing and Masking Alarm Traps

The trap masking configuration menu is located under: **Configuration > System > Management > Manager list > Traps.** For more information, refer to *Configuring Alarm Traps* in Chapter 4.

List of Alarm Traps

Refer to *Table 6-37* for all the alarm traps that are implemented in ACE-3600.

Table 6-37. List of Alarm Traps

Number Trap	Name
1.	Cold Start
2.	Agent Status Changed
3.	TFTP status changed
4.	Authentication failure
5.	Power failure
6.	Fan failure
7.	Port status change – for SFP
8.	Redundancy status*
9.	Redundancy switch
10.	Link down – for ETH ports only
11.	Link up – for ETH ports only
12.	Loss Of Signal (LOS Physical Layer)*
13.	Loss Of Frame (LOF Physical Layer)*
14.	Loss Of ATM Cell Delineation (LCD ATM Layer)*
15.	Signal Label Mismatch (SLM Physical Layer)*
16.	Loss Of Pointer (LOP Physical Layer)* – for ATM-155 ports only
17.	Loss of Pointer (LOP Path Physical Layer) – for Channelized-155 ports only
18.	Loss of Pointer (LOP VT Physical Layer) – for Channelized-155 ports only
19.	Out of Frame (OOF Physical Layer) – for Channelized-155 ports only
20.	Alarm Indication Signal Received (AIS Line Physical Layer)*
21.	Alarm Indication Signal Received (AIS Path Physical Layer)*
22.	Alarm Indication Signal Received (AIS VT Physical Layer)* – for Channelized-155 ports only
23.	Remote Defect Indication Received (RDI Line Physical Layer)*
24.	Remote Defect Indication Received (RDI Path Physical Layer)*

Number	Trap Name
25.	Remote Defect Indication Received (RDI VT Physical Layer)* – for Channelized-155 ports only
26.	Bit Interleaved Parity Error (BIP Section Physical Layer)* – for ATM-155 ports only
27.	Bit Interleaved Parity Error (BIP Line Physical Layer)* – for ATM-155 ports only
28.	Bit Interleaved Parity Error (BIP Path Physical Layer)* – for ATM-155 ports only
29.	Far End Block Error (FEBE Line Physical Layer)* – for ATM-155 ports only
30.	Far End Block Error (FEBE Path Physical Layer)* – for ATM-155 ports only
31.	Excessive Error Detect received (EED Line Physical Layer)* – for Channelized-155 ports only
32.	Excessive Error Detect received (EED Path Physical Layer)* – for Channelized-155 ports only
33.	Excessive Error Detect received (EED VT Physical Layer)* – for Channelized-155 ports only
34.	Signal Degrade received (SD Line Physical Layer)* – for Channelized-155 ports only
35.	Signal Degrade received (SD Path Physical Layer)* – for Channelized-155 ports only
36.	Signal Degrade received (SD VT Physical Layer)* – for Channelized-155 ports only
37.	Payload Mismatch received (SLM Path Physical Layer)* – for Channelized-155 ports only
38.	Payload Mismatch received (SLM VT Physical Layer)* – for Channelized-155 ports only
39.	Loss of Multi-frame received (LOMF Path Physical Layer) – for Channelized-155 ports only
40.	VP loopback failed (Fault Management in ATM layer)*
41.	VP continuity loss (Fault Management in ATM layer)*
42.	VP AIS Alarm Received (Fault Management in ATM layer)*
43.	VP RDI Received (Fault Management in ATM layer)*
44.	VC loopback failed (Fault Management in ATM layer)*
45.	VC continuity loss (Fault Management in ATM layer)*
46.	VC AIS Alarm Received (Fault Management in ATM layer)*
47.	VC RDI Received (Fault Management in ATM layer)*
48.	IMA Group Status Change
49.	Station clock failure*
50.	Module change
51.	Card mismatch*

Note ** Also implemented as an active alarm.*

Corrective Measures

Depending on the reported alarm and its severity, change the unit configuration or check the integrity of ports, connections or standalone devices (such as switches, routers, etc.) that take part in the particular application.

If the alarm/problem persists, refer to *Troubleshooting* or *Technical Support*.

6.4 Testing the Unit

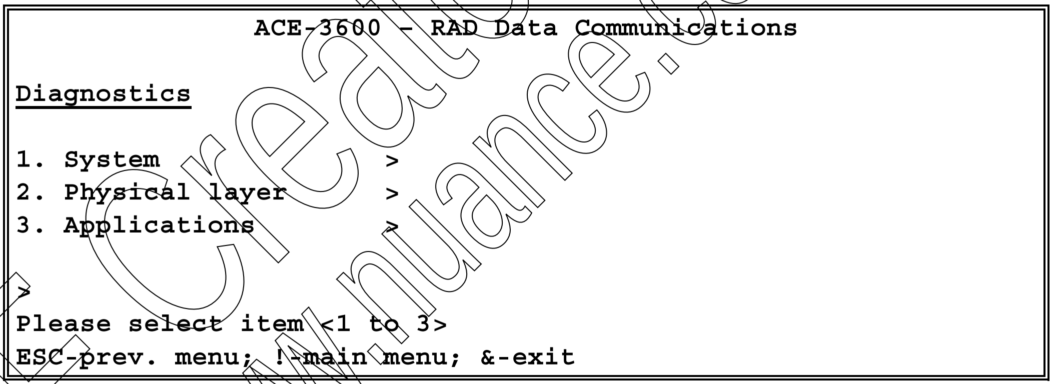
ACE-3600 can be tested in order to diagnose possible setbacks. This includes:

- *Displaying Self-Test Results*
- *Performing Physical Loopback Tests*
- *Performing Application Tests*

➤ To access the unit's diagnostics options:

- From the main menu, select Diagnostics.

  The Diagnostics menu is displayed.



```
                  ACE-3600 - RAD Data Communications

Diagnostics

1. System                   >
2. Physical layer           >
3. Applications             >

>
Please select item <1 to 3>
ESC-prev. menu; !-main menu; &-exit
```

Figure 6-38. Diagnostics Menu

Table 6-38. Diagnostics Menu Options

Parameter	Description	Possible Values
System	Access the self-test results option	Refer to *Figure 6-39*
Physical layer	Access the physical layer diagnostics options	Refer to *Figure 6-42*
Applications	Access the application diagnostics options	Refer to *Figure 6-44*

Displaying Self-Test Results

ACE-3600 performs a self-test upon power-up, and their results can displayed in the Self Test Results screen. In the results screen, "Pass" means that the test has passed successfully (no error/malfunction has been found), and "Fail" means that the test has failed (an error/malfunction has been found).

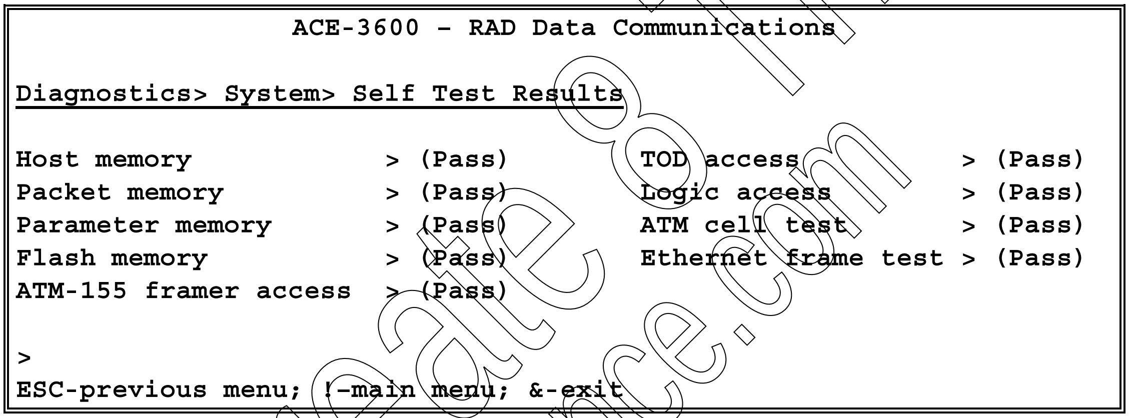
➤ To access the Self Test Results screen:

1. From the Diagnostics menu, select System.

   The System menu is displayed.

2. Select Self Test Results.

   The self-test results are displayed.



```
                    ACE-3600 - RAD Data Communications

Diagnostics> System> Self Test Results

Host memory             > (Pass)      TOD access           > (Pass)
Packet memory           > (Pass)      Logic access         > (Pass)
Parameter memory        > (Pass)      ATM cell test        > (Pass)
Flash memory            > (Pass)      Ethernet frame test  > (Pass)
ATM-155 framer access   > (Pass)

>
ESC-previous menu; !-main menu; &-exit
```

Figure 6-39. Self Test Results

Performing Physical Loopback Tests

ACE-3600 supports two types of user-defined physical loopback operations on ATM ports:

- Internal loopback – returns the transmitted data at the physical layer to the receive path. The internal physical loopback includes a configurable timeout mechanism that ends the loopback operation after expiry of the user-defined period.
- External loopback – returns the received data at the physical layer to the transmit path.

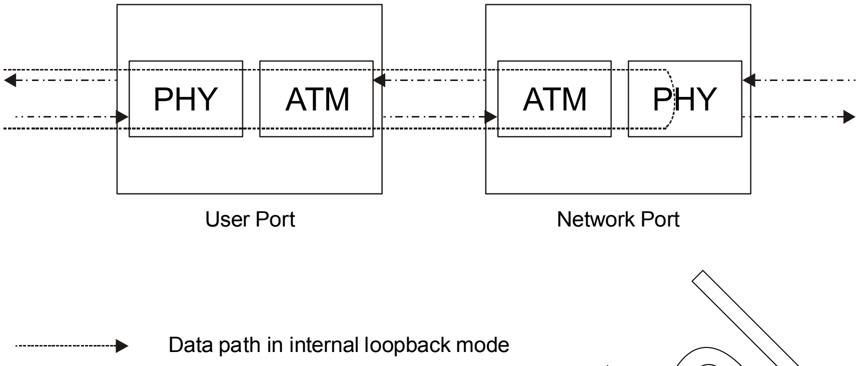


Figure 6-40. Data Path in Internal Loopback Mode

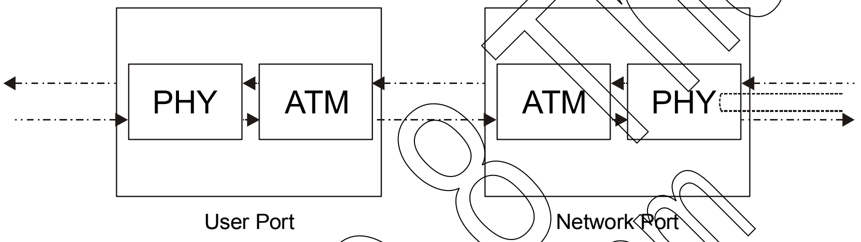


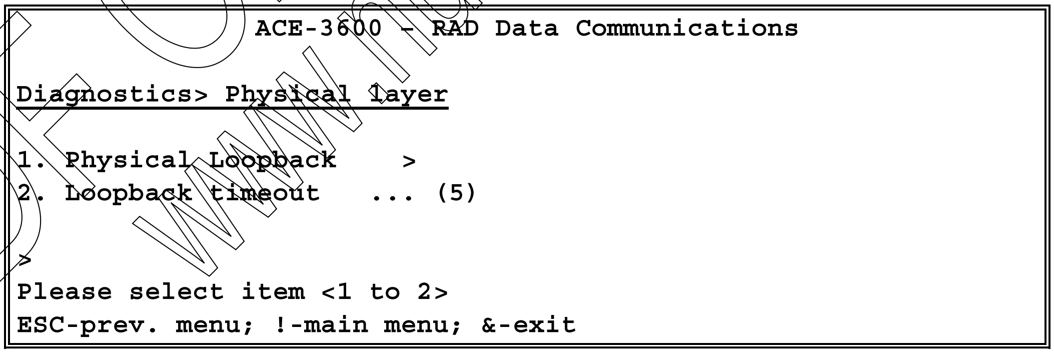
Figure 6-41. Data Path in External Loopback Mode

The physical loopback includes a configurable timeout mechanism to terminate the loopback operation upon expiry of the assigned period.

➤ To access the physical loopback diagnostics menu:

- From the Diagnostics menu, select Physical Layer.

  The Physical Layer diagnostics menu is displayed.



```
               ACE-3600 - RAD Data Communications

Diagnostics> Physical layer

1. Physical Loopback     >
2. Loopback timeout    ... (5)


>
Please select item <1 to 2>
ESC-prev. menu; !-main menu; &-exit
```

Figure 6-42. Physical Layer Diagnostics Menu

Table 6-39. Physical Layer Menu Parameters

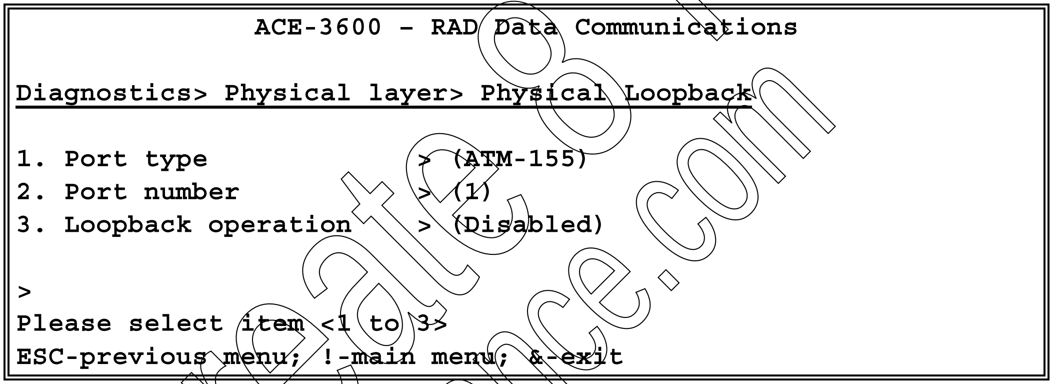
Parameter	Description	Possible Values
Physical Loopback	Access the physical loopback diagnostics.	Refer to *Figure 6-43*

Parameter	Description	Possible Values
Loopback timeout	The duration of the loop operation in minutes, to be preformed in the diagnostics. Once the defined period is over, the loop is terminated and the Loopback Operation parameter is reverted to Disable (see *Figure 6-43*). The loopback timeout is applicable for both external and internal loops.	1–300 Default: 5

➤ To access the physical loopback diagnostics options:

- From the Physical Layer menu, select Physical Loopback.

  The Physical Loopback menu is displayed.



```
                ACE-3600 - RAD Data Communications

Diagnostics> Physical layer> Physical Loopback

1. Port type              > (ATM-155)
2. Port number            > (1)
3. Loopback operation     > (Disabled)

>
Please select item <1 to 3>
ESC-previous menu; !-main menu; &-exit
```

Figure 6-43. Physical Loopback Diagnostics Menu

Table 6-40. Physical Loopback Diagnostics Menu Parameters

Parameter	Description	Possible Values
Port type	Type of the diagnosed port	ATM-155 Default: ATM-155
Port number	Number of the diagnosed port	1–8 for ATM-155
Loopback operation	The loopback operation mode: • Disable – The loopback mode is disabled. • External – The received signal for this interface is looped back out through the corresponding transmitter in the return direction. • Internal – The signal that is about to be transmitted is connected to the associated incoming receiver.	Disable External Internal Default: Disable

Performing Application Tests

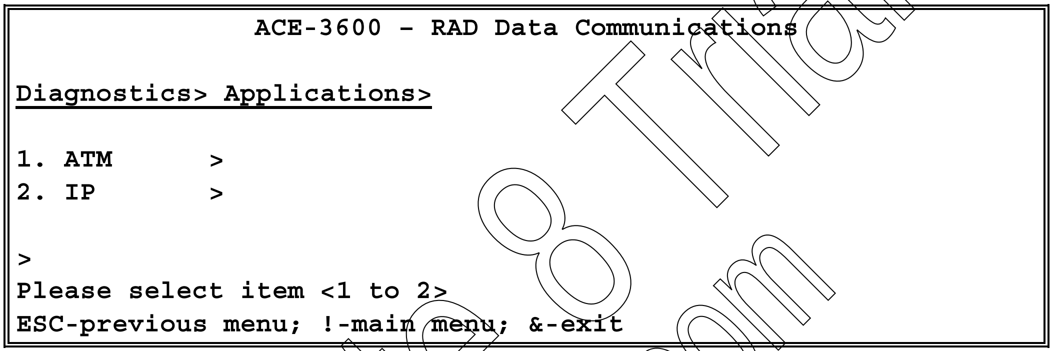
Application-level tests are performed at the following categories:

- *Performing ATM Cell Tests*
- *Performing IP Connectivity Tests*.

➤ To access the application diagnostics menu:

- From the Applications menu (see *Figure 6-44*), select Applications.

  The application diagnostic options are displayed.



```
                    ACE-3600 - RAD Data Communications

Diagnostics> Applications>

1. ATM       >
2. IP        >

>
Please select item <1 to 2>
ESC-previous menu; !-main menu; &-exit
```

Figure 6-44. Application Diagnostics Options

Performing ATM Cell Tests

ATM cell tests can be manually invoked and tested from the Cell Test menu.

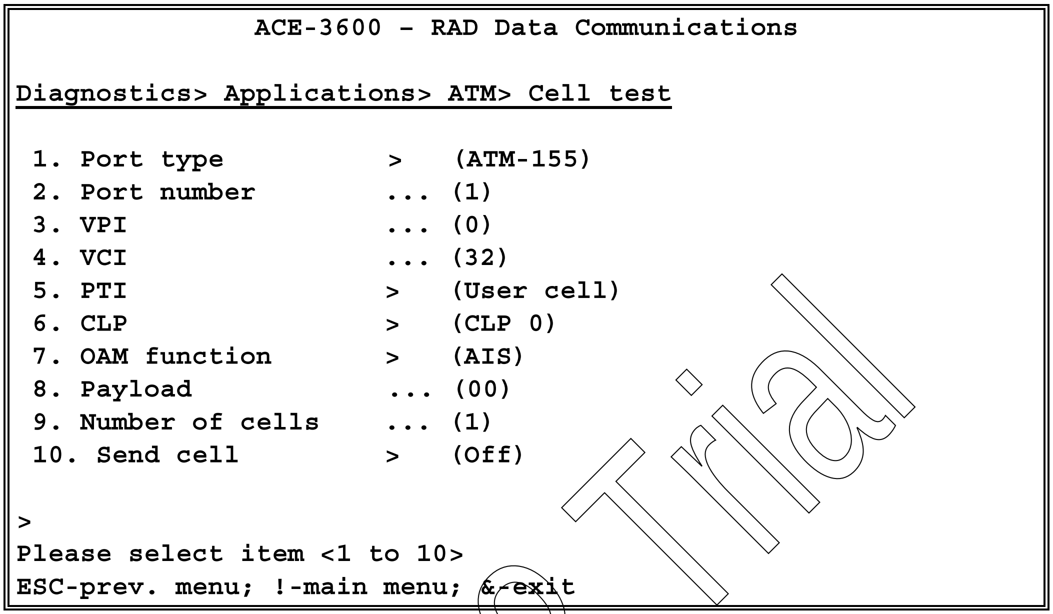
➤ To access the ATM Cell Test menu:

1. From the Applications menu, select ATM.

   The ATM diagnostics menu is displayed.

2. Select Cell Test.

   The Cell Test menu is displayed.



```
                 ACE-3600 - RAD Data Communications

Diagnostics> Applications> ATM> Cell test

 1. Port type          >   (ATM-155)
 2. Port number        ... (1)
 3. VPI                ... (0)
 4. VCI                ... (32)
 5. PTI                >   (User cell)
 6. CLP                >   (CLP 0)
 7. OAM function       >   (AIS)
 8. Payload            ... (00)
 9. Number of cells    ... (1)
 10. Send cell         >   (Off)

>
Please select item <1 to 10>
ESC-prev. menu; !-main menu; &-exit
```

Figure 6-45. Cell Test Menu

Table 6-41. Cell Test Menu Parameters

Parameter Description		Possible Values
Port type	Port type (either physical or logical)	ATM-155
Port number	The ATM port number	1–4 for ATM-155
VPI	The cell test's VPI	0–4095
VCI	The cell test's VCI	32–65535
PTI	The cell test's PTI. Valid only for F5 OAM cells.	User cell OAM segment OAM end-to-end Default: User cell
CLP	The cell test's CLP	CLP 0 CLP 1 Default: CLP 0
OAM function	The OAM function of the cell test. ***Note:*** *Applicable only in case of an OAM PTI (see PTI above) or VCI 3/4.*	AIS RDI CC
Payload	Payload content of the ATM cell. ***Note:*** *In case of OAM PTI or VCI3/VCI4 (F4 or F5 OAM cells), the payload is automatically set as* ***6A****, and it cannot be changed.*	00–FF Hex Default: 00
Number of cells	The amount of cells to be sent in this test	1–10000 Default: 1

Parameter	Description	Possible Values
Send cells	Use this command to start or stop the sending the cells. When off, no cells are sent.	Send Off Default: Off

Performing IP Connectivity Tests

The IP connectivity tests include two types of tests:

- Ping test – allows you to send packet shares towards a specified IP address
- IP route tracing – allows you to send trace-route packets towards a specified IP address.

Pinging IP Addresses

Pinging helps determining the connectivity of ACE-3600 with a remote unit over an IP network.

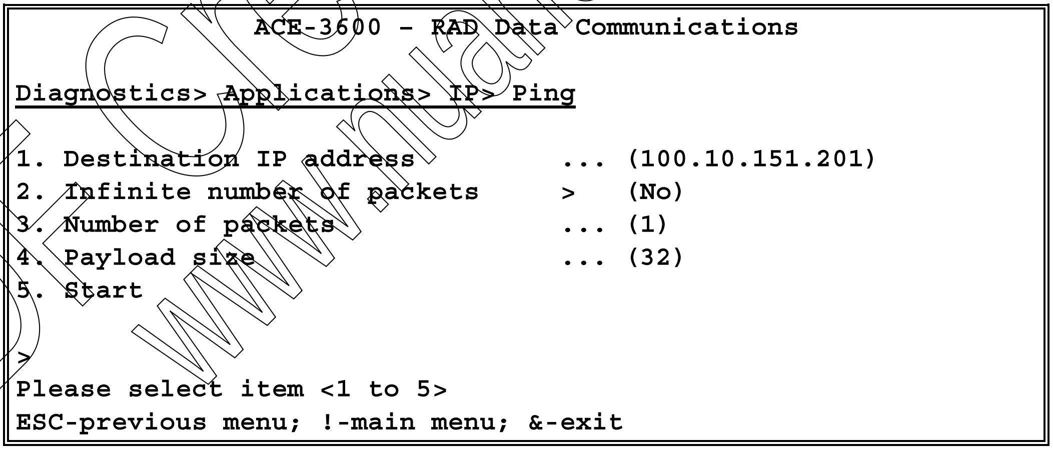
➤ To perform a Ping test:

1. From the Applications diagnostics menu (see *Figure 6-44*), select IP.

   The IP menu appears.

2. From the IP menu, select Ping.

   The Ping test options are displayed.



```
                   ACE-3600 - RAD Data Communications

Diagnostics> Applications> IP> Ping

1. Destination IP address          ... (100.10.151.201)
2. Infinite number of packets      >   (No)
3. Number of packets               ... (1)
4. Payload size                    ... (32)
5. Start

>
Please select item <1 to 5>
ESC-previous menu; !-main menu; &-exit
```

Figure 6-46. Ping Menu

Table 6-42. Ping Options

Parameter	Description	Possible Values
Destination IP address	Specify the destination IP address towards which the ping packet is to be sent	0.0.0.0–255.255.255.255 Default: 0.0.0.0

Parameter	Description	Possible Values
Infinite number of packets	Defines whether the ping packets are sent infinitely or according to a specific number of packets defined below.	No Yes Default: No
Number of packets	A specific number of packets to be sent. Valid only if No is selected above.	1–10000 Default: 1
Payload size	Size of the ping payload, in bits.	32–1450 Default: 32
Start/Stop	Activates the ping test according to the parameters above. To stop the pinging, re-select this option or exit the Ping menu.	

Note *Only one ping session is allowed at a time.*

Tracing IP Routes

Tracing an IP route allows you to trace bottlenecks over the IP network.

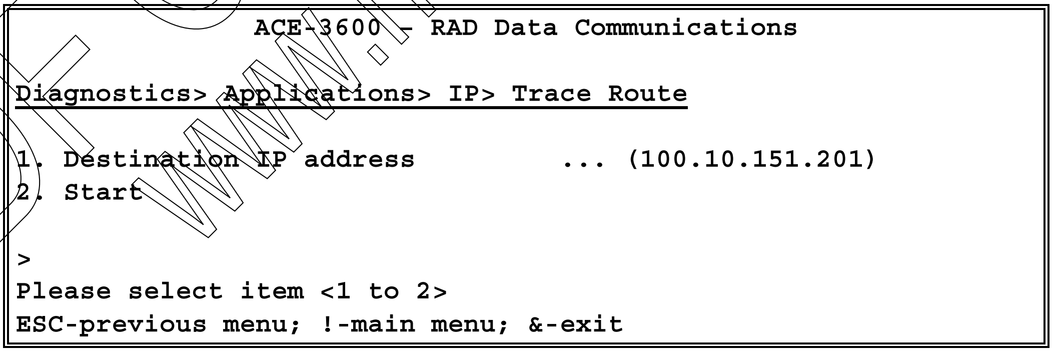
➤ To perform a route tracing:

1. From the Applications diagnostics menu (see *Figure 6-44*), select IP.

   The IP menu appears.

2. From the IP menu, select Trace Route.

   The Trace Route menu is displayed.



```
              ACE-3600 - RAD Data Communications

Diagnostics> Applications> IP> Trace Route

1. Destination IP address         ... (100.10.151.201)
2. Start

>
Please select item <1 to 2>
ESC-previous menu; !-main menu; &-exit
```

Figure 6-47. Trace Route Menu

Table 6-43. Trace Route Options

Parameter	Description	Possible Values
Destination IP address	Specify the destination IP address towards which the trace-route packets are to be sent	0.0.0.0–255.255.255.255 Default: 0.0.0.0

Parameter	Description	Possible Values
Start/Stop	Activates the route tracing towards the specified IP address. To stop the tracing, re-select this option or exit the Trace Route menu.	

Note *Only one route tracing session is allowed at a time.*

6.5 Troubleshooting

The following troubleshooting chart is based on LED indications or other inputs.

Use this chart to identify the cause of a problem that may arise during operation. For detailed description of the LED indicators functions, refer to *Chapter 3*.

To correct the reported problem, perform the suggested remedy actions. If a problem cannot be resolved by performing the suggested action, please contact RAD technical support (see *Section 6.8*).

Table 6-44. Troubleshooting Chart

Fault/Problem	Probable Cause	Remedy Action
The unit is "dead" (POWER LED is off)	No power	Check that both ends of the power cable are properly connected.
The unit is "dead" (POWER LED is off)	Blown fuse	Disconnect the power cable from both ends and replace the fuse with another fuse of proper rating.
SYSTEM RDY LED blinks	Self test failed	Access the Self Test Result screen to locate the failure and then send the unit for repair. If the screen is not accessible, sent the unit for repair.
ATM-155 SYNC LED is off	ATM-155 Rx path failure	• Check the ATM-155 statistics • (ATM-155) Upon AIS, check remote unit status • Check the fiber or cable and Rx levels, as well as the remote unit Tx level

Fault/Problem	Probable Cause	Remedy Action
ATM-155 SYNC LED blinks	ATM-155 Tx path failure	• Check the ATM-155 to verify RDI received • Check the Tx optical power to see whether it is in range. If out of range, send it for repair • Check the fiber optic connections
Ethernet LINK LED is off	Ethernet cable problem	• Check the Ethernet cable to see whether a cross or straight cable is needed • Check/replace Ethernet cable • Check range to be within limits • Check the port by connecting to a different port switch at the remote end • Send the device for repair
ATM service problems	Physical layer problems	• Check ATM-155 statistics. • Follow remedial action described in ATM-155 SYNC LED is off and ONET/SDH SYNC LED blinks.
ATM service problems	ATM layer problems	• Check the ATM OAM statistics. If AIS or RDI is received, check ATM network modes. • Use CC to check ATM connection integrity.
Echo in voice		• Check the network delay and try to decrease the delay • Try to decrease the CDVT buffer setting

6.6 Recovering ACE Units

This section highlights possible scenarios that may have led to failure. It explains how to recover ACE-3600 assuming those scenarios.

Note *This section applies to Version 5.2 of all devices that belong to the ACE-3000 family. Certain scenarios and possible solutions may therefore not apply to your specific ACE unit.*

ACR Failure

The ACE device features an Adaptive Clock Recovery (ACR) mechanism, designed to track a synchronous clock source over PSN-based networks. The mechanism utilizes a dedicated Uni-Directional PW for the clock recovery process running between the Distribution unit and the Recovery unit.

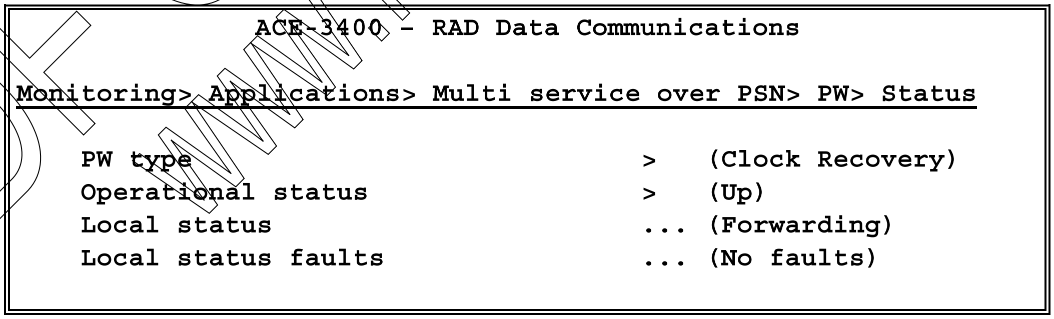
The issues in need to be addressed:

- Status of the clock recovery PW
- Status of the remote port generating the clock stream.

Determining the Condition of the Clock Recovery PW

➤ To determine the condition of the Clock Recovery PW:

1. Go to Monitoring›Applications›Multiservice over PSN›PW›Status.
2. Select the clock recovery PW index.



```
                  ACE-3400 - RAD Data Communications

Monitoring> Applications> Multi service over PSN> PW> Status

    PW type                                >   (Clock Recovery)
    Operational status                     >   (Up)
    Local status                           ... (Forwarding)
    Local status faults                    ... (No faults)
```

3. Ensure that Operational Status is Up and Local Status set to Forwarding.

If the ACR PW is in Down state, continue investigating using the PW/VCCV-BFD Failure procedure (RAT Entry #3), as outlined below:

1. Go to Monitoring›System›Clock›Recovered clock›Status.
2. Select Recovered ID and observe the status of the ACR.

```
    Clock State                              >   (Holdover)
 1. Recovered ID[1 - 1]                      ... (1)
```

In case of an ACR failure, the clock should be in Holdover state, which keeps the last known clock frequency and maintains it with a +/- 1ppb offset per day.

- Go to Monitoring>System>Clock>Recovered clock>Statistics.

```
    RX Packets                               ... (35266)
    Lost Packets                             ... (0)
    Out Of Order Packets                     ... (0)
    Buffer Underflow                         ... (0)
```

The ACR PW runs in 100 pps rate. Make sure that the Rx counter is indeed increasing at that rate. If PW packets are not received, you have to check the remote distribution unit status (part 2).

The lost packets ratio should be below 0.01%.

If lost or mis-ordered packets or buffer underflows are increasing, continue the testing using the packet loss (RAT Entry#6) or underflow procedures (RAT Entry #9).

1. Go to Monitoring>System>Clock>Current clock.
2. Check whether the current clock source is set to Recovered.

```
    Active Clock                             >   (Master)
    Source                                   >   (Recovered)
    Recovered ID                             ... (1)
```

➤ If the clock source is not set to Recovered:

1. Go to Configuration>System>Clock>Master clock.
2. Ensure that the Master clock is set to Recovered.

```
 1. Source                                   >   (Recovered)
 2. Revertive                                >   (Yes)
 3. Wait To Restore (sec)[1 - 720]           ... (1)
 4. Recovered ID[1 - 1]                      ... (1)
```

3. Go to Configuration>System>Clock>Recovered clock.
4. Ensure that the ACR is associated with the Adaptive Clock PW.

```
 1. Recovered ID[1 - 1]                      ... (1)
 2. Activity                                 >   (Enable)
 3. Type                                     >   (Adaptive)
 4. PW number[1 - 66]                        ... (1)
 5. Source quality                           >   (Stratum 1)
 6. Network type                             >   (Type A)
```

If the parameters above are correctly set, try restarting the ACR mechanism as explained below.

➤ To restart the ACR mechanism:

1. Go to Configuration>System>Clock>Master clock.
2. Change the Master clock source from Recovered to Rx Clock.

```
 1. Source                              >    (Rx Clock)
 2. Revertive                           >    (Yes)
 3. Wait To Restore (sec)[1 - 720]      ...  (1)
 4. Port type                           >    (E1)
 5. Port number [1 - 16]                ...  (1)
```

3. Save your changes.

4. Change the Master clock source back from Rx Clock to Recovered.

```
 1. Source                              >    (Recovered)
 2. Revertive                           >    (Yes)
 3. Wait To Restore (sec)[1 - 720]      ...  (1)
 4. Recovered ID[1 - 1]                 ...  (1)
```

Determining the Condition of the Clock Recovery PW on the Distribution Unit

In order to generate the Clock PW packets, the TDM interface that will be the clock source of the node should be in sync/up state.

➤ To determine the status of the Clock Recovery PW:

1. Go to Configuration > System > Clock > Master clock.

```
1. Source                               >    (Rx Clock)
...
4. Port type                            >    (ATM-155)
5. Port number[1 - 16]                  ... (1)
```

2. Go to Monitoring > System > Active alarms.

3. Make sure that the clocking interface is not in LOS condition.

4. If it is in LOS condition, try using an alternative clock port for the system clock (another E1 port, STM-1 port etc).

5. If another clocking port unavailable, make sure that the clocking interface is properly connected and that the clocking device connected to this port is operational. Validate physical connections by replacing wires, ports etc.

6. If the physical level is operating properly, go to Monitoring > Applications > Multiservice over PSN > PW > Status.

7. Ensure that the PW Operational status is Up and the local status is set to Forwarding.

```
    PW Number[1 - 66]                   ... (1)
    PW type                             >   (Clock Distribution)
    Operational status                  >   (Up)
    Local status                        ... (Forwarding)
    Local status faults                 ... (No faults)
    Remote status                       ... (N/A)
    Remote status faults                ... (-)
    Out PW Label[16 - 1048575]          ... (16)
```

8. If the PW Operational status is Down, continue investigating using the PW/VCCV-BFD Failure procedure (RAT Entry #3).

9. If the cause of the failure is still unknown, reboot the clock recovery unit.

➤ To reboot the clock recovery unit:

1. Go to Utilities and select Device Reset.
2. Press <Y> to confirm your request.

   The device resets.

```
Are you sure (Y/N)?
Confirm by pressing “y”, the device will reboot in 5 seconds.
```

Note *The entire device resets, causing service outage for the duration of the boot process and the PW sync time.*

If rebooting the device proves ineffective, replace the Recovery unit and contact Tech Support.

Physical Link Failures

Physical link failures may occur due to physical malfunction of the relevant interface either on the ACE unit or the device connected to it. It is also possible that the wire connecting the device is physically damaged or has been removed.

➤ To determine the source of the physical link failures:

1. Go to Monitoring>Applications>Multiservice over PSN>PW>Status.
2. Select the clock recovery PW index.
3. Go to Monitoring>System>Active alarms.
4. Identify the port reporting on the LOS state.

➤ If the relevant alarm report does not appear:

1. Go to Configuration>Physical layer>Port>E1/T1/STM-1/OC-3/GbE/ETH.
2. Verify that the relevant port is enabled.

```
  2. Port activation                     >    (Enable)
```

3. Go to Diagnostics>System>Self-test results.
4. Check that there is no failed component related to the faulty interface.

```
    Host memory                          ... (PASS)
    Packet memory                        ... (PASS)
    Parameter memory                     ... (PASS)
    Flash memory                         ... (PASS)
    Fast Ethernet access                 ... (PASS)
    E1/T1 framer access                  ... (PASS)
    TOD access                           ... (PASS)
```

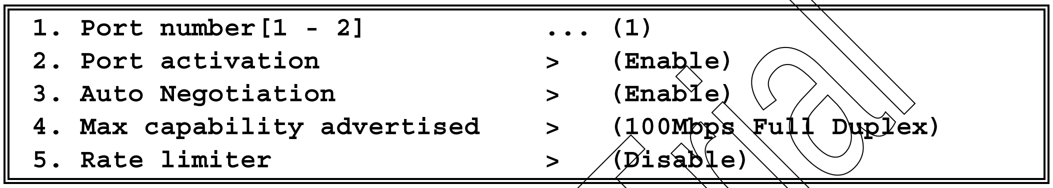
5. If Fail appears on the relevant interface, replace the unit or switch to the redundant Main Card.
6. Go to Configuration>System>Protection>Main card redundancy.

7. Select Switch to other Card.

   The redundant main card becomes active.

➤ In case of Ethernet interfaces:

1. Go to Configuration › Physical layer › Port › Ethernet.
2. Check that the Auto Negotiation, Speed and Duplex modes match the configured values on the access switch/router.



```
1. Port number[1 - 2]            ... (1)
2. Port activation               >   (Enable)
3. Auto Negotiation              >   (Enable)
4. Max capability advertised     >   (100Mbps Full Duplex)
5. Rate limiter                  >   (Disable)
```

3. Once the physical fault has been identified, continue with the following recovery actions:
   a. Replace the cable and check cable wiring.
   b. Use a different port on cross connecting/patch panel devices connected to the ACE.
   c. Check the connected device port physical layer.
   d. Replace the ACE unit.

PW Logical Failure

The reason for a PW failure may be related to one of the following sections:

- Physical layer fault of the underlying infrastructure
- Logical layer fault of the underlying transport protocols:
  - IP
  - PPPoE
  - LDP
  - VCCV-BFD logical failure.

Determining Physical Layer Faults

➤ To determine physical layer faults:

1. Go to Monitoring › Physical layer › Port › Ethernet › Status.
2. Ensure that the relevant ETH/GbE port carrying the PW is connected and synchronized at the highest supported speed.

```
    MAC address                      ... (00-20-D2-28-D1-AB)
    Mode                             >   (Full Duplex)
    Rate                             >   (100Mbps)
    Status                           >   (Connected)
```

➤ To continue the physical link failure analysis if the relevant PW is not connected:

1. Go to Monitoring >Physical layer >Port >Ethernet >**Statistics**.
2. Verify that traffic is transmitted and received by the relevant ETH/GbE port.

```
    Rx Correct frames                              ... (175)
    Rx Correct bytes                               ... (12220)
    Tx Correct frames                              ... (175)
    Tx Correct bytes                               ... (12220)
    Rx FCS errors                                  ... (0)
    Rx Congestion dropped                          ... (0)
    Rx Alignment errors                            ... (0)
    Single collisions                              ... (0)
    Multiple collisions                            ... (0)
    Deferred transmit                              ... (0)
    Late collisions                                ... (0)
```

3. Ensure that there are no errors, such as FCS, Rx alignment and collisions.

Errors indicate a problem on the physical layer (FCS errors) or duplex issues working opposite the access/switch router.

Massive FCS/collision errors will dramatically affect the ability of the PW to create a valid connection.

To determine logical layer faults of the underlying infrastructure, follow the instructions in the next section.

Logical Layer Faults

This section explains on identifying errors on IP (ARP), PPPoE, LDP and VCCV-BF.

IP (ARP)

➤ To determine logical layer faults on IP (ARP):

1. Go to Monitoring >Applications >Router >ARP table.
2. Verify that the remote device (Layer 2 networks) or default gateway MAC address was learnt by the local ACE unit.

```
  IP address       MAC address
  192.168.100.1    00-20-D2-2A-60-55
```

3. If this is not the case, attempt to ping the address in its subnet from the local ACE unit:

➤ To ping the remote device:

1. Go to Diagnostics >Applications >IP >**Ping**.
2. Specify the remote device's IP address and then select **Start**.

The local ACE unit starts pinging the remote device.

```
 1. Destination IP address                    ... (0.0.0.0)
 2. Infinite number of packets                >   (No)
 3. Number of Packets[1 - 10000]              ... (1)
 4. Payload Size[32 - 1450]                   ... (32)
 5. Start
```

➤ If no response is received:

1. Check that the remote device is properly connected and configured (IP addresses and routing).
2. Check the path connectivity using the trace route command.

➤ To use trace route to check the path connectivity:

1. Go to Diagnostics›Applications›IP›Trace Route.
2. Start the race route.

```
 1. Destination IP address                    ... (0.0.0.0)
 2. Start
```

PPPoE

In the case of PPPoE, you must have an operational PPPoE session active.

➤ To determine logical layer faults on PPPoE:

1. Make sure to have an operational PPPoE session active.
2. Go to Monitoring›Logical layer›PPPoE.

```
    Session status                       >   (Down)
    Session id                           ... (0)
    Remote MAC                           ... (00-00-00-00-00-00)
    Local MAC                            ... (00-00-00-00-00-00)
    Actual back-off[sec]                 ... (0)
    PPP LCP status                       >   (Down)
    PPP IPCP status                      >   (Down)
    PPP authentication                   >   (None)
    Local IP                             ... (0.0.0.0)
    Remote MRU                           ... (0)
```

3. Check the status of the PPPoE session and what negotiation parts opposite the BRAS/LNS were completed successfully.
4. In case the local IP is not received, check the credential allocation for the session on the RADIUS server.

➤ To check the credential allocation:

1. Go to Configuration›Logical layer›PPPoE.

```
 1. ID[1 - 4]                                 ... (-)
 2. AC name                                   ... (-)
 3. Service name                              ... (-)
 4. Scheduled restart                         >   (-)
 5. Back-off random range[sec][0 - 600]       ... (-)
 6. Minimum authentication level              >   (-)
 7. Username                                  ... (-)
 8. Password                                  ... (-)
 9. Confirm password                          ... (-)
10. VLAN tagging                              >   (-)
```

2. Reenter the user name and the password for the session in order to restart the PPPoE session.
3. Check the minimum authentication level (CHAP/PAP) to match the security settings on the LNS.

LDP

This applies if LDP is used to exchange PW and tunnel labels.

➤ To monitor the LDP:

- Go to Monitoring › Applications › MPLS › LDP › Hello.

```
LDP ID         Peer LDP ID         Type     Interval   Time left
```

VCCV-BFD

The VCCV-BFD is a keep-alive mechanism that monitors the path between the PW devices and is used to extend failure messages between units.

In case the BFD fails to receive the keep-alive message in the given time-frame, a proper notification is sent and the PW is disabled (Down).

➤ To analyze the status of the BFD mechanism:

- Go to Monitoring › Applications › Multiservice over PSN › PW › Status.

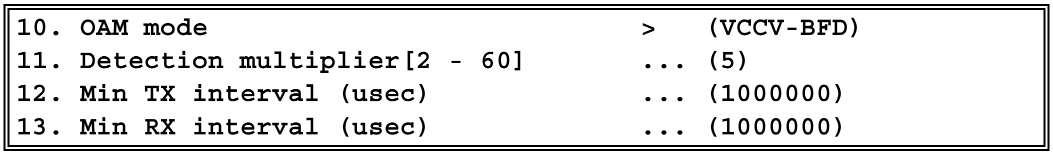
```
    PW Number[1 - 66]                      ... (2)
    PW type                                >   (ATM VP N to 1)
    VCCV_BFD status                        >   (Up)
```

There are four basic states for the BFD mechanism:

- Init: The BFD failed to receive any BFD messages from the remote unit. Check if on the remote unit BFD is enabled.
- Control-detection-time-expired: The local system did not get BFD packets from each other at the predefined time interval. Check the network path between the ACE unit and the remote unit.

  Increase the detection multiplier and the Min Tx interval to see if the alarm can be cleared.

  - To access the Detection Multiplier and Min TX parameters, go to Configuration › Applications › Multiservice over PSN › PW › General parameters.



```
10. OAM mode                            >   (VCCV-BFD)
11. Detection multiplier[2 - 60]        ... (5)
12. Min TX interval (usec)              ... (1000000)
13. Min RX interval (usec)              ... (1000000)
```

- Neighbor-signaled-session-down: The remote system does not get the BFD packets from the local system. The local system gets BFD packets from the remote system.

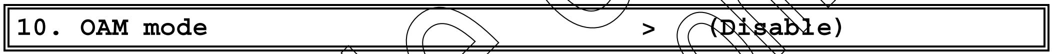
  Check if BFD messages are indeed received on the remote unit. If not continue using the same PW procedure on the remote unit.

- No-diagnostic: Both the local system and the remote system get the BFD packets from each other at the predefined time interval.

  If the BFD keep-alive cannot synchronize, disable the BFD on both PW units to overrule possible network filtering of the messages.

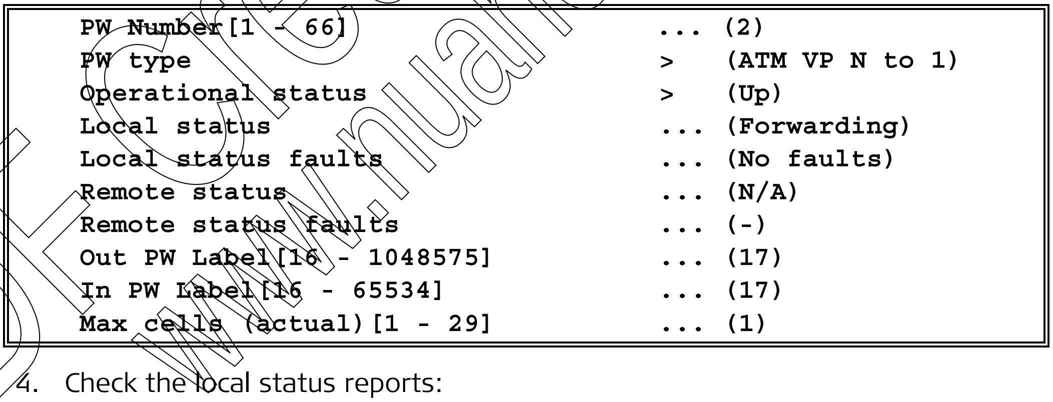
➤ To disable the BFD:

1. Go to Configuration › Applications › Multiservice over PSN › PW › General parameters and set OAM Mode to Disable.



```
10. OAM mode                            >   (Disable)
```

2. If VCCV_BFD status is Up, check the network filtering, as the firewall may be blocking VCCV-BFD messages.
3. In case BFD is not activated, go to Monitoring › Applications › Multiservice over PSN › PW › Status.



```
    PW Number[1 - 66]                    ... (2)
    PW type                              >   (ATM VP N to 1)
    Operational status                   >   (Up)
    Local status                         ... (Forwarding)
    Local status faults                  ... (No faults)
    Remote status                        ... (N/A)
    Remote status faults                 ... (-)
    Out PW Label[16 - 1048575]           ... (17)
    In PW Label[16 - 65534]              ... (17)
    Max cells (actual)[1 - 29]           ... (1)
```

4. Check the local status reports:

   PSN-RX Fault - The reasons that the PW Local Status is PSN RX Fault can be one (or more) of the following:

   - The BFD is Down-Detection time expired.
   - The Physical link which carries the PW is disconnected.

5. If in Forwarding state, go to Monitoring › Applications › Multiservice over PSN › PW › Statistics.
6. Check whether there are Tx packets toward PSN side and also Rx packets (provided that the Attachment Circuit is generating traffic).

```
    ETH Port 1   PW type ATM VP N to 1
    RX packets                              ... (0)
    RX congestion dropped                   ... (0)
    TX packets                              ... (473)
    TX congestion dropped                   ... (0)
    TX timeout                              ... (0)
    Packet loss event                       ... (0)
    Mis-order dropped packets               ... (0)
    Reordered packets                       ... (0)
    Unknown VP/VC cells                     ... (0)
```

➤ If packets have not been received, proceed as follows:

1. Check PW In/Out labels on both end PW devices.
2. Go to Configuration › Applications › Multiservice over PSN › PW › General parameters and change the In/Out labels used on the end points to another value to rule out duplication issues.

```
5. Out PW label[16 - 1048575]               ... (17)
6. In PW label[16 - 65534]                  ... (17)
```

3. Check if the LDP mode is used. An LDP PW ID means that it is activate.
4. To check on the LDP mode, go to Configuration › Applications › Multiservice over PSN › PW › General parameters.

```
4. Provisioning mode                        >   (LDP PW id)
```

5. In LDP/MPLS mode, change the Tunnel label/Label range.
6. Check whether the LDP PW ID is the same on both end PW devices and whether it is unique to the PW identified below:
7. To view the PW parameters, go to Configuration › Applications › Multiservice over PSN › PW › General parameters.

```
4. Provisioning mode                        >   (LDP PW id)
5. PW ID[1 - 4294967295]                    ... (5)
```

8. If the situation remains unchanged, check the path connectivity connecting the PW end points, either by enabling BFD or validating the path using the PSN OAM tools.

Device Disconnected

The device is no longer reachable remotely (telnet/SNMP/Web)

Note *In case of remote management loss to the ACE unit, you should use a local serial connection to analyze the problem.*

Management failure can be related to:

- Management path disconnected
- Incorrect access parameters
- Failure of the Management plane in the ACE unit.

Management Path Disconnections

Do the following:

1. Check that the physical interface used to manage the unit is active.
   - If inactive, follow the Physical Link failure procedure.
2. Check if there is ping connectivity from the management system to the ACE unit and vice versa:

➤ To perform the ping test:

1. Go to Diagnostics › Applications › IP › Ping.
2. Enter the IP address of the ACE unit and select Start.

```
1. Destination IP address          ... (Manager IP Address)
2. Infinite number of packets      >   (No)
3. Number of Packets[1 - 10000]    ... (1)
4. Payload Size[32 - 1450]         ... (32)
5. Start
```

If the ping times out, continue using the Trace Route option as follows:

1. Go to Diagnostics › Applications › IP › Trace Route.
2. Enter the IP address of the ACE unit and select Start.

```
1. Destination IP address          ... (0.0.0.0)
2. Start
```

3. Check network connectivity issues and firewall settings.
4. Check whether the ACE unit's router Interface (host IP) is configured correctly:.
5. To check the router interface, go to Configuration › Applications › Router › Interface.

```
1. Number[1 - 32]                      ... (1)
2. Name                                ... (Interface-1)
3. IP address                          ... (192.168.100.2)
4. IP mask                             ... (255.255.255.0)
```

6. Make sure that the correct routes are defined on the ACE unit to enable it to reach the management network.
7. To do so, go to Configuration › Applications › Router › Static route.

```
1. IP address                          ... (192.168.100.1)
2. IP mask                             ... (255.255.255.0)
3. Next hop                            ... (0.0.0.0)
4. Next hop interface number[1 - 32]   ... (1)
```

Incorrect Access Parameters

➤ To verify management access parameters:

1. Go to Configuration › System › Management › Management access.

```
 1. SNMP                                   >   (Enable)
 2. Telnet                                 >   (Enable)
 3. WEB                                    >   (Enable)
```

2. For SNMP access, check that the communities settings match those on the Management system.

   To do so, go to Configuration › System › Management.

```
 7. Read community                       ... (public)
 8. Write community                      ... (public)
 9. Trap community                       ... (public)
```

3. For SNMP access, make sure that the Management system's IP address is defined under the device manager list.

   To do so, go to Configuration › System › Management › Manager list.

```
 1. IP address                           ... (192.168.100.154)
 2. Trap mask                            >   (None)
```

4. Make sure that the specific managed interface is enabled for management.

   To do so, go to Configuration › Applications › Router › Interface.

```
 8. Management access                    >   (Enable)
```

Failure of the Management Plane in the ACE Unit

If the procedures the parameters are properly configured, capture alarms and log file:

1. Go to Monitoring › System › Active Alarm
2. Go to Monitoring › System › Event log › View event log.
3. Restart the device and contact tech support.
   - To restart the device, go to Utilities and select Reset Device.

```
Are you sure (Y/N)?
Confirm by pressing "y", the device will reboot in 5 seconds.
```

Loss of ATM Cells

ACE units may discard cells for the following reasons:

- Physical line errors (CRC errors)
- Policing/Shaping issues.
- Rx congestions
- Packet loss/missorder.

Physical Line Errors

In case of physical line errors, cells might be discarded due to bad HEC. To monitor RX, TX and HEC cells, do the following:

1. Go to Monitoring > Applications > ATM > Port.

```
    TX cells                        ... (0)
    RX cells                        ... (0)
    Uncorrected HEC cells           ... (0)
```

2. Perform a physical loopback on the monitored port and generate cells from the adjacent ATM device. To start the physical loopback, go to Diagnostics > Physical layer > Physical Loopback.

```
 1. Port type                             >    (E1)
 2. Port number[1 - 16]                   ...  (1)
 3. Loopback operation                    >    (External)
```

3. If the problem persists, replace the cable connecting the devices.
4. If the problem still persists, replace the ACE unit.
5. Check whether the ATM interface is reporting LCD (loss of cell delineation). To do so, go to Monitoring > System > Active alarms and look for the LCD event.

Policing/Shaping Issues

In case of an Rx congestion drop, it is possible that the error is related to shaping settings. Continue using the Rx congestion failure procedure.

If the number of policing discarded frames is increasing, the settings of the policing mechanism may cause the loss of cells.

```
    RX congestion dropped                 ... (0)
    Policing disc(0)                      ... (0)
    Policing disc(0+1)                    ... (0)
```

➤ To check the ATM policing parameters:

1. Go to Configuration > Applications > Multiservice over PSN > PW > Service parameter > Attachment circuit.

   The Attachment Circuit menu appears with the In TD parameter.

```
6. In TD[0 - 99999]                       ... (3)
```

2. Take a note of the In TD parameter.
3. Go to Configuration > Applications > ATM > Traffic descriptor (TD).
4. Enter the TD index you noted from the PW In TD.

```
1. Traffic descriptor number[1 - 99999]     ... (3)
2. Service category                         >   (CBR)
3. Mode                                     >   (Policing)
```

Before changing any TD settings, consult with the network planning /architecture division, as you will need a specific TD value. The choice of this value may also affect unrelated network services.

Rx Congestions

The loss of cells can also be experienced due to Rx congestions. In order to determine this, go to Monitoring >Applications >Multiservice over PSN >PW >Statistics.

```
                                            ... (N)
RX congestion dropped                       ... (0)
```

- Continue using the Rx congestion failure procedure.

Packet loss/Misorder

Check the Packet Loss Event counter to examine the amount and frequency of the misordered packets. To do so, go to Monitoring >Applications >Multiservice over PSN >PW >Statistics.

```
   Packet loss event                       ... (0)
```

- Continue using the Packet loss/Misorder failure procedure.

Packet Loss/Packets Mis-order

Packet loss/mis-order events are usually caused by the PSN network carrying the PW packets. The most common causes are congestions, BW bottlenecks, and poor queuing performance, etc.

The ACE unit can easily identify these impairments and some corrective measures can be taken on the ACE unit to minimize or eliminate them.

➤ To enable detecting packet loss and misorder:

- Go to Configuration >Applications >Multiservice over PSN >PW >General parameters and enable Sequence Number.

```
8. Sequence number                       >   (Enable)
```

If Sequence Number is disabled, packet loss and misorder cannot be detected.

Packet Mis-ordering

➤ To check for the amount and frequency of mis-ordered packets:

- Go to Monitoring >Applications >Multiservice over PSN >PW >Statistics.

```
Press (N) to see more counters
Mis-order dropped packets              ... (0)
Reordered packets                      ... (0)
```

Reordered packets are originally mis-ordered packets, which have been returned to the correct order by the ACE device.

Mis-order dropped packets are packets, which could not be reordered by the ACE unit.

➤ To configure packet reordering:

1. Go to Configuration>Applications>Multiservice over PSN>General>ATM parameters.
2. Make sure to enable PW Reordering.

```
 1. PW miss-order window size (packets)      >   (4)
 2. PW reordering                            >   (Enable)
```

For TDM PWs the reorder feature is enabled by default.

If both the mis-ordered dropped packets counter and the reorder counter are increasing, the mis-order window size might be too small. Increase the mis-order window size. Note that increasing the window size will add delay.

In order to reduce the chance of mis-order, try increasing the gap between consecutive frames transmitted by the ACE unit. This can be controlled by increasing the timeout and/or the max cell per packet (concatenation) in ATM PWs or the payload size in TDM PWs:

➤ To access the concatenation parameter in ATM PWs:

- Go to Configuration>Applications>Multiservice over PSN>PW>Service parameters.

```
 1. MAX cells concatenation[1 - 29]       ... (1)
 2. Timeout mode                          >   (Enable)
 3. PW timeout (usec) [100 - 5000000]     ... (100)
```

➤ To access the payload size parameter in TDM PWs

- Go to Configuration>Applications>Multiservice over PSN>PW>Service parameters.

```
 1. payload size (frames in packet)[2 - 256]     ... (8)
    payload size (bytes)                         ... (248)
```

➤ If no change is detected in performance:

1. Correct the network performance.
2. Make sure that QoS is active for traffic transmitted towards the PSN.

➤ To correct for packet loss:

1. Check the following counter to examine the amount and frequency of lost packets. To do so, go to Monitoring>Applications>Multiservice over PSN>PW>Statistics.

```
ATM PWs
    Packet loss event                         ... (0)
TDM PWs
    Missing packets                           ... (0)
```

2. Check that frames are not being discarded on the ETH/GbE physical level on both the receiving ACE unit and the transmitting device:
3. Go to Monitoring > Physical layer > Port > Ethernet > Statistics.

```
    Rx Correct frames                          ... (643666)
    Rx Correct bytes                           ... (189088942)
    Tx Correct frames                          ... (643763)
    Tx Correct bytes                           ... (189097238)
    Rx FCS errors                              ... (0)
    Rx Congestion dropped                      ... (0)
```

4. Check that the transmitting device is not losing any packets due to transmit congestion events that are eventually reported as missing packets on the receiving device.
5. Go to Monitoring > Applications > Multiservice over PSN > PW > Statistics.

```
    TX congestion dropped                     ... (0)
    TX timeout                                ... (0)
```

6. Reduce the throughput of the transmitted traffic to help minimize the packet loss events caused by BW/congestions on the network.

Note

- *Reducing the overall transmitted throughput will always cause an increase of the delay.*
- *All changes must be performed on both units simultaneously.*
- *Service will be unavailable until both the receiving and the transmitting devices are properly configured.*

➤ To access the max cells concatenation parameter (ATM):

- Go to Configuration > Applications > Multiservice over PSN > PW > Service parameters.

```
 1. MAX cells concatenation[1 - 29]       ... (1)
 2. Timeout mode                          >   (Enable)
 3. PW timeout (usec) [100 - 5000000]     ... (100)
```

➤ To access the payload size parameter (TDM):

- Go to Configuration > Applications > Multiservice over PSN > PW > Service parameters.

```
 1. payload size (frames in packet)[2 - 256]    ... (8)
    payload size (bytes)                       ... (248)
```

With regard to packet loss, check the following:

MTU

- Check that the MTU transmitted by the ACE does not exceed the smallest MTU configured in the network

QoS

- Check that QoS is enabled on the network for the PW traffic on the entire path (end –to-end) and in both directions.
- If VLAN is used, check that the expected VID and p bits are configured on the PW.
- If MPLS EXP bits are used, check that the expected EXP bits are configured under the PW.
- If IP TOS is used, check that the expected TOS byte is configured correctly.
- Go to Configuration›Applications›Multiservice over PSN›PW›PSN parameters.

```
    PW number [1 - 66]                  ... (2)
    PW name                             ... (Data)
    PSN type                            >   (MPLSoIP)
 1. TOS[0 - 255]                        ... (0)
 2. EXP bits[0 - 7]                     ... (0)
 3. VLAN tag                            >   (Enable)
 4. VLAN ID[0 - 4094]                   ... (0)
 5. VLAN priority[0 - 7]                ... (0)
```

Power Supply and Fan Failure

If the log file reports a power supply failure or a fan failure, do the following:

1. Go to Monitoring›System›Event log›View event log OR

   Under the active alarms list, go to Monitoring›System›Active alarms.
2. Identify the unit that reports the failure.
3. Go to Inventory.

```
        Index  Description
     1. 1001   RAD.ACE-3200.Chassis
     2. 4001   RAD.ACE-3200.PS
     3. 4003   RAD.ACE-3200.Fan
```

Note *The power supply and the fan tray can only be replaced in ACE-3400/3402/3600 units. In case of ACE-3100/3200/3105/3205/3220, the entire unit must be replaced*

Changing the Fan Tray

After removing a faulty fan tray, the new fan tray must be inserted immediately.

➤ To remove the fan tray:

1. Using a flathead screwdriver, unscrew the two screws that tighten the tray to the unit.
2. Carefully pull the fan tray out of the chassis.

➤ To install the new fan tray:

1. Carefully check the fan tray for foreign objects and dirt that may have been trapped inside, and remove them.
2. Insert the fan tray in the left chassis slot, and slide it in until its rear connector engages the mating connector on the backplane.
3. Secure the fan tray by tightening its two screws using a flathead screwdriver.

Changing the Power Supply Module

➤ Before deciding on changing the PS module:

- Verify there was no momentary power failure causing a PS flip
- Check that the power source is operative.

➤ To remove a hot-swappable power supply unit:

1. Make sure to disconnect the power supply cable before removing the power supply module.
2. Using a flathead screwdriver, unscrew the two tightening screw that secure the unit to the chassis.
3. Carefully pull and remove the power supply unit from the chassis.

➤ To install the hot-swappable power supply unit:

1. Carefully slide the new power supply unit into its slot until the unit's rear connector engages the mating connector on the backplane, and the power supply unit fits into its place.
2. Using a flathead screwdriver, secure the PS unit with the two tightening screws.

Connecting to AC Power

AC power is supplied to ACE-3400, ACE-3402 via a 3-prong plug. AC power should be supplied through the 1.5m (5 ft) standard power cable terminated by a 3-prong plug. The cable is provided with the unit.

Two power cables may be connected to the unit simultaneously.

Redundant Main Modules (MC)

ACE-3600, ACE-3400 and ACE-3402 allow installing two main modules to ensure continuous operation when one module is reset, restarted, or stops operating for any reason. In such cases, the redundant main module immediately takes over the unit, using its own pre-configured settings.

This protective mechanism is available provided that the following conditions are met:

- The two installed main modules are identical, in terms of both their hardware and software versions.
- Configuration database is identical.
- Inter-module communication is valid.
- Redundancy support is activated (configured to ON).

The Standby MC cannot be viewed while offline.

➤ **To verify that the requirements protective mechanism (redundancy) are met:**

HW Version

1. Go to Inventory.
2. Scroll to the right using CTRL+R.

```
        HW revision     FW revision      1.1-C\0-A
```

Note *Inspecting the Standby main module (offline card), the hardware would require a forced redundancy flip that might affect data.*

3. Go to Configuration › System › Protection › Main card redundancy.
4. Switch to the other card.
5. In case of a mismatch between the installed hardware versions, replace the standby MC.

SW Version

1. Go to Inventory.
2. Scroll to the right using CTRL+R.

```
    Name                SW revision
 1  ACE-3400            5.20B2T1/Boot-3.00-233MHz
```

Note *Inspecting the Standby MC (offline card), the hardware would require a forced redundancy flip that might affect data.*

3. Go to Configuration › System › Protection › Main card redundancy.
4. Switch to the other card.
5. In case of a mismatch between the installed SW versions, replace the standby MC.

Configuration Database

➤ To ensure that the DB on both MC is identical:

1. Go to Configuration › System › Protection › Main card redundancy.
2. Select Configuration update to other card.

    The configuration update is followed by Standby MC reset.

MC Redundancy is Configured to ON

The redundancy can deactivated if desired. In order to enable an automatic switch over, the redundancy must be enabled (ON).

➤ To enable the redundancy:

- Go to Configuration › System › Protection › Main card redundancy.

```
 1. Card redundancy                              >    (On)
```

➤ To monitor redundancy data:

- Go to Monitoring › System › Protection › Card redundancy.

```
    Active main card              >    (Card B)
    Redundancy status             >    (Configuration mismatch)
```

Card Absent A/B

If the MC module is physically missing, check if the reported missing MC was removed. If not, replace the reported MC.

Communication Loss

A loss of communication may be reported in the following cases:

- A new main card module is inserted and not yet initialized.
- Reset to other card or a Configuration Update to the Other Card command was executed.
- A problem in the communication between the two main modules has occurred.

If none of the above are the cause of the communication loss, try resetting the Standby MC.

➤ To reset the Standby MC:

1. Go to Configuration › System › Protection › Main card redundancy.
2. Reset the other card.

If the error persists, replace the MC in question.

Hardware mismatch

In cases in which the two main modules do not have the same hardware version, replace the main module so that the HW versions are compatible.

Software mismatch

In cases in which the two main modules do not have the same software version, update the software as explained below.

➤ To update the software version:

1. Go to Configuration › System › Protection › Main card redundancy.
2. Select Software Update to other card.

Configuration mismatch

In cases in which the two main modules do not have the same configuration, update to the other card configuration.

➤ To update card configuration:

1. Go to Configuration › System › Protection › Main card redundancy.
2. Select Configuration Update to other card.

➤ To extract the log file:

1. Go to Monitoring › System › Event log › View event log.
2. Alternatively, under the active alarms list, go to Monitoring › System › Active alarms.

   In case of consecutive switch over between modules, try to increase the Wait to Restore time. This defines the length of delay required between two consecutive switch operations. The WTR time can be changed only when the redundancy protection is turned off.
3. To change the WTR, go to Configuration › System › Protection › Main card redundancy and under WTR time, specify a different time.

```
1. Card redundancy                        >    (On)
2. WTR time (sec)[1 - 60]                 ...  (5)
```

4. If this error persists, contact Tech Support.

Underruns – TDM Pseudowire

The Jitter buffer failed to compensate PSN packet delay variations.

Note *The PDV (Packet Delay Variation) Buffer is used to compensate for PDV in PSN networks. When the network PDV exceeds the configured depth of the Jitter buffer, an Underrun will occur, resulting in jitter buffer re-initialization process.*

Underruns may also be related to clocking mis-configuration or a fault of the remote TDM interface, which results in a termination of transmission.

➤ To correct PDV related underruns:

1. Go to Monitoring>Applications>Multiservice over PSN>PW>Statistics.

```
    ETH Port 1   PW type Basic CES PSN
    RX packets                          ... (13293)
    TX packets                          ... (40771)
    Missing packets                     ... (0)
    Mis-order dropped packets           ... (0)
    Reordered packets                   ... (0)
    Malformed packets                   ... (0)
    Jitter buffer underrun              ... (1)
```

2. Observe the frequency of the Jitter buffer underruns.
   - In cases where they periodically recur, continue investigating the clocking settings and the topology.
   - The frequency of the Underruns can be easily analyzed using the log file. In cases where a specific pattern cannot be identified, continue as follows:
3. Go to Monitoring>System>Event log>View event log.

```
  2008-07-16  10:01:25 | Underrun    End        PW 3
  2008-07-16  10:01:25 | PW          Up         3 - 3
  2008-07-16  10:01:24 | Rx R=1      Start      PW 3
| 2008-07-16  10:01:24 | Underrun    Start      PW 3
v 2008-07-16  10:01:24 | PW          Down       3 - 3
  2008-07-16  10:00:23 | Rx R=1      End        PW 3
  2008-07-16  09:50:33 | Underrun    End        PW 3
  2008-07-16  09:50:33 | PW          Up         3 - 3
  2008-07-16  09:50:32 | Rx L|M=100  End        PW 3
  2008-07-16  09:50:04 | Rx R=1      Start      PW 3
```

   - Rx R=1 means that the remote unit was experiencing Underrun condition.
   - Rx L|M=100 means that the remote unit is reporting on failure on the TDM interface.
   - When Rx L|M is up together with Underrun event, continue with the fault on the remote TDM interface procedure.
   - In case the missing packets counter is also increasing along with the underruns, it is possible that the underruns are simply caused by the massive packet loss events and not by high PDV.
   - In this case, continue using the packet loss troubleshooting procedure.
4. Check that the ETH/GbE uplink is running at Full-Duplex mode:
5. Go to Monitoring>Physical layer>Port>Ethernet>Status.

```
    MAC address                      ... (00-20-D2-2A-60-55)
    Mode                             >   (Full Duplex)
```

6. Increase the jitter buffer configured depth.

   The configured jitter buffer cannot be changed on the fly, which means it would require deleting the relevant PW.

7. Go to Configuration >Applications >Multiservice over PSN >PW >Service parameters.
8. Check the current jitter buffer settings.

```
2. Jitter buffer (usec)[1000 - 32000]    ... (3000)
```

9. Go to Configuration >Applications >Multiservice over PSN >PW.

```
 1. PW number [1 - 66]                    ... (3)
 2. PW name                               ... (Voice)
 3. General parameters                    >
 4. PSN parameters                        >
 5. Service parameters                    >
```

10. Select Remove and confirm your request.
11. Recreate the PW using the new jitter buffer settings. While choosing a new value, the addition in ms to the previously configured value will be added to the overall end-to-end delay.
12. Ensure there is no degradation on the service level (echo, protocol outages, etc).

If increasing the buffer to its maximum size did not help, it is required to identify the network element, which is causing the high PDV values. High PDV values can be caused by the following:

- LAN Congestions
- Overloaded queuing mechanisms
- Routing tables updates
- Load sharing
- Re-Route events

Clock Related Underruns

In cases where the underruns are periodic, their occurrence might be related to incorrect clocking configuration.

Review the elements active clocking settings to rule out a situation where there is more than one clock source in the network.

➤ To rule out more than one clock source in the network:

- Go to Monitoring >System >Clock >Current clock.

```
 Active Clock                >   (“the current active clock”)
```

If the active clock does not fit the clocking scenario, continue troubleshooting by indentifying the Primary clocking interface; as follows:

1. Go to Configuration >System >Clock >Master clock.

```
 1. Source                               >    (Rx Clock)
 2. Revertive                            >    (Yes)
 3. Wait To Restore (sec)[1 - 720]       ... (1)
 4. Port type                            >    (E1)
 5. Port number[1 - 16]                  ... (1)
```

2. Check the physical status of the clocking interface and continue using the Physical Link failure procedure.
3. In case the ACR is not functioning properly (when configured) continue using the ACR failure procedure.

Fault on the remote TDM interface related underruns

If the underrun is also associated with the Rx L|M=100 alarm, check the status of the remote DATA interface (not the clocking interface). To do so, do the following:

- Go to Monitoring>Physical layer>Port>E1.

```
   LOS        ... (0         FEBE                ... (0)
   LOF        ... (0)        BES                 ... (0)
   LCV        ... (0)        DM                  ... (0)
   LCD        ... (0)        ES                  ... (0)
   RAI        ... (0)        SES                 ... (0)
   AIS        ... (0)        UAS                 ... (0)
                             Rx frame slips      ... (0)
```

If LOS or AIS are increasing, the attached PW will not be sending traffic to the remote unit.

1. In case of LOS, continue using the Physical Link failure procedure.
2. In case of AIS, check the connected equipment for the reason it is generating AIS towards the ACE unit.

Rx Congestions

This may occur if the buffer located between the PW packets towards the ATM has overflowed.

Note *The Rx Congestion dropped counter represents the number of packets dropped due to congestion on the receive direction, i.e. from the PSN side to the ATM direction.(Packet Delay Variation) Buffer is used to compensate for PDV in PSN networks.*

➤ To check the Rx Congestion counter for amount and frequency of dropped packets:

- Go to Monitoring>Applications>Multiservice over PSN>PW>Statistics.

```
RX congestion dropped                    ... (0)
```

Possible causes:

- ATM BW issues
- Insufficient PSN→ATM buffer size
- Shaping problems
- Bursty traffic coming from the remote device.

ATM Bandwidth issues

Check that the ATM attachment circuit related to the PW is providing the expected amount of bandwidth:

IMA

Check the number of E1 links belonging to the IMA group:

1. Go to Configuration › Applications › ATM › IMA.

```
11. Links in group                        >    (1)
```

2. Go to Monitoring › Applications › ATM › IMA › Group status.
3. Check the number of active links in the IMA group.

```
    Active TX links                       ... (1)
    Active RX links                       ... (1)
```

4. Go to Monitoring › Applications › ATM › IMA › Group status and check the available cell rate of the IMA group.

```
... (N)
    Available TX cell rate                ... (4489)
    Available RX cell rate                ... (4489)
```

5. In case the available cell rate is lower than expected from the group, continue with the IMA failure procedure.

STM-1/CO-3 (155)

1. Go to Configuration › Physical layer › Port › ATM-155.
2. Check that the output cell rate is not lower than the expected transmission rate.

```
5. Output rate (cps)[100 - 353208]        ... (353208)
```

Insufficient PSN→ATM buffer size

The PSN-to-ATM buffer size is determined according to the number of cells per packet using the following formula:

ATM buffer [cells] = [max cell per frame] x 50

➤ To increase the buffer size:

1. Go to Configuration >Applications >Multiservice over PSN >PW >Service parameters.
2. Increase the MAX cell concatenation value

```
   1. MAX cells concatenation[1 - 29]           ... (1)
```

Shaping problems

In case the traffic transmitted to the ATM side is shaped by the ACE unit, check the shaping parameters configuration:

1. Check the PW Traffic Descriptor (TD) index.
2. Go to Configuration >Applications >Multiservice over PSN >PW >Service parameter >Attachment circuit.

```
7. Out TD[1 - 99999]                    ...  (1)
```

3. Check the TD index parameters
4. Go to Configuration >Applications >ATM >Traffic descriptor (TD).

```
Traffic descriptor number[1 - 99999]    ...  (1)
Service category                        >    (CBR)
```

Before changing the TD settings, please advise network planner/architecture, as this might affect other services.

Bursty traffic coming from the remote device

There might be a situation in which the remote unit is receiving traffic on the ATM user interface at a rate that is causing temporary burstiness, which cannot be handled by the receiving unit's ATM→PSN buffer.

In these cases, possible solutions include enabling policing on the remote ACE unit in order to allow the ATM traffic to be policed before transmitting to the PSN.

➤ To define a new Policing TD on the remote ACE:

- Go to Configuration >Applications >ATM >Traffic descriptor (TD).

```
 1. Traffic descriptor number[1 - 99999]     ... (1)
 2. Service category                         >   (CBR)
 3. Mode                                     >   (Policing)
```

Another solution would be enabling the shaping on the ATM device connected to the remote ACE unit so that the bursty ATM traffic is shaped before being transmitted to the ACE unit.

IMA Failure

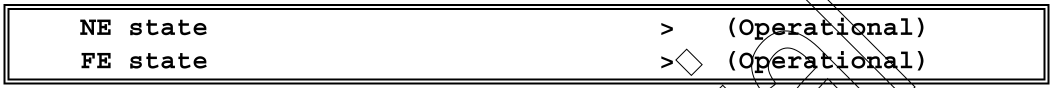
Full or partial failure of the IMA group may be caused by the following events:

- Physical failure of the E1/T1 links in the IMA group

- Number of active links is below the minimal number configured
- Large differential delay between links in the group
- Problem in the IMA control protocol (ICP) between the two machines
- Clocking problems.

➤ To check the status of the IMA group:

- Go to Monitoring>Applications>ATM>IMA>Group status.



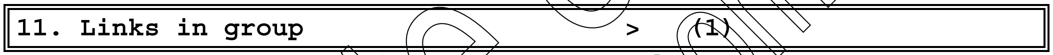
```
    NE state                                 >   (Operational)
    FE state                                 >   (Operational)
```

If the group is not operational, continue below:

Physical Failure

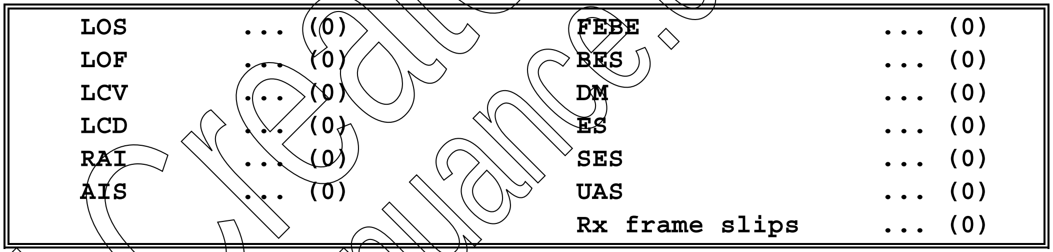
➤ To determine which links are enabled for the problematic IMA group:

1. Go to Configuration>Applications>ATM>IMA.



```
11. Links in group                         >   (1)
```

2. Go to Monitoring>Physical layer>Port>E1.



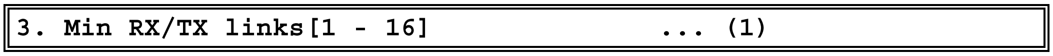
```
    LOS       ... (0)             FEBE              ... (0)
    LOF       ... (0)             BES               ... (0)
    LCV       ... (0)             DM                ... (0)
    LCD       ... (0)             ES                ... (0)
    RAI       ... (0)             SES               ... (0)
    AIS       ... (0)             UAS               ... (0)
                                  Rx frame slips    ... (0)
```

In case of LOS alarm, continue investigation using the Physical Link failure procedure.

Minimal Number of Active Links

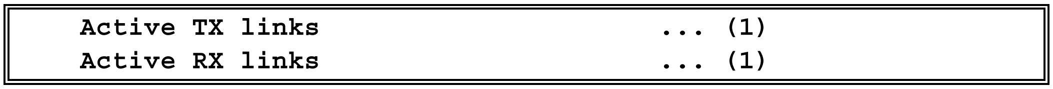
➤ To check the number of minimal active links in the IMA group:

1. Go to Configuration>Applications>ATM>IMA.



```
3. Min RX/TX links[1 - 16]                   ... (1)
```

2. Check the actual number of active links.
3. Go to Monitoring>Applications>ATM>IMA>Group status.



```
    Active TX links                          ... (1)
    Active RX links                          ... (1)
```

In case of a lower number, try to reduce the Min Rx/Tx links under the IMA configuration to a lower value in order to allow the operating links to restore the IMA group.

Differential delay

➤ To check the current observed maximum differential delay between the IMA links:

1. Go to Monitoring › Applications › ATM › IMA › Group status.

```
... (N)
    Max observed differential delay     ... (0)
```

2. Check the value does not exceeds the maximum differential delay allowed.
3. Go to Configuration › Applications › ATM › IMA.

```
  6. Max differential delay (ms)[1 - 100]    ... (25)
```

If the observed value is higher than the permitted one, increase the allowed maximum differential delay.

Clocking issues

➤ To check the clocking configuration on the IMA group:

- Go to Configuration › Applications › ATM › IMA.

```
9. Common TX clock source                  >   (System)
```

If set to system, check the status of the current clock as follows:

1. Go to Monitoring › System › Clock › Current clock.

```
    Active Clock                           >   (Master)
    Source                                 >   (Recovered)
    Recovered ID                           ... (1)
```

2. Check that the settings of the clock match the clock settings on the opposite unit.

Clocking issues might also cause OIF (Out of IMA Frame) irregularities (except during SES or UAS IMA at the near end).

- Go to Monitoring › Applications › ATM › IMA › Link statistics.

```
OIF                                        ... (0)
```

IMA protocol issues

➤ To check that the Group ID is the same on the ACE IMA and remote IMA group:

- Go to Configuration › Applications › ATM › IMA.

```
4. Group ID[0 - 255]                       ... (0)
```

Check that the IMA protocol version is the same on the ACE IMA group and the remote IMA group:

- Go to Configuration › Applications › ATM › IMA.

```
8. IMA version                          >    (1.1)
```

In case there are problems in the IMA control plane (ICP cells), check the following:

1. Go to Monitoring>Applications>ATM>IMA>Link statistics.

```
    Violation                           ... (0)
```

2. Check the number of ICP cells that are in error, invalid or missing.
3. Go to Configuration>Applications>ATM>IMA.

```
12. Restart group
Confirm by pressing "Y"
```

The IMA group restarts.

4. Restart the group on the opposite device connected to the ACE unit.
5. If the problem persists, physically disconnect all active links and reconnect them.
6. If the problem still persists, reset the ACE unit:
7. Go to Utilities.

```
 2. Device reset
 Are you sure (Y/N)?
```

If the problem still persists, contact Tech Support.

6.7 Frequently Asked Questions

Q Does ACE-3600 support ATM over PSN and ATM switching at the same time?

A Yes, both function types are supported by the unit and can be utilized simultaneously.

Q What kinds of AAL types does ACE-3600 support over a packet-switched network?

A ACE-3600 supports all AAL type (AAL1, AAL2, and AAL5) and transfers them via the PSN transparently.

Q What exactly is the timeout mechanism?

A When using the ATM cell concatenation mechanism, ACE-3600 stores the data cells until the maximum number of concentrated cells is reached. TDM traffic, however, requires continuous delivery of data. Accordingly, ACE-3600 uses the timeout mechanism to reduce the cell storage time before encapsulated data is sent towards the PSN. The timeout delay value can be set between 100 to 5,000,000 microseconds. The timer accuracy is +500 microseconds.

Q In packet-switched traffic, what triggers the sending of a packet?

A ACE-3600 has several trigger of sending packet towards the PSN:

- When reaching the maximum cells concatenation number
- When the timeout timer has expired
- When the end of AAL5 (SDU bit=1, configurable) is received.

Q How can an ATM VPs (virtual paths) be mapped to a pseudowire?

A Any ATM VP can be mapped to a PW using 1:1 mode (1 VP per PW) or N:1 mode (N VPs per PW).

Figure 6-48 demonstrates how VPs can be mapped to pseudowires in the 1:1 encapsulation mode (for more information, refer to *Appendix E*).

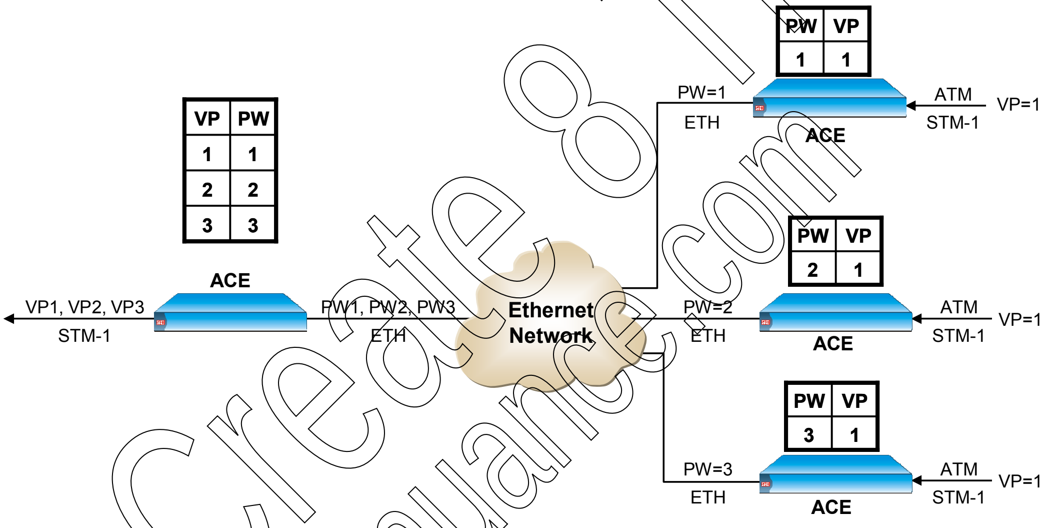


Figure 6-48. VP Mapping to PW

Q What kind of QoS does ACE-3600 support over packet-switched networks?

A ACE-3600 complies with 802.1p and 802.1q for L2 (VLAN), EXP bits of MPLS and for the ToS/DSCP of the IP layer. You can assign a QoS to each PW (configurable).

Q How can one calculate the required Ethernet bandwidth for a PW based on the ATM parameters?

A Bandwidth utilization depends on the ATM connection rate, mapping methods (VPoPSN or VCoPSN), network type (L2/MPLS or IP), VLAN existence and number of concatenated cells. A calculator that calculates the bandwidth based on these parameters can be obtained from *Technical Support*.

Q How can end-to-end OAM be maintained over a packet-switched network?

A ACE-3600 transfers transparent End-to-End OAM over the PSN. You can set the Intermediate mode for the OAM Descriptor, in order to instruct ACE-3600 to transparently forward the ATM OAM cells as user data over the PSN . For more information, refer to *Chapter 4* and *Appendix F*.

Q How does the pseudowire connectivity check (VCCV-BFD) works?

A BFD control messages are generated by both the local and remote ACE units, on both directions of the pseudowire. When the local ACE unit does not receive control messages from the remote ACE unit during a number of transmission intervals, it declares that the PW on its receive (RX) direction is down. The PW then enters a defect forwarding state on the local ACE unit. In addition, the local ACE generates "control-detection-time-expired" packets towards the remote ACE, and the remote ACE replies with "neighbor-signal-session-down" packets. For more information, refer to *Appendix F*.

Q What is "Misorder" in the context of packet-switched traffic?

A In packet-switched traffic, some packets are not received according to their predefined sequence number. This condition is defined as misorder. Accordingly, to allow proper de-capsulation of ATM/TDM traffic, ACE-3600 has a mechanism that fixes this condition by re-ordering the received packets correctly.

You can enable or disable the ordering mechanism, and also set the 'number of packets' window (0, 1, 2, 4, 8, 16 or 32 packets) in which ACE-3600 will try to fix erroneous packet sequences (misorders). For more information, refer to *Chapter 4*.

6.8 Technical Support

Technical support for ACE-3600 can be obtained from the local distributor from whom it was purchased.

For further information, please contact the RAD distributor nearest you or one of RAD's offices worldwide. This information can be found at RAD's Web site: http://www.rad.com/ (for offices location, click **About RAD** > **Worldwide Offices** ; for distributors location, click **Where to Buy** > **End Users**).

Appendix A

Connector Pinouts

This appendix details the various connector pinouts available in ACE-3600.

A.1 STM-1/OC-3c or GbE SFP Connector

Figure A-1 illustrates the fiber optic connectors of the SDH/SONET (ATM-155) or GbE interface, using SFP transceivers:

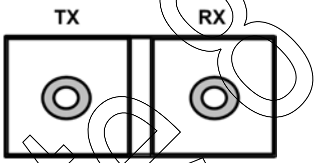


Figure A-1. TX/RX Optical Connectors Diagram (in an SFP unit)

For the specifications of RAD's SFP transceivers, refer to *Table 1-1* in Chapter 1.

A.2 Electrical Gigabit Ethernet Connector

The Gigabit Ethernet connector is provided via an SFP transceiver. RAD's SFP-9G (if ordered) has an electrical 1000BaseT connector, wired as follows (using a 4-pair twisted cable):

Table A-1. Electrical Gigabit Ethernet Port in SFP-9G

Pin	Function
1	A+
2	A –
3	B+
4	C+
5	C –
6	B –
7	D+
8	D –

A.3 Management Ethernet Connector

ACE-3600 has one Ethernet port for out-of-band management, with an RJ-45 connector.

Table A-2. Ethernet RJ-45 Connector Pin Assignment

Pin Designation		Description
1	ETH_RX_P	RX+
2	ETH_RX_N	RX-
3	ETH_TX_P	TX+
4	Not connected	–
5	Not connected	–
6	ETH_TX_N	TX-
7	Not connected	–
8	Not connected	–

A.4 Station Clock Connector

The station clock port is an E1/T1-compliant balanced (75Ω) port. The port's wiring, however, allows the sharing (optional) of the station clock source with other devices via a special split cable connection. This split physical connection enables tracking of the timing signals that originate from the received E1/T1 data (cascading loop connection). The port's incoming data is for timing purposes only.

Table A-3 specifies the station clock connector wiring and *Figure A-2* illustrates how the clock source can be shared.

Table A-3. Station Clock RJ-45 Connector Pin Assignment

Pin Designation		Description
1 STA_R_TIP		RX+
2 STA_R_RIN	G	RX-
3 Not	connected	–
4	STA_T_TIP	Tx+ for cascading loop the incoming data
5	STA_T_RING	Tx- for cascading loop the incoming data
6 Not	connected	–

Table A-3. Station Clock RJ-45 Connector Pin Assignment (Cont.)

Pin Designation		Description
7	TTL input	Input signal (TTL level), for unbalanced interface identification
8	GND	Grounding

Note *For an unbalanced (120Ω) E1 clock source connection, use only the RAD adapter cable (CBL-RJ45/2BNC/E1). Other adapter cables may not have the required wiring for detecting the current of the unbalanced interface. For the connection instructions, refer to Connecting to an Unbalanced E1 Clock Source in Chapter 2.*

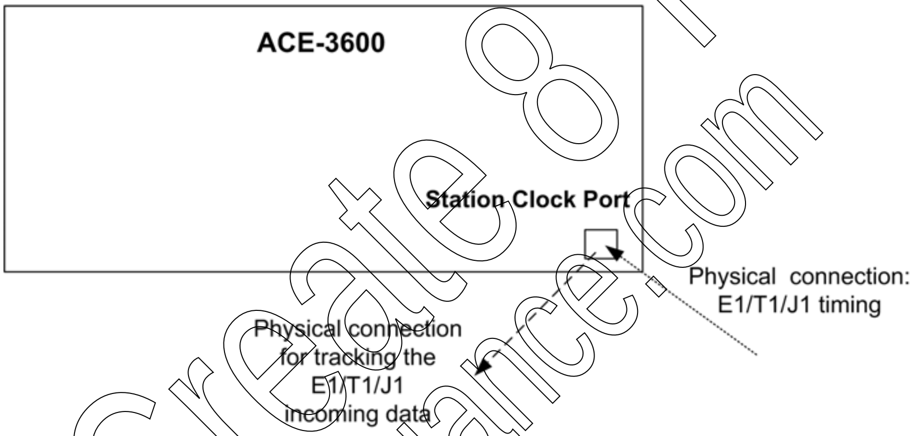

ACE-3600
Station Clock Port
Physical connection: E1/T1/J1 timing
Physical connection for tracking the E1/T1/J1 incoming data

Figure A-2. Station Clock Sharing

Only an experienced technician should make this kind of physical cable connection. For more information, contact technical support.

A.5 Control Connector

The control connector of ACE-3600 is an RJ-45 8-pin female connector with a serial RS-232 DCE interface, intended for connection to an ASCII-based terminal. Connector pin functions are listed in *Table A-4*.

- To connect a supervision terminal that has a 9-pin connector to the control connector, use the appropriate adapter cable (CBL-RJ45/D9/F/STR, supplied). *Figure A-3* shows the wiring diagram of this cable.

Table A-4. Control Connector RJ-45 Pin Assignment

Pin	Function
1	GND
2	Not connected
3	Receive Data (RXD) from terminal
4	Not connected
5	Transmit Data (TXD) to terminal
6	Not connected
7	GND
8	Not connected

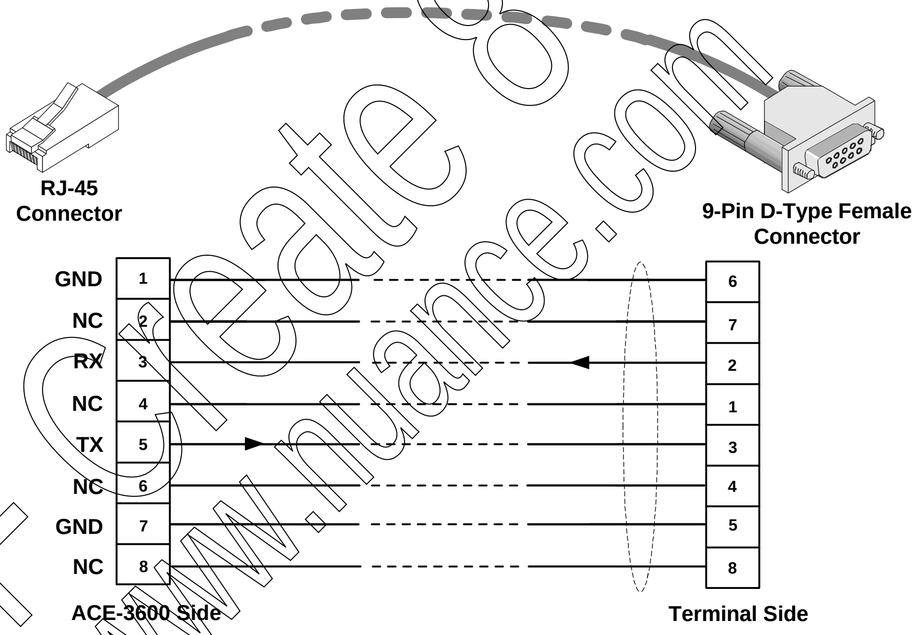


Figure A-3. Wiring of RJ-45 to DB-9 Adapter Cable (CBL-RJ45/D9/F/STR)

Appendix B

Boot Management

B.1 Introduction

This appendix provides a description of the ACE-3600 boot procedure via an ASCII terminal for downloading the boot software.

The ACE-3600 software is stored in the flash memory of two sections: the **boot sector** and the **file system**.

- Boot sector – contains a boot program that ACE-3600 loads initially. Once loaded, it calls up the rest of the program from the file system.
- File system – contains up to two compressed copies of the unit's application code. One application copy is called the **operating file**, and the other (if exists) is called the **backup file**. The operating file is the default-executable ACE-3600 application code. The backup file is used whenever the operating file is absent or corrupted.

Caution

- The boot code of the device should not be tampered with. It should ONLY be handled by authorized personnel, or after contacting RAD Technical Support.
- Formatting the file system means deleting all files in the system, including the software-operating main, backup and configuration files.

B.2 Booting ACE-3600

ACE-3600 boots up automatically. After powering up, no user intervention is required, except when the user wishes to access the file system to modify or update the ACE-3600 application software.

Boot Sequence

The following is a description of the boot sequence. If the system is working normally, the entire process is completed within two minutes as follows:

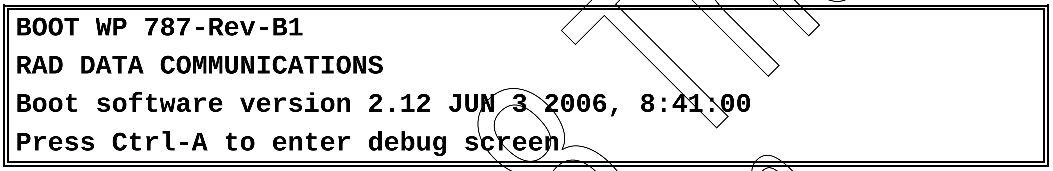
1. The boot program searches for the operating file in the file system. If the file exists, the program continues.
   - If the operating file does not exist, the boot program searches for the backup file. If the backup file is found, it is used instead of the operating file and the boot process continues.

- If there is no backup file, you must download a file via the XMODEM protocol or via TFTP. The received file is saved as the operating file in the file system.

2. Files in the file system are compressed and automatically decompressed into the RAM before execution begins.
3. After decompression, the software starts to execute and the user can begin working.

Using the Boot Options

When ACE-3600 is turned on, the first screen that appears is the main boot screen.

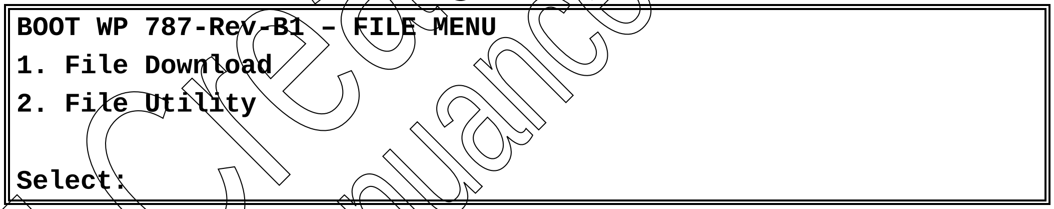


```
BOOT WP 787-Rev-B1
RAD DATA COMMUNICATIONS
Boot software version 2.12 JUN 3 2006, 8:41:00
Press Ctrl-A to enter debug screen
```

Figure B-1. Main Boot Screen

If during the boot Ctrl-A is not pressed, the boot proceeds as described in *Boot Sequence* on page *B-1*.

If during the boot Ctrl-A is pressed, the boot options screen appears.



```
BOOT WP 787-Rev-B1 – FILE MENU
1. File Download
2. File Utility

Select:
```

Figure B-2. Boot Options Screen

Performing File Download

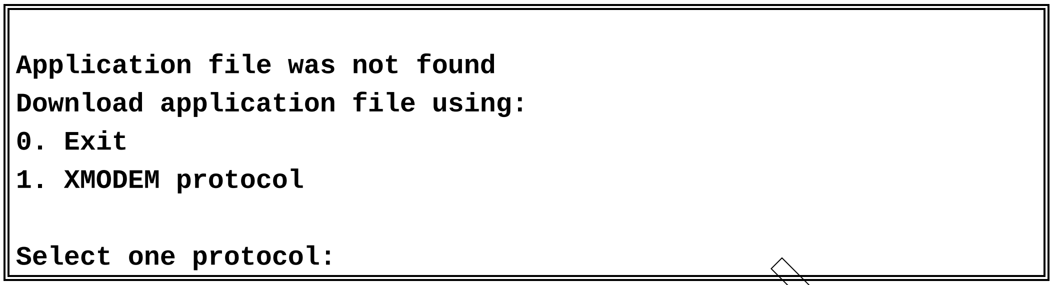
File downloading allows you to download a new software application file (a newer or a previous version) into the unit using the XMODEM protocol. In order to use this functionality, two conditions must apply:

- No application file exists
- File Download was selected after Ctrl-A was pressed.

➤ To download an application file:

- Type 1 in the boot options screen (see *Figure B-2*).

  The download options appear.



```
Application file was not found
Download application file using:
0. Exit
1. XMODEM protocol

Select one protocol:
```

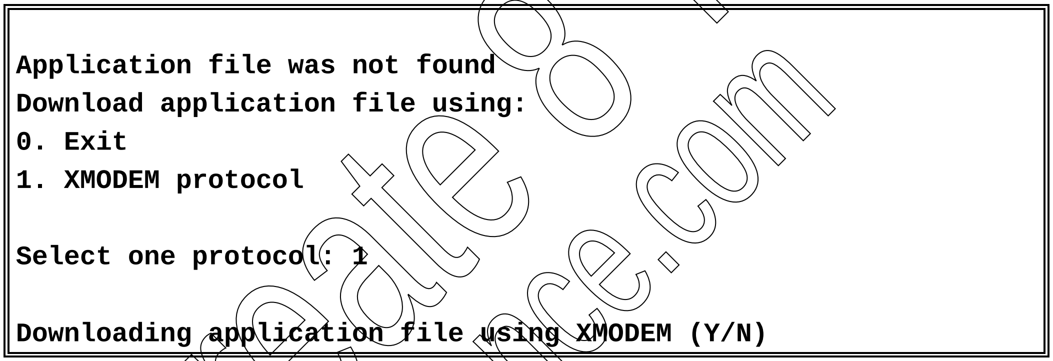
Figure B-3. Application Download Options

Downloading via XMODEM

➤ To download an application file via XMODEM:

1. Select XMODEM Protocol from the application download options.

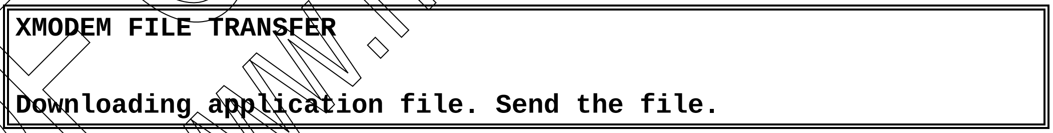
   A confirmation message appears.



```
Application file was not found
Download application file using:
0. Exit
1. XMODEM protocol

Select one protocol: 1

Downloading application file using XMODEM (Y/N)
```

2. Type Y.

   The XMODEM File Transfer screen appears and downloading begins from the XMODEM designated source.



```
XMODEM FILE TRANSFER

Downloading application file. Send the file.
```

Figure B-4. XMODEM File Transfer Screen

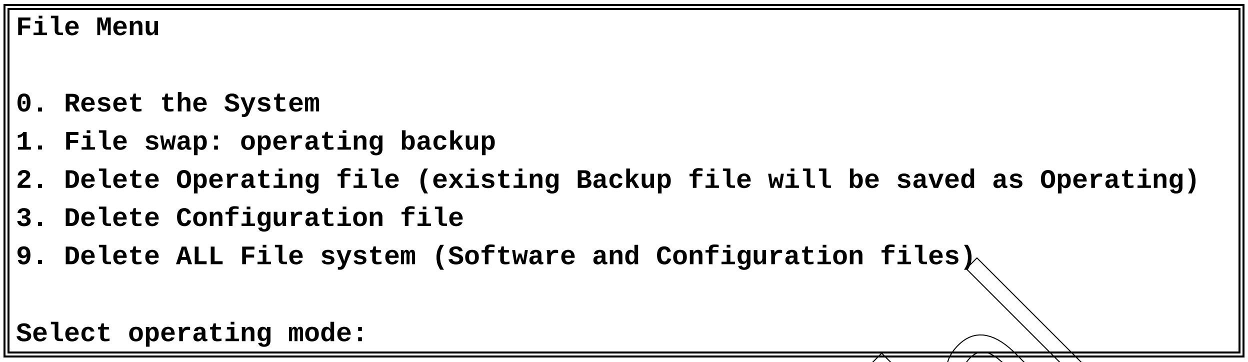
Using the File Menu

The File Menu allows you to perform basic file transfer operations. These operations are optional.

➤ To access the File Menu:

- In the boot options screen (see *Figure B-2*), type 2.

  The File Menu appears.



```
File Menu

0. Reset the System
1. File swap: operating backup
2. Delete Operating file (existing Backup file will be saved as Operating)
3. Delete Configuration file
9. Delete ALL File system (Software and Configuration files)

Select operating mode:
```

Figure B-5. File Menu

From the File Menu you can:

- Reset the system by pressing 0.
- Perform a swap of the operating and backup files by pressing 1.
- Delete the operating file by pressing 2. In such a case, the backup file automatically becomes the operating file.
- Delete all configuration files by pressing 3.

Caution Deleting the configuration files voids all configuration settings made for the unit.

- Format the files system by pressing 9.

Caution Formatting the file system means deleting all files in the system, including the software-operating main, backup and configuration files.

If you choose to exchange or delete files, an appropriate confirmation message is displayed. The operation is carried out once you press Y.

Appendix C

ATM OAM Functionality

C.1 Introduction

ACE-3600 provides F4 and F5 ATM OAM support that complies with ITU-I.610.

The main OAM features of ACE-3600 are:

- Each side of a VP/VC cross-connection (connection point) can be set as an intermediate or segment endpoint, according to its OAM descriptor.
- The ATM host or CES connection is set as a VC endpoint (end-to-end or segment point).
- A segment endpoint can run a Continuity Check (CC) mechanism per connection point in Source mode, Sink mode or both.
- AIS state is declared upon AIS, LOC or physical failure detection, and ends after no failure is detected for 3.5 seconds.
- OAM cells are inserted into the cell stream ahead of the shaper.
- OAM loopback cells can be used to determine connectivity at specific points in a network or between networks, including packet-switched networks on which ATM traffic is encapsulated.

C.2 OAM Modes of Operation over ATM

There are five modes in which OAM can operate over ATM networks:

- *VP Intermediate Point*
- *VC Intermediate Point*
- *VP Segment Point*
- *VC Segment Point*
- *VC End-to-End Point*.

VP Intermediate Point

When a VP connection point (CP) is set as an intermediate point, it operates as follows:

- If the other side of the VP XC is also set as an intermediate point:
  - F4 segment, F5 segment and end-to-end OAM cells are forwarded transparently to the other side of the XC.

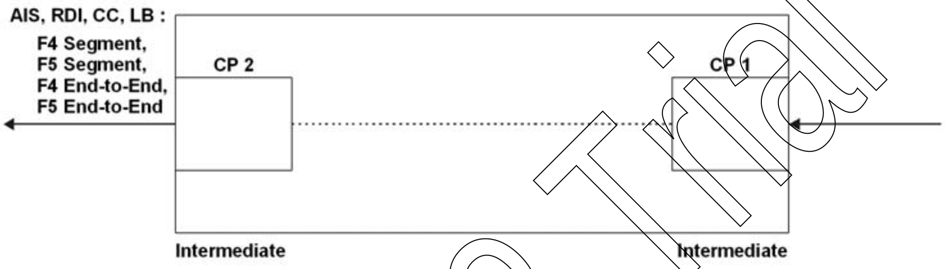


Figure C-1. VP Intermediate Point – Case A

  - When a failure is detected on the physical port, AIS state is declared and F4 segment AIS and end-to-end AIS cells are generated towards the forward direction.

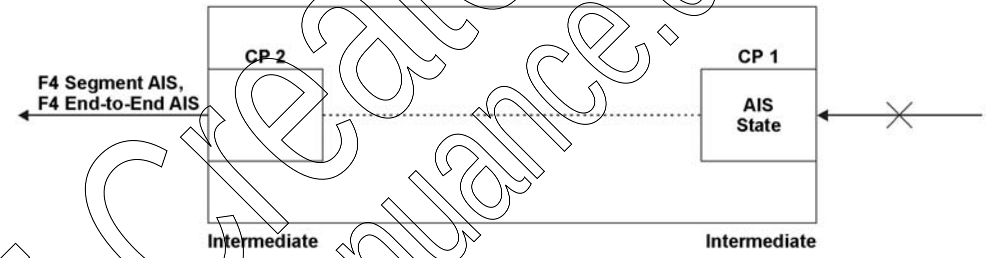


Figure C-2. VP Intermediate Point – Case B

- If the other side of the VP XC is set as a segment point:
  - F4 end-to-end, F5 segment and F5 end-to-end OAM cells are forwarded transparently to the other side of the XC. F4 segment OAM cells are dropped from the cell stream, while F4 segment AIS, RDI and CC cells are counted.

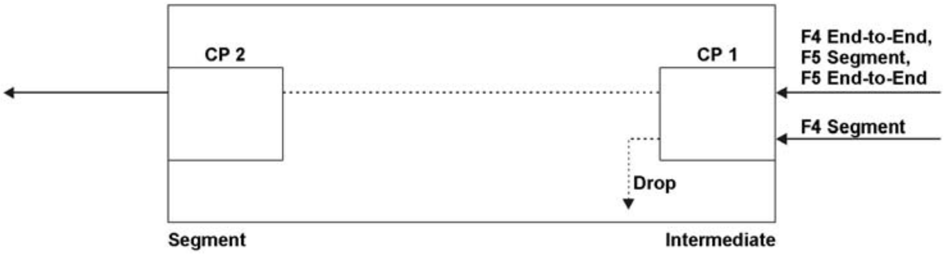


Figure C-3. VP Intermediate Point – Case C

- When a failure is detected on the physical port, AIS state is declared and F4 end-to-end AIS cells are generated towards the forward direction.

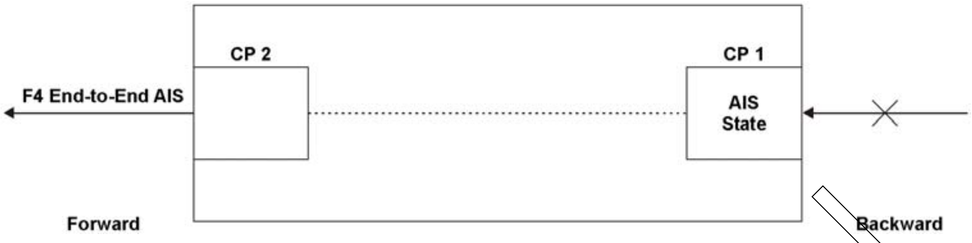


Figure C-4. VP Intermediate Point – Case D

- For OAM loopback cells (see *C.3 OAM Loopback*), an ID match check determines the loopback state:

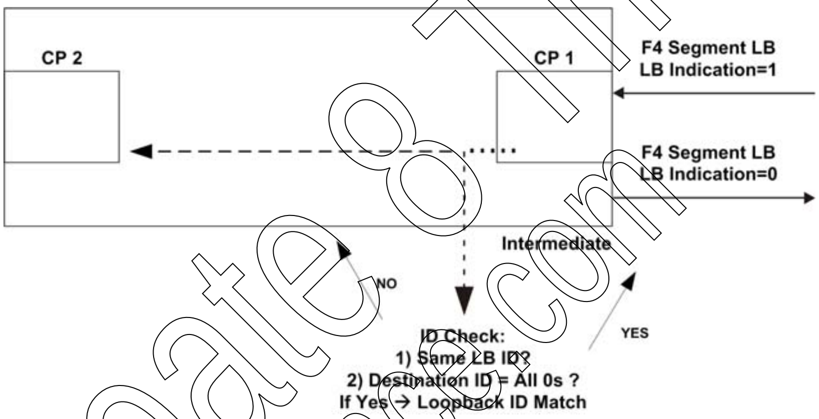


Figure C-5. VP Intermediate Point – Case E

VC Intermediate Point

When a VC connection point is set as an intermediate point, it operates as follows:

- If the other side of the VC XC is also set as an intermediate point:
  - F5 segment and end-to-end OAM cells are forwarded transparently to the other side of the XC. F4 segment and end-to-end OAM cells are dropped from the cell stream.

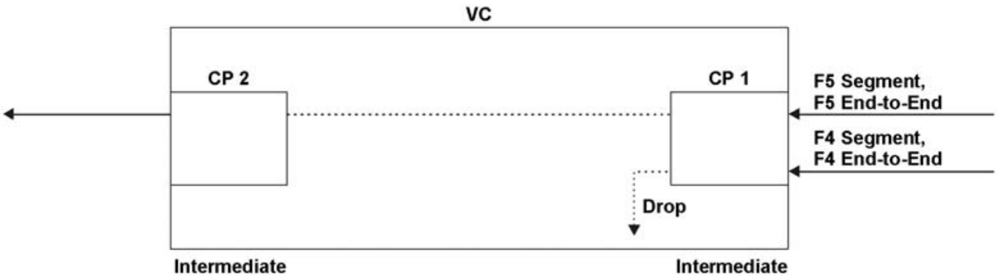


Figure C-6. VC Intermediate Point – Case A

  - When a failure is detected on the physical port, AIS state is declared and F5 segment AIS together with end-to-end AIS cells are generated towards the forward direction.

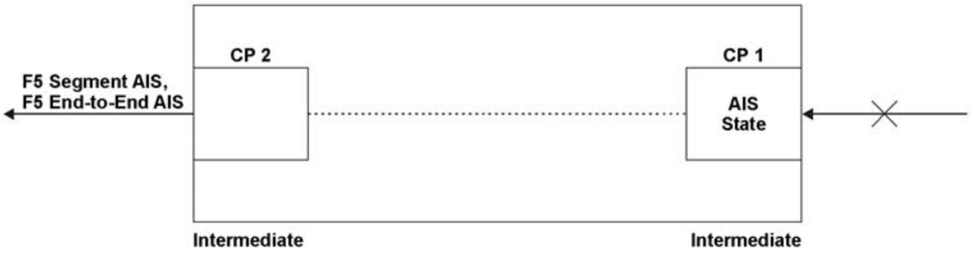


Figure C-7. VC Intermediate Point – Case B

- If the other side of the VC XC is set as a segment point:
  - F5 end-to-end OAM cells are forwarded transparently to the other side of the XC. F4 segment and end-to-end and F5 segment OAM cells are dropped from the cell stream.

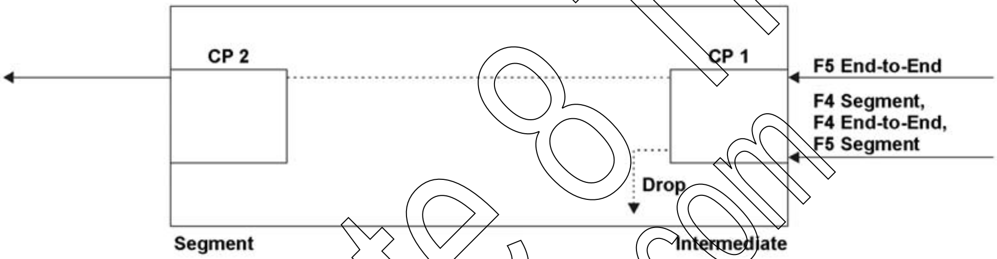


Figure C-8. VC Intermediate Point – Case C

- When a failure is detected on the physical port, AIS state is declared and F5 end-to-end AIS cells are generated towards the forward direction.

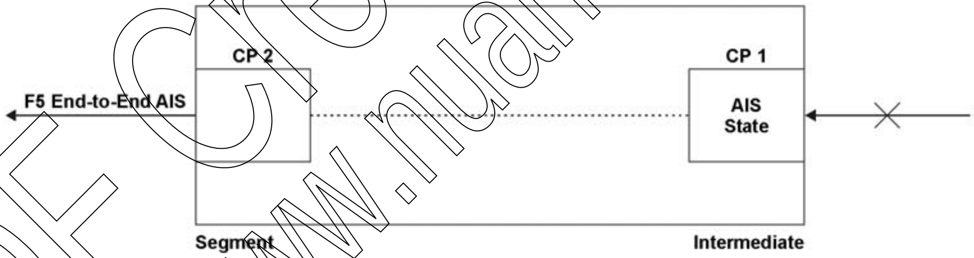


Figure C-9. VC Intermediate Point – Case D

- For OAM loopback cells (see *C.3 OAM Loopback*), an ID match check determines the loopback state:

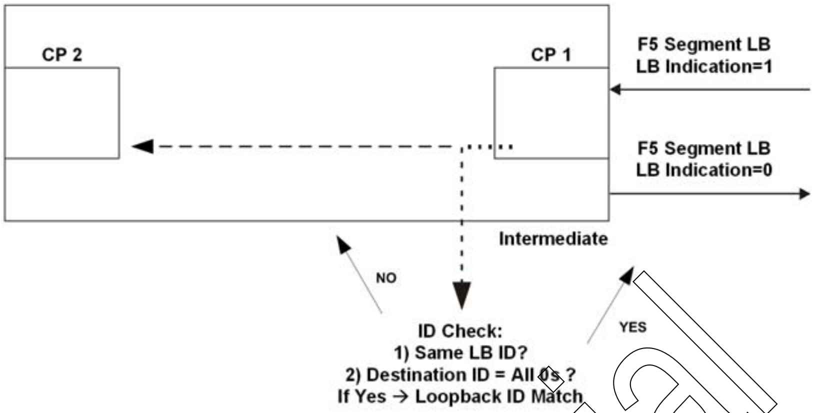


Figure C-10. VC Intermediate Point – Case E

VP Segment Point

When a VP connection point is set as a segment point, it operates as follows:

- F4 end-to-end, F5 segment and end-to-end OAM cells are forwarded transparently to the other side of the XC. F4 segment OAM cells are dropped from the cell stream, while F4 segment AIS, RDI and CC cells are monitored.

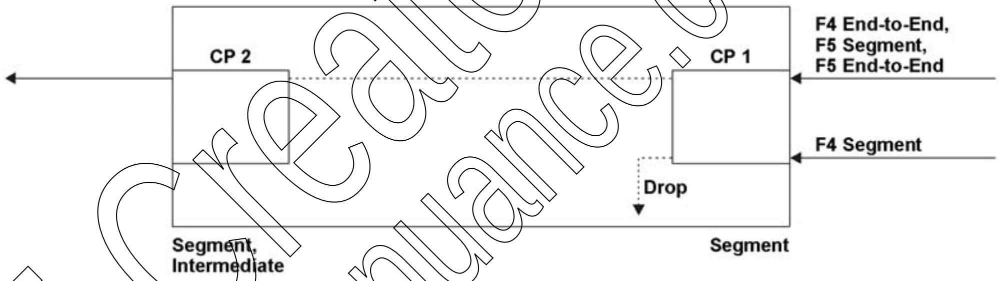


Figure C-11. VP Segment Point – Case A

- When F4 segment AIS cells are received on the connection point, AIS state is declared. F4 end-to-end AIS cells are generated towards the forward direction, while F4 segment RDI cells are generated towards the backward direction.

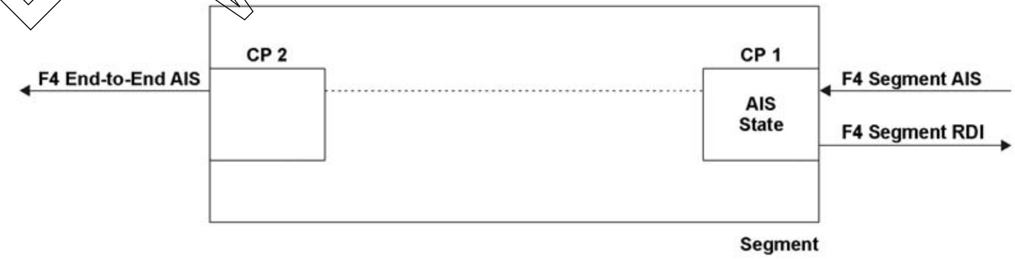


Figure C-12. VP Segment Point – Case B

- When a failure is detected on the physical port, AIS state is declared. F4 end-to-end AIS cells are generated towards the forward direction, while F4 segment RDI cells are generated towards the backward direction.

Figure C-13. VP Segment Point – Case C

- When a VP segment point is set as a CC source point, F4 segment CC cells are generated towards the backward direction.

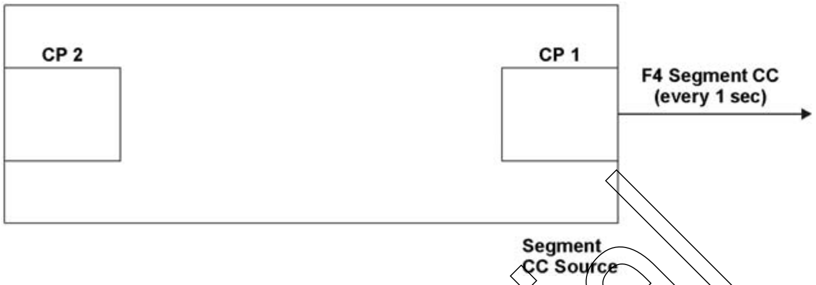


Figure C-14. VP Segment Point – Case D

- When a VP segment point is set as a CC sink point, F4 segment CC cells are expected to be received every second. If no CC cell has been received during the last 3.5 seconds, an AIS state is declared, F4 end-to-end AIS cells are generated towards the forward direction and F4 segment RDI cells are generated towards the backward direction.

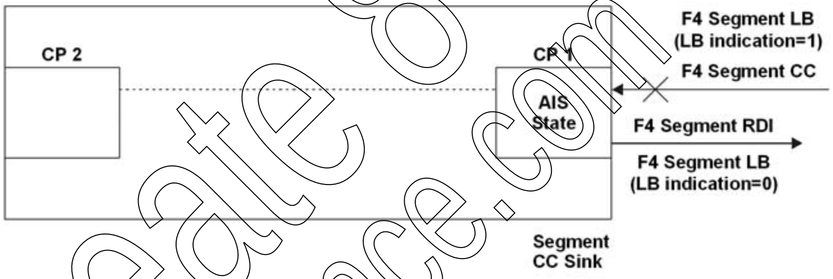


Figure C-15. VP Segment Point – Case E

- When a VP segment point is set as CC both, it behaves both as source and sink point.
- For OAM loopback cells (see *C.3 OAM Loopback*), an ID match check determines the loopback state (see *Figure C-16*), and delays are calculated if the loopback cell has been authenticated and returned within 5 seconds (see *Figure C-17*):

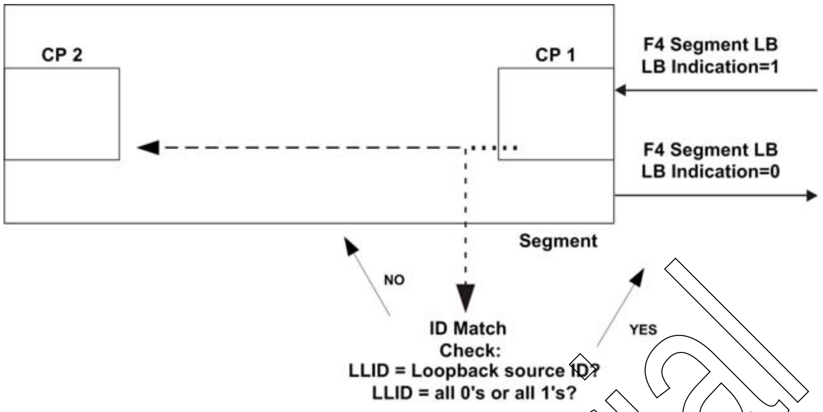


Figure C-16. VP Segment Point – Case F

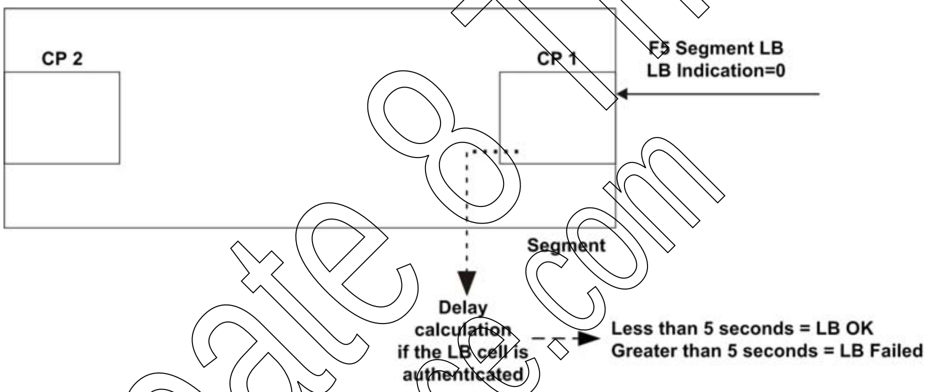


Figure C-17. VP Segment Point – Case G

VC Segment Point

When a VC connection point is set as a segment point, it operates as follows:

- F5 end-to-end OAM cells are forwarded transparently to the other side of the XC. F4 segment, F5 segment and end-to-end OAM cells are dropped from the cell stream, while F5 segment AIS, RDI and CC cells are monitored.

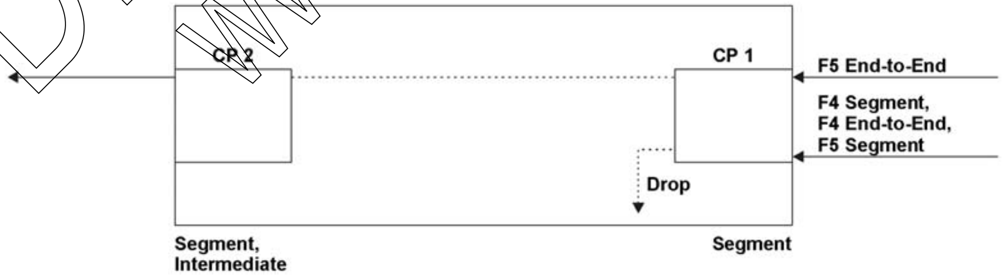


Figure C-18. VC Segment Point – Case A

- When F5 segment AIS cells are received, AIS state is declared. F5 end-to-end AIS cells are generated towards the forward direction, while F5 segment RDI cells are generated towards the backward direction.

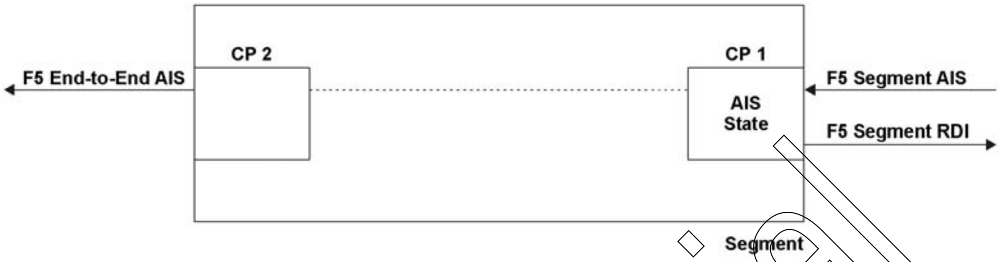


Figure C-19. VC Segment Point – Case B

- When a failure is detected on the physical port, AIS state is declared. F5 end-to-end AIS cells are generated towards the forward direction, while F5 segment RDI cells are generated towards the backward direction.

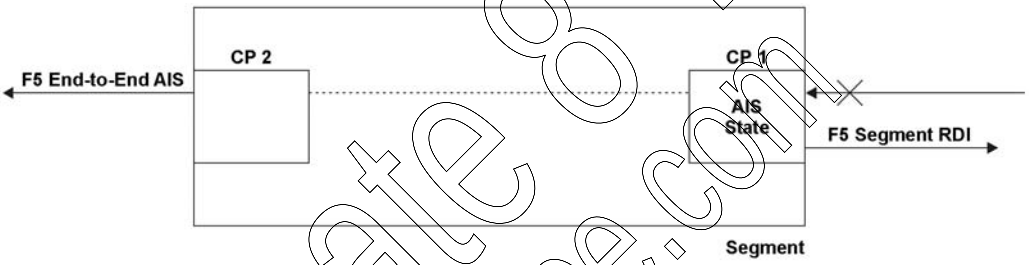


Figure C-20. VC Segment Point – Case C

- When a VC segment point is set as a CC source point, F5 segment CC cells are generated towards the backward direction every second.

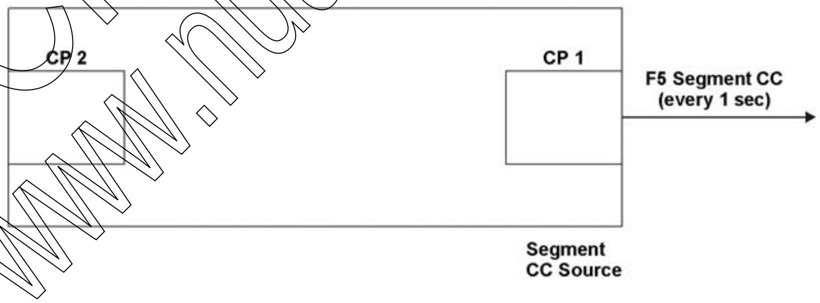


Figure C-21. VC Segment Point – Case D

- When a VC segment point is set as a CC sink point, F5 segment CC cells are expected to be received every second. If no CC cell has been received during the last 3.5 seconds, AIS state is declared. F5 end-to-end AIS cells are generated towards the forward direction, while F5 segment RDI cells are generated towards the backward direction.

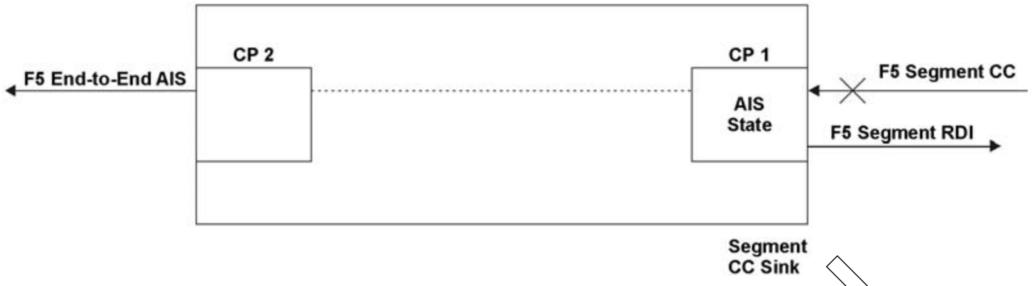


Figure C-22. VC Segment Point – Case E

- When a VC segment point is set as CC both, it functions both as a source and a sink point.
- For OAM loopback cells (see *C.3 OAM Loopback*), an ID match check determines the loopback state (see *Figure C-23*), and delays are calculated if the loopback cell has been authenticated and returned within 5 seconds (see *Figure C-24*):

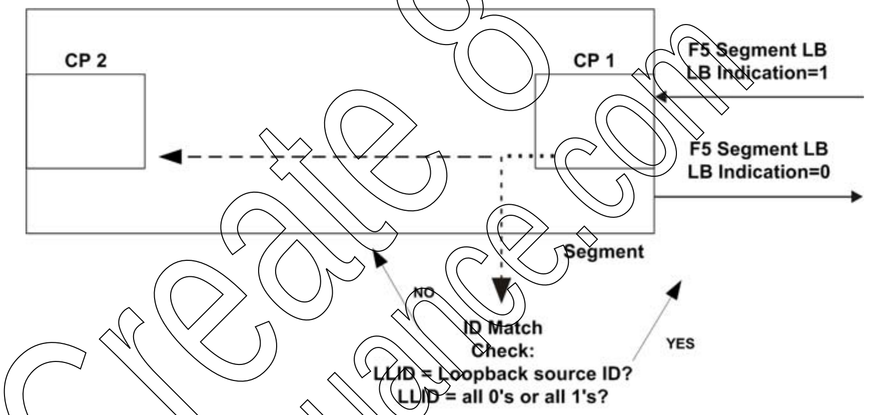


Figure C-23. VC Segment Point – Case F

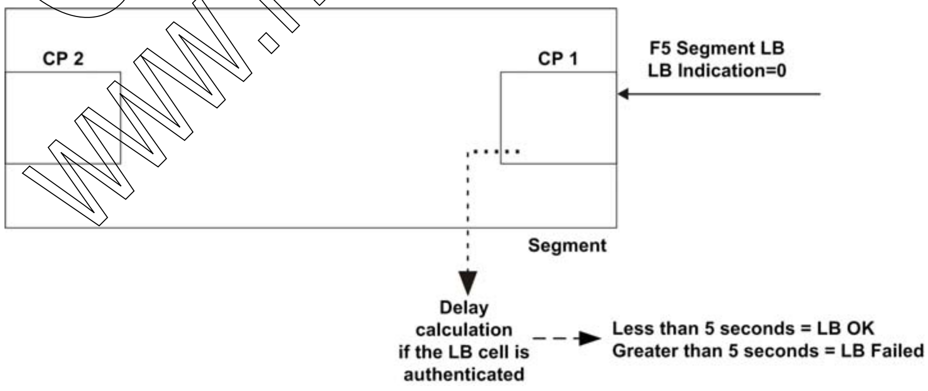


Figure C-24. VC Segment Point – Case G

VC End-to-End Point

When a VC connection point is set as an endpoint (end-to-end), it operates as follows:

- F4 and F5 segment and end-to-end OAM cells are dropped from the cell stream. F5 end-to-end AIS, RDI and CC cells are monitored.

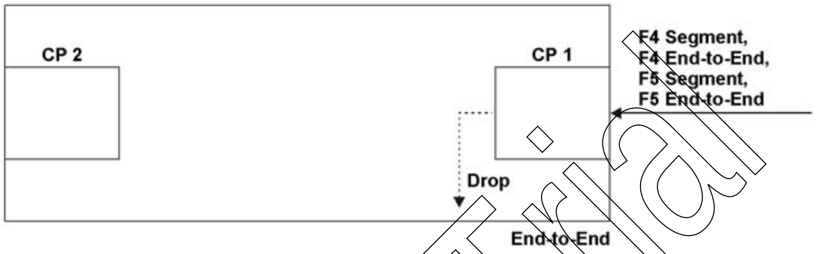


Figure C-25. VC Endpoint – Case A

- When F5 end-to-end AIS cells are received, AIS state is declared and F5 end-to-end RDI cells are generated towards the backward direction.

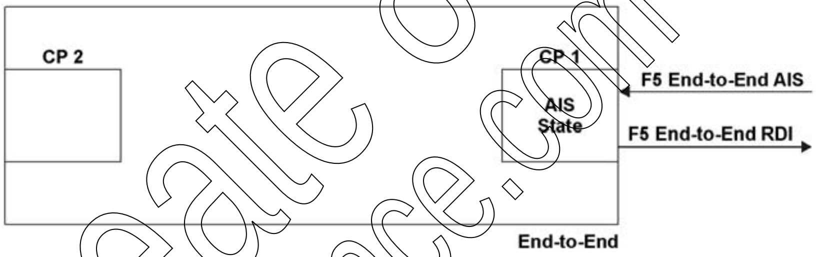


Figure C-26. VC Endpoint – Case B

- When a failure is detected on the physical port, AIS state is declared and F5 end-to-end RDI cells are generated towards the backward direction.

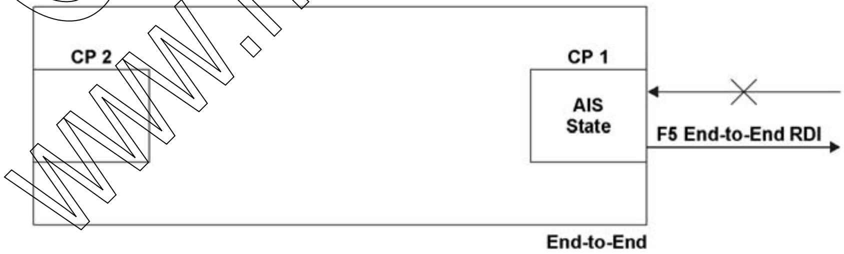


Figure C-27. VC Endpoint – Case C

- When a VC endpoint is set as a CC source point, F5 end-to-end CC cells are generated towards the backward direction every second.

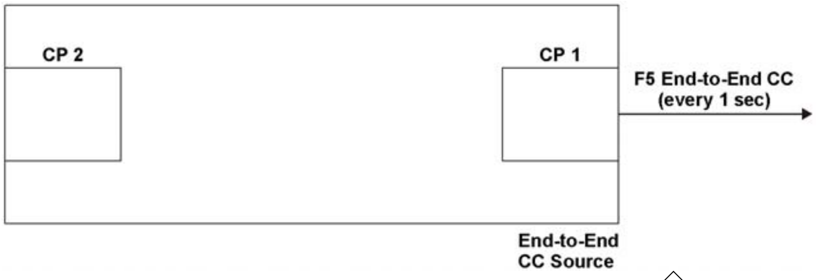


Figure C-28. VC Endpoint – Case D

- When a VC endpoint is set as a CC sink point, F5 end-to-end CC cells are expected to be received every second. If no CC cell has been received during the last 3.5 seconds, AIS state is declared and F5 end-to-end RDI cells are generated towards the backward direction.

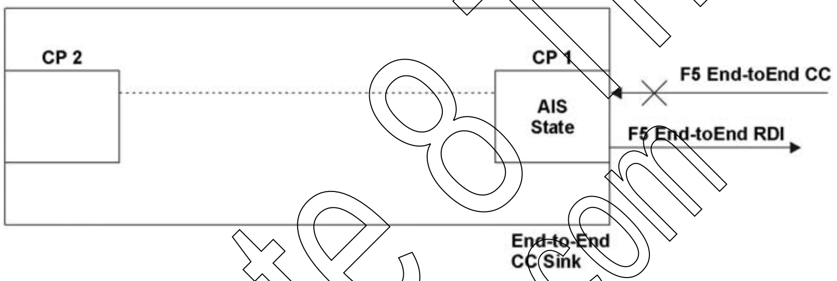


Figure C-29. VC Endpoint – Case D

- When a VC end point is set as CC both, it functions both as a source and a sink point.
- For OAM loopback cells (see *C.3 OAM Loopback*), an ID match check determines the loopback state (see *Figure C-30*), and delays are calculated if the loopback cell has been authenticated and returned within 5 seconds (see *Figure C-31*):

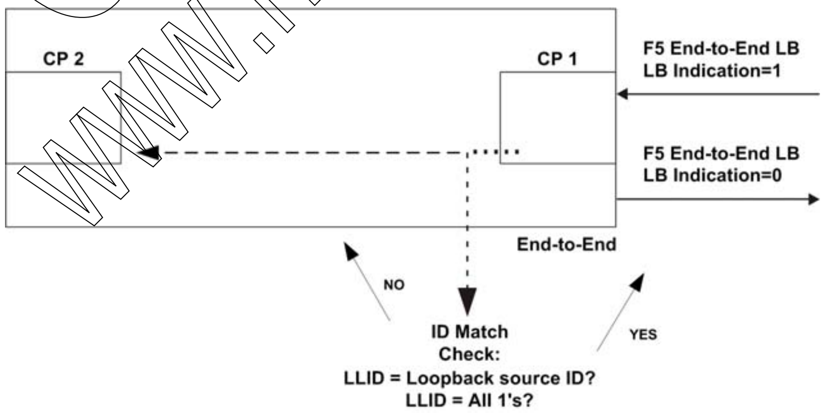


Figure C-30. VC End Point – Case E

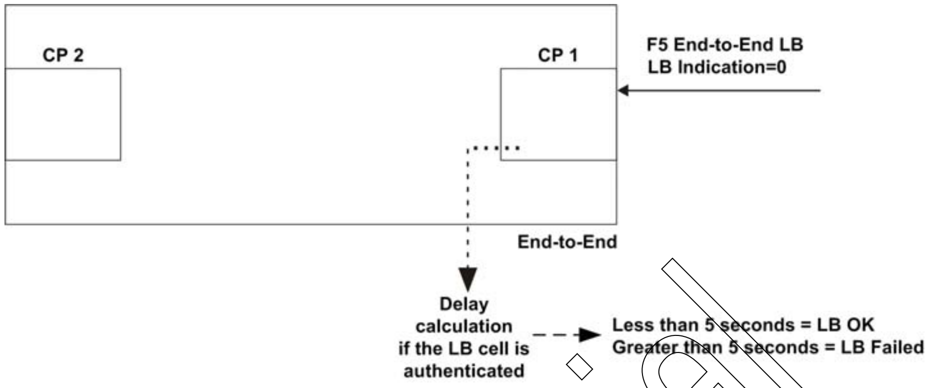


Figure C-31. VC End Point – Case F

Note *Only an ATM host connection can be set as a VC endpoint.*

C.3 OAM Loopback

OAM loopback cells are used to determine connectivity at specific points in a network or between networks. OAM cells are part of the F4 and F5 OAM service, which allows fault management for VPs and VCs. Loopback cells can be defined as **Segment** or **End-to-End**.

OAM loopback support includes the following functionality:

- OAM loopback cell generation – If OAM loopback generation is enabled for a VC/VP at a certain CP, a loopback cell is sent for this VC/VP once every 5 seconds. The loopback cell is inserted towards the uplink (Tx) direction and must be looped through another CP back to the origin point, all within no more than 5 seconds.
- OAM loopback reply – Each CP must:
  - Have the ability to receive OAM LB cells that are addressed to it, regardless of whether the OAM LB generation is enabled
  - Loop the cells back towards the originator according to the standard definitions.
- Min/max/average delay statistics – loopback statistics is updated for each VP/VC that generates OAM loopback, upon each time a loopback cell completes a roundtrip before the 5 seconds loopback cycle period is over. Statistics are available for both current and previous intervals.

Appendix D

Clock Modes

This appendix explains the different clock modes (system timing) supported by ACE-3600.

D.1 Overview

The ACE-3600 ATM clock mechanism supports the synchronization (frequency lock) of all ports to a single clock source, which serves as the system clock of the device.

The system clock is referenced from the incoming (RX) traffic of either the clock of a specific STM-1/OC-3c port, which was chosen to serve as a benchmark for all other ports, or the clock of an external E1/T1 source connected to the ACE-3600 dedicated station clock (without transferring any data via the station clock port).

The synchronization of all ports to a single system clock source is achieved by:

- Configuring the system's master and fallback clocks (see *Section D.2*, *System Clock Configuration*)
- Configuring the transmit (TX) clock of each specific STM-1/OC-3c port (see *Section D.3*, *Transmit Clock Configuration*).

Clock States

Three clock states are possible (also see *Figure D-1*):

- State A – The master (primary) clock is the active system clock
- State B – The fallback (secondary) clock is the active system clock
- State C – Both the master and fallback clocks of the port are inactive. In this case, the system clock is automatically provided by the internal clock chip, named 'SEC', in one of the following modes:
  - Hold-over mode – The SEC chip reinstates the timing of the previously active master/fallback clock source, providing that the previous clock was active for at least two minutes. Holdover mode is set in slow hold-over frequency averaging, which means that the averaging filter gives a -3db response rate for approximately 110 minutes.
  - Free-run mode – The SEC chip generates the clock by itself, if the hold-over mode could not be initiated.

Clock Availability

The master and fallback clocks can be either:

- Available – the relevant port's clock (master or fallback) *can* serve the active system clock, for example when the line is OK and the port is enabled; or
- Not Available – the relevant port's clock (master or fallback) *cannot* serve as the system clock, due to port disabling, failure in the receive (RX) line, or lack of configuration for the fallback clock.

Accordingly, the ACE-3600 clock mechanism sets the active system clock to an available clock (master or fallback).

However, in the non-reversible mode (when the Revertive mode is disabled; for more information, see *Setting the Master Clock* in Chapter 4), the fallback clock continues to be the system clock even if the master clock becomes available.

Triggers for Clock State Transitions

There are several triggers that may cause a clock state transition:

- The master/fallback receive (RX) line has failed
- The master/fallback receive (RX) line has been restored
- The master/fallback clock's port has been disabled
- The master/fallback clock's port has been enabled
- The master/fallback clock configuration has changed.

The following figure illustrates the clock state transitions:

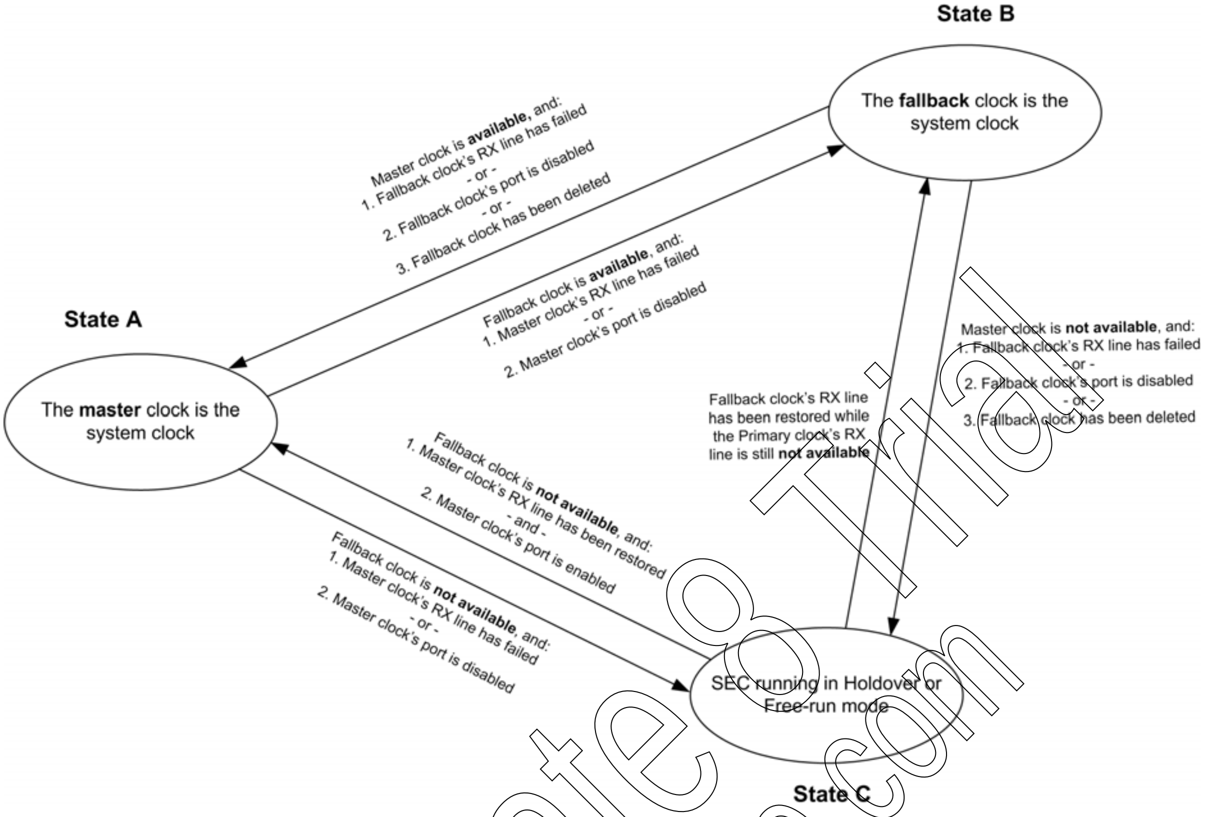

State B
The fallback clock is the system clock
Master clock is available, and:
1. Fallback clock's RX line has failed
- or -
2. Fallback clock's port is disabled
- or -
3. Fallback clock has been deleted
Fallback clock is available, and:
1. Master clock's RX line has failed
- or -
2. Master clock's port is disabled
State A
The master clock is the system clock
Master clock is not available, and:
1. Fallback clock's RX line has failed
- or -
2. Fallback clock's port is disabled
- or -
3. Fallback clock has been deleted
Fallback clock's RX line has been restored while the Primary clock's RX line is still not available
Fallback clock is not available, and:
1. Master clock's RX line has been restored
- and -
2. Master clock's port is enabled
Fallback clock is not available, and:
1. Master clock's RX line has failed
- or -
2. Master clock's port is disabled
SEC running in Holdover or Free-run mode
State C

Figure D-1. Clock State Transitions

D.2 System Clock Configuration

The system clock configuration is performed in accordance with the following guidelines:

- Two system clocks can be set – **Master** and **Fallback**. The master clock has a default configuration (ATM-155); the fallback clock configuration is optional.
- The master/fallback clock configuration can be derived from:
  - The receive (RX) clock of a **physical port's incoming data**, sent from a remote device (usually from the RNC if ACE-3600 is used as a central gateway; see *Section D.4, Typical Clock Mode*).
  - The receive (RX) clock of the ACE-3600 station clock port. The station clock port can be the active system clock only if it was selected as the master or fallback clock (for more information, see *Configuring the Clock Source* in Chapter 4). Otherwise (without selecting it), the station clock port is regarded as a disabled port that cannot provide any clock indication.

Note

- *If the station clock stream is received in QRSS pattern, the TX clock is sent as QRSS data.*
- *If you disable a port that is configured as the system clock, or define the system clock source (master or fallback) for a port that is already disabled – the port becomes unavailable (inactive).*

For details regarding the clock configuration procedures, refer to *Chapter 4*.

D.3 Transmit Clock Configuration

ACE-3600 allows the transmit (TX) clock source of each port to be set to **System** mode, which means that the transmit clock of the port is retrieved from the incoming (RX) data of the **previously set system clock** port (see previous section).

For more information, refer to *Chapter 4*.

D.4 Typical Clock Mode

In the following application (see *Figure D-2*), the master clock is retrieved from the RNC via an STM-1/OC-3c link, connected to one of the ACE-3600 ATM-155 ports. This port serves as the master clock source.

At the same time, the TX clock of all other ATM-155 ports is set to System mode, which means that their TX clock is retrieved from the selected ATM-155 port's RX clock.

In this configuration, the fallback clock is derived from the protected ATM-155 port in APS mode. If APS is not used, an E1/T1-based clock source can be used via the station clock port.

ACE-3600 distributes the clock over the PSN towards the ACE-3100 and ACE-3200 remote peers, which can recover the clock.

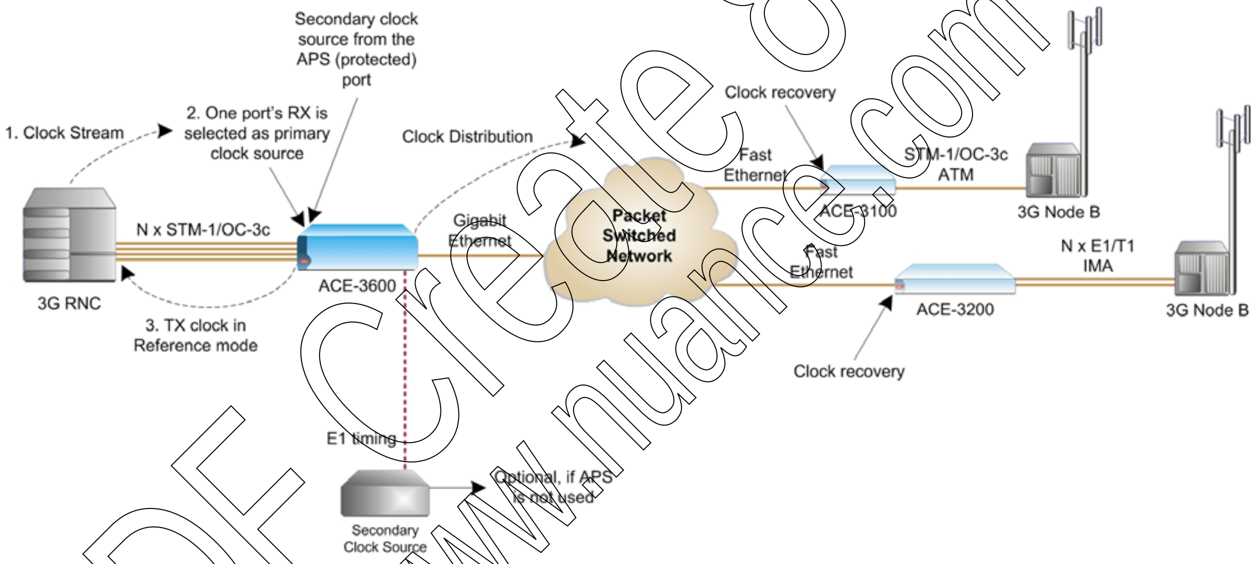


Figure D-2. Typical Clock Mode

Appendix E

Encapsulation over PSN

This appendix describes the encapsulation of ATM and TDM cells, transported over the packet-switched network (PSN) and handled by ACE-3600. This includes the following topics:

- *Basic Pseudowire (PW) Encapsulation*
- *Encapsulation over Different PSN Types* – which describes:
  - *MPLS/Layer-2 Packet Format*
  - *MPLS over IP Packet Format*
  - *MPLS over GRE Packet Format*
  - *MPLS Packet with/without PHP*
  - *UDP over IP Packet Format*
- *ATM Service Encapsulation* – which describes:
  - *One-to-One (1:1) ATM PW Encapsulation*
  - *N-to-One (N:1) ATM PW Encapsulation*
  - *AAL5-SDU ATM PW Encapsulation*
- *TDM Service Encapsulation* – which describes:
  - *CESoPSN Control Word*
- *Clock Encapsulation*.

E.1 Basic Pseudowire (PW) Encapsulation

A pseudowire (PW) packet comprises the following data components (see *Figure E-1*):

- Ethernet header – contains the DA (destination MAC address), SA (local MAC address) and Ethernet network type.
- PSN header – defines the PSN transport type: MPLS, UDP over IP, MPLS over IP, MPLS over GRE and PPPoE.
- Control Word – a data control as defined in the relevant IETF RFCs and drafts.
- Payload – the service payload (ATM or TDM payload), which contains the actual traffic data.

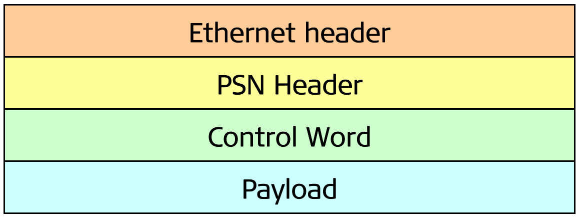


Figure E-1. Basic PW Structure

E.2 Encapsulation over Different PSN Types

Pseudowire connections may be encapsulated in different formats, depending on the type of PSN used in the application. The supported formats are: MPLS/Layer-2, MPLS over IP, MPLS over GRE, UDP over IP, and PPPoE.

MPLS/Layer-2 Packet Format

The following figure illustrates the MPLS or Layer-2 encapsulation format:

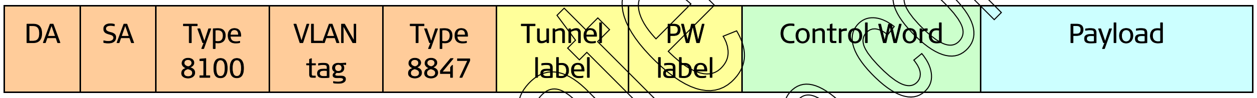


Figure E-2. MPLS/Layer-2 Encapsulation Format

Table E-1. MPLS/Layer-2 Encapsulation Parameters

	Parameter Name	Purpose
	DA	Destination MAC address of the remote peer or next hop unit. 6 bytes long.
	SA	MAC address of the device. 6 bytes long.
Optional	Type 8100	If VLAN support is enabled, the Ethernet packet type is set to 0x8100. 2 bytes long.
	VLAN tag	If VLAN support is enabled, this tag includes the VLAN ID and its priority; configured per PW. 2 bytes long.
	Type 8847	MPLS packet type – 0x8847. 2 bytes long.
Optional	Tunnel label	Label of the PW tunnel between ACE-3600 and the PE. This parameter is manually configured per PW/peer and per direction, or dynamically learned using LDP. 4 bytes long. A different value is possible for the RX and TX directions (tunnel in/out).
	PW label	Label of the Pseudowire; manually defined per PW and per direction, or dynamically learned using LDP. 4 bytes long.

Control Word	Contains the sequence number and control bits. 4 bytes long.
Payload	The service data carried on the frame, depending on the PW type.

MPLS over IP Packet Format

The following figure illustrates the MPLS over IP encapsulation format:

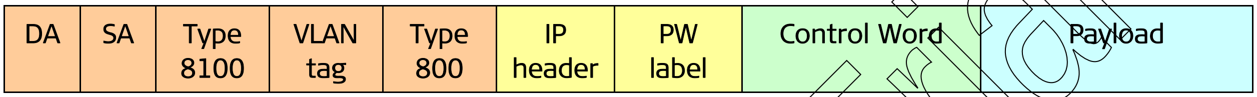


Figure E-3. MPLS over IP Encapsulation Format

Table E-2. MPLS over IP Parameters

	Parameter Name	Purpose
	DA	Destination MAC address of the remote peer or next hop unit. 6 bytes long.
	SA	MAC address of the device. 6 bytes long.
Optional	Type 8100	If VLAN support is enabled, the Ethernet packet type is set to 0x8100. 2 bytes long.
	VLAN tag	If VLAN support is enabled, this tag includes the VLAN ID and its priority; configured per PW. 2 bytes long.
	Type 800	IP packet type – 0x800. 2 bytes long.
	IP header	The protocol field of the IPv4 header is set to 137 (MPLS in IP). 20 bytes long.
	PW label	Label of the Pseudowire; manually defined per PW and per direction, or dynamically learned using LDP. 4 bytes long.
	Control Word	Contains the sequence number and control bits. Optional for some PW types. 4 bytes long.
	Payload	The service data carried on the frame, depending on the PW type.

MPLS over GRE Packet Format

The following figure illustrates the MPLS over GRE encapsulation format:

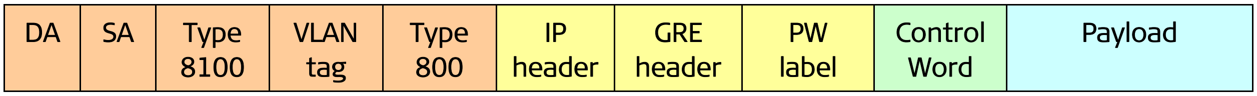


Figure E-4. MPLS over GRE Encapsulation Format

Table E-3. MPLS over GRE Encapsulation Parameters

	Parameter Name	Purpose
	DA	Destination MAC address of the remote peer or next hop unit. 6 bytes long.
	SA	MAC address of the device. 6 bytes long.
Optional	Type 8100	If VLAN support is enabled, the Ethernet packet type is set to 0x8100. 2 bytes long.
	VLAN tag	If VLAN support is enabled, this tag includes the VLAN ID and its priority; configured per PW. 2 bytes long.
	Type 800	IP packet type – 0x800. 2 bytes long.
	IP header	The protocol field of the IPv4 header is set to 47 (GRE). 20 bytes long.
	GRE header	The Protocol Type field of the GRE header is set to 0x8847 (MPLS). 4 bytes long.
	PW Label	Label of the Pseudowire; manually defined per PW and per direction, or dynamically learned using LDP. 4 bytes long.
	Control Word	Contains the sequence number and control bits. 4 bytes long.
	Payload	The service data carried on the frame, depending on the PW type.

MPLS Packet with/without PHP

The following figures illustrate the MPLS packet format with and without PHP (for more information, refer to *Chapter 1*).

PHP Disabled – Control Packet

DA	SA	Type 8100	VLAN tag	Type 8847	Tunnel label	IP header	UDP	LDP

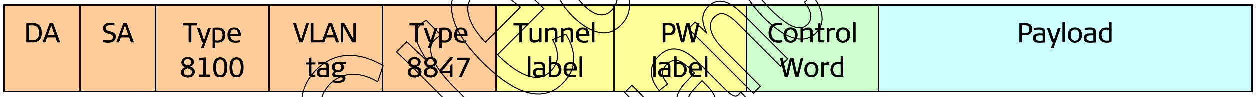
Figure E-5. MPLS Control Packet when PHP is Disabled

Table E-4. Encapsulation Parameters

Parameter Name	Purpose
DA	Destination MAC address of the remote peer or next hop unit. 6 bytes long.
SA	MAC address of the device. 6 bytes long.

	Parameter Name	Purpose
Optional	Type 8100	If VLAN support is enabled, the Ethernet packet type is set to 0x8100 . 2 bytes long.
	VLAN tag	If VLAN support is enabled, this tag includes the VLAN ID and its priority; configured per PW. 2 bytes long.
	Type 8847	MPLS packet type – 0x8847. 2 bytes long.
	Tunnel label	Label of the PW tunnel between ACE-3600 and the PE. This parameter is manually configured per PW/peer and per direction, or dynamically learned using LDP. 4 bytes long. A different value is possible for the RX and TX directions (tunnel in/out).
	IP header	The protocol field of the IPv4 header is set to 17 (UDP). 20 bytes long.
	UDP	UDP bytes
	LDP	LDP bytes

PHP Disabled – Data Packet



DA	SA	Type 8100	VLAN tag	Type 8847	Tunnel label	PW label	Control Word	Payload

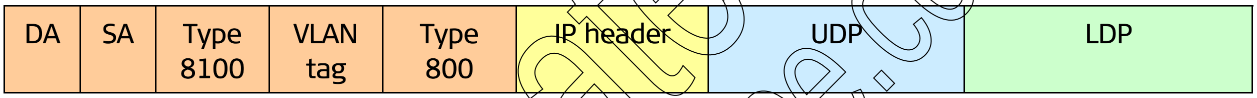
Figure E-6. MPLS Data Packet when PHP is Disabled

Table E-5. Encapsulation Parameters

	Parameter Name	Purpose
	DA	Destination MAC address of the remote peer or next hop unit. 6 bytes long.
	SA	MAC address of the device. 6 bytes long.
Optional	Type 8100	If VLAN support is enabled, the Ethernet packet type is set to 0x8100 . 2 bytes long.
	VLAN tag	If VLAN support is enabled, this tag includes the VLAN ID and its priority; configured per PW. 2 bytes long.
	Type 8847	MPLS packet type – 0x8847. 2 bytes long.

Parameter Name	Purpose
Tunnel label	Label of the PW tunnel between ACE-3600 and the PE. This parameter is manually configured per PW/peer and per direction, or dynamically learned using LDP. 4 bytes long. A different value is possible for the RX and TX directions (tunnel in/out).
PW label	Label of the Pseudowire; manually defined per PW and per direction, or dynamically learned using LDP. 4 bytes long.
Control Word	Contains the sequence number and control bits. Optional for some PW types. 4 bytes long.
Payload	The service data carried on the frame, depending on the PW type.

PHP Enabled – Control Packet



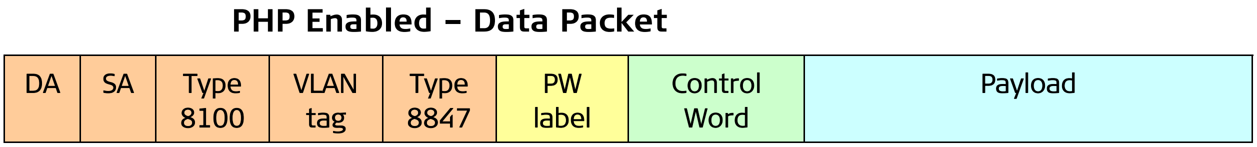
DA	SA	Type 8100	VLAN tag	Type 800	IP header	UDP	LDP

Figure E-7. MPLS Control Packet when PHP is Enabled

Table E-6. Encapsulation Parameters

Parameter Name	Purpose
DA	Destination MAC address of the remote peer or next hop unit. 6 bytes long.
SA	MAC address of the device. 6 bytes long.
Type 8100	If VLAN support is enabled, the Ethernet packet type is set to 0x8100 . 2 bytes long.
VLAN tag	If VLAN support is enabled, this tag includes the VLAN ID and its priority; configured per PW. 2 bytes long.
Type 800	MPLS packet type – 0x800. 2 bytes long.
IP header	The protocol field of the IPv4 header is set to 17 (UDP). 20 bytes long.
UDP	UDP bytes
LDP	LDP bytes

Optional



PHP Enabled – Data Packet

DA	SA	Type 8100	VLAN tag	Type 8847	PW label	Control Word	Payload

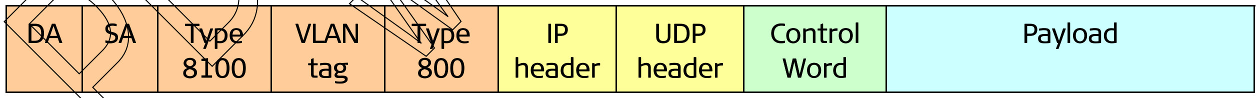
Figure E-8. MPLS Data Packet when PHP is Enabled

Table E-7. Encapsulation Parameters

	Parameter Name	Purpose
	DA	Destination MAC address of the remote peer or next hop unit. 6 bytes long.
	SA	MAC address of the device. 6 bytes long.
Optional	Type 8100	If VLAN support is enabled, the Ethernet packet type is set to 0x8100 . 2 bytes long.
	VLAN tag	If VLAN support is enabled, this tag includes the VLAN ID and its priority; configured per PW. 2 bytes long.
	Type 8847	MPLS packet type – 0x8847. 2 bytes long.
	PW label	Label of the Pseudowire; manually defined per PW and per direction, or dynamically learned using LDP. 4 bytes long.
	Control Word	Contains the sequence number and control bits. Optional for some PW types. 4 bytes long.
	Payload	The service data carried on the frame, depending on the PW type.

UDP over IP Packet Format

The following figure illustrates the UDP over IP encapsulation format:



DA	SA	Type 8100	VLAN tag	Type 800	IP header	UDP header	Control Word	Payload

Figure E-9. UDP over IP Encapsulation Format

Table E-8. UDP over IP Encapsulation Parameters

Parameter Name	Purpose
DA	Destination MAC address of the remote peer or next hop unit. 6 bytes long.
SA	MAC address of the device. 6 bytes long.

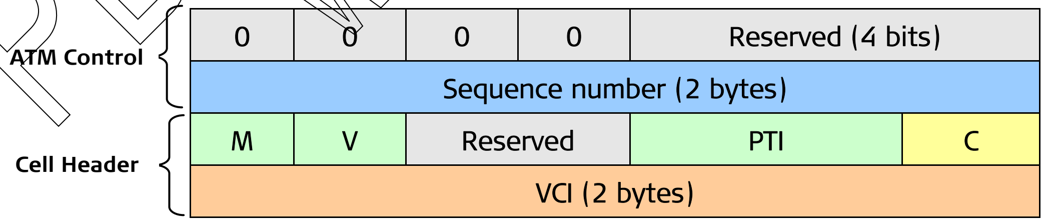
	Parameter Name	Purpose
Optional	Type 8100	If VLAN support is enabled, the Ethernet packet type is set to 0x8100 . 2 bytes long.
	VLAN tag	If VLAN support is enabled, this tag includes the VLAN ID and its priority; configured per PW. 2 bytes long.
	Type 800	IP packet type – 0x800. 2 bytes long.
	IP header	The protocol field of the IPv4 header is set to 17 (UDP). 20 bytes long.
	UDP header	8 bytes long; contains the details of: • UDP source port – identifies the PW label of the destination unit • UDP destination Port – uses TDMoIP protocol number: 0x85E (2142)
	Control Word	Contains the sequence number and control bits. 4 bytes long.
	Payload	The service data carried on the frame, depending on the PW type.

E.3 ATM Service Encapsulation

ATM traffic is encapsulated in either the one-to-one or N-to-1 mode.

One-to-One (1:1) ATM PW Encapsulation

In the one-to-one (1:1) ATM PW mapping mode (selectable), one ATM VCC/VPC is mapped to a single pseudowire link. The following figure illustrates the packet format in 1:1 mode:



ATM Control	0	0	0	0	Reserved (4 bits)
	Sequence number (2 bytes)				
Cell Header	M	V	Reserved	PTI	C
	VCI (2 bytes)				

Figure E-10. 1:1 Encapsulation Structure

Table E-9. 1:1 Encapsulation Parameters

Parameter Name	Purpose
Sequence number	An unsigned 16-bit rounded number for guaranteeing an ordered packet delivery.

Parameter Name	Purpose
M	Transport mode bit of the control byte; indicates whether the packet contains an ATM cell or a frame payload (cell mode = 0; frame mode = 1).
V	Indicates whether the VCI field is present in the packet; its value is either 0 or 1.
PTI	The 3-bit Payload Type Identifier (PTI) value; copied form the PTI bits of the encapsulated ATM cell header.
C	Indicates the CLP (Cell Loss Priority) value of the encapsulated cell; copied from the encapsulated ATM cell header.
VCI	The 16-bit Virtual Circuit Identifier (VCI). Valid only if V=1 (see above).

The following figure illustrates the multiple cells concatenation in 1:1 mode:

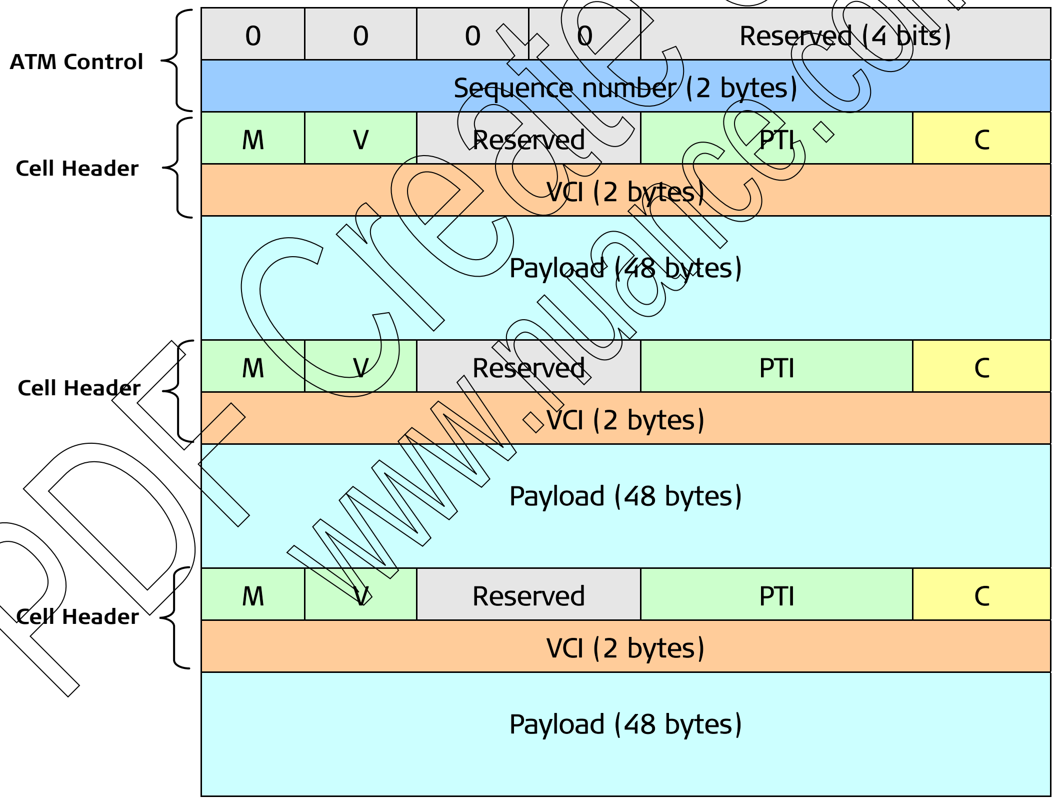


Figure E-11. Multiple Cells Concatenation in 1:1 Encapsulation Mode

N-to-One (N:1) ATM PW Encapsulation

In N-to-one (N:1) mapping mode (selectable), one or more ATM VCCs/VPCs are mapped to a pseudowire link. The following figure illustrates the packet format in N:1 mode:

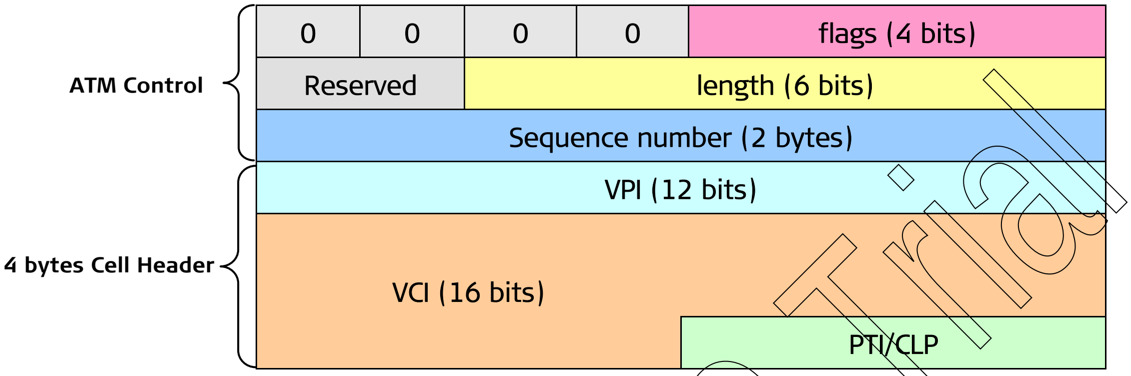


Figure E-12. N:1 Encapsulation Structure

The following figure illustrates the multiple cells concatenation in N:1 mode:

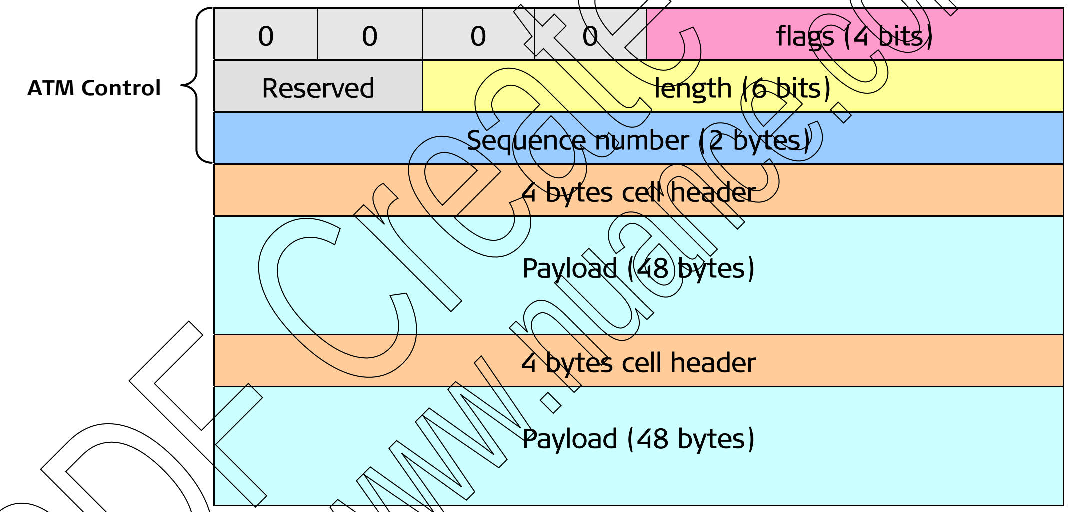


Figure E-13. Multiple Cells Concatenation in 1:1 Encapsulation Mode

AAL5-SDU ATM PW Encapsulation

The AAL5-SDU control word for an ATM PW has the following structure:

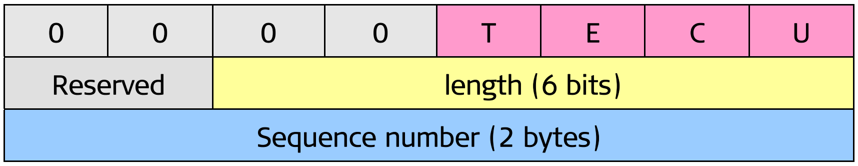


Figure E-14. AAL5-SDU Control Word Structure

Table E-10. AAL5-SDU Control Word Parameters

Parameter Name	Purpose
Reserved	Reserved for future use; assigned with 0 value.
T	Transport type bit. If set to 1, the packet contains an ATM admin cell. If not set, the PDU contains an AAL5 payload.
E	EFCI bit. Set to 1 if the EFCI bit of one or more cells in the AAL5 CPCS-SDU is set also to 1. Otherwise, it is set to 0.
C	CLP bit. Set to 1 if the CLP bit of one or more cells in the AAL5 CPCS-SDU is set also to 1. Otherwise, it is set to 0.
U	Command/response field bit. Set to 0.
Sequence number	A 16 bits, unsigned and rounded number that can be used to guarantee ordered packet delivery.

E.4 TDM Service Encapsulation

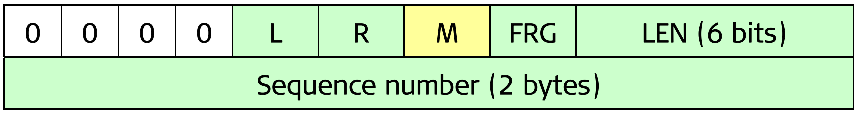
Generally, TDM traffic can be encapsulated over PSN in two modes:

- CESoPSN – CES (Circuit Emulation Services) over PSN
- SAToP – Structure-Agnostic over Packet (not supported in ACE-3600).

Note *Although ACE-3600 does not support TDM services, the clock stream is encapsulated using the CESoPSN format. For more information, see Clock Encapsulation.*

CESoPSN Control Word

The following figure illustrates the structure of the CESoPSN Control Word:



0	0	0	0	L	R	M	FRG	LEN (6 bits)
Sequence number (2 bytes)								

Figure E-15. CESoPSN Control Word Structure

Table E-11. CESoPSN Control Word Parameters

Parameter Name	Purpose
Bits 0–3	Structure bits that their value must be zero
L	If set, indicates that the TDM data carried in the payload in invalid due to a TDM circuit failure
R	Remote receive failure (PSN RDI) on the PSN side

Parameter Name	Purpose
M	A 2-bit modifier field that further defines the failure if the **L** parameter was set: • L|M=000 means no failure; the payload must be processed as received • L|M=100 means TDM failure; the TDM data is invalid • L|M=010 means RDI state of the TDM attachment circuit (AC)
FRG	Fragmentation field for services with CAS
LEN	Used to specify the length of the CESoPSN packet (CESoPSN header size + the payload size) if it is less than 64 bytes. If the total length is 64 bytes or more, the LEN value is set to zero.
Sequence number	Used to provide the common PW sequencing functions, as well as the detection of lost packets

E.5 Clock Encapsulation

The clock encapsulation is based on the CESoPSN format (see *CESoPSN Control Word*). The maximum payload size is 512 bytes.

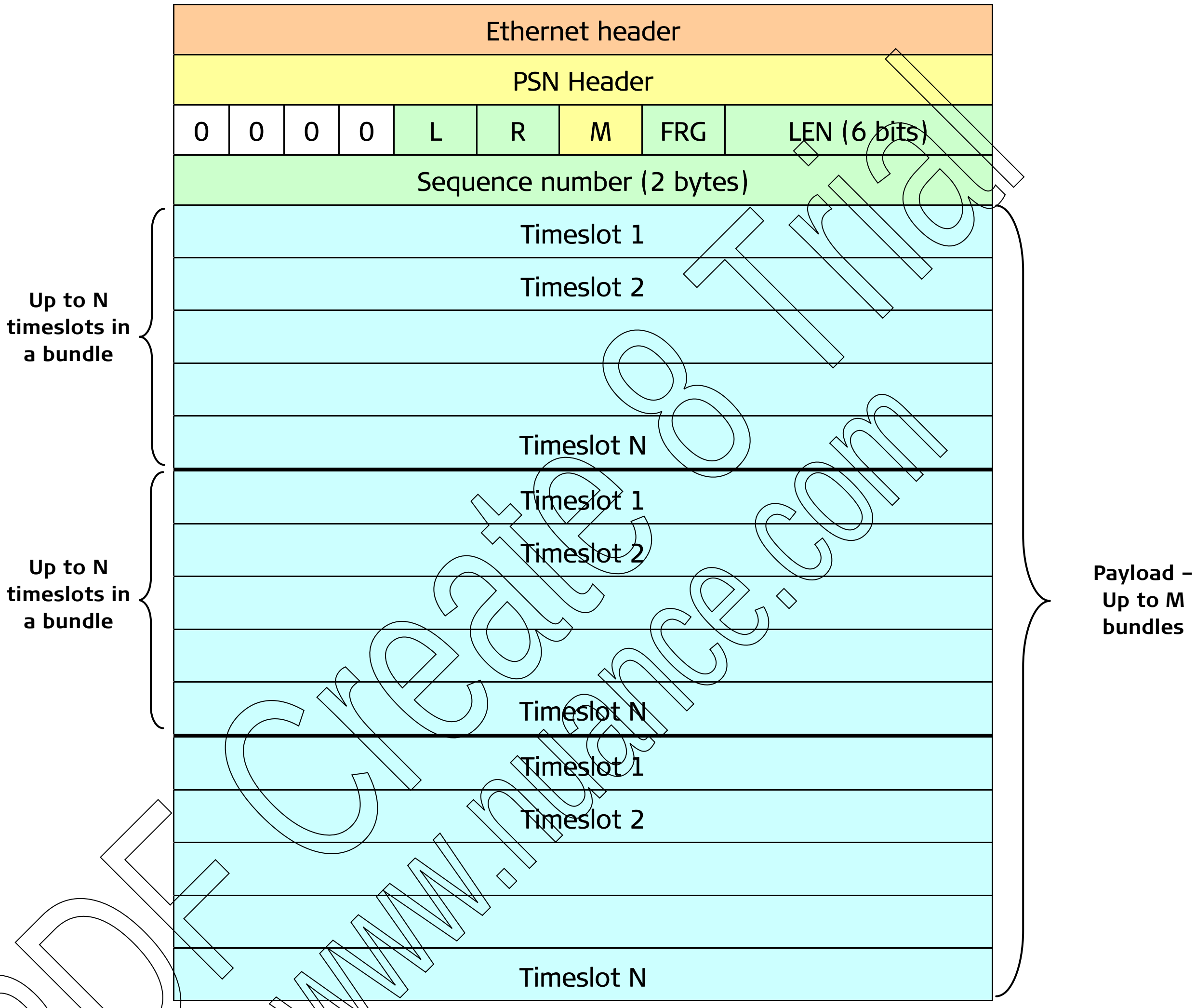


Figure E-16. Clock Encapsulation

The TDM payload illustrated above consists of the following parameters:

- N – number of timeslots in a bundle
- M – number of bundles in a packet
- L – the packet payload size in bytes (up to 512 bytes), calculated by multiplying N by M (N×M)
- D – the packetization delay in milliseconds, calculated by dividing L by N×8 (L / N×8).

Appendix F

Alarm Forwarding

When interworking between ATM and packet-switched networks, it is necessary to deliver alarms from end-to-end. The ACE-3600 alarm forwarding mechanism translates PSN and ATM link failures to alarms that are sent to the customer equipment on each end of the application.

ACE-3600 sends either F4 or F5 Segment/End-to-End AIS alarms towards the ATM backbone side, and performs VCCV-BFD connectivity checks with the PSN side.

In all ATM over PSN applications, the ATM point is configured as VP or VC Intermediate or segment point. All F4/F5 OAM cells that are received on the ATM interface are encapsulated by ACE-3600 over the PSN.

F.1 PSN-to-ATM Alarm Forwarding

Failures on the PSN side are propagated by ACE-3600 towards the ATM side. The following figures illustrate the unit's behavior and alarm types used in case of logical/physical Ethernet link failures, depending on the ATM connection type/assignment (VP or VC, Intermediate or Segment point).

VP/VC Intermediate Point

When the ATM interface is defined as **Intermediate** point, the following forwarding cases are possible:

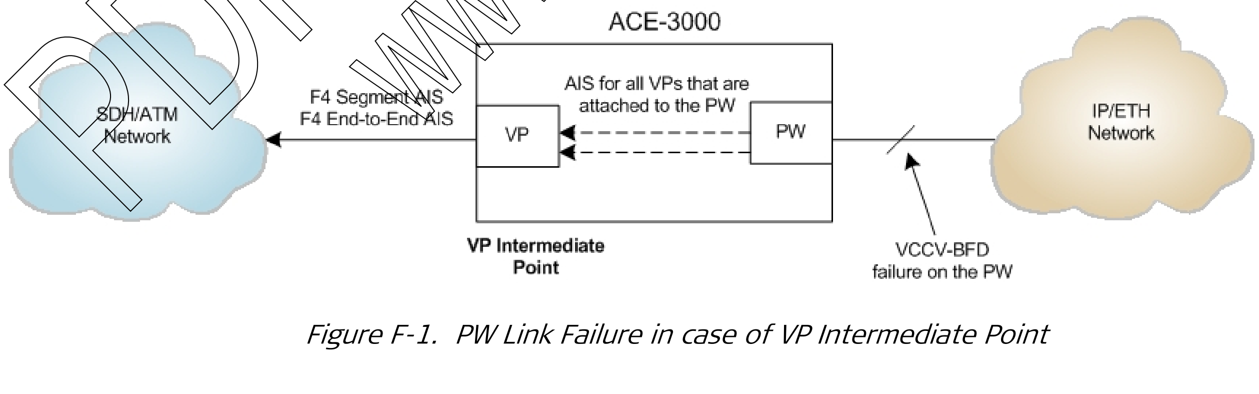


Figure F-1. PW Link Failure in case of VP Intermediate Point

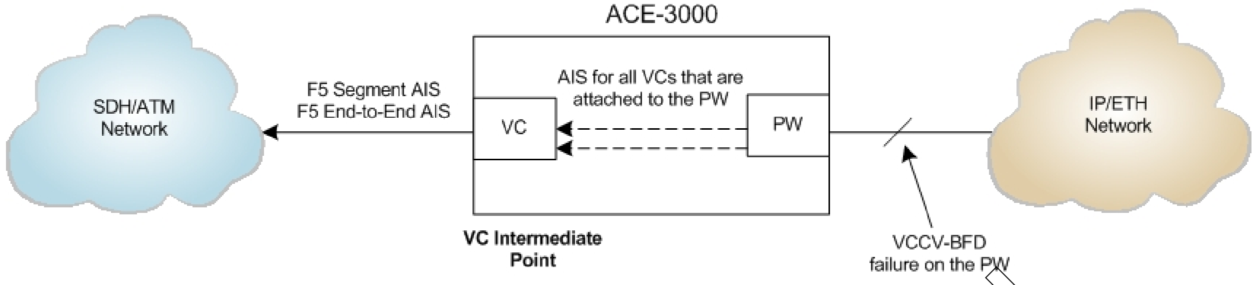


Figure F-2. PW Link Failure in case of VC Intermediate Point

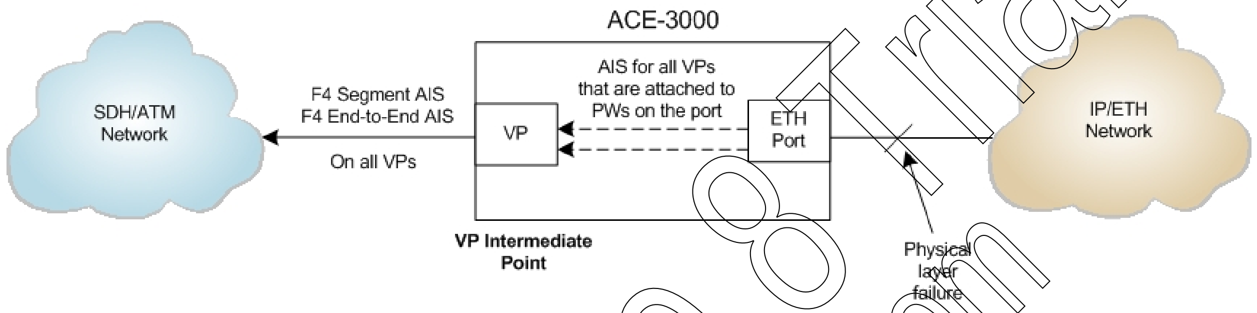


Figure F-3. Physical ETH Failure in case of VP Intermediate Point

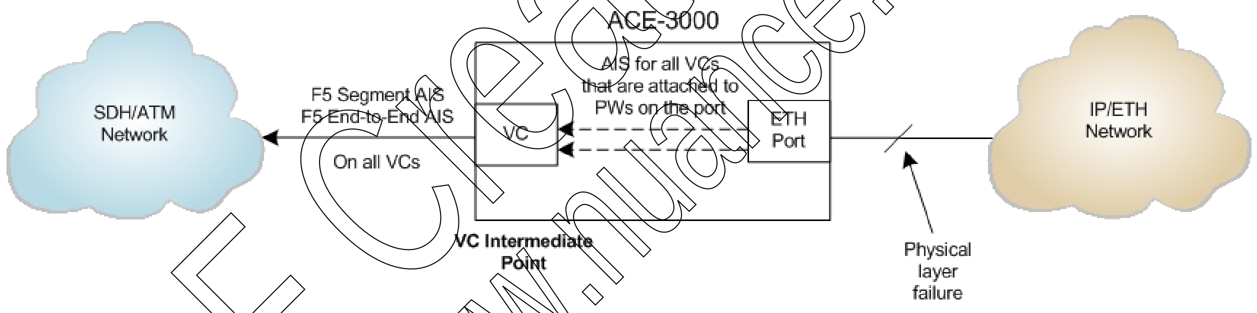


Figure F-4. Physical ETH Failure in case of VC Intermediate Point

VP/VC Segment Point

When the ATM interface is defined as Segment point, the following forwarding cases are possible:

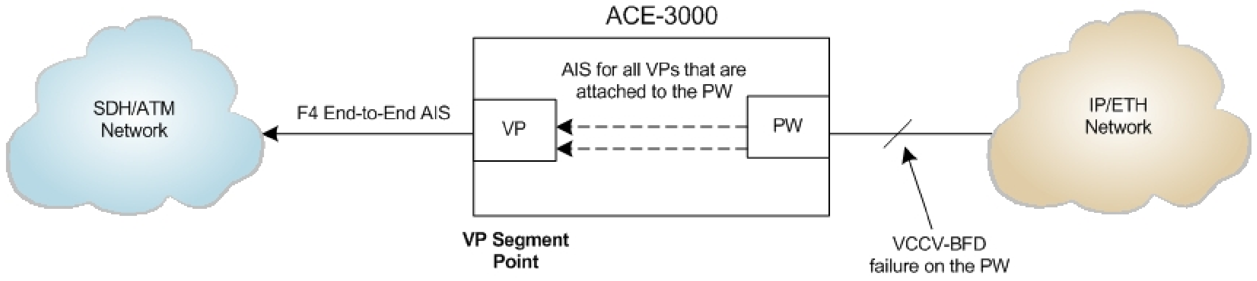


Figure F-5. PW Link Failure in case of VP Segment Point

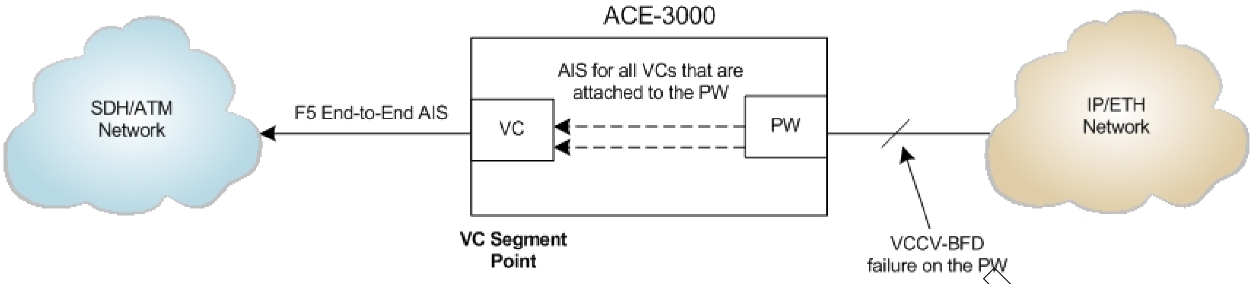


Figure F-6. PW Link Failure in case of VC Segment Point

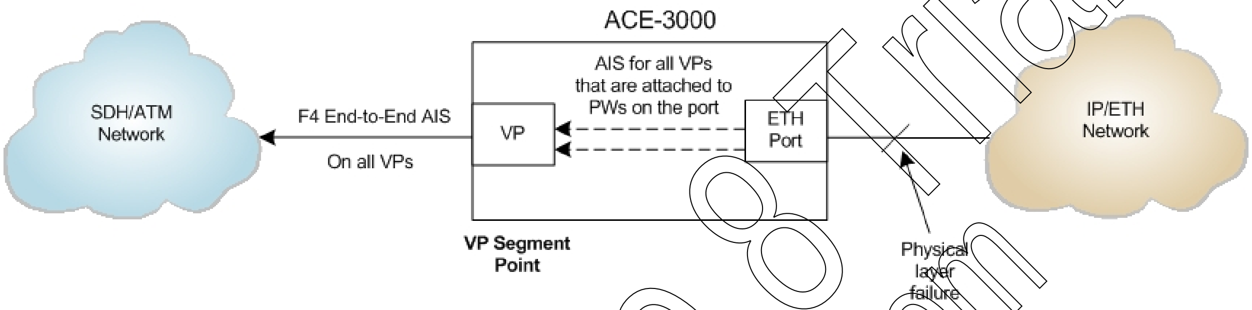


Figure F-7. Physical ETH Failure in case of VP Segment Point

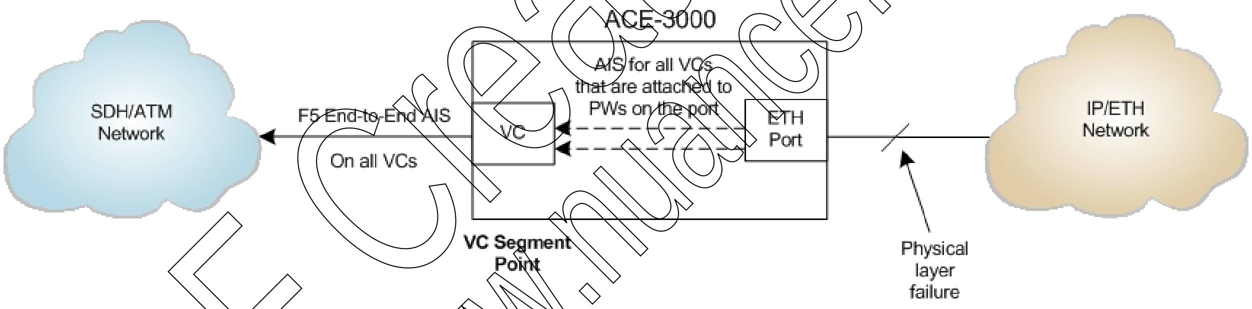


Figure F-8. Physical ETH Failure in case of VC Segment Point

VCCV-BFD Connectivity Check

The PW link connectivity check and alarm forwarding over a packet-switched network is performed as follows (see *Figure* F-9):

a. BFD control messages (packets) are generated per PW by both ACE-3600 and the remote ACE unit, each towards the PSN direction.

b. When ACE-3600 does not receive the BFD control messages from the remote ACE unit during a number (predefined) of transmission intervals, it declares that the specific PW is down on its receive (RX) direction.

c. ACE-3600 generates 'control-detection-time-expired' packets for the specific faulty PW towards the remote ACE.

d. The remote ACE declares a 'neighbor-signal-session-down' state for the PW, and, when possible, sends corresponding packets under this label.

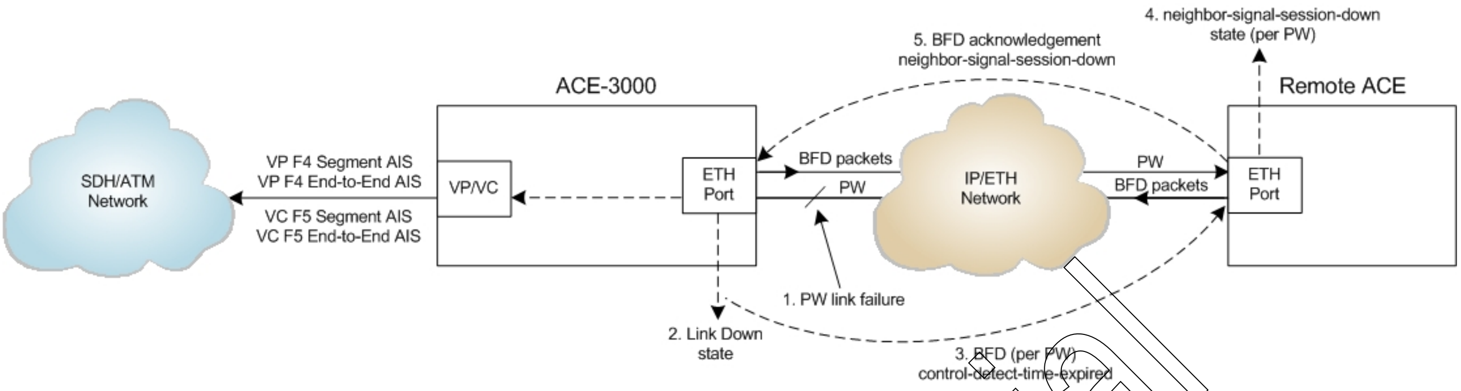


Figure F-9. PW Link Failure and Alarm Forwarding/Acknowledgement over a PSN

F.2 ATM-to-PSN Alarm Forwarding

Vice-versa, failures on the ATM side are propagated by ACE-3600 towards the PSN side. The following figures illustrate the ACE-3600 behavior and alarm types used in case of physical ATM link failures, depending on the ATM connection type (VP or VC).

VP/VC Intermediate Point

When the ATM interface is defined as **Intermediate** point, ACE-3600 forwards alarms regarding any port-level failure. This includes the following cases:

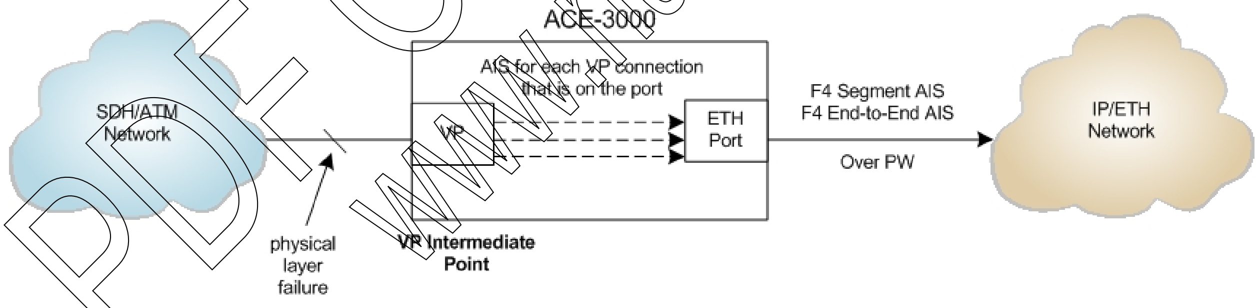


Figure F-10. Physical ATM Failure in case of VP Intermediate Point

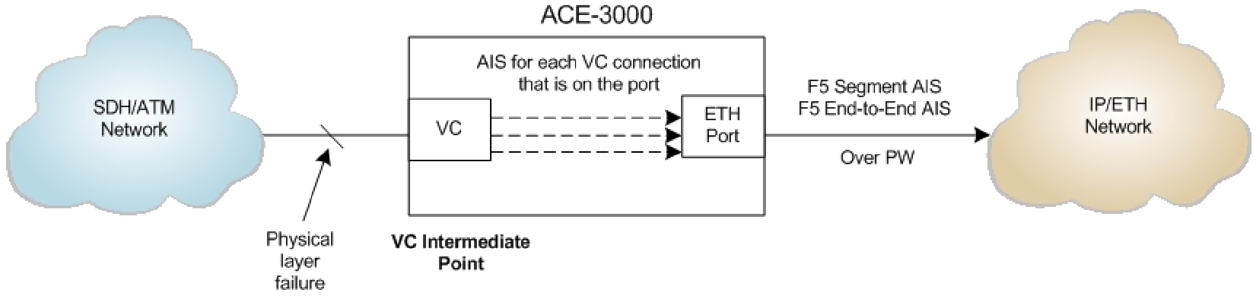


Figure F-11. Physical ATM Failure in case of VC Intermediate Point

VP/VC Segment Point

When the ATM interface is defined as **Segment** point, ACE-3600 forwards alarms regarding either port-level failures or any specific VP or VC connection failure. This includes the following cases:

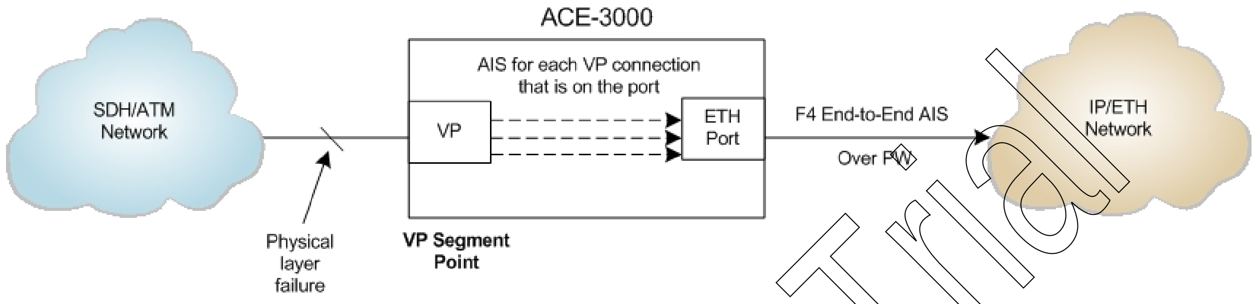


Figure F-12. Physical ATM Failure in case of VP Segment Point

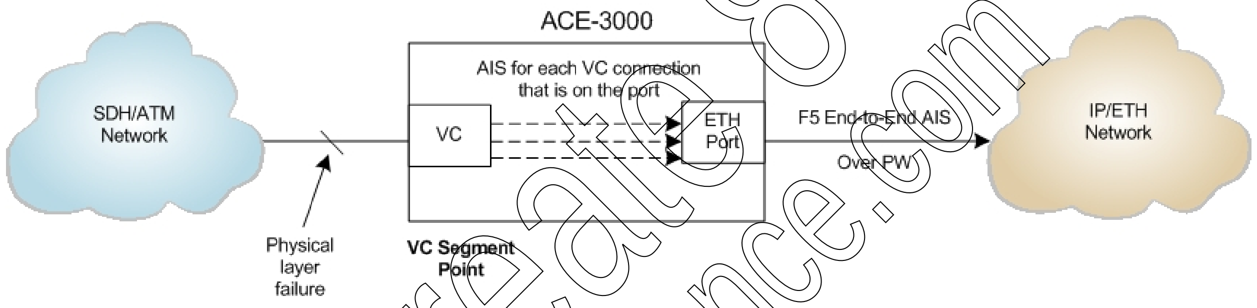


Figure F-13. Physical ATM Failure in case of VC Segment Point

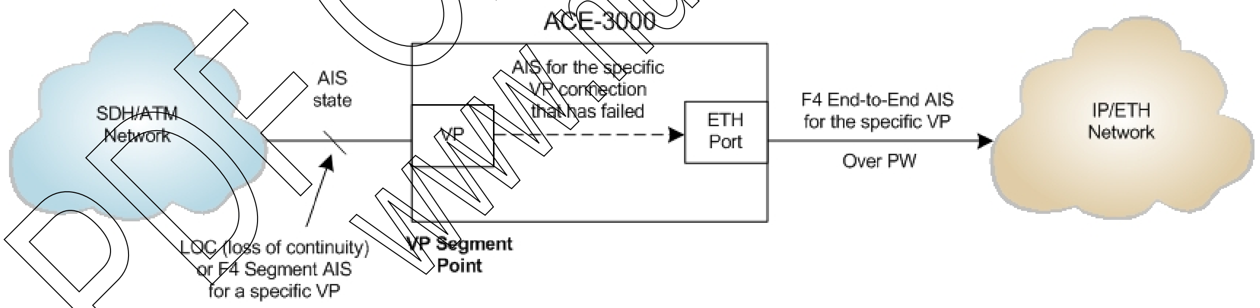

ACE-3000
SDH/ATM Network
AIS state
AIS for the specific VP connection that has failed
VP
ETH Port
F4 End-to-End AIS for the specific VP
Over PW
IP/ETH Network
LOC (loss of continuity) or F4 Segment AIS for a specific VP
VP Segment Point

Figure F-14. VP Failure in case of VP Segment Point

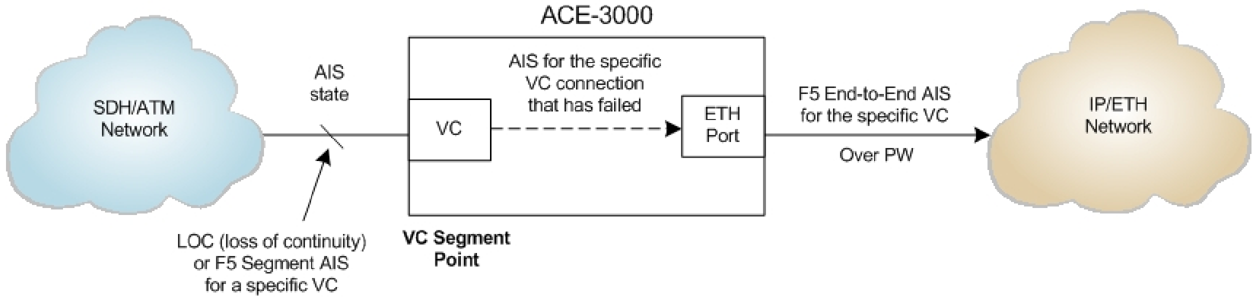

ACE-3000
SDH/ATM Network
AIS state
AIS for the specific VC connection that has failed
VC
ETH Port
F5 End-to-End AIS for the specific VC
Over PW
IP/ETH Network
LOC (loss of continuity) or F5 Segment AIS for a specific VC
VC Segment Point

Figure F-15. VC Failure in case of VC Segment Point

Index

RAD
data communications
The Access Company

24 Raoul Wallenberg Street, Tel Aviv 69719, Israel
Tel: +972-3-6458181, Fax +972-3-6483331, +972-3-6498250
E-mail: erika_y@rad.com, Web site: http://www.rad.com

Customer Response Form

RAD Data Communications would like your help in improving its product documentation. Please complete and return this form by mail or by fax or send us an e-mail with your comments.

Thank you for your assistance!

Manual Name: ACE-3600 Ver. 5.2

Publication Number: 493-200-11/08

Please grade the manual according to the following factors:

	Excellent	*Good*	*Fair*	*Poor*	*Very Poor*
Installation instructions	□	□	□	□	□
Operating instructions	□	□	□	□	□
Manual organization	□	□	□	□	□
Illustrations	□	□	□	□	□
The manual as a whole	□	□	□	□	□

What did you like about the manual?

Error Report

Type of error(s) or problem(s):

□ Incompatibility with product

□ Difficulty in understanding text

□ Regulatory information (Safety, Compliance, Warnings, etc.)

□ Difficulty in finding needed information

□ Missing information

□ Illogical flow of information

□ Style (spelling, grammar, references, etc.)

□ Appearance

□ Other ______________________________

Please list the exact page numbers with the error(s), detail the errors you found (information missing, unclear or inadequately explained, etc.) and attach the page to your fax, if necessary.

Please add any comments or suggestions you may have.

You are:

□ Distributor

□ End user

□ VAR

□ Other

Who is your distributor? ______________________________

Your name and company: ______________________________

Job title: ______________________________

Address: ______________________________

Direct telephone number and extension: ______________________________

Fax number: ______________________________

E-mail: ______________________________

Publication No. 493-200-11/08

Order this publication by Catalog No. 803721

International Headquarters

24 Raoul Wallenberg Street
Tel Aviv 69719, Israel
Tel. 972-3-6458181
Fax 972-3-6498250, 6474436
E-mail market@rad.com

North America Headquarters

900 Corporate Drive
Mahwah, NJ 07430, USA
Tel. 201-5291100
Toll free 1-800-4447234
Fax 201-5295777
E-mail market@rad.com

www.rad.com

RAD
data communications
The Access Company