

## The ZXCTN 6000 Packet Transport Networks Series Enabling New Services and Network Convergence

- The ZXCTN 6200 Packet Transport Networks offers high-performance, carrier-class multiservice transport platform



### Overview

The ZXCTN 6200 supports any-to-any Layer 2 and Layer 3 network and/or service interworking reliably and concurrently. It provides service providers a graceful migration path to a converged packet transport network based on MPLS/MPLS-TP.

The ZXCTN 6200 enables connection-oriented characteristics of the traditional transport network such as SDH-like OAM, perfect protection mechanisms and powerful management, while maintaining the superior statistical multiplexing and flexible deployment of pure IP networks.

The ZXCTN 6200 performs a wide range of interfaces with unmatched service flexibility. It enables service providers the ability to deliver mobile backhaul services, business-class IP and carrier Ethernet services, Asynchronous Transfer Mode (ATM) and Time Division Multiplexing (TDM) private leased line services at speeds from E1 to STM-4 and Ethernet services from 10 Mbps to 10 Gbps. The ZXCTN 6200 offers a switching capacity of 44 Gbps in a fully redundant, nonblocking shelf.

### Feature Highlights

#### **Any to Any True Service Interworking at Line Rate**

Based on pseudowire architecture, a unified MPLS core for Layer 2 services and TDM transport enables any customer with any Layer 1 or Layer 2 access technologies such as ATM, Ethernet/VLAN, metro Ethernet and TDM to communicate with

each other, regardless of access media. All I/O slots can support service interworking at line rate.

#### **Any Service, Any Channel, Any Port**

The ZXCTN 6200 can support Layer 1 to Layer 3 services on single platform with the flexibility of any service, over any channel and any port with the industry's most comprehensive and flexible multi-service interfaces supporting: IP, MPLS, ATM, GFP, TDM, pseudowire circuits and link aggregation. A variety of line cards are implemented to support packets, cells, TDM circuits, and mixing and matching of Fast and Gigabit Ethernet, optical and electrical, and multi-rate SDH physical line modules.

#### **Carrier-Class Reliability**

The ZXCTN 6200 is a fully redundant platform providing carrier-class reliability. It offers a perfect end-to-end protection mechanism for the services transported. At the access side, ZXCTN 6200 supports Link Aggregation Group (LAG), Virtual Router Redundancy Protocol (VRRP), Inverse Multiplexed ATM (IMA) E1 group and Linear Multiplex Segment Protection (LMSP) for the access links with STM-N. As to the network-level protection, the ZXCTN 6200 offers Linear Protection (both in LSP and PW layers), Ring Protection (Wrapping and Steering) and FRR. Especially the ZXCTN 6200 provides Dual-homing protection and Dual Nodes Interconnection (DNI) protection to address failures of core single node and access single link and failures occurred at more than one point respectively. Meanwhile NSF for service forwarding, Graceful Restart for protocols (such as OSPF, BGP, LDP and RSVP and so on) and hot standby redundancy for key components like switching card and power

unit are all supported. The ZXCTN 6200 offers best-in-class high availability that is field-proven and time tested in more than a dozen carrier networks worldwide.

### **Next Generation Synchronization Technology**

The cost-effectiveness and versatility of packets transport networks is driving the convergence of services. Many services place new timing and synchronization requirements onto the packet network. The ZXCTN 6200 enables carriers to provide SONET/SDH-like Layer 1 timing throughout the network via Synchronous Ethernet. The ZXCTN also provides IEEE 1588v2 Packet Timing Protocol to distribute timing through mixed networks and architect an LTE-ready network where both frequency and phase are required.

### **Carrier-Class OAM**

The ZXCTN 6200 supports a rich set of OAM features defined in the latest versions of IEEE, ITU, and IETF standards, including:

- IEEE 802.3ah Ethernet in the First Mile (EFM) physical layer, OAM, including link events and remote loopback
- IEEE 802.1ag CFM
- ITU-T Y.1731 Ethernet OAM
- 802.1ab Link Layer Discovery Protocol (LLDP)
- ITU-T G.8114 OAM for T-MPLS layer networks
- GACH+ITU-T Y.1731 MPLS-TP OAM
- MPLS OAM, including LSP ping/trace, BFD and their extensions

These capabilities enable the ZXCTN 6200 to monitor the status of system and network links; measure the performance of customer services; confirm that link and service throughput and quality conform to SLAs; and distribute this management information across point-to-point, point-to-multipoint, and multipoint-to-multipoint connections.

### **Reconfigurable GateWay**

With the evolution and convergence of networks, it is required to interwork with different types of networks in many scenarios: the legacy and the newly-built, the packet-based and the TDM-based. The ZXCTN 6200 offers multiple embedded SDH, ATM and Ethernet gateway boards that are available to support hybrid networking of SDH, ATM, IP/MPLS and Ethernet, OAM

interworking, and to enable mutual security and unified network management.

## **Customer Benefits**

### **Enhanced Service Level Agreements (SLA)**

The ZXCTN 6200 opens up new revenue streams by offering meaningful SLAs. These SLAs extend QoS contracts previously available only for ATM circuits to new and advanced broadband data services such as Ethernet and IP. Mission-critical services can now exist on technologies previously limited to traditional best-effort performance.

### **Superior Traffic Management**

The ZXCTN 6200 ensures that policies defining SLAs for each service contract are honored. The state-of-the-art QoS processing technology provides deterministic and granular per-flow and per-service SLA bandwidth management. Service-aware queuing techniques and traffic shaping help ensure predictability through varying levels of network utilization.

### **Evolutionary Migration of Legacy Networks**

The ZXCTN 6200 supports open, standards-based software and hardware to interface with legacy equipment and protocols. Deployed legacy multiservice networks can be integrated with the ZXCTN 6200-based network as part of a nondisruptive migration.

### **Enabling New Revenue Streams**

With the enhanced SLA and superior MPLS traffic engineering, the ZXCTN 6200 enables service providers to offer high-growth IP services using MPLS L2 VPN or L3 BGP/MPLS VPN, while supporting legacy SDH/PDH and ATM services from the same platform.

### **Guaranteed Service Availability**

The perfect reliability mechanisms and redundant hardware assures no single point of failure, non-service affecting product upgrades, Layer 2 and Layer 3 protocol GR, in-service network expansion and carrier-class protection and switching to maximize fault tolerance and performance. Carrier-class design provides full redundancy in common equipment and software resiliency features enable maximum service and network uptime.

### **Investment Protection**

While increasing the breadth of the service portfolio, the ZXCTN 6200 extends service providers' investment in legacy network equipment by scaling its capacity as customer demands grow, without forklift upgrades. With significant high-density and high-speed capabilities, the ZXCTN 6200 accommodates growth in both end-user traffic and services. The switch fabric is highly scalable, providing up to 44 Gbps of nonblocking performance in a 3RU-high single chassis.

#### Capex Reduction

Service providers frequently maintain multiple core service networks based on the individual end-customer services being offered. The ZXCTN 6200 provides a consolidated network infrastructure, collapsing multiple overlay networks to reduce the total number of network elements. Capital expenditures are further reduced with industry-leading technology, density and performance improvement.

#### Opex Reduction

The ZXCTN 6200 reduces truck rolls, lowers spares inventory and minimizes operational costs for service providers:

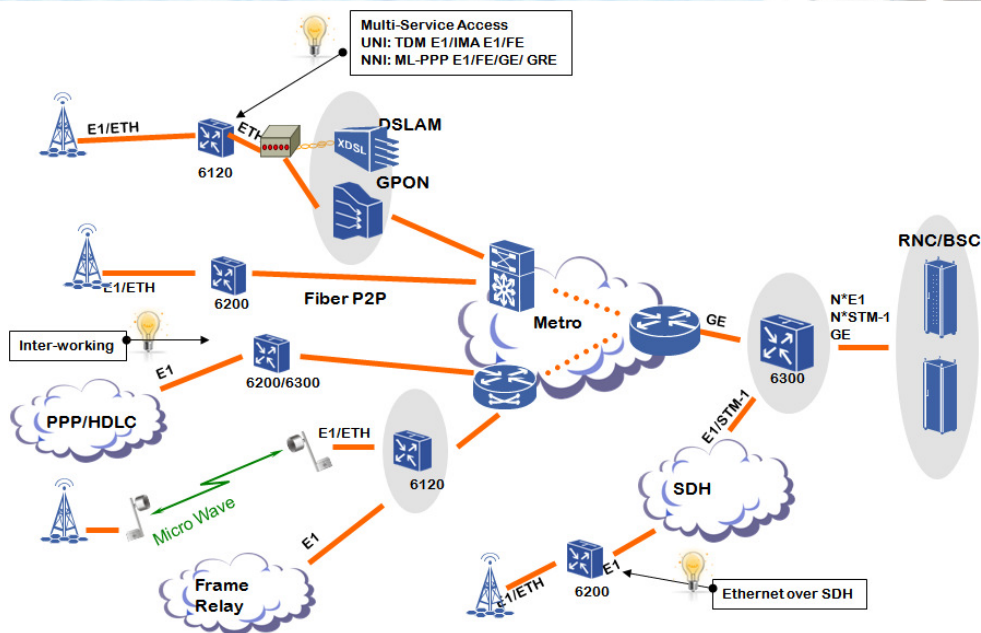
- Low power consumption mechanism is employed and the maxim power consumption is less than 200W which saves a large sum of money for service providers.
- Software-defined E1 card enables one single card to access services of TDM, ATM, MLPPP, FR, PPP and HDLC. Also one single Ethernet card supports both FE and GE speeds.

In addition, the Graphic network management and E2E service configuration further reduces operational complexity of managing multiple networks or network layers in the service provider network. Reduced operations costs are facilitated to bring greater profits and revenues.

#### Applications and Services

The ZXCTN 6200 enables service providers to offer the following services on converged network architecture, benefiting from new revenue opportunities while maintaining their legacy investments:

- Layer 1/Layer 2 Legacy Services
  - Private line service via TDM circuit emulation
  - ATM service (Layer 2 VPN)
  - Ethernet service defined in MEF, including E-LINE, E-LAN and E-TREE
- MPL2 Layer 2 VPNs
  - VPWS for point-to-point TDM, ATM, and Ethernet/VLAN (Layer 2 VPN)
  - VPLS and H-VPLS for large-scale multipoint-to-multipoint connectivity
- MPLS/BGP Layer 3 VPNs
  - High-performance Layer 3 VPNs
  - IP VPN using GRE
- Wireless Transport
  - 3G migration
  - Wireless backhaul
  - RAN aggregation
  - Wireless core
  - TDM circuit emulation for 2G transport
  - FMC
- Triple Play Services
  - IP telephony
  - IPTV
  - Broadcast TV
  - VoIP



## ZXCTN 6200 Architecture

### Switch, Clock and Control Cards (SCC)

The SCCs are the central resource of the ZXCTN 6200 for both data-plane switching and the control and management functionality. The highly scalable, efficient and redundant switch fabric is distributed across the SCCs. The ZXCTN 6200 provides 1+1 hot-standby redundancy for the SCC units to ensure non-interruption of the services in case the main SCC unit fails. The switch fabric has the following switching and fault tolerant features:

- Fully nonblocking switching architecture
- Highly efficient and deterministic performance
- Carrier-class routing/switching around internal failures
- Scalable single-stage, low-latency design to achieve up to 44 Gbps in a 3RU-high single chassis

### Line Cards

Each of the four line card slots in the ZXCTN 6200 chassis can be used for any card type (except the 10GE card), removing the burden of complex pre-engineering and future scenario planning. The eight supported card types are: a 4-port channelized

STM-1/4 card, a 4-port ATM STM-1 card, a 16-port E1 interface card, a 4-port optical&4-port electrical combo Ethernet card, an 8-port optical Ethernet card, an 8-port electrical Ethernet card, a PPP POS STM-N/OC-N card and an optical application card. The 4-port ATM STM-1 card supports ATM over SDH with ATM VP/VC switching and circuit emulation processing. The channelized STM-1/4 card supports TDM and ML-PPP with ports configurable for STM-1 or STM-4 operation. The E1 card supports IMA, TDM and multiclass MLPPP. The combo card allows mixing and matching of optical and electrical ports, giving four Ethernet interfaces per slot. The electrical Ethernet card has eight ports of auto-sensing 10/100/1000 Base-TX ports and the optical Ethernet card has eight ports of supporting 100/1000 Ethernet with small form factor pluggable (SFP). While a 1-port 10G Ethernet card can be used in either of the two slots at the bottom of the chassis, which gives two 10GE ports totally. The PPP POS STM-N/OC-N card can interwork with routers and the OA card can be used to extend transport distance. Combined with the switch fabric, the line cards provide the ZXCTN 6200 the ability to offer integrated and highly efficient data forwarding across multiple services.

Switching Capacity	44Gbps
Chassis Design	Backplane
No. of SCC per Chassis	2


 Bringing you Closer

<b>No. of LC per Chassis</b>	4
<b>Redundancy</b>	Fully redundant platforms to provide carrier-class reliability
	1+1 redundancy on SCC and power units
	Access side protection, including LAG, VRRP, IMA, LMSP, MLPPP
	TMPLS/MPLS-TP linear and ring protection
	MPLS protection, including 1:1 linear protection and FRR
<b>Mechanical Dimensions</b>	Height: 5.1 in / 13.1 cm; Width: 19 in / 48.3 cm; Depth: 9.5 in / 24 cm
<b>No. of chassis per 7ft rack</b>	4
<b>Weight (fully configured)</b>	28.9 lbs (13kg)
<b>Cooling</b>	Right to left air flow
<b>Electrical Power</b>	Two redundant power units
<b>Maximum Power</b>	200W
<b>DC</b>	Input voltage range: -40V~-59.5V
<b>Maximum Thermal Output</b>	1024 BTU/hr
<b>Temperature</b>	32° F 113° F/-5° C 55° C
<b>Maximum Altitude</b>	Up to 4,000 m (13,123 ft)
<b>Operational Relative Humidity</b>	5-95% no condensing

## Technical Specifications

### ZXROS (Router Operation System)

The ZXROS platform provides a standards-based set of open protocols and control planes to offer varieties service functions and performances required by metro Ethernet switch. It facilitates new SLAs for existing services that require no change of the end-user customer or customer premise equipment.

#### ■ SCC

- 512 MB SDRAM
- 128 MB flash

#### ■ LC

- 64 MB SDRAM
- Line rate performance for all packet sizes

#### ■ System Management and Alarm Interfaces

- 10/100 Mbps Ethernet (RJ-45) ports for remote and console connections
- 10/100 Mbps Ethernet (RJ-45) ports for out-of-band management
- Alarm Cut-Off (ACO) switch
- LEDs for power, temp, fan, status and alarm (critical, major and minor)

#### ■ Regulatory Compliance

- Safety
- UL 60950-1
- EN 60950-1:2001
- CSA C22.2 No. 60950-1
- AS/NZS 60950.1:2003
- EN 60825-1:1994, A11, A2
- EMC/Immunity
- FCC Part 15 Class A
- ETSI EN300 386 V1.3.1 (2001-09)

### Software Specifications

#### ■ Layer 3 Protocol Supported

- Routing: BGP4, IS-IS, OSPF
- Advanced Routing features: BGP extension for MPLS and BGP graceful restart
- IS-IS: Graceful Restart, Jumbo Frames, Domain-wide Prefix Distribution, Mesh Groups, IGP Shortcuts

- OSPF: Stateful Redundancy, NSSA, IGP Shortcuts, Multiple Instances, graceful restart
- MPLS: LDP, RSVP-TE
- Advanced MPLS Features: MPLS traffic engineering, RSVP-TE, IS-IS-TE, OSPF-TE, Constraint-based Shortest Path First (CSPF)
- RSVP-TE: Stateful redundancy, fast reroute (FRR) with sub 50ms failover, backup LSPs
- LDP: Graceful restart, fault tolerant, LDP over RSVP tunnels
- IP VPN: RFC2547bis/4364 MP-BGP, OSPF multi-instance, overlapping VPNs, Full mesh and hub/spoke VPN topologies
- Policies: Access lists, prefix lists, route maps, AS-path lists, extended community lists
- DHCP relay

#### ■ Layer 1 and 2 Protocol Supported

- ATM and IMA
- Ethernet/VLAN, link aggregation, E-line and E-LAN, VPLS, H-VPLS, Q-in-Q STP, RSTP, MSTP
- EoS and GFP
- TDM: SAToP, CESoPSN
- HDLC
- ML-PPP
- Pseudowires based on Martini Draft for ATM, Ethernet/VLAN, PPP, HDLC and TDM traffic encapsulation

#### ■ Traffic Management

- MPLS traffic engineering using OSPF-TE, ISIS-TE, RSVP-TE, LDP over RSVP tunnel
- CSPF routing
- E-LSP (EXP inferred)
- CAC at LSP level
- Weighted Fair Queuing (WFQ)
- Policing at the ingress (Dual leaking bucket algorithm with 3 color marking + explicit drop)
- Shaping at the egress and ingress
- Weighted Random Early Detection (WRED) and/or Tail Drop (TD)
- Hierarchical queuing

- SLAs are applied (both policing and shaping) on Per-Flow Queues
- Multi-class pseudowires
- Weighted QoS
- **Carrier Class Resiliency**
  - ZXCTN 6200 upgrade without affecting services and minimal customer traffic loss
  - Fully redundant platforms to provide carrier-class reliability
  - Hot-swappable switch fabric and line cards
  - 1+1 hot-standby redundancy for SCCs both on data plane and control plane
  - 1+1 hot-standby redundancy for power units
  - Nonstop forwarding for all traffic during control plane switchover
  - Routing resiliency: OSPF and RSVP-TE stateful redundancy, OSPF, ISIS, BGP and LDP graceful restart
  - Database redundancy: RIB and FIB routing and forwarding table, OSPF-TE and ISIS-TE traffic engineering database, CAC, VPLS MAC address
  - Data path protection: Supports redundant LSPs and LSP fast reroute in sub-50 ms, link aggregation and SDH LMSP protection, ATM IMA, MLPPP, VRRP, STP, RSTP, MSTP, H-VPLS, backup pseudowires and VRRP, loop detection blocking
  - Pseudowire redundancy: dual-homing
  - TMPLS/MPLS-TP protection: LSP 1+1/1:1, Wrapping protection, SD protection
  - Dual Node Interconnection protection
  - BFD support for OSPF, IS-IS, BGP, LDP and RSVP LSP
- Ethernet services disruption detection and diagnostics: port mirroring, continuity check (includes VPLS) link trace and loopback, as per IEEE 802.1ag (Draft) service OAM
- MPLS services disruption detection and diagnostics: LSP ping and trace, pseudowire Virtual Circuit Connectivity Verification (VCCV) and Bidirectional Forwarding Detection (BFD)

#### ■ Security

Well-defined secure network element access, extensive monitoring and disaster recovery methods based on layered, reliable and scalable security architecture:

- Operating system security using protected memory and modular processes
- Management plane security using multi-level security matrix for secure EMS/NMS access, SNMPv3 security support, SFTP RADIUS, TACACS+, forensics capability for security audit or threat diagnostics, network database backup for disaster recovery
- Control plane security against DDoS and TCP SYN attacks and MD5 authentication for IP, ATM/FR and MPLS
- Data plane security for flexible class based traffic protection, E911 regulation for public safety, flexible access control list, lawful interception, resource protection, spoofing

#### ■ OAM

Extensive network diagnostics capabilities are implemented to detect and diagnose abnormalities in the network. The feature set includes, but not limited to:

- GACH+ITU-T Y.1731 MPLS-TP OAM
- IEEE 802.3ah Ethernet in the First Mile (EFM) physical layer, OAM, including link events and remote loopback
- ITU-T Y.1731 Ethernet OAM

## Standards Compliance

### ■ TCP/IP

- RFC 768 User Datagram Protocol (UDP)
- RFC 791 Internet Protocol (IP)
- RFC 792 Internet Control Message Protocol (ICMP)
- RFC 793 Transmission Control Protocol (TCP)
- RFC 813 Window and Acknowledgement Strategy in TCP/IP
- RFC 815 IP Datagram Reassembly Algorithms
- RFC 826 Address Resolution Protocol (ARP)
- RFC 854 Telnet Protocol Specification
- RFC 879 The TCP Maximum Segment Size and Related Topics
- RFC 894 Standard for Transmission of IP Datagrams over Ethernet
- RFC 919 Broadcasting Internet Datagrams
- RFC 1042 Standard for the Transmission of IP Datagrams over IEEE 802 Network
- RFC 1191 Path MTU Discovery
- RFC 1256 ICMP Router Discovery Messages
- RFC 1305 Network Time Protocol (NTP) Version 3
- RFC 1323 TCP Extensions for High Performance
- RFC 1350 TFTP Version 2 (revision of RFC 783)
- RFC 1812 Requirements for IP Version 4 Routers
- RFC 1918 Address Allocation for Private Internets
- RFC 2018 TCP Selective Acknowledgment
- RFC 2390 Inverse Address Resolution Protocol
- RFC 3768 Virtual Router Redundancy Protocol (VRRP)
- RFC 4950 ICMP Extensions for Multiprotocol Label Switching

### ■ IP Multicast

- RFC 3046 DHCP Relay Agent Information Option
- Draft-IETF- magma-snoop: Considerations for IGMP and MLD Snooping Switches

### ■ RSVP-TE

- RFC 2205 Resource ReSerVation Protocol (RSVP)
- RFC 2209 Resource ReSerVation Protocol (RSVP) — Version 1 Message Processing Rules

- RFC 2702 Requirements for Traffic Engineering Over MPLS
- RFC 2747 RSVP Cryptographic Authentication
- RFC 2961 RSVP Refresh Overhead Reduction Extensions
- RFC 3097 RSVP Cryptographic Authentication (revision of RFC 2747)
- RFC 3209 RSVP-TE: Extensions to RSVP for LSP Tunnels
- RFC 3210 Applicability Statements for Extensions to RSVP for LSP Tunnels
- RFC 3270 Multi-Protocol Label Switching (MPLS) Support of Differentiated Services
- RFC 3564 Requirements for Support of Differentiated Services-aware MPLS Traffic Engineering
- RFC 4090 Fast Reroute Extensions to RSVP-TE for LSP Tunnels
- RFC 4124 Protocol Extensions for Support of Differentiated-Service-Aware MPLS Traffic Engineering
- RFC 4125 Maximum Allocation Bandwidth Constraints Model for Diff-Serv-aware MPLS Traffic Engineering
- RFC 4127 Russian Dolls Bandwidth Constraints Model for Diff-Serv-aware MPLS Traffic Engineering
- RFC 4561 Definition of a Record Route Object (RRO) Node-Id Sub-Object

### ■ CIDR

- RFC 1519 Classless Inter-Domain Routing (CIDR) an Address Assignment and Aggregation

### ■ GFP

- ITU-T G.7041/Y.1303 Generic Framing Procedure (GFP)

### ■ OSPF

- RFC 2328 OSPF Version 2
- RFC 3101 The OSPF Not So Stubby Area Option
- RFC 3137 OSPF Stub Router Advertisement
- RFC 3623 Graceful OSPF Restart

- RFC 3630 Traffic Engineering Extensions to OSPF v2
  - RFC 4136 OSPF Refresh and Flooding Reduction in Stable Topologies
  - RFC 4576 Using a Link State Advertisement (LSA) Options Bit to Prevent Looping in
  - BGP/MPLS IP Virtual Private Networks (VPNs)
  - RFC 5250 The OSPF Opaque LSA Option
- **IS-IS**
- ISO/IEC 10589: IS-IS Routing Protocol
  - RFC 1142 OSI IS-IS Intra-Domain Routing Protocol
  - RFC 2966 Domain-wide Prefix Distribution with Two-Level IS-IS
  - RFC 3373 Three-Way Handshake for IS-IS Point-to-Point Adjacencies
  - RFC 3567 Intermediate System to Intermediate System Cryptographic Authentication
  - RFC 3784 ISIS-TE
  - RFC 3847 Restart signaling for IS-IS
- **BGP**
- RFC 2385 Protection of BGP Sessions via the TCP MD5 Signature Option
  - RFC 2439 BGP Route Flap Damping
  - RFC 2858 Multiprotocol Extensions for BGP-4
  - RFC 2918 Route Refresh Capability for BGP-4
  - RFC 3107 Carrying label information in BGP
  - RFC 4271 A Border Gateway Protocol (BGP-4) (Revision of RFC 1771)
  - RFC 4360 BGP Extended Communities Attribute
  - RFC 4456 BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP) (R)
  - RFC 4724 Graceful Restart Mechanism for BGP
  - RFC 4760 Multiprotocol Extensions for BGP-4
  - RFC 4893 BGP Support for Four-octet AS Number Space
- **MPLS**
- RFC 3031 MPLS Architecture
  - RFC 3032 MPLS Label Stack Encoding
  - RFC 3036 LDP Specification
  - RFC 3215 LDP State Machines
  - RFC 3270 MPLS Support for Differentiated Services
  - RFC 3346 Applicability Statement for Traffic Engineering with MPLS
  - RFC 3443 Time to Live (TTL) Processing in Multi-Protocol Label Switching (MPLS) Networks
  - RFC 3478 Graceful Restart Mechanism for Label Distribution Protocol
  - RFC 3564 Requirements for Support of Differentiated Services-aware MPLS Traffic Engineering
- **VPLS and H-VPLS**
- RFC 4762 Virtual Private LAN Services over MPLS
- **Ethernet**
- IEEE 802.1d Bridging
  - IEEE 802.1p Priority
  - IEEE 802.1q VLAN
  - IEEE 802.1ad Q-in-Q/VLAN stacking
  - IEEE 802.1ag (Draft) service OAM
  - IEEE 802.3 10Base-T
  - IEEE 802.3u 100Base-TX
  - IEEE 802.3x Flow Control
  - IEEE 802.3z 1000Base-SX/LX
  - IEEE 802.3ad Link Aggregation
  - IEEE 802.3ae 10 Gbps Ethernet
  - IEEE 802.3x Ethernet Flow Control
  - IEEE 802.3 with 802.2 SAP
  - IEEE 802.3 with 802.2 SNAP
- **BFD**
- Draft-IETF-BFD-base: Bidirectional Forwarding Detection
  - Draft-IETF-generic: Generic Application of BFD
  - Draft-IETF-BFD-MPLS: Bidirectional Forwarding Detection for MPLS LSPs
- **Pseudowires**
- RFC 3916 Requirements for Pseudo-wire Emulation Edge-to-Edge (PWE3)
  - RFC 3985 PWE3 Architecture

- RFC 4026 Provider Provisioned Virtual Private Network (VPN) Terminology
  - RFC 4379: Detecting MPLS Data Plane Failures
  - RFC 4446: IANA Allocations for Pseudo Wire Edge to Edge Emulation
  - RFC 4447: Pseudowire Setup and Maintenance using LDP
  - RFC 4448: Encapsulation Methods for Transport of Ethernet Frames Over MPLS
  - RFC 4553: Structure-Agnostic TDM over Packet (SAToP)
  - RFC 4717: Encapsulation Methods for Transport of ATM over MPLS Networks
  - RFC 4816: ATM Transparent Cell Transport Service
  - RFC 5086: Structure-Aware Time Division Multiplexed (TDM) Circuit Emulation Service over Packet Switched Network (CESoPSN)
  - Draft-IETF-PWE3-VCCV: Pseudo Wire Virtual Circuit Connectivity Verification (VCCV)
  - Draft-IETF-PWE3-CW: PWE3 Control Word for Use over an MPLS PSN
  - Draft-IETF-BFD-MPLS: Bidirectional Forwarding Detection (BFD) for MPLS LSPs
  - Draft-IETF-pwe3-ms-pw-requirement: Requirements for Multi-segment Pseudowire Emulation Edge to Edge
  - Draft-IETF-pwe3-segmented-pw: Segmented Pseudowires
- **PPP**
    - RFC 1334 PPP Authentication Protocols
    - RFC 1661 PPP (Point-to-Point Protocol)
    - RFC 1662 PPP in HDLC-like Framing
    - RFC 1990 PPP Multilink Protocol
    - RFC 1994 PPP Challenge Handshake Authentication Protocol
    - RFC 2686 Multi-Class Extension to Multi-Link PPP
- **GRE**
    - RFC 1701 Generic Route Encapsulation (GRE)
    - RFC 1702 Generic Route Encapsulation over IPv4 networks
- RFC 2784 Generic Routing Encapsulation (GRE) (revision of RFC 1701)
- **OAM**
    - ITU-T Y.1731 OAM functions and mechanisms for Ethernet based networks
    - RFC 4379 Detecting MPLS Data Plane Failures
    - Draft-bhh-mpls-tp-oam-y1731-05
    - Draft-IETF-PWE3-VCCV: Pseudo Wire Virtual Circuit Connectivity Verification (VCCV)
    - Draft-IETF-BFD-MPLS: Bidirectional Forwarding Detection for MPLS LSPs
    - IEEE 802.1ag Service OAM
    - IEEE 802.3ah Link OAM
- **TDM**
    - ITU-T G.703 Physical/electrical characteristics of hierarchical digital interfaces
    - ITU-T G.704 Synchronous frame structures used at 1544, 6312, 2048, 8448 and 44 736 kbit/s hierarchical levels
    - ITU-T G.706 Frame alignment and cyclic redundancy check (CRC) procedures relating to basic frame structures defined in Recommendation G.704
    - ITU-T G.707 Network Node Interface for the Synchronous Digital Hierarchy (SDH) (V2003)
    - ITU-T G.774 Synchronous Digital Hierarchy (SDH) - Management Information Model
    - ITU-T G.774.01 Synchronous Digital Hierarchy (SDH) performance monitoring for the network element view
    - ITU-T G.774.02 Synchronous digital hierarchy (SDH) configuration of the payload structure for the network element view
    - ITU-T G.774.03 Synchronous digital hierarchy (SDH) management of multiplex-section protection for the network element view
    - ITU-T G.774.05 Synchronous Digital Hierarchy (SDH) management of connection supervision functionality (HCS/LCS) for the network element view

- ITU-T G.774.06 Synchronous digital hierarchy (SDH) unidirectional performance monitoring for the network element view
  - ITU-T G.774.07 Synchronous Digital Hierarchy (SDH) management of lower order path trace and interface labeling for the network element view
  - ITU-T G.7041 Generic framing procedure (GFP)
  - ITU-T G.7042 Link capacity adjustment scheme (LCAS) for virtual concatenated signals
  - ITU-T G.780 Terms and definitions for SDH networks
  - ITU-T G.783 Characteristics of SDH equipment functional blocks
  - ITU-T G.784 Synchronous digital hierarchy (SDH) management
  - ITU-T G.803 Architecture of transport networks based on the synchronous digital hierarchy (SDH)
  - ITU-T G.826 Error performance parameters and objectives for international, constant bit rate digital paths at or above the primary rate
  - ITU-T G.831 Management capabilities of transport networks based on the synchronous digital hierarchy (SDH)
  - ITU-T G.832 Transport of SDH elements on PDH networks - Frame and multiplexing structures
  - ITU-T G.841 Types and characteristics of SDH network protection architectures
  - ITU-T G.842 Interworking of SDH network protection architectures
  - ITU-T G.957 Optical interfaces for equipments and systems relating to the synchronous digital hierarchy
  - ITU-T G.958 Digital line systems based on the synchronous digital hierarchy for use on optical fiber cables
  - ITU-T M.2100 Performance limits for bringing-into-service and maintenance of international PDH paths, sections and transmission systems
  - ITU-T M.2101 Performance limits for bringing-into-service and maintenance of international SDH paths and multiplex sections
  - ITU-T M.2120 International multi-operator paths, sections and transmission systems fault detection and localization procedures
- **Clock**
    - ITU-T G.811 Timing characteristics of primary reference clocks
    - ITU-T G.812 Timing requirements of slave clocks suitable for use as node clocks in synchronization networks
    - ITU-T G.813 Timing characteristics of SDH equipment slave clocks (SEC)
    - ITU-T G.823 Control of Jitter and Wander within Digital Networks Which Are Based on the 2048 KBIT/S Hierarchy Series
    - ITU-T G.824 Control of Jitter and Wander Within Digital Networks Which are Based on the 1544 kbit/s Hierarchy
    - ITU-T G.825 The control of jitter and wander within digital networks which are based on the synchronous digital hierarchy (SDH)
    - ITU-T G.8261/Y.1361: Timing and synchronization aspects in packet networks
    - ITU-T G.8262/Y.1362: Timing characteristics of a synchronous Ethernet equipment slave clock (EEC)
    - ITU-T G.8264/Y.1364: Distribution of timing information through packet networks
    - IEEE 1588v2 IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems
  - **T-MPLS**
    - ITU-T G.805 Generic functional architecture of transport networks
    - ITU-T G.810 Definitions and terminology for synchronization networks
    - ITU-T G.8101 Terms and Definitions for Transport MPLS
    - ITU-T G.8110.1 Architecture of Transport MPLS (T-MPLS) Layer Network
    - ITU-T G.8112 Interfaces for the Transport MPLS (T-MPLS) Hierarchy

- ITU-T G.8113 Requirements for OAM function in T-MPLS based networks
  - ITU-T G.8114 Mechanism for OAM function in T-MPLS based networks
  - ITU-T G.8121 Characteristics of T-MPLS equipment functional blocks
  - ITU-T G.8131 T-MPLS Linear Protection Switching
  - ITU-T G.8132 T-MPLS shared protection ring
- **QoS**
- RFC 2475 Architecture for Differentiated Services
  - RFC 3086 Definition of Differentiated Services Per Domain Behaviors and Rules for their Specification
  - RFC 3246 An Expedited Forwarding PHB (Per-Hop Behavior)
  - RFC 3247 Supplemental Information for the New Definition of the EF PHB (Expedited Forwarding Per-Hop Behavior)
  - RFC 3260 New Terminology and Clarifications for Diffserv
  - RFC 4127 Russian Dolls Bandwidth Constrains Model for Diffserv-aware MPLS Traffic Engineering.
- **SNMP**
- RFC 1157 Simple Network Management Protocol (SNMP)
  - RFC 1215 Convention for Defining Traps for Use with SNMP
  - RFC 1904 Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2)
  - RFC 1905 Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)
  - RFC 1906 Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)
  - RFC 2570 SNMP Version 3 Framework
  - RFC 2578 Structure of Management Information Version (SIMv2)
  - RFC 3411 An Architecture for Describing Simple Network Management protocol (SNMP) Management Frameworks
- RFC 3412 Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
- **Security**
- RFC 1321 The MD5 Message-Digest Algorithm
  - RFC 1492 Access Control Protocol or TACACS
  - RFC 1858 Security Considerations for IP Fragment Filtering
  - RFC 1948 Defending Against Sequence Number Attacks
  - RFC 2385 Protection of BGP Sessions via the TCP MD5 Signature Option
  - RFC 2759 Microsoft PPP CHAP Extensions, Version 2
  - RFC 2827 Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address
  - RFC 2865 Remote Authentication Dial-In User Service (RADIUS)
  - RFC 3097 RSVP Cryptographic Authentication — Updated Message Type Value
  - RFC 3101 The OSPF Not So Stubby Area (NSSA) Option
  - RFC 3195 Reliable Delivery for Syslog
  - RFC 3414 User-based Security Model (USM) for Version 3 of the Simple Network Management Protocol (SNMPv3)
  - RFC 3567 IS-IS Cryptographic Authentication
  - Draft-ylonen-ssh-protocol The SSH (Secure Shell) Remote Login Protocol
  - Cisco Proprietary TACACS+