



## Product Overview

---

This section describes the functionality and the features of the Cisco ONS 15302 R2.0.

### 2.1 Functional Overview

The main R1.0 to R2.0 enhancement is the introduction of GFP/LCAS, which is a Ethernet framing standard to transport Ethernet packets in virtual containers through a SDH network. Additionally this edition introduces a new option for management connectivity, which will simplify design and configuration of a network supplied by Cisco. All features in this release is aligned with new releases of ONS 15305.

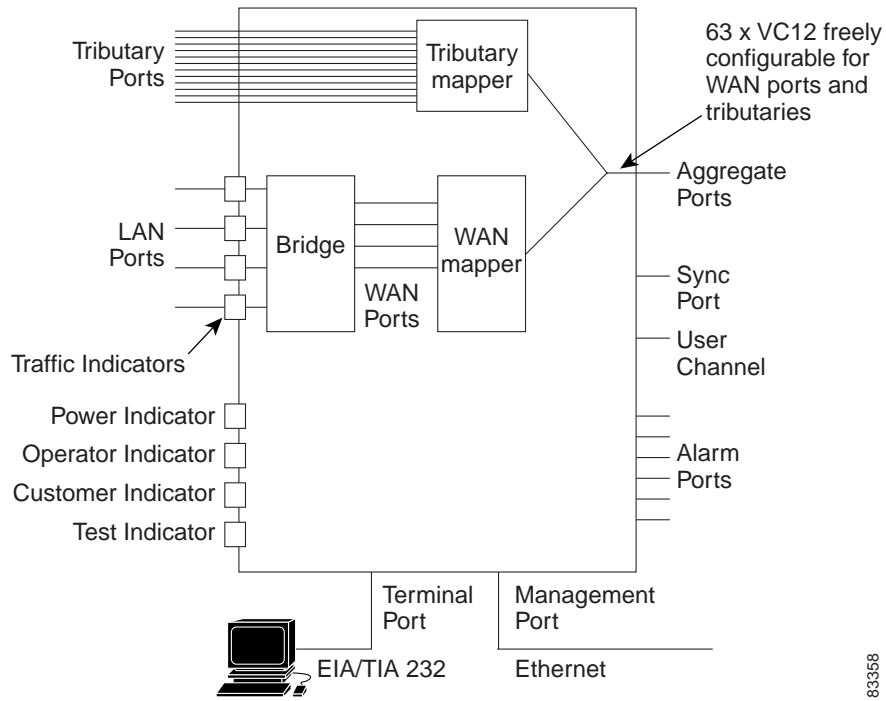
The ONS 15302 is an Integrated Access Device mainly intended for use in fibre optic networks, but can also be supplied as a hardware option with support for electrical STM-1. The ONS 15302 combine IP- and TDM-traffic, by running IP- along with TDM-channels inside an SDH STM-1 frame structure that can be easily carried across the network. The bandwidth of the IP-channel is configurable up to 100 Mb/s true “wire-speed”. The IP part of the ONS 15302 R2.0 consists of a L2/L3 switch.

Each tributary interface (E1) is mapped into a VC-12 container while the WAN traffic can be transported via either nxVC-3 or nxVC12.

The ONS 15302 have room for a plug-in module, which adds more WAN-ports to achieve multiple connections with differentiated bandwidth per customer and/or service.

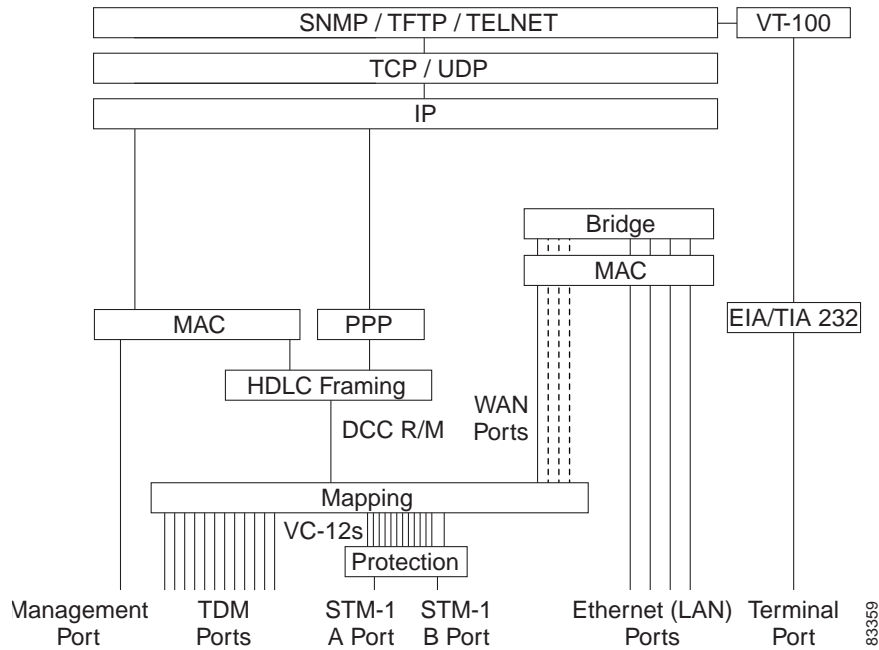
The ONS 15302 management solution is based on an embedded SNMP agent. The CiscoEdgeCraft, a SNMP Craft utility cover any operators' need is supplied with the deliveries of ONS 15302. Minimum required to operate and configure the ONS 15302 is a simple VT100 command line interface (CLI) for direct communication with the embedded SNMP agent.

Figure 2-1 ONS 15302 Functional Overview



From an element management perspective, the ONS 15302 is a multi-protocol machine with several types of interfaces as shown in Figure 2-2.

Figure 2-2 Functional Model for the ONS 15302



# 2.2 Features

This section describes the features of the Cisco ONS 15302 R2.0

## 2.2.1 SDH Multiplexing and Mapping

The aggregate interface supports only terminal multiplexer functions, with a mixture of terminated VC-12 and/or VC-3 container as indicated in Figure 2-4.

The internal structure of the ONS15302 is depicted in Figure 2-3. The bridge/router receives an Ethernet frame/IP datagram on one of the ports and decides on which port to send it out. The Ethernet Mapper maps the Ethernet frames into VC-12/VC-3 containers while the Tributary Mapper converts between E1 signals and VC-12s. The SDH Multiplexer is responsible for the multiplexing of VC-12/VC-3 containers into STM-1. The VC-12/VC-3 containers are sent to - and received from - either the Tributary Mapper or the Ethernet Mapper.

Figure 2-3 Multiplexing and Mapping in the ONS 15302

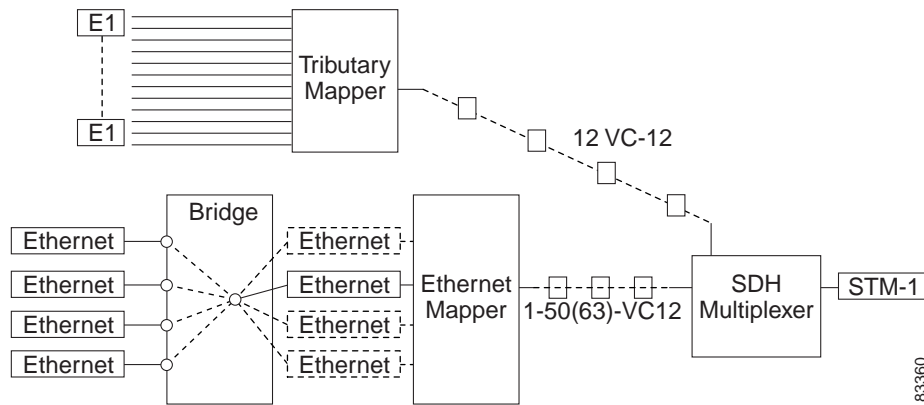
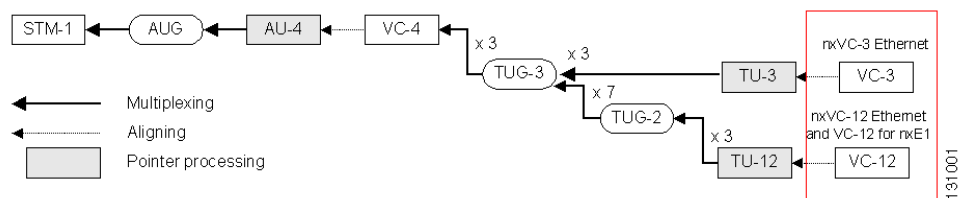


Figure 2-4 Multiplexing Structure in STM-1



The mapping between the tributary interfaces and the WAN port is fully flexible. An example of mapping is shown in Table 2-1.

Table 2-1 Example of a Mapping Scheme for ONS 15302

VC-12 (KLM)	Linked to
1.1.1	TRIBUTARY (1)
2.1.1	TRIBUTARY (2)

*Table 2-1 Example of a Mapping Scheme for ONS 15302 (continued)*

VC-12 (KLM)	Linked to
3.1.1	TRIBUTARY (3)
1.2.1	TRIBUTARY (4)
2.2.1	TRIBUTARY (5)
3.2.1	TRIBUTARY (6)
1.3.1	TRIBUTARY (7)
2.3.1	TRIBUTARY (8)
3.3.1	WAN-PORT (Only one WAN port is used)
1.4.1	WAN-PORT (Only one WAN port is used)
2.4.1	WAN-PORT (Only one WAN port is used)
... and so forth until...	
3.5.3	WAN-PORT (Only one WAN port is used)
1.6.3	WAN-PORT (Only one WAN port is used)
2.6.3	TRIBUTARY (9)
3.6.3	TRIBUTARY (10)
1.7.3	TRIBUTARY (11)
2.7.3	TRIBUTARY (12)
3.7.3	Unused

The VC-12 containers can be freely allocated to the different WAN ports or the tributary ports.

## 2.2.2 Protection

The ONS 15302 offers 1+1 linear Multiplex Section Protection (MSP). The protocol used for K1 and K2 (b1-b5) is defined in ITU-T G.841, clause 7.1.4.5.1. The protocol used is 1+1 bi-directional switching compatible with 1:n bi-directional switching.

The operation of the protection switch is configurable as described in [Table 2-2](#).

*Table 2-2 Protection Switch Parameters*

Parameters	Description	Default Settings
MSP Enabled	<ul style="list-style-type: none"> <li>Enabled</li> <li>Disabled</li> </ul>	Disabled
Switching Type	<ul style="list-style-type: none"> <li>Unidirectional</li> <li>Bidirectional</li> </ul>	Unidirectional
Operation Type	<ul style="list-style-type: none"> <li>Revertive</li> <li>Non-revertive</li> </ul>	Enabled
Wait to restore time	Number of seconds to wait before switching back to the preferred link after it has been restored	300 seconds

*Table 2-2 Protection Switch Parameters (continued) (continued)*

Parameters	Description	Default Settings
Preferred Link	Identifier of the preferred working link	Always LINK A for ONS 15302 R2.0
Switching Command for active port	<ul style="list-style-type: none"> <li>• Clear</li> <li>• Lockout of Protection,</li> <li>• Forced Switched to Protection</li> <li>• Forced Switched to Working</li> <li>• Manual Switched to Protection</li> <li>• Manual Switched to Working</li> <li>• Exercise</li> <li>• No-Command</li> </ul>	No-Command
Working Link	Identifier of the current working link	—
Local Request	Local request contained in K1 byte	—
Remote Request	Remote request contained in K1 byte	—
PERSISTENCY FILTER ALARM ON	Filtering of transient alarms. Defines the number of seconds an alarm must be on to be registered.	—
PERSISTENCY FILTER ALARM OFF	Filtering of transient alarms. Defines the number of seconds an alarm must be off to be registered.	—
ALARM REPORTING	ENABLED or DISABLED. Set the alarm reporting capability for this object. See <a href="#">Table 2-3</a>	—

*Table 2-3 Protection alarm*

Alarm ID	Description
MSP	Problem with MSP signalling with another NE across K1/K2 bytes.

## 2.2.3 Performance Monitoring

The ONS 15302 offers full G.826 performance monitoring at the RS, MS, VC-4, and VC-12 levels in the SDH hierarchy. This includes B1 near end in RSOH section, B2 near and far end in MSOH section, B3 near and far end at VC-4 level and BIP-2 near and far end at VC-12 level.

The ONS 15302 calculates excessive error and degrade signal defects assuming Poisson distribution of errors, according to ITU-T G.826.

The excessive error defect (dEXC) is detected if the equivalent BER exceeds a preset threshold of  $10 \exp -5$ , and be cleared if the equivalent BER is better than  $10 \exp -6$ , according to ITU-T G.806.

The degraded signal defect (dDEG) is detected if the equivalent BER exceeds a preset threshold of  $10 \exp -X$ , where  $x=6,7,8$  or  $9$ . The dDEG is cleared if the equivalent BER is better than  $10 \exp -(X+1)$ , according to ITU-T G.806. The threshold is individually configurable for the different levels in the SDH hierarchy, from  $10 \exp -6$  to  $10 \exp -9$ .

## 2.2.4 Synchronization

ONS 15302 can synchronize to the following sources:

- An STM-1 interface (working link or backup link)
- The dedicated 2048 kHz sync input (Sync Port)
- A tributary port (PRA mode)
- A local oscillator

Tributary synchronization is only relevant when in PRA mode at the chosen tributary.

The synchronization source is a configurable parameter. If it is impossible to synchronize to the selected source, an alarm will be raised, and the system will automatically switch to free running, that means the local oscillator.

Switchback to the selected source is performed automatically whenever it becomes possible again. The alarm is cleared when the switchback is successful.

The ONS 15302 operates in three different modes:

- Locked
- Holdover
- Free running

The default synchronization source is the local oscillator. The tolerance for this oscillator is  $\pm 10$  ppm. ONS 15302 also provides a 2048 kHz sync output for synchronization of external equipment.



Note

The ONS 15302 does not support SSM signaling in the S1 byte. By default transmitted value is “do not use”.



Note

SSM signalling in S1 byte support in the ONS 15302 is not relevant since the network element does only support the configuration of one single sync-source at the time. In case of a protected device, i.e. an hardware variant of ONS 15302 with two aggregate interfaces configured in 1+1 MSP protection, the configuration of synchronisation source should be set to `sync-source=active`.

## 2.3 Ethernet over SDH mapping

This chapter describes the Cisco ONS 15302 Ethernet over SDH mapping.

### 2.3.1 Mapping modes

The ONS 15302 R2.0 supports two different modes of Ethernet over SDH (EOS) mapping

- Proprietary mapping combined with inverse multiplexing at VC-12 level
- GFP-F mapping, combined with VCAT, at VC-12 and VC-3 level, and LCAS



Note

The support of the different EOS modes are dependent on the WAN module inserted. WAN module with ICS 01 supports Proprietary mapping, WAN module with ICS 02 supports Proprietary mapping and GFP-F mapping on a pr. port basis.

#### 2.3.1.1 Proprietary mapping

The ONS 15302 R2.0 provides a proprietary mapping scheme for mapping of Ethernet traffic into a number of VC-12 containers.

The HDLC encapsulated Ethernet frames are mapped into a number of VC-12 containers in a round-robin fashion with an inverse multiplexer function. The mapping process is described in [2.2.1 SDH Multiplexing and Mapping, page 2-3](#).

A total differential delay of up to 8ms is supported.

The total bandwidth for one WAN channel is 100 Mbps or 50xVC-12 containers. AXCESSIT Proprietary VC-12 mapping scheme for Ethernet take advantage of 2,16 Mbps in each VC-12, which means that 47xVC-12 are sufficient to transport 100Mbps Ethernet.

The VC-12 k.l.m reference assignment for the Ethernet WAN port is fully flexible, and controlled in the same way as a VC-12 cross connect.

The sequence number attached to each VC-12 is used for alarm indication only in case of a sequence mismatch, the sequence number is not used for reordering of the incoming VC-12's. The order of VC's carrying Ethernet traffic between two WAN-ports therefore needs to be obtained.

In case of a failure on one of the VC-12's, the effected VC-12 is removed from the channel, allowing the traffic to flow on the remaining VC-12 connections. RDI is used to indicate a failure to the remote side.

#### 2.3.1.2 Standardised mapping

The ONS 15302 R2.0 supports standardised ways of mapping Ethernet over SDH. The mapping schemes includes mapping protocol, concatenation scheme and control protocols.

### 2.3.1.2.1 Generic Framing Procedure

ONS 15302 R2.0 supports framed mapped GFP (GFP-F) according to ITU-T 7041. The GFP implementation supports the following functions:

- The implementation only supports GFP null extension header
- Client data frames are supported
- Client management frames are supported
- For control frames, the implementation only supports GFP idle frames insertion and processing, other unspecified control frames are dropped
- Standard GFP scrambling is supported, with the polynomial  $1+x^43$
- The implementation supports the optional data FCS insertion and checking via the PFI bit
- The implementation supports frame sizes from 9 bytes up to 64kbytes (only sizes from 64 bytes to 9k bytes are applicable for this implementation)

### GFP Alarm and Event Conditions

The GFP implementation supports the following alarm and event conditions:

- GFP Frame Delineation Loss Event, LFD
- Payload Mismatch, PLM
  - Alarm based on detection of PTI field value in ITU-T G.7041
- User Payload Mismatch, UPM
  - Alarm based on detection of UPI field value in ITU-T G.7041
- Payload FCS Mismatch, PFM.
  - Alarm based on detection of PFI field value in ITU-T G.7041
- Extension Header Mismatch, EXM
  - Alarm based on detection of EXI field value in ITU-T G.7041

### GFP Performance Monitoring

The GFP implementation collects the following performance parameters:

- Total number GFP frames transmitted and received
- Total number Client management frames transmitted and received
- Number of bad GFP frames received, based upon payload CRC calculation
- Number of cHEC corrected errors
- Number of cHEC uncorrected errors
- Number of tHEC corrected errors
- Number of tHEC uncorrected errors
- Number of Dropped GFP frames Downstream



A degrade alarm is available for the following performance parameters:

- Number of bad GFP frames received, based upon payload CRC calculation, degFCS
- Number of tHEC corrected and uncorrected errors, degtHEC

The deg alarms are handled in a similar way as the SDH degrade alarms.

### 2.3.1.2.2 Virtual Concatenation (VCAT) and LCAS

The ONS 15302 R2.0 supports virtual concatenation according to ITU-T 707. The VCAT implementation supports the following functions:

- VC-12-nV, where n=1..50
- VC-3-nV, where n=1..3

The VC-x level is individually configurable pr. mapper port, a mix of different VC-x levels in one VCG group is not allowed.

A total differential delay of up to 62ms is supported for the different VCG groups.

ONS 15302 R2.0 supports the LCAS protocol in conjunction with VCAT as defined in ITU-T 7042. The LCAS protocol implemented covers the following functions:

- Automatically temporary removal of a faulty VCAT member
- Automatically insertion of a temporary removed VCAT member when the fault is repaired
- Hitless increase of the VCG capacity by adding a VCG new member
- Hitless decrease of the VCG capacity by removing a current VCG member
- Inter-working with equipment supporting VCAT but not supporting LCAS

### VCAT and LCAS configuration modes

The ONS 15302 R2.0 offers two different operation modes for the VCAT and LCAS functionality, the two modes are:

- 1.VCAT with LCAS enabled
- 2.VCAT without LCAS enabled

#### Mode 1

VCAT with LCAS enabled is always uni-directional, which enables the possibility to have different capacity in each direction, but requires a separate cross connect/capacity setup in each direction.

#### Mode 2

When VCAT is used without LCAS, there is no mechanism for removing of a faulty VC container in a VCG group. To solve this problem the ONS 15302 R2.0 implements, in addition to the standard mode, a proprietary mode.

The following configuration is available in mode 2:

- Default mode, unidirectional connections with the possibility of configuring symmetric capacity as explained in mode 1. Same features as in mode 1 but without LCAS
- SoftLCASBidirectional mode

If SoftLCASBidirectional mode is enabled, the cross connections are uni-directional, but bi-directional. In addition RDI signalling are enabled. A faulty container in a VCG group is removed based upon the VC alarm condition or based upon RDI signalling (similar to the proprietary mapping). This will allow a VCG group to continue operation even if the VCG has a failed member. This configuration mode is proprietary.

## VCAT and LCAS Alarm and Event Conditions

The following alarms related to the VCAT and LCAS are reported by default:

**Table 2-4** *Default alarms - VCAT and LCAS*

Alarm	Description
LOM	Vcat, loss of multiframe
SQM	Vcat sequence indicator mismatch
LOA	Lcas loss of alignment for channels with traffic
GIDERR	Lcas Group Id different for active channels
LCASCRC	Lcas CRC error detected
NONLCAS	Lcas non-Lcas source detected
PLCR	Lcas partial loss of capacity receive
TLCR	Lcas total loss of capacity receive
PLCT	Lcas partial loss of capacity transmit
TLCT	Lcas total loss of capacity transmit
FOPR	Lcas failure of protocol
SQNC	Inconsistent SQ numbers

In addition to the above default alarms, the following alarms are available if enabled from the management system:

**Table 2-5** *Optional alarms - VCAT and LCAS*

Alarm	Description
acMstTimeout	Lcas acMst timeout
rsAckTimeout	Lcas RS-ack timeout
eosMultiple	Lcas two or more channels have EOS
eosMissing	Lcas one channel has EOS
sqNonCont	Lcas missing SQ detected in set of channels
sqMultiple	Lcas equal SQ for two or more channels
sqOor	Lcas SQ outside of range

*Table 2-5 Optional alarms - VCAT and LCAS (continued)*

Alarm	Description
mnd	Lcas member not deskewable
ctrlOor	Lcas undefined Ctrl-word for one or more channels

## 2.4 Switch Features (Bridging)

The bridge is a transparent multi port remote Ethernet bridge as specified in IEEE 802.3. The Bridge consists of four LAN ports and four WAN port. Each port may have its own MAC address, but in most configurations one MAC address for the whole bridge is sufficient. The four LAN ports support 10/100BaseT Ethernet for UTP cables. Both 10 Mbit/s (Mbps) and 100 Mbit/s (Mbps) are supported with auto negotiation. The LAN ports are compatible with IEEE 802.3.

In addition to standard bridging functionality support, the ONS 15302 also support provider bridge functionality.

### 2.4.1 L2 Bridging

The bridge supports the following features:

- MAC switching
- Static MAC entries
- Support of up to 32k MAC addresses
- Automatic Learning & Ageing for MAC addresses
- Auto negotiation (speed/duplex)
- Fixed Ethernet Port settings i.e. 10/100 half/full duplex
- MAC Multicast
- Transparent Bridging
- Port-based Virtual LANs (VLANs)
- VLAN by Port and VLAN by Port and Protocol
- IEEE 802.1Q VLAN tagging compliance (VLAN id. 1-4000)
- Head of Line Blocking prevention
- Back pressure and flow control Handling
- IGMP snooping
- Mirroring Port
- IEEE 802.1p priorities (Strict Policy, 4 queues)
- GARP VLAN registration protocol (GVRP)
- MTU Size 6144 bytes

- Rapid spanning tree protocol according to 802.1w

The filtering rate of the bridge is able to operate at full wire speed. The forwarding rate is only limited by the forwarding interface speed, i.e. the selected WAN port speed.

The ONS 15302 R2.0 also support a LAN-WAN port correlation function used in architectures requiring Ethernet protection. The port correlation function, if enabled on a LAN port, reflects the status of the corresponding WAN port on the actual LAN port. This means that if the operational capacity of the WAN port is 0, due to a network error, the corresponding LAN port is disabled, allowing external equipment to very rapidly detect the network error and thereby switch to the other path.

## 2.4.2 L2 Provider Bridging Functionality

In addition to the standard L2 functionality the following Provider Bridge functionality is supported:

- Tag insertion/removal for Provider bridging/ VLAN tunnelling support
- Protocol tunnelling, offering transparency of the following MAC addresses/protocols:
  - All MAC addresses in the range from 0180C2000000 to 0180C20000FF, except...01, is transported transparently, including the following protocols: RSTP, MSTP, STP, GVRP, GMRP, LACP and 802.1x

The offering of Provider bridging /VLAN tunnelling and protocol tunnelling enables the user to offer transparent Ethernet services in a L2 network with guaranteed security, also called L2 VPN's. The functionality is enabled at the ingress and egress ports in the network.

The Ethertype used for the Tag insertion is 0xFFFF, inter operability with other systems using 0x8100 is obtained by enabling Ethertype swapping on the WAN ports. This functionality is only supported on the new WAN module.

## 2.4.3 Quality of Service

The QoS features can be used to allocate bandwidth for users or applications at layer 2 and layer 3.

The ONS 15302 performs the following functions:

- Classification:
  - Identifying which packet get which treatment
- Metering
  - Measuring a flow of packets to see if it conforms to desired measurement
- Policing
  - Taking actions on frames according to whether they conform or not

Traffic shaping is not performed by the ONS 15302.

The ONS 15302 allows the operator full control each element of the packet/frame handling.

The QoS implementation supports several profile types, where each profile defines the nature of handling applied to frames belonging to that profile (e.g. amount of BW to be provided). A Classifier is a definition of which parts of the frames contents should be used to decide which frame belongs to which profile (e.g. which header bytes are of interest). Rules within each profile detail for each frame with a specific combination of values in the “interesting” bytes, which actions to take.

The following profiles are possible:

- Reserved Bandwidth allocation (“BW guarantee”) - A specific amount of Bandwidth is reserved for this profile. Traffic will not be allowed to go above this limit.
- Minimum BW guarantee - A specific amount of Bandwidth is reserved for this profile, but traffic may use more than the reserved amount, if available, at the best-effort service class.
- Reserved Bandwidth with Minimum Delay Guarantee - Traffic in this profile has reserved bandwidth, as explained above, and in addition is forwarded with minimum delay (i.e. sent before traffic belonging to one of the above profiles).
- Reserved Bandwidth with Minimum Delay Guarantee per session - Traffic in this profile is composed of a number of Sessions (identified by appropriate classifiers) with each one getting a specified Bandwidth reservation, as defined above, and with traffic for this profile being forwarded with the minimum delay, as explained above.

The two Minimum Delay Guarantee options are only available for Layer 3 (IP) QoS.

The following classifiers are possible:

- For each protocol supported (IP and Bridging) the user should define which header fields are of interest. Each such group of bytes is a classifier.
- Using the Policy MIB the user may specify fields in a general manner, using their offset. Using the Simple MIB, pre-defined possibilities cover the standard header fields of each protocol (e.g. Addresses, Ports, etc.).
  - In IP the predefined fields are: Source/Destination Addresses and ports, Protocol (TCP/UDP), TOS type.
  - For Layer 2 switching, predefined fields are Input Port only

The following rules are possible:

- After classifiers and profiles are defined, they are used to define rules by which frames/packets are assigned to one of the profiles defined, and the actions to be carried out on matching frames/packets.
- Each rule contains a pattern to match (values to match in the fields of interest in the classifier) and action definitions. Actions possible are:
  - Assign to a profile
  - Modifications to frame/packet fields (e.g. re-writing DSCP for IP packets, New VPT for bridged traffic, etc.)
  - Forward, drop, or send to the CPU etc.

### 2.4.3.1 Limitations

It's important to know that packet priority mechanism is overruled by QoS and packets will not be served according to their priority. The Ethernet ports do not support auto-negotiation in this mode and the port settings must therefore be fixed configured for 10 or 100Mbit/s.

When defining aggregate flow values as part of the bandwidth limitation parameters in the QoS configuration, a non-linear distribution happens where the actual bandwidth differs from what may be expected. This is a result of the algorithm used in the switching chip. A calculated ratio may be provided to translate between the configured parameters and the resulted bandwidth. Bandwidth Guarantee, Minimum Bandwidth Guarantee and Minimum Delay are all aggregate profiles. When configuring the intended rate for one of these profiles the rate to configure depends on the total number of sessions transmitted in the profile's range.

A session means each stream of traffic that is different from the others in a set of classifier fields but still belongs to the same profile. For instance if the user defines IP classification based upon protocol and destination IP address, but configures the rule based only on destination IP address then each additional stream of traffic which goes to the same destination but has a different protocol number will represent an additional session in the profile's range. Two traffic streams that have the same destination IP and the same protocol number represent a single session. The first session will get 1/2 of the configured bandwidth, the second session will get 1/3, third will get 1/4, and so on.

The following table presents different scenarios:

*Table 2-6 Scenarios - Intended rate vs. Rate to configure*

Number of Sessions in profile	Intended Bandwidth in Kbps.	Rate to configure in Kbps
1	2000	4000
1	4000	8000
1	1000	2000
2	2000	2400
2	4000	4800
2	1000	1200
3	2000	1846
3	6000	5538
3	4000	3692
3	3000	2769

## 2.5 TDM Features

This section describes the Cisco ONS 15302 TDM features.

### 2.5.1 Tributary Ports

ONS 15302 provides 12 120 ohm 2.048 MHz Tributary Ports on the customer side. 75 ohm operation is supported by adding an external balun.

Each Tributary Port can be individually configured to run in one of the following modes:

- G.703 Transparent (TRA)
- ISDN Primary Rate Access (PRA)



Note

PRA is implemented according to ETS 300011 and ETS 300233. The ONS 15302 can only implement the PRA NTE functions.

### 2.5.1.1 Transparent Transmission Mode.

In this mode 2.048 Mbit/s plesiochronous data and timing are transferred independently of frame structure. The two directions of transmission are completely independent of each other.

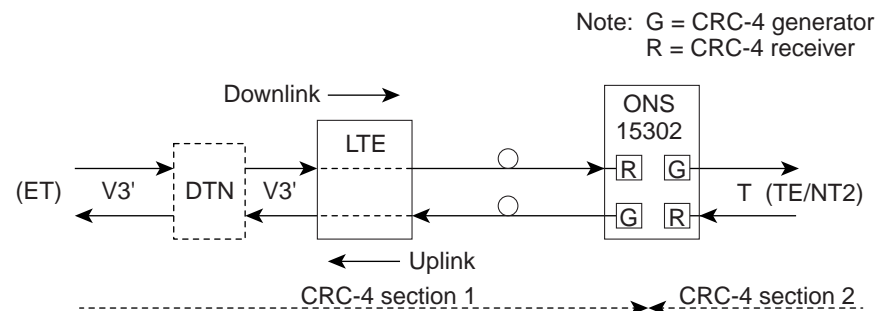
Downstream AIS is generated on loss of signal or loss of optical frame alignment.

### 2.5.1.2 ISDN Primary Rate Access (PRA) Transmission Mode.

The functional layout compliant to pr. ETS 300 233 is shown below.

DTN	Digital Network
V3' and V3	ISDN Reference Points, Exchange Termination Interface
T	ISDN Reference Point, Customer Interface
Downlink	Signal direction from Exchange Termination (ET)
Uplink	Signal direction to Exchange Termination (ET)

*Figure 2-5 ONS 15302 ISDN PRA Configuration*



83362

## 2.5.2 Downlink Transfer

The LTE is transparent to the 2 Mbit/s (Mbps) signal. However, monitoring the G.704 multiframe format is performed for detection of loop back 1 command from the Exchange Termination (TS 0 bit Sa6).

The NTE terminates CRC-4 section 1 by the Receiver (R) circuits, which pass the signal to the Generator (G) circuits with indication of basic frame start. The G circuits generate new TS 0 basic frame and multiframe to CRC-4 section 2, and pass transparently TS1 - TS31 and from TS 0 the RAI bit and the Sa-bits 4 to 8. AIS is generated to the TE on loss of signal and when R circuits have lost alignment to G.704 basic frames.

## 2.5.3 Uplink

The NTE terminates CRC-4 section 2 in the R circuits, which pass the signal to the G circuits with indication of basic frame start. The G circuits generate new TS 0 basic frame and multiframe to CRC-4 section 1 and pass transparently TS1- TS31 and from TS 0 the RAI bit and the Sa-bits 4,7 and 8.

The G circuits generate substituted frames to the ET on loss of signal or loss of alignment to basic G.704 frames from TE.

The LTE is transparent to the 2 Mbit/s (Mbps) signal.

On loss of optical line signal, the LTE generates an auxiliary pattern AUXP=1010.. to the ET.

## 2.5.4 Supervision by the Exchange Termination (ET)

The TS 0 bits Sa5 and Sa6 are used for supervision. Bit Sa5 being 0 downlink and 1 uplink, indicates the direction of transmission.

### 2.5.4.1 ET generated Downlink Sa6 Codes

Normal condition Sa6 = 0000

Loop back 1 command to LTE Sa6 = 1111

Loop back 2 command to NTE Sa6 = 1010

### 2.5.5 NTE generated Uplink Sa6 Codes

*Table 2-7 Time Slot 0 Signalling in PRA Mode*

Condition	Uplink report to Exchange Termination	Comments
Normal Operation	Sa6 = 00XX RAI = 0 Sa5 = 1	XX reports bit errors related to CRC-4 section 2
AIS Received at V3	Sa6 = 1111 RAI = 1 Sa5 = 1	RAI Generated by TE
Loss of Signal V3 (FV3) Loss of line signal or downlink FA (FC5)	Sa6 = 1110 RAI = 1 Sa5 = 1	RAI Generated by TE



*Table 2-7 Time Slot 0 Signalling in PRA Mode (continued)*

Condition	Uplink report to Exchange Termination	Comments
Loss of Signal at T (FC4)	Sa6 = 1100 RAI = 0 Sa5 = 1	The NTE generates substituted frames with RAI=0. Reporting of other failure conditions has priority.
Power failure (NTE dying gasp)	Sa6 = 1000 RAI = X Sa5 = 1	Reporting of this failure condition has the highest priority.
Loss of Line Signal at LTE (FC1)	AUXP	Auxiliary alarm indication pattern(1010..) generated by the LTE.
Loop back 1 activated by downlink Sa6=1111	Sa6 = 1111 RAI = 1 Sa5 = 0	The downlink signal is looped back fully transparently in the LTE.
Loop back 2 activated by downlink Sa6=1010	Sa6 = 00XX RAI = 1 Sa5 = 0	The TS1-TS31 and the TS 0 bits RAI, Sa4, 7 and 8 of the downlink signal are looped back by the NTE. Sa5 is changed to 0 by the NTE to indicate loop back condition.

## 2.5.6 Handling of CRC-4 Errors

CRC-4 errors detected in R circuits downlink and uplink are inserted as E bits to the ET and TE respectively.

If multiframe alignment is not obtained, the NTE reports all E bits 0 error.

Detected bit errors related to CRC-4 section 2 are reported to the ET by use of the two last bits of the Sa6 code in normal operational condition.

*Table 2-8 CRC-4 Section 2 Bit*

	Events	Sa6
a)	CRC-4 errors detected by the NTE:	0010
b)	CRC-4 errors reported as E-bits from the TE:	0001
	a) + b) or no MF alignment to signal received from the TE:	0011

ITU-T Rec.G.706, ANNEX B is applied to CRC-4 section 2 which means that the NTE stops searching for MF alignment after a given period of time without further actions. Continuous Sa6 = 0011 indicates to the ET that quality information is not available from CRC-4 section 2.

## 2.6 Test Loops

Two test loops are provided per Tributary Port, one in the customer direction (LL3) and one in the network direction (LL2), (Figure 2-6). One Tributary Port can have only one loop activated at a time. The test loops can be activated, deactivated and monitored by the management system. The loop control logic depends on the tributary mode (TRA or PRA).

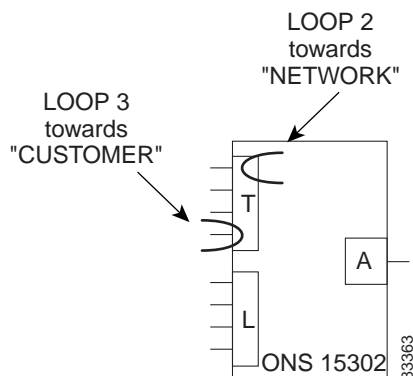
- In TRA mode the management system can operate the loops at any time as long as the port is enabled.
- In PRA mode the loops are supposed to be controlled by some exchange termination equipment (ET) via inband channel 0 control bits. In this mode it is not possible to operate the loops from the ONS 15302 management system.

It is possible to change the tributary mode regardless of the state of the loops. If the mode is changed, the loops will be cleared. The Test LED is on if any tributary loop is activated, regardless of the tributary mode.

To change the tributary mode, the loop must be cleared.

The Test Indicator LED is on if any tributary loop is closed, regardless of the tributary mode. This release does not support any monitor points.

*Figure 2-6 Test Loops Schematic View*



## 2.7 Alarm Ports

The ONS 15302 provides facilities to report four auxiliary alarm inputs for associated equipment, for example power unit failure, battery condition, cabinet door etc. These alarms are activated by an external loop between a pair of contacts.

The polarity of the auxiliary alarm input ports is a configurable parameter, this means alarm can be defined either as a loop closed or a loop open condition.

The alarms are reported to the management system. Each alarm input port may have an individual configurable textual description associated with it.

The ONS 15302 provides also support for two alarm output ports (Alarm out 1 and Alarm out 2) used to signal equipment alarms and traffic related alarms. Alarm out 1 and Alarm out 2 reflect the status of the operator LED and the customer LED respectively.

## 2.8 LED Indicators

The LED indicators are used to visualize the ONS 15302 status:

**Table 2-9 LED Functionality on the WAN Module Side**

Identity	Color	State On	State Flashing	State Off
PWR (Power)	Green	Presence of power	NA	Power failure
OPER (Operation)	Red	Alarm detected on aggregate interface	NA	No alarm detected on aggregate interface
CUST (Customer)	Red	Alarm detected on tributary or LAN interface	NA	No alarm detected on tributary or LAN interface
TEST (Test)	Yellow		One or more test are activated	
LAN 1	Green	Link is present	Traffic is present	Link down
LAN 2	Green	Link is present	Traffic is present	Link down
LAN 3	Green	Link is present	Traffic is present	Link down
LAN 4	Green	Link is present	Traffic is present	Link down

**Table 2-10 LED Functionality on the Connector Array Side**

Identity	Position	Color	State On	State Flashing	State Off
PWR (Power)		Green	Presence of power	NA	Power failure
OPER (Operation)		Red	Alarm detected on aggregate interface	NA	No alarm detected on aggregate interface
CUST (Customer)		Red	Alarm detected on tributary or LAN interface	NA	No alarm detected on tributary or LAN interface
TEST (Test)		Yellow		One or more test are activated	
LANn (n-1,2,3,4)	Left	Green	100 MBits/s (Mbps)	NA	NA
LANn (n-1,2,3,4)	Left	Yellow	10 MBits/s (Mbps)	NA	NA
LANn (n-1,2,3,4)	Right	Green	Link OK	Ethernet traffic in operation	Link down

## 2.9 User Channel

A transparent user channel is provided (F1 byte in RSOH) for transportation of general data. The interface is balanced RS485 and supports synchronous 64 kbit/s or asynchronous 19.2 kbit/s by configuration.

## 2.10 Automatic System Clock Setting

The ONS 15302 supports time protocol (RFC 868) for automatic date and time adjustment. To utilize this feature a TP server must be available in the network.

Because the time protocol provides UTC (GMT) only, and does not take into account the Day Light Saving Time (summer time), an additional parameter (UTC Delta) allows the user to get the local time. This parameter must be adjusted twice a year to take into account the Day Light Saving Time.

Relevant ONSCLI commands are found in [Table 2-11](#) to [Table 2-13](#).

*Table 2-11 Current Device Time*

ONSCLI Command	Description	Format
TIME (SYSTEM)	Should be adjusted during first time installation. In case of periods with lacks of power the Time settings will be kept in memory for a period of 48 hours	hh:mm:ss

*Table 2-12 Current Device Date*

ONSCLI Command	Description	Format
DATE	Should be adjusted during first time installation. In case of periods with lacks of power the Date settings will be kept in memory for a period of 48 hours.	yyyy-mm-dd

*Table 2-13 UTC Delta*

ONSCLI Command	Description	Format
UTC-DELTA	Used to adjust the GMT time received from the server to the local time, and to possibly take into account the Day-Light Saving Time. Default setting: 0	integer[-720:720min]



Note

This parameter is not recommended or required to configure when using the CiscoEdgeCraft as configuration tool since this calculation is best maintained by the management system.

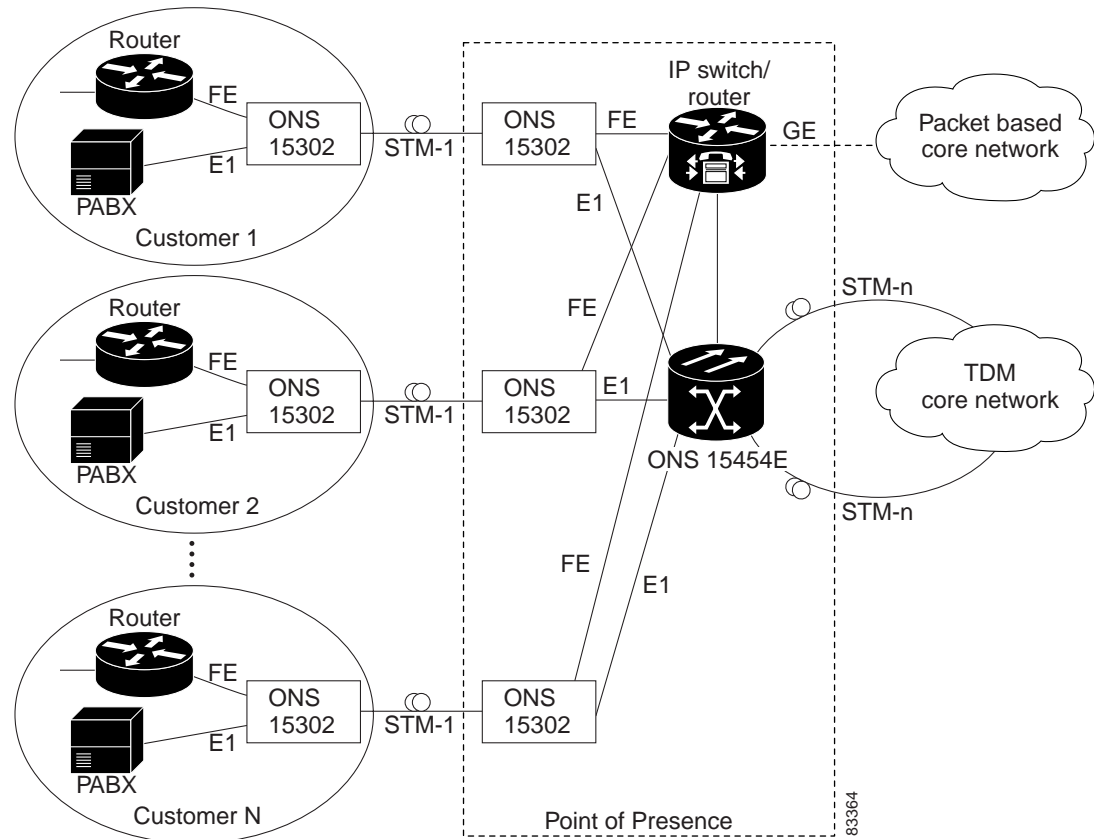
## 2.11 Applications

The following subsections describes different Cisco ONS 15302 applications.

### 2.11.1 Back to Back Application

Normally the ONS 15302 at the customer site is connected to an ONS 15302 at the operator point of presence (PoP). A number of these systems can be connected in a star network and the Ethernet traffic is groomed by an Ethernet switch before it is transmitted to the core network. [Figure 2-7](#) shows the layout of a typical system with the ONS 15302 incorporated. The network in this figure does not have a separate Ethernet backbone network, but this could easily be supported.

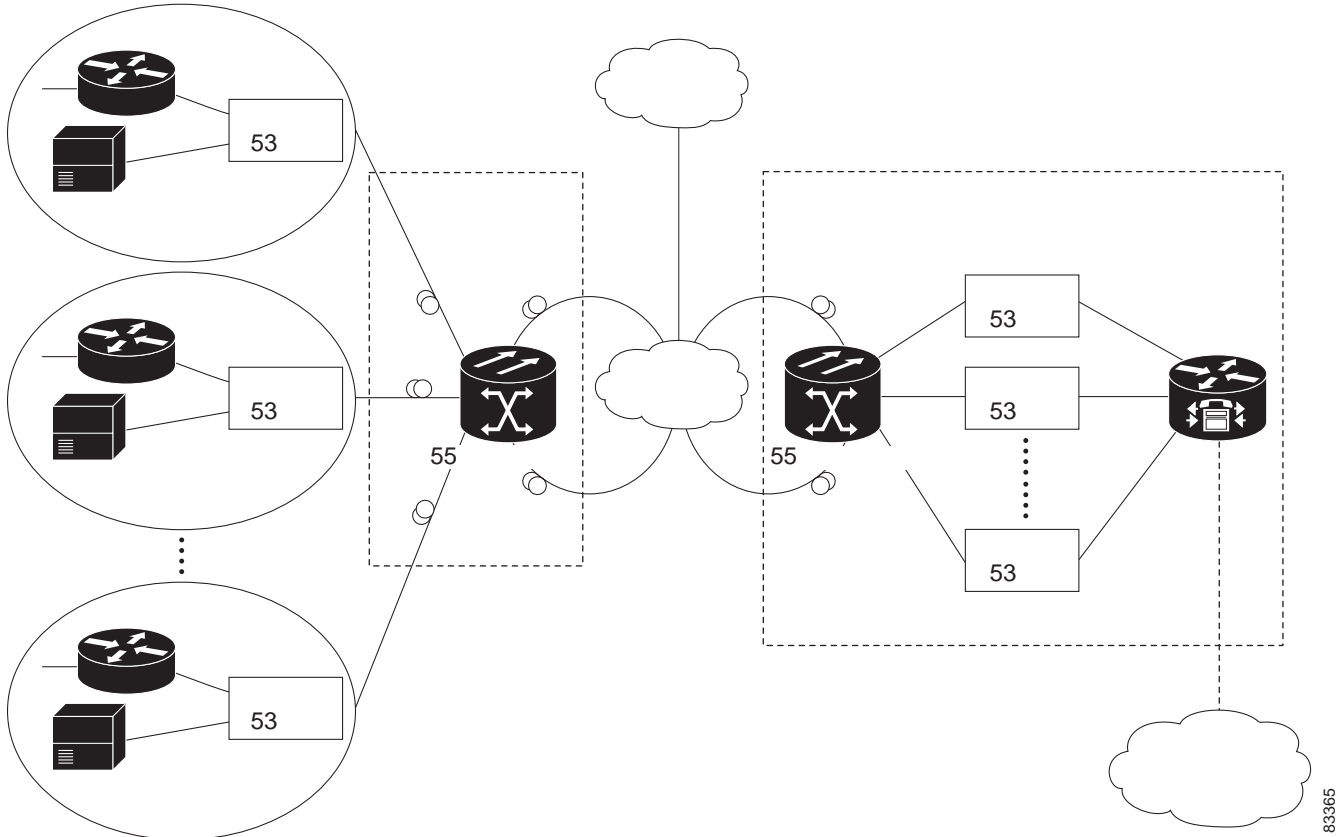
*Figure 2-7 Back to Back Configuration across the Access Loop*



## 2.11.2 Remote Back to Back Application

The ONS 15302 can also be directly connected to the SDH transport network if the operator wants to do Ethernet grooming at a different site as shown in the figure below.

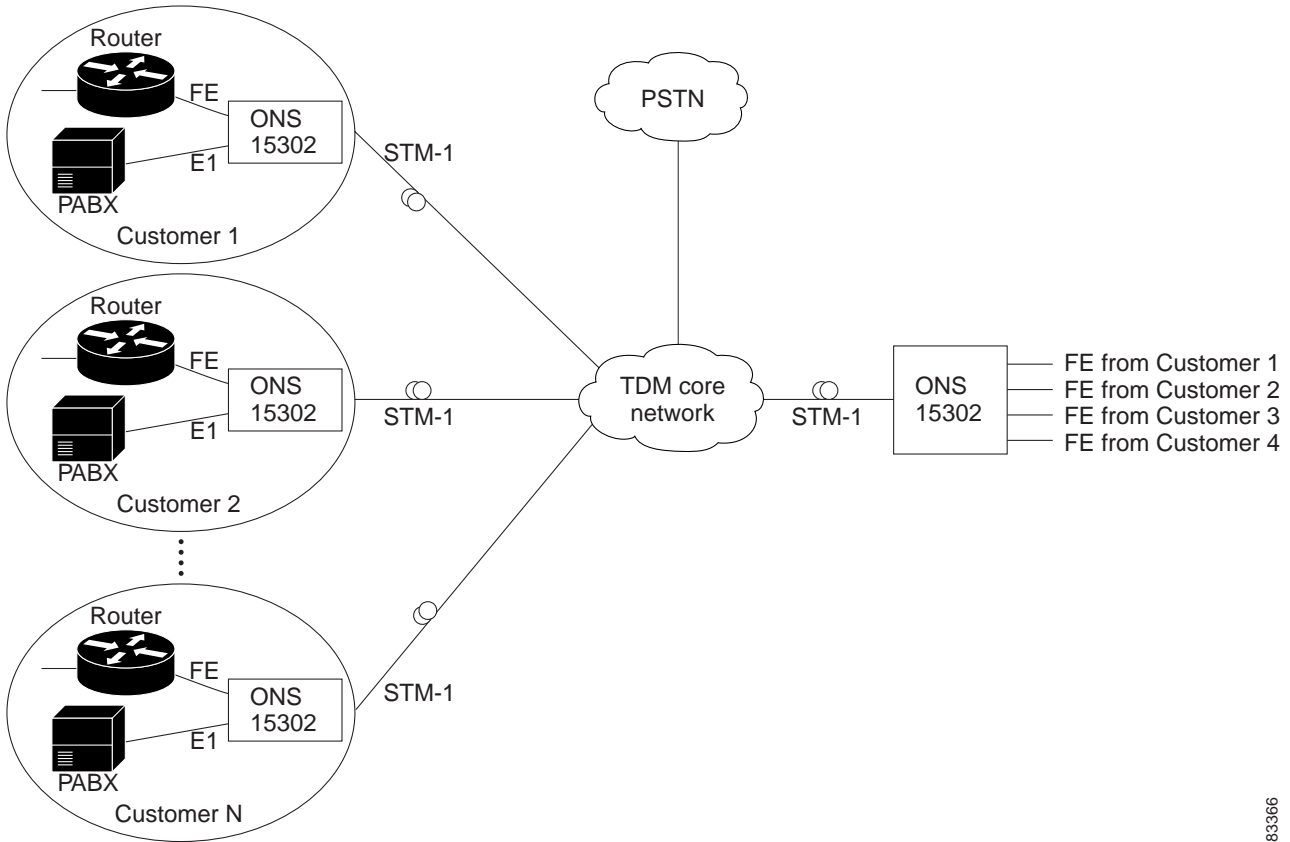
Figure 2-8 Typical System with no Local Grooming in the PoP



## 2.11.3 Headquarter Office to Branch Office

The ONS 15302 can be connected to four different ONS 15302 units without any additional Ethernet switch [Figure 2-9](#).

Figure 2-9 Typical System when connected to an ONS 15302

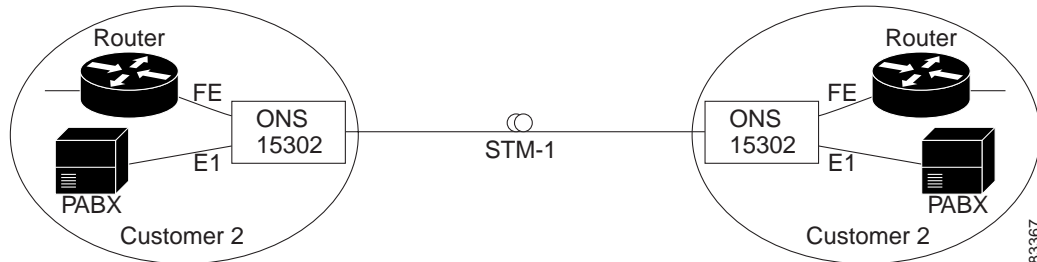


83366

## 2.11.4 Campus Application

The ONS 15302 can also be connected back to back without any connection to external networks [Figure 2-10](#).

Figure 2-10 Typical Network when used in a Campus Application



83367

## 2.12 Management

The following main features are supported by the ONS 15302 management system:

- Alarm Handling
- Configuration Management
- Performance Monitoring
- Test Support
- Backup/Restore
- Software Download
- Security

The ONS 15302 management solution is based on an embedded SNMP agent, which can be accessed locally or from a remote management application.

### 2.12.1 Supported MIBs

In addition to the enterprise specific MIBs, the standard MIBs in the below [Table 2-14](#) are partly supported. Partly supported means that relevant parts of the listed MIBs are implemented and used to manage the associated features in the NEs (Network Elements). Not all parts of the MIBs are used, and there are other features in the NEs not managed through standard MIBs (because covering standard MIBs for the latter features do not exist).

*Table 2-14 ONS 15302 MIBs*

RFC #	Mnemonic	Title
1213	MIB-II	Management Information Base for Network Management of TCP/IP-based internets: MIB-II
1724	RIP2-MIB	RIP Version 2 MIB Extensions
1471	PPP-LCP-MIB	The Definitions of Managed Objects for the Link Control Protocol of the Point-to-Point Protocol
1473	PPP-IP-NCP-MIB	The Definitions of Managed Objects for the IP Network Control Protocol of the Point-to-Point Protocol
1493	BRIDGE-MIB	Definitions of Managed Objects for Bridges
1757	RMON-MIB	Remote Monitoring (RMON) Management Information Base
1850	OSPF-MIB	OSPF Version 2 Management Information Base
2096	IP-FORWARD-MIB	IP Forwarding Table MIB
2233	IF-MIB	The Interfaces Group MIB using SMIV2
2495	DS1-MIB	Definitions of Managed Objects for the DS1, E1, DS2 and E2 Interface Types
2558	SONET-MIB	Definitions of Managed Objects for the SONET/SDH Interface Type
2665	EtherLike-MIB	Definitions of Managed Objects for the Ethernet-like Interface Types.
2674	P-BRIDGE-MIBQ-BRIDGE-MIB	Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions



Table 2-14 ONS 15302 MIBs (continued)

RFC #	Mnemonic	Title
2932	IPMROUTE-STD-MIB	IPv4 Multicast Routing MIB
2933	IGMP-STD-MIB	Internet Group Management Protocol MIB
2934	PIM-MIB	Protocol Independent Multicast MIB for IPv4

## 2.12.2 Command Line Interface (ONSCLI)

ONS 15302 supports a serial EIA/TIA 232 interface called ONSCLI. ONSCLI is a line oriented ASCII based management interface, which provides a simple local connection to any VT100 compatible terminal. ONSCLI is protected by a password.

The ONS 15302 also supports the connection of a remote ONSCLI terminal over Telnet/IP.

### 2.12.2.1 Various ONSCLI Management Access Solutions

ONS 15302 is managed by means of the Optical Network System Command Line Interface (ONSCLI). ONSCLI is an ASCII based VT100 terminal interface. The ONS 15302 can be fully managed by means of the ONSCLI interface.

Figure 2-11 Local Management with ONSCLI

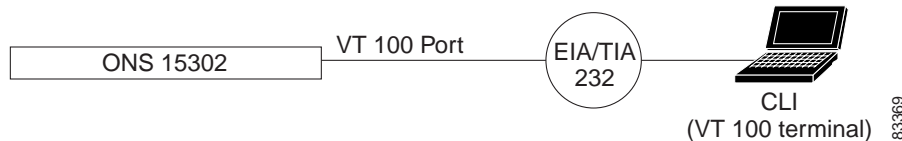
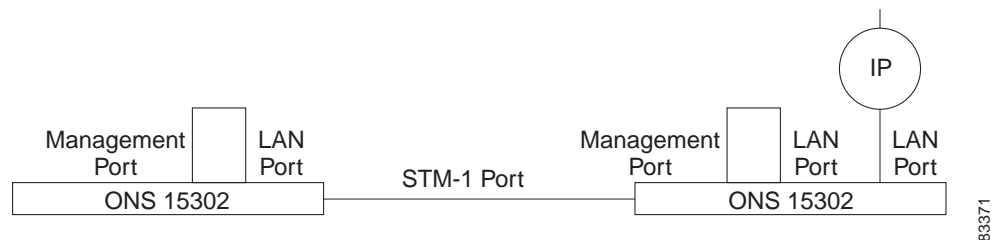


Figure 2-12 Possible Remote Management via In Band Traffic



(Looping remote LAN Port to Management Port. See [Inband via one of the LAN Ports](#), page 2-26 for restrictions).



**Note** Only one session (local or remote) is allowed at a time.

## 2.12.3 Management Connectivity

A local Ethernet interface, called the Management Port, is available for connecting to a management DCN. This port is compatible with IEEE 802.3 and supports 10/100BaseT Ethernet for UTP cables.

If an ONS 15302 has no connectivity to the management DCN via the Management Port, mechanisms for transporting management information in the STM-1 DCC channel are provided.

The ONS 15302 management system is based on SNMP and an IP based DCN. However, if an IP based DCN is not available, ONS 15302 provides a mechanism for connecting via IpPPP based DCN.

### 2.12.3.1 Ways of Connecting to the Management DCN

ONS 15302 can connect to the management DCN in different ways:

#### Via the dedicated Ethernet Connector (Management Port)

This solution assumes that both ONS 15302s in a pair have local IP- or OSI connectivity.

#### Via a proprietary HDLC based Protocol in the STM-1 DCC (DCC-R or DCC-M)

This solution assumes that one of the two ONS 15302s in a pair has IP connectivity via the Management Port and that the DCC channel is transparent between the two devices. In this mode, packets received via the Management Port are broadcasted over the DCC HDLC if the MAC address is within the range assigned to Cisco.

#### Inband via one of the LAN Ports

In this case the Management Port must be physically connected to one of the LAN ports via an external HUB. The management traffic is carried over the Bridge WAN port. If the ONS 15302 device is not managed by the customer itself, the LAN port used for management must belong to a separate VLAN, this means only three ports are left for customer access.

#### IP Inband

IP inband means that LAN and WAN ports are carrying management traffic together with customer traffic. The configuration is described in [2.14 DCN Configurations Supported, page 2-27](#).

When using IP inband, the management traffic can be routed or switched (using VLANs). If routed, the routing is carried out in hardware (FFT) if IP routing is enabled. Otherwise, IP forwarding is used, this means software based.

Every ONS 15302 has one and only one IP address allocated to it. ONS 15302 also keeps the IP address of its mate ONS 15302. This simplifies the toggling between two ONS 15302s in a pair. In addition, the flexibility above implies the actual DCN strategy must be decided and configured per device (parameters like DCC enable/disable, IP/HDLC etc.).

All ONS 15302 protocol stack options for implementing the above DCN strategies is illustrated in [Figure 2-2](#).

## 2.13 DCN Features

The required DCN protocol support is shown in [Figure 2-2](#).

The ONSCLI apply the standards in [Table 2-15](#).

*Table 2-15 Protocol Standards*

Abbreviation	Standard
Bridge	IEEE 802.1d - Media Access Control Bridges, 1998 Edition Revision (incorporating IEEE 802.1p). The requirements in chapter 0 apply.
MAC / LLC	IEEE 802.x - Information Processing Systems - Local Area Networks
HDLC	ISO 4335 - High level Data Link Control (HDLC) procedures
IP	RFC 791 - Internetwork Protocol
RS-232	EIA/TIA 232
TCP	RFC 793 - Transmission Control Protocol (TCP)
UDP	RFC 768 - User Datagram Protocol (UDP)
PPP	RFC 1661 - The Point to Point Protocol

### 2.13.1 SDH DCC Channels

Both DCCR (Regenerator Section) and DCCM (Multiplexer Section) channels are supported independently. Note that both channels should not be active on the same port simultaneously, as this will result in looping of the traffic. Activation/deactivation of DCC channels is configurable on a per port basis. The SDH DCC IP/PPP transport mechanism supports only traffic on the DCC-R. The DCC-M is by default turned off, when the IP/PPP/DCC-R mode is enabled.

#### TELNET

Telnet sessions are possible via all paths of management traffic. Multiple Telnet sessions are not possible.

#### Security

It is possible to restrict management access to the ONS 15302.

## 2.14 DCN Configurations Supported

In this context the term DCN (Data Communication Network) is used to denote the network that transports management information between a management station and the NE. This definition of DCN is sometimes referred to as MCN (Management Communication Network). The DCN is usually physically or logically separated from the customer network.

The ONS 15302 management solution is based on SNMP over IP. The main purpose of the DCN implementation is to provide connectivity to the SNMP Agent inside the OSN 15302 via different DCN topologies. The DCN implementation also support transport of management traffic between other Cisco or third party nodes.

Although the management application is IP-based, the DCN solution also support OSI-only and mixed IP/OSI-networks at layer 2 and 3. The various options and features related to different DCN topologies are specified throughout this section.

In general, the term OSI in this section is used to denote a CLNP-routed network, ie. it is only used for L3. Higher level OSI-protocols are not considered. At L2 different protocols are supported, including LAP-D. The ONS 15302 OSI-implementation supports CLNP, IS-IS Level 1 and Level 2 and ES-IS.

For the IP In-band L2 topology the management traffic is switched/routed between LAN/WAN ports. When IP-addressing a VLAN IF (id 100000-104000) the management connectivity is obtained at wire-speed along with the user traffic or on a separate WAN-port dedicated for management.

For all other cases, the following applies:

- The DCN traffic is always routed (IP or OSI) between the management interfaces.
- Two different router modes are available for management connectivity.
  - One operates for Numbered mode and the second operates in Un-numbered mode. Both routers are not accessible for DCN purpose simultaneously, and a system mode is introduced to enable desired router.
- Software based DCN routing does not require a routing licence.

Most topologies in the following sections assume standard numbered IP interfaces, ie. every interface connected to the router takes an IP address and a subnet. However, from R2.0 on, a new feature called IP Unnumbered Interfaces is supported. With this feature the device will need only one IP address .

## 2.14.1 Management Interfaces

The following interfaces may be used to carry management traffic.

### 2.14.1.1 Management port

The ONS 15302 has a dedicated Ethernet port for management, called the Management Port. This port can be used for local management, e.g. connecting a craft terminal. It can also be used for connecting to a separate external management network. The management port can be turned off to avoid unauthorised local access. The management port cannot be member of a VLAN.

### 2.14.1.2 LAN ports

The LAN ports are FE Ethernet ports used for connecting customer IP traffic to the OSN 15302. LAN-ports in ONS 15302 are connected to the switch and can be used to carry management traffic.

### 2.14.1.3 WAN ports

The WAN ports are device internal FE Ethernet ports that can be mapped into one or more virtual containers of an SDH STM-n signal. From a DCN perspective, there are no functional differences between LAN and WAN ports in ONS 15302.

### 2.14.1.4 DCC channels

The SDH architecture defines data communication channels (DCC) for transport of management traffic in the regenerator section ( $DCC_R$  - 192 kbit/s) and in the multiplexer section ( $DCC_M$  - 576 kbit/s).

The two SDH-links in ONS 15302 may terminate up to 4 DCC channels (2  $DCC_R$  and/or 4  $DCC_M$ ). All DCC channels may be active simultaneously, but this depends on the selected mode. Activation/deactivation of DCC channels is configurable on a per port basis.

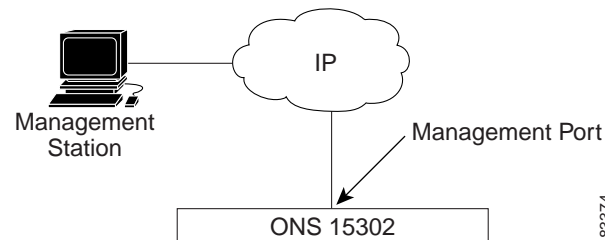
### 2.14.1.5 Local VT-100 serial port

Also this RS-232 interface is regarded as a management interface, although it does not relate to the various DCN topologies described throughout the rest of this section. In ONS15302 full management capability is provided over the ONSCLI.

## 2.14.2 DCN on Management Port

This configuration is applicable for users connecting an IP based DCN directly to the ONS 15302. For this type of connection, the management port is used, see [Figure 2-13](#).

*Figure 2-13 DCN on Management Port*

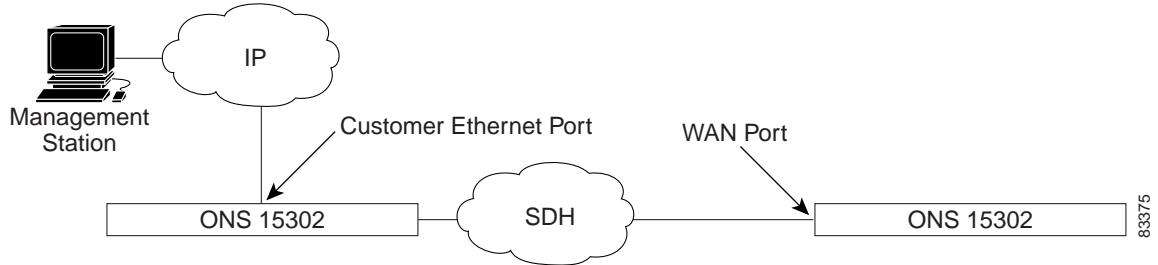


### 2.14.3 DCN on customer Ethernet Port or WAN Port

This configuration is applicable if the user is connected to one of the customer Ethernet ports, or one of the WAN ports (in band management). IP-Inband means that LAN and WAN ports are carrying management traffic together with customer traffic. This is useful in topologies where (parts of) the SDH-network is owned by a different operator which does not allow a third party to use the DCC capacity. With IP in-band it is possible to build tunnels between islands that have other DCN solutions.

In ONS 15302 all LAN- and WAN-ports are connected to the switch. Any LAN- or WAN-port may be used to carry in-band management traffic, assuming an IP-address is assigned to it, or to the VLAN it belongs to. Between LAN/WAN ports the switching is always at wire-speed. Between LAN/WAN and other management interfaces the traffic is always routed by the CPU. It is possible to split management traffic from user traffic by assigning dedicated LAN/WAN ports to management traffic.

Figure 2-14 DCN on Customer Ethernet Port or WAN Port



## 2.14.4 PPP/DCC DCN

PPP/DCC means that the management IP-traffic is carried in PPP over the SDH DCC channels according to NSIF-DN-0101-001. The PPP implementation supports RFC1661 (PPP), RFC1662 (PPP in HDLC-like framing) and RFC1332 (IPCP).

Each PPP/DCC channel connects to the IP router individually. Normally this would take one IP subnet per DCC-link, and this is how previous versions of AXX155E would behave.

However, from ONS 15302 R2.0 on a more comprehensive PPP/DCC strategy is supported. This strategy is based on the feature called IP Unnumbered Interfaces, and the rest of this section assumes this option.

The IP Unnumbered concept allows the system to provide IP processing on a serial interface or in general a point-to-point without assigning it an explicit IP address. The IP unnumbered interface borrows the IP address of another interface already configured on the system/router (ie. the Management Port), thereby conserving network and address space, and making the system easier to configure, manage and maintain.

With IP Unnumbered, all nodes connected via PPP-links may be on the same IP subnet. An essential part of the implementation is the DCN ARP Proxy Agent, which makes sure that connectivity between the nodes is obtained without having to provision static routes. The Proxy Agent builds entries for all the DCN IP destinations, and will reply to ARP requests on behalf of them.

IP Unnumbered is regarded as a main mode, and can not be combined with other modes that require numbered interfaces. This implies that this PPP/DCC option can not be combined with IP Inband or OSI.

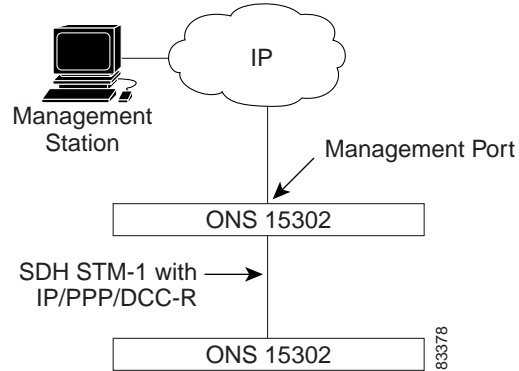
### 2.14.4.1 Compatibility issues

The ONS 15302 R2.0 is able to provide DCN connectivity with all types of AXXESSIT devices already deployed, including the installed base of ONS 15302 devices with an earlier software revision. Hence, two additional DCN options, are supported; PPP/DCC for numbered interfaces and proprietary IP/DCC communication.

### 2.14.4.2 PPP/DCC (IP over PPP)

ONS 15302 supports PPP/DCC also on numbered interfaces. This option can not co-exist with the IP unnumbered version of PPP/DCC. However, the numbered variant of PPP/DCC has the advantage that it can be used in combination with all other DCN modes.

Figure 2-15 IP DCN connectivity to a 3rd Party Network Element

**Note**

In the previous ONS 15302 release (R1.0), PPP was only supported over DCC<sub>R</sub>. The R2.0 supports both DCC<sub>M</sub> and DCC<sub>R</sub>.

### 2.14.4.3 IP/DCC (IP over HDLC)

This configuration is applicable for a user having a subnet of Cisco devices and an IP based DCN connected to the management port of the ONS 15302.

IP/DCC is a non-standard IP broadcast mechanism used for conveying management information on the SDH DCC channels in a network of Cisco devices only. The IP datagrams are encapsulated in HDLC frames before they are sent out on the SDH DCC. Broadcast in this context means that the AXXESSIT devices emulate a shared medium on the SDH DCC channels at the MAC layer. Packets with destination MAC different from the device's MAC are forwarded transparently to the active DCC Tx channel(s).

In order not to saturate the DCC with unnecessary traffic, a filtering mechanism for MAC frames can be enabled. If the filter is enabled, MAC frames received via the management port are broadcasted over DCC only if their destination MAC address is within the range assigned to a Cisco system.

An ONS 15302 configured to broadcast management traffic over the management port and DCC (as described above) can be used to provide IP DCN connectivity to a 3rd party network element via its Management Port, provided that the filter mechanism for MAC frames is disabled.

The IP/DCC option has two special restrictions, imposed by the proprietary pseudo-broadcast mechanism:

- Maximum one DCC per link (M or R)
- The broadcast solution cannot be used in a MSP protection configuration, which involves one, or more radio hops

Figure 2-16 Broadcasting over Management Port and HDLC- DCC

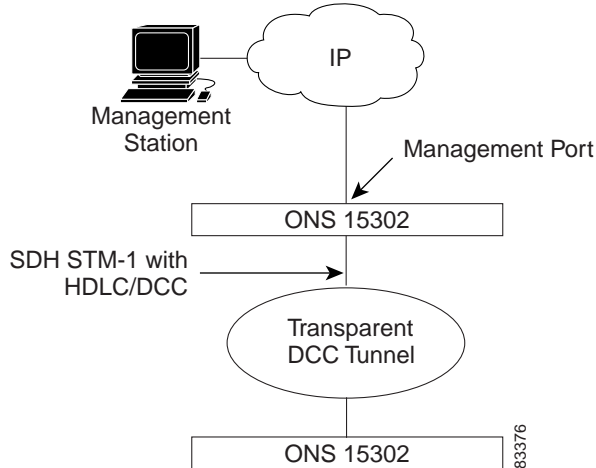
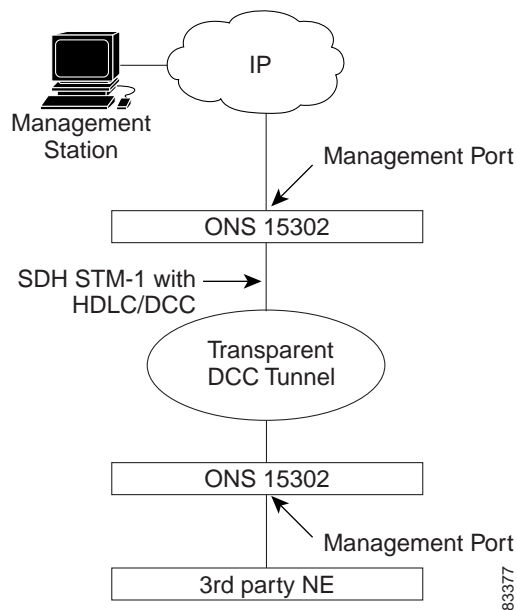


Figure 2-17 IP DCN connectivity to a 3rd Party Network Element



## 2.14.5 Protection

The two SDH-links in ONS 15302 are protected by means of MSP (1+1 link protection)

For MSP protected links, the DCN behavior depends on the DCN mode:

- If the mode is PPP/DCC (numbered or unnumbered) or IP/DCC (broadcast), the management traffic over DCC follows the user traffic, i.e. traffic is sent over both links (working and protecting), but received only from the active link.
- In all other modes, the two DCC channels will be individual interfaces to the router (CLNP and/or IP), and switch-over will be handled at routing level.



## 2.14.6 Security

In order to prevent unauthorized access to the SNMP Agent, the following security and traffic control features are supported

### 2.14.6.1 Management Port On/Off

The Management Port can be turned on and off, thereby preventing unauthorized local access to the management network.

### 2.14.6.2 SNMPv1 Community

The SNMPv1 packet contains a password (called community string) that must be known by both the manager and the agent. Different community names can be defined for read and read/write access. The community string is, however, transferred un-encrypted.

### 2.14.6.3 SNMP Manager Identity

This is an enhancement of the SNMPv1 Community feature. Here, the SNMP manager's IP address must be configured in the device subject to management. Only legal combinations of community name and source IP address in SNMP requests are accepted.

### 2.14.6.4 SNMP Read/Write control

The access rights of the registered management systems can be set to read/write or read only.

### 2.14.6.5 VLAN (802.1Q)

This security mechanism relates to the IP in-band option only: By configuring a separate VLAN for the management traffic and assigning an IP address to it, the end-users will not be able to access the device or generate traffic into the management VLAN.

### 2.14.6.6 ONSCLI Access Control

ONSCLI is protected by user name and password. ONSCLI is by default a superuser and can block all remote SNMP users by changing the access rights and passwords. Remote CLI access via Telnet must in addition have a Telnet password.

## 2.15 ONS 15302 Management

The description of the ONS 15302 management system refers to manageable objects as listed in [Table 2-16](#).

*Table 2-16 Managed Object*

Object Name	#	Description
Device	1	The ONS 15302 unit itself
Bridge Port	5	The four LAN Ports plus the WAN Port mapped into the STM-1
Tributary Port	4	The 2048 kHz tributary interfaces
Aggregate Port	1(2)	The STM-1 aggregate. Optical or Electrical. Dual ports for MSP (1+1) or single fiber operation.
Auxiliary Port	4	The general purpose auxiliary interfaces
Bridge	1	Common Bridge functionality, like VLAN and Spanning Tree

## 2.16 Fault Management

The following subsections describes Cisco ONS 15302 fault management.

### 2.16.1 Alarm Handling

The alarms are related to a managed object as defined in [Table 2-16](#).

The ONS 15302 keeps a record of current and historical alarm events.

The list of current alarms contains the following parameters for each alarm:

- Timestamp
- Alarm Object (for example. Tributary Port 1, Aggregate Port)
- Alarm Identifier
- KLM value if applicable
- Port Affected
- Alarm Description

Port alarms are suppressed if the port itself is disabled. In order to avoid alarm flooding, alarms at different levels are correlated. Lower order alarms are suppressed if a more important alarm at a higher level is active.

In addition to the alarms, the ONS 15302 may generate a number of events. The events are not stored in the current alarm list, but they are appended to the historical alarm list in the same way as the alarms. The historical alarm list contains the same parameters per alarm as the current alarm list, and in addition the following parameter:

- Event Type (RAISED, CLEARED or EVENT)

Both the alarms and the events generate SNMP traps. The traps can be sent to a number of management stations. It is possible to turn SNMP trap sending on or off on a per manager basis. This is the only alarm filtering mechanism provided by the ONS 15302.



Note

The bridge port LOSLA alarm is handled slightly different from the rest of the alarms. If a bridge port is unconnected or if it is forced down by the operator, it will cause a LOSLA event, which goes into the historical alarm list like other alarms. These alarms will, however, not cause a red LED to be lit, and they will not be stored in the current alarm list like the other alarms.



Note

The LPPLM alarm is only supported for the VC-12 containers used by the tributary ports. It is not supported for the VC-12(s) constituting the WAN port.



Note

The MSDEG and LPDEG alarms are based on the near end BER counters over 20 seconds intervals.

*Table 2-17 Criteria for Turning Alarms On and Off*

Alarm	ON	OFF
MSDEG	> 10 exp -7	< 10 exp -8
LPDEG	> 10 exp -6	< 10 exp -7

## 2.16.2 Alarm Severity

The Alarm Severity is configurable per alarm object. Default values are assigned automatically as shown in [Table 2-19](#).

### 2.16.2.1 Alarm Definition

The list below contains all the alarms that are defined for the ONS 15302. For some of the Alarm IDs, the direction (RX or TX) is an integral part of the name. This terminology is used for the direction:

- RX: Downlink (from network to customer)
- TX: Uplink (from customer to network)

*Table 2-18 ONS 15302 Alarms*

Alarm		Description	Default Severity
ONS15302	HWFAIL	Hardware failure.	Critical
	LOSSY	Loss of external sync.	Minor
	SyncHoldOver	Loss of configured synchronisation source	Major
	TEMP	Too high temperature in the unit i.e. above +45° Celsius	Critical
	FAN	FAN failure.	Major
ALARM	AUX	Dry contact alarm.	Warning

Table 2-18 ONS 15302 Alarms (continued)

Alarm		Description	Default Severity
SDH (STM-1)	LOS	Loss of STM-1 signal.	Critical
	LOF	Loss of frame alignment on the STM-1 signal.	Critical
	TD	Transmit Degrade on laser (Not applicable for electrical interface).	Minor
	TF	Transmit fail on laser (Not applicable for electrical interface).	Critical
RS	TIM	Trace Identifier mismatch (J0-byte).	Critical
	CSF	Communication subsystem failure, DCCR communication failure. (Just applicable for OSI-routing)	Minor
	EXC	Excessive error defect. BER > E-5	Major
	DEG	Degraded signal defect. BER > E-6 - E-9 (default E-6)	Minor
MS	AIS	Alarm Indication signal.	Minor
	EXC	Excessive error defect.	Major
	DEG	Degraded signal defect.	Minor
	RDI	Remote Defect indication.	Minor
	CSF	Communication subsystem failure, DCCM communication failure. (Just applicable for OSI-routing)	Minor
MSP	MSP	Problem with MSP (1+1 protection) signalling with another NE across K1/K2 bytes.	Minor
AU4	LOP	Loss of pointer	Critical
	AIS	Alarm indication signal	Minor
VC4	LOM	Loss of multi-frame alignment	Critical
	UNEQ	Unequipped.	Minor
	TIM	Trace identifier mismatch (J1-byte).	Critical
	PLM	Payload mismatch.	Critical
	EXC	Excessive error defect. BER > E-5	Major
	DEG	Degraded signal defect. BER > E-6 - E-9 (default E-6)	Minor
	RDI	Remote defect indication.	Minor
TU12	AIS	Alarm indication signal.	Minor
	LOP	Loss of pointer.	Critical

Table 2-18 ONS 15302 Alarms (continued)

Alarm		Description	Default Severity
VC12	UNEQ	Unequipped.	Minor
	TIM	Trace identifier mismatch (J2-byte).	Critical
	PLM	Payload mismatch.	Critical
	EXC	Excessive error defect. BER > E-5	Major
	DEG	Degraded signal defect. BER > E-6 - E-9 (default E-6)	Minor
	RDI	Remote defect indication.	Minor
Tributary (E1)	LOSTX	Loss of signal.	Critical
	AISRX	Alarm indication signal network side.	Warning
	LFARX	Loss of frame alignment customer side.	Major
	LFATX	Loss of frame alignment customer side.	Major
	UNASS	Tributary (E1) activated but not mapped to an available VC-12.	Critical
Ethernet WAN-port Proprietary	WANDELAY	Differential VC-12 delay for the WAN port is greater than +/-6,5ms	Critical
	seqFail	Seq wrong channel number p2p, i.e. wrong order of VC-12 allocated to a WAN-port...or one or more VC-12 containers not carrying Ethernet traffic terminated on the WAN-port.	Critical

## 2.16.3 Alarm Definitions

The different alarms together with their relations to the managed objects are defined in [Chapter 9](#), “Managed Objects,”

## 2.16.4 Alarm Parameters

[Table 2-19](#) defines the parameters associated with an alarm.

Table 2-19 Alarm Parameters

Parameter	Description
Timestamp	Date/Time of alarm event
Alarm Object	Object subject to alarm situation. Should contain both object type (class) and identification (instance).
Alarm Identifier	Short form alarm description, for example LOS
Alarm Description	Alarm description, for example Loss of signal

*Table 2-19 Alarm Parameters (continued)*

Parameter	Description
Alarm Severity	According to ITU-T X.733
Event Type	Raised, Cleared or Event. Applicable for alarm log only. Event means alarm with no duration.

The Alarm Severity is configurable per alarm object. Default values are assigned automatically.

## 2.16.5 Alarm Suppression

Alarms are suppressed if the object subject to alarm is disabled. It is possible to inhibit alarm reporting for a specific managed object. It is possible to inhibit all alarms from one ONS 15302. All SDH and PDH objects have two configurable persistency filters:

- Persistency filter alarm on: alarms must have been on for a certain amount of time before being reported.
- Persistency filter alarm off: alarms must have been off for a certain amount of time before being cleared.

In addition, the STM-1 interfaces follow the alarm suppression, ([Table 2-20](#)).

*Table 2-20 Alarm Suppression*

Object-Id	Alarm-Id	Suppress the following alarms
SDH	LOS	yes
	LOF	yes
RS	TIM	yes
	CSF	no
	EXC	no
	DEG	no
MS	AIS	yes
	CSF	no
	RDI	no
	EXC	no
	DEG	no
MSP	MSP	no
AU4	LOP	yes
	AIS	yes

*Table 2-20 Alarm Suppression (continued)*

Object-Id	Alarm-Id	Suppress the following alarms
VC-4	UNEQ	yes
	TIM	yes
	EXC	no
	DEG	no
	RDI	no
	PLM	yes
	LOM	yes
TU12	LOP	yes
	AIS	yes
VC-12	UNEQ	yes
	TIM	yes
	EXC	no
	DEG	no
	RDI	no
	PLM	yes
Tributary	AISRX	yes
	LFARX	yes

### 2.16.5.1 Alarm Suppression for Tributary Tx-Alarms

*Table 2-21 Alarm Suppression for Tributary Tx-Alarms*

Object-Id	Alarm-Id	Suppress the following alarms
Tributary	LOSTX	yes
LFATX	LFATX	yes

### 2.16.5.2 VC-4 Alarm Suppression for EXC/DEG

*Table 2-22 VC-4 Alarm Suppression for EXC/DEG*

Object-Id	Alarm-Id	Suppress the following alarms
VC-4	EXC	yes
	DEG	no

### 2.16.5.3 RS Alarm Suppression for EXC/DEG

*Table 2-23 RS Alarm Suppression for EXC/DEG*

Object-Id	Alarm-Id	Suppress the following alarms
RS	EXC	yes
	DEG	no

### 2.16.5.4 MS Alarm Suppression for EXC/DEG

*Table 2-24 MS Alarm Suppression for EXC/DEG*

Object-Id	Alarm-Id	Suppress the following alarms
MS	EXC	yes
	DEG	no

### 2.16.5.5 VC-12 Alarm Suppression for EXC/DEG

*Table 2-25 VC-12 Alarm Suppression for EXC/DEG*

Object-Id	Alarm-Id	Suppress the following alarms
VC-12	EXC	yes
	DEG	no

## 2.16.6 Alarm Collection

It is possible to view the alarms of all ONS 15302 devices present in the network, for example currently reachable from the management system. The ONS 15302 device stores a list of all current alarms and a log of alarm events. The size of the log of alarm events is 1000 entries.

## 2.16.7 Alarm Classification

It is possible for the operator to change the assignment of alarm severity for each pair of Object Type Alarm ID.

The possible severity levels are:

- WARNING
- MINOR
- MAJOR
- CRITICAL



## 2.16.8 Alarm Indication

The Customer LED on indicates that one or more Tributary alarms are on.

The Operator LED on indicates any alarm on, other than AUX alarms and Tributary alarms.

It is possible to define an alarm severity threshold for each LED defining which alarm severity shall turn on the corresponding LED.

## 2.17 Configuration Management

The following subsections describes Cisco ONS 15302 configuration management.

### Backup and Restoration of Configuration Data

It is possible to back up the configuration data of an ONS 15302 device. It is possible to reload the configuration from the back up. The back up media must be a central repository.



---

**Note** This feature is only possible from a GUI based Element Manager.

---

### Software Download (Remote Access)

It is possible to download a new software version to the ONS 15302 device.

The download process does not influence traffic processing of TDM traffic (E1s) unless the update/upgrade includes FPGA changes. Ethernet traffic will always influence the Ethernet traffic running via LAN/WAN - ports and remote management connectivity will not be maintained during the reset period. The new software is used when booting after the next restart. The previous software version is saved in the device. If booting with the new software fails, the ONS 15302 reboots with the old software, and an alarm is raised.

The software can be downloaded locally via the management interface or remotely via the DCC channels.

### Device Reset

It is possible to reset (reboot) the device with or without resetting the current configuration. Reboot have minimal impact on traffic processing. The following situations will affect Ethernet/IP traffic and require a Device reset to become operative:

- After configuration and changes of OSI(CLNP) related parameters (Ethernet/IP traffic affecting)
- When decreasing/increasing entries in tunable tables e.g. maxARP, maxIP-forwarding, maxVLAN's, maxDHCP, maxBridge, etc.
- Software upgrade without FPGA fix (Ethernet/IP traffic affecting)
- Software upgrade with FPGA fix (All traffic affected)

## Device Replacement

It is possible to replace an ONS 15302 device with a new one with an identical physical configuration.

No manual configuration on the device is required. The ONS 15302 is assigned one IP address automatically from a BootP server. In addition, the BootP reply contains a reference to a configuration file, and the IP address of the FTP/TFTP server from where this file can be downloaded. Once the configuration has been received, the ONS 15302 must be rebooted.

## Managed Object Attributes

All attributes defined in the chapter [Chapter 9, “Managed Objects,”](#) are available for read or read/write access by the management applications specified in [“Command Line Interface \(ONSCLI\)”](#) section on [page 25](#).

## 2.18 Performance Monitoring

The performance monitoring functions specified in [Table 2-26](#) is available in ONSCLI.

### 2.18.1 Aggregate Port

[Table 2-26](#) defines the mapping between the dialogue parameters and MIB variables for the Aggregate Port Statistics submenu.

*Table 2-26 Aggregate Port Statistics Parameter Mappings*

Parameter	MIB variable(s)	Comment
Aggregate Port		Choice between A or B
Path/Section		Choice between RS, MS, VC-4, or VC-12
VC-12 (KLM)	axx155TribPortMapPort ifStack LowerLayer (rfc1573) axx155SdhVc12MoTable axx155WanVc12Klm	Only valid if Path/Section choice is VC-12.ifIndex of tributary.ifIndex of VC-12 connected to tributary.K.L.M value of VC-12 connected to tributary.K.L.M value of VC-12s connected to WAN.
Date/Time	rndManagedTime rndManagedDate	
Current Interval Time Elapsed	sonetMediumTimeElapsed (rfc2558)	
Current ES	sonetSectionCurrentESs (rfc2558) sonetLineCurrentESs (rfc2558) sonetPathCurrentESs (rfc2558) sonetVTCurrentESs (rfc2558)	Regenerator Section. Multiplex Section. VC-4. VC-12.
Current Far End ES	sonetFarEndLineCurrentESs(rfc2558) sonetFarEndPathCurrentESs(rfc2558) sonetFarEndVTCurrentESs(rfc2558)	Multiplex Section. VC-4. VC-12.
Current SES	sonetSectionCurrentSESs (rfc2558) sonetLineCurrentSESs (rfc2558) sonetPathCurrentSESs (rfc2558) sonetVTCurrentSESs (rfc2558)	Regenerator Section. Multiplex Section. VC-4. VC-12.
Current Far End SES	sonetFarEndLineCurrentSESs(rfc2558) sonetFarEndPathCurrentSESs(rfc2558) sonetFarEndVTCurrentSESs(rfc2558)	Multiplex Section. VC-4. VC-12.
Current BBE	sonetSectionCurrentBBEs sonetLineCurrentBBEs sonetPathCurrentBBEs sonetVTCurrentBBEs	Regenerator Section. Multiplex Section. VC-4. VC-12.
Current Far End BBE	sonetFarEndLineCurrentBBEs sonetFarEndPathCurrentBBEs sonetFarEndVTCurrentBBEs	Multiplex Section. VC-4. VC-12.

Table 2-26 Aggregate Port Statistics Parameter Mappings (continued)

Parameter	MIB variable(s)	Comment
Current UAS	sonetSectionCurrentUASs sonetLineCurrentUASs (rfc2558)sonetPathCurrentUASs (rfc2558)sonetVTCurrentUASs (rfc2558)	Regenerator Section. Multiplex Section. VC-4. VC-12.
Current Far End UAS	sonetFarEndLineCurrentUASs(rfc2558)s onetFarEndPathCurrentUASs(rfc2558)so netFarEndVTCurrentUASs(rfc2558)	Multiplex Section. VC-4. VC-12.
Index	sonetLineIntervalNumber (rfc2558) sonetPathIntervalNumber (rfc2558) sonetVTIntervalNumber (rfc2558)	Multiplex Section. VC-4. VC-12.
Timestamp	rndManagedTime rndManagedDate sonetMediumTimeElapsed (rfc2558) sonetLineIntervalNumber (rfc2558) sonetPathIntervalNumber ((rfc2558) sonetVTIntervalNumber ((rfc2558)	Timestamp must be calculated from these values and index. Multiplex Section. VC-4. VC-12.
ES	sonetSectionIntervalESs (rfc2558) sonetLineIntervalESs (rfc2558) sonetPathIntervalESs (rfc2558) sonetVTIntervalESs (rfc2558)	Regenerator Section. Multiplex Section. VC-4. VC-12.
Far End ES	sonetFarEndLineIntervalESs(rfc2558) sonetFarEndPathIntervalESs(rfc2558) sonetFarEndVTIntervalESs(rfc2558)	Multiplex Section. VC-4. VC-12.
SES	sonetSectionIntervalSESs (rfc2558) sonetLineIntervalSESs (rfc2558) sonetPathIntervalSESs (rfc2558) sonetVTIntervalSESs (rfc2558)	Regenerator Section. Multiplex Section. VC-4. VC-12.
Far End SES	sonetFarEndLineIntervalSESs(rfc2558) sonetFarEndPathIntervalSESs(rfc2558) sonetFarEndVTIntervalSESs(rfc2558)	Multiplex Section. VC-4. VC-12.
BBE	sonetSectionIntervalBBEssonetLineInterv alBBEs sonetPathIntervalBBEssonetVTIntervalB BEs	Regenerator Section. Multiplex Section. VC-4. VC-12.
Far End BBE	sonetFarEndLineIntervalBBEs sonetFarEndPathIntervalBBEs sonetFarEndVTIntervalBBEs	Multiplex Section. VC-4. VC-12.
UAS	sonetSectionIntervalUASssonetLineInterv alUASs (rfc2558) sonetPathIntervalUASs (rfc2558) sonetVTIntervalUASs (rfc2558)	Regenerator Section. Multiplex Section. VC-4. VC-12.
Far End UAS	sonetFarEndLineIntervalUASs(rfc2558) sonetFarEndPathIntervalUASs(rfc2558) sonetFarEndVTIntervalUASs(rfc2558)	Multiplex Section. VC-4. VC-12.

## 2.18.2 Bridge Port

Performance counters for the Bridge ports (including the WAN port) are available for the manager via the following variables in the RMON MIB:

- etherStatsDropEvents
- etherStatsOctets
- etherStatsPkts
- etherStatsBroadcastPkts
- etherStatsMulticastPkts
- etherStatsCRCAlignErrors
- etherStatsUndersizePkts
- etherStatsOversizePkts
- etherStatsFragments
- etherStatsJabbers
- etherStatsCollisions
- etherStatsPkts64Octets
- etherStatsPkts65to127Octets
- etherStatsPkts128to255Octets
- etherStatsPkts256to511Octets
- etherStatsPkts512to1023Octets
- etherStatsPkts1024to1518Octets

As opposed to the Aggregate port counters, the Bridge port counters must be started and stopped by the operator.

ONS 15302 keeps no history records for the Bridge port counters.

### 2.18.2.1 Ping

An IP ping service is available in the ONS 15302.

This service is available in all management solutions. In ONSCli this option can be found under the Service menu options. With this service, ping series with different parameters to a number of different devices can be started. The result of each sequence is displayed in the Ping Table. The ping session supports different packet sizes as well as number of pings generated for reply.

## 2.19 Software Download (Local Access)

It is possible to load a new software version by means of a PC directly attached to the ONSCli Port. This service requires local operator presence at the ONS 15302. Refer to [Chapter 5, “Troubleshooting”](#) for more information.

The file is loaded by means of the X modem protocol, and the transfer rate is 15.200 kbit/s.

**Note**

Booting the system triggers local software download. Hence, the traffic is lost during the loading.

*Table 2-27 S7software Download Parameters*

Parameters	Description
File Name	Software File to be downloaded

## 2.20 Security

The management access to the ONS 15302 is controlled by parameters in a community table. This table can only be modified by users with Super access rights. The parameters in the community table are only visible for Super users.

For each defined user, the following parameters must be provided:

- IP address
- Community string
- Access Right (READ-ONLY, READ-WRITE, SUPER)
- Traps (Enable or Disable)

One management station (IP address) may have several users with different access rights. These users are identified by means of the community string.

The ONSCLI access is controlled by means of a password, one for the local access and one for the Telnet access. A management station Super user can modify the ONSCLI password.

The ONSCLI user has Super access rights.

## 2.21 Management Logs

This subsection summarizes the various logs used for alarms, errors and statistics as visualized in [Figure 2-18](#) Management logs.

In addition to the logs described in [Table 2-28](#), the system provides logs for troubleshooting, containing detailed debug information. These logs are not available for normal users, and they are not specified in this document.

Figure 2-18 Management Logs

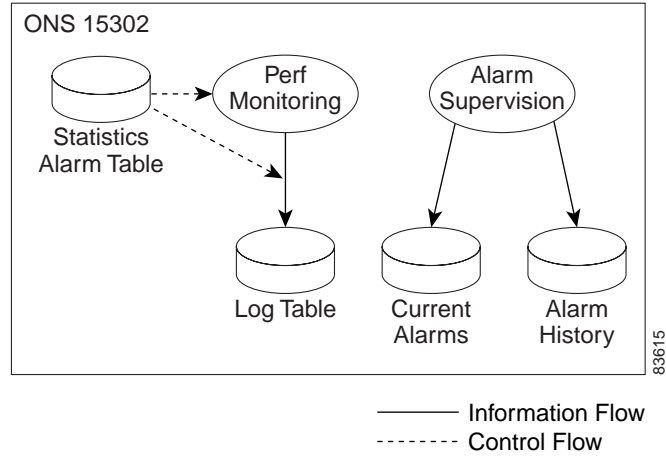


Table 2-28 Management Logs

Name	Location	Description
Statistics Alarm Table	ONS 15302	Controls the monitoring of Bridge and LAN port performance. It contains definition of threshold alarms and also decides if performance alarms shall be logged locally in Log Table, or sent as trap to the manager or both. This table corresponds to the RMON alarm table.
Log Table	ONS 15302	This table contains the logged performance alarms controlled by the Statistics Alarm Table. This table corresponds to the RMON log table.
Current Alarms	ONS 15302	This table contains all alarms currently on.
Alarm History	ONS 15302	This table contains a log of all events, including alarm events. The latest 1000 events are stored.

