Ascend

TECHNICAL BACKGROUNDER

MAX TNT Technical Backgrounder

Version 1.06

This document provides a technical introduction and overview of the MAX TNT product line. For additional technical information on the MAX TNT please refer to the MAX TNT product documentation available on the Ascend FTP site. For additional information on related Ascend products please see the MAX Technical backgrounder for MAX 1800, 2000 and 4000 technical information. See the GRF Architecture guide for technical information on the GRF 400 IP Switch.

ASCEND

Table of Contents

1. MAX TNT Introduction

Integrated Multiprotocol WAN Access Switching for Analog, ISDN, Frame Relay and xDSL Services

The MAX TNT™ is a high-performance, standards-based WAN access switch designed for the large-scale access requirements of Internet service providers, carriers and major corporations. The MAX TNT provides a unique combination of feature richness, T3-level scalability and carrier-class robustness. With support for up to 672 DS0 circuits and a full range of access technologies, the MAX TNT reduces rack space requirements while driving down price per port. Fully-compliant with existing network infrastructures, authentication standards and SNMP management protocols, the MAX TNT was designed to integrate all your analog and digital, switched and leased-line access needs in a single, compact and easily managed device.

The MAX TNT has a modular architecture that can provide access to the Internet or global corporate network services. The chassis and expansion module system lets you design custom configurations that satisfy a broad range of applications and bandwidth requirements; from medium density corporate LAN access needs, to large central office "MegaPOP™s". The MAX TNT is a proven, reliable solution that utilizes the same core operating system code refined and proven in over 30,000 MAX installations in the world's leading Internet service providers.

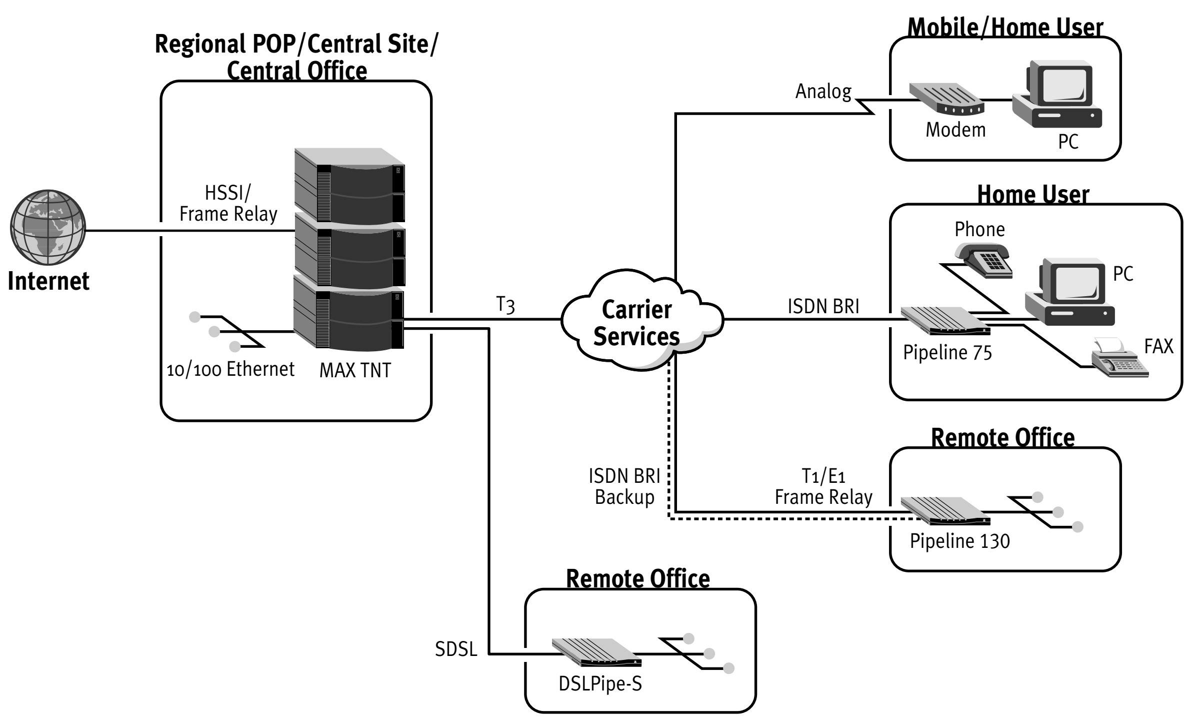

Figure 1 – MAX TNT provides industry-leading scalability, compatibility and reliability for high-density applications.

The unique MAX TNT architecture allows easy integration of existing analog and digital networks while providing a smooth growth path into state-of-the-art WAN access technologies. The integrated design of the MAX TNT saves you money by allowing you to aggregate analog, ISDN, Frame Relay and xDSL networks into a single platform; providing bandwidth consolidation opportunities while minimizing the network management task.

With its flexible and scalable architecture, the MAX TNT allows you to start with a single MAX TNT shelf to address medium-density network requirements and expand with additional MAX TNT shelves and WAN access technologies as user needs and preferences dictate. No changes in the chassis, core operating system or management software is required. Software options for the MAX TNT allow you to add firewall and Virtual Private Networking capabilities for security and added revenue or cost saving opportunities.

Ascend established the following design goals when creating the MAX TNT:

Design Objectives	How MAX TNT Achieves Objectives
Compatibility with existing network infrastructure	Support for all standard WAN and LAN access media and routing protocols, as well as authentication, accounting, security and SNMP management standards
High reliability	Three-shelf architecture with integrated relays for redundancy on intershelf bus; Redundant, hot-swappable power supplies; distributed processing; hot-swappable expansion modules; expandable memory sufficient to store multiple software images for fail-safe software upgrades; redundant T3 support; support for internal and external clocking – with a stratum 4 internal clock; load-sharing across modem modules and HDLC/Hybrid Access™ modules.
Security	Support for RADIUS, TACACS/+, PAP, CHAP, Token-based security, ATMP and PPTP and optional built-in firewall software. Planned implementation of L2TP, L2F and IPSec encryption
Flexibility	Slot-independent support for all popular LAN and WAN media including: 10Base-T, 100Base-T, T1, E1, T3, HSSI, serial and emerging standards of IDSL, SDSL and RADSL. Add the expansion modules you need, when you need them.
High-performance with cost-effectiveness.	Multiple High-speed RISC CPUs, distributed processing support and route caches on every expansion module. High-capacity and multi-access speed support results in industry-leading performance and price per port for this class of access switch.
Scalability/High Capacity	Support for the broadest range of access speeds: 52 Mbps High Speed Serial Access (HSSI), T1/E1 to T3 speeds on the WAN, 10Base-T and 100Base-T on the network interface, and from 300 baud analog modems to 6 Mbps RADSL modems for client access. Start with a single chassis and expand as needed. Support for up to three 16-slot shelves per MAX TNT system and up to 672 simultaneous calls (672 DS0s) or 4094 PVCs over Frame Relay links.
Manageability	Comprehensive SNMP management, support for Telnet, Syslog, and Ascend's NavisAccess™ network management platform

2. Applications

The MAX TNT was designed for three primary applications

- Internet access
- Corporate remote access
- Carrier data concentration

In each of these applications the MAX TNT provides unparalleled scalability, flexibility and minimized total cost of ownership.

It is well established that network and Internet access requirements are growing rapidly, WAN and client access technologies are evolving quickly and there is significant pressure on organizations to minimize the total cost of ownership of their WAN solutions. Only the MAX TNT offers the scalability and flexibility to address these three important market trends.

Ascend – the Internet Leader

The MAX TNT is specifically designed to meet the exacting needs of the Network Service Provider (NSP) by supporting all dial-in services in one compact network access switch (NAS). With integrated 56 Kbps digital modems and high-speed WAN interfaces, the MAX TNT allows you to expand service offerings while reducing costs.

Concentrating a large variety of access lines and technologies into a single MAX TNT allows efficiencies in management, maintenance and bandwidth aggregation. Already over 85 of the 100 largest Internet/Network Service Providers use the MAX TNT to be more competitive. In total over 5,000 POPs worldwide utilize the MAX family of WAN access switches, making Ascend the market leader by a wide margin.

According to the Quarter 4, 1996 Dell'Oro market research report, Ascend is the market share leader with an estimated 76% of the PRI access concentrator sales. ISPs are moving to Ascend solutions and T3, T1/E1 or PRI trunks for POP connections to gain better call flexibility and cost savings. The MAX has gained an unmatched product position as an indispensable element in an ISP's access solution. In fact, over 42% of all analog access concentrator ports are Ascend MAX ports, and Ascend has over 2.2 million ports installed worldwide.

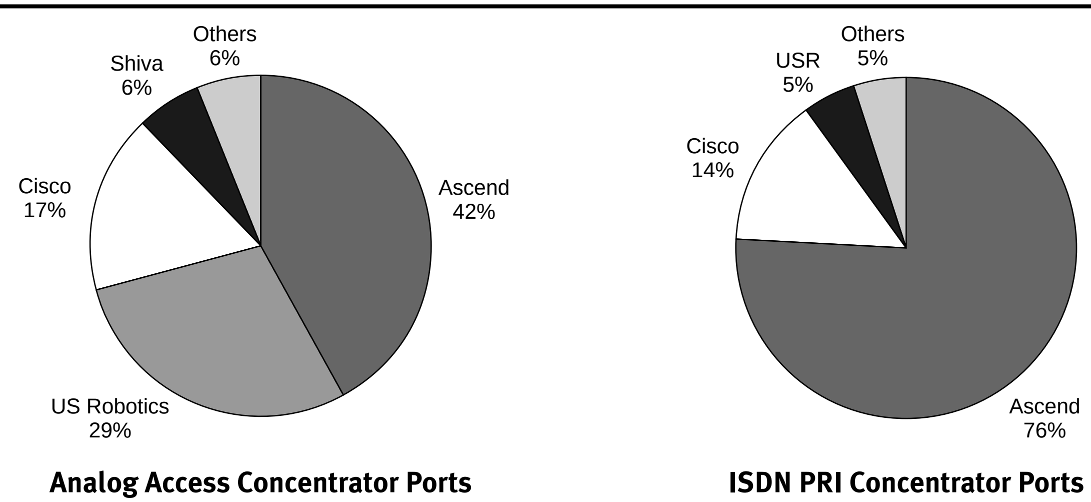

Figure 2 – Ascend leads in worldwide market share.

The MAX TNT allows a network service provider (NSP) to start with a smaller installation of a few T1/E1 circuits supporting up to several hundred customers, and to easily and cost-effectively grow to support up to a T3 circuit or 28 T1s, with a range of access technologies and thousands of customers.

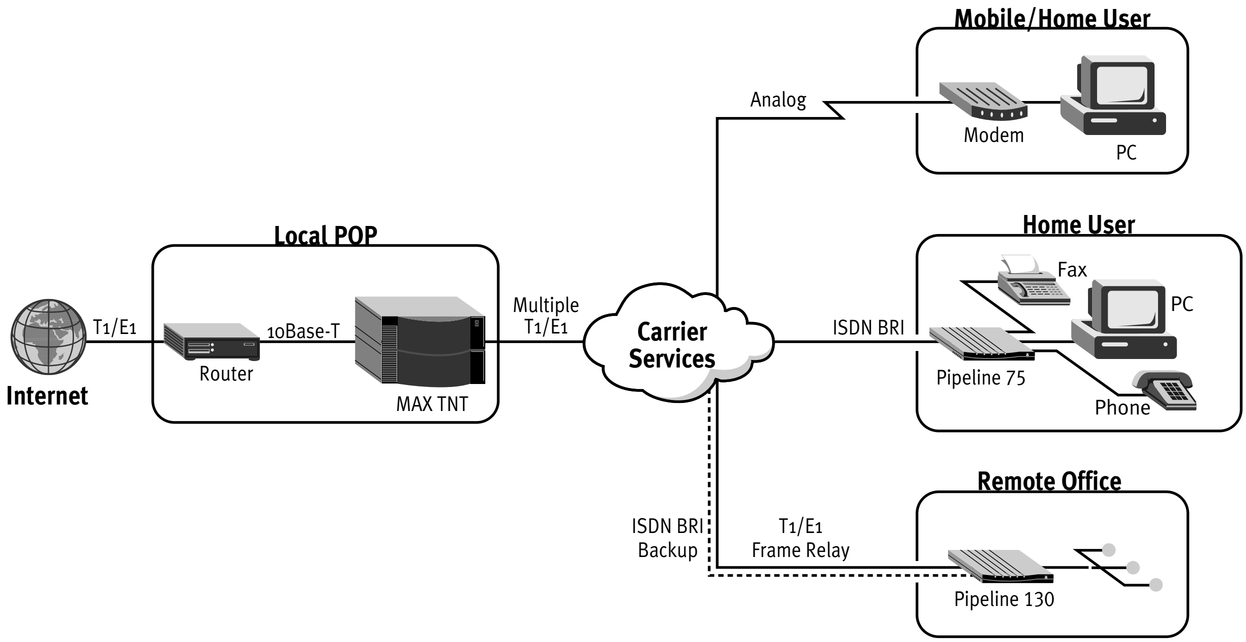

Figure 3 – MAX TNT supports simple configurations and lowers bandwidth needs.

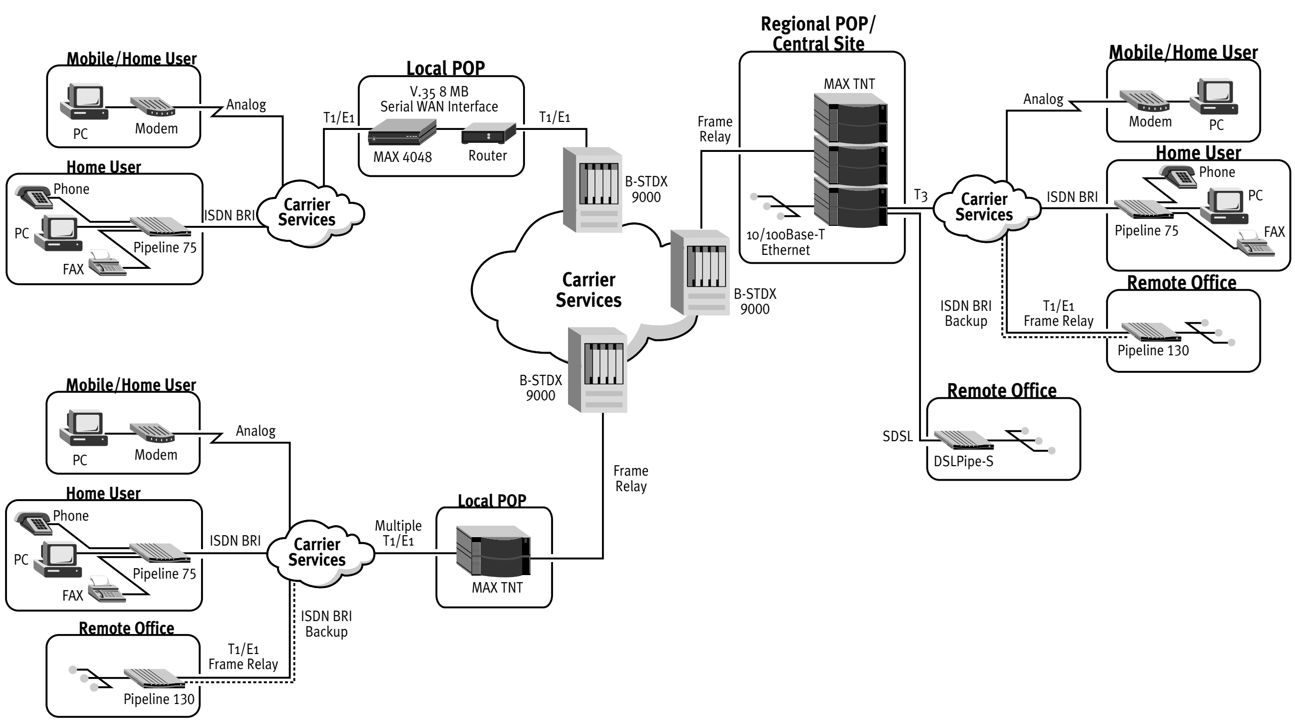

Figure 4 – MAX TNT scales to nation-wide, high-bandwidth applications.

Carrier Applications

The MAX TNT provides carriers and Competitive Access Providers (CAPs) the opportunity to quickly and cost-effectively expand their data services to meet the needs of a broad range of markets.

The MAX TNT is an ideal platform for carrier data networks because it provides the robust architecture and scalability that carriers need for their high-availability networks with thousands of customers. The MAX TNT is based on technology and code base that has proven, already its reliability in the field in thousands of MAX access switches.

In the increasingly competitive telecommunications and data communications market carriers and CAPs require flexibility and scalability to handle a wide variety of access speeds and WAN technologies. This minimizes capital costs while preserving the ability to quickly respond to customer demand as needed and to increase revenue with new services. With its fault-tolerant architecture and support for a broad array of access technologies the MAX TNT allows interoperability with the widest possible range of customer equipment and requirements. In addition, the MAX TNT's advanced authentication, dynamic firewall and virtual private network technology provide the security and internetworking capabilities that customers demand.

Industry-leading technologies from Ascend help allow carriers and CAPs to become market leaders in their own right. Ascend invented the IDSL technology that allows dedicated 128 Kbps data services that don't burden central office switches with packet-based data. This technology allows Carriers to begin xDSL service quickly while maintaining full compatibility with the large installed base of ISDN products already on the market. Migration to higher speed services is as easy as plugging in one of the new SDSL or RADSL expansion modules.

The MAX TNT architecture addresses the full spectrum of connectivity types, while minimizing management overhead with its integrated management approach and standardized interfaces. The entire MAX TNT chassis and all the expansion modules can be managed directly via SNMP from a generic SNMP management station, via Telnet or via the powerful Ascend NavisAccess management application.

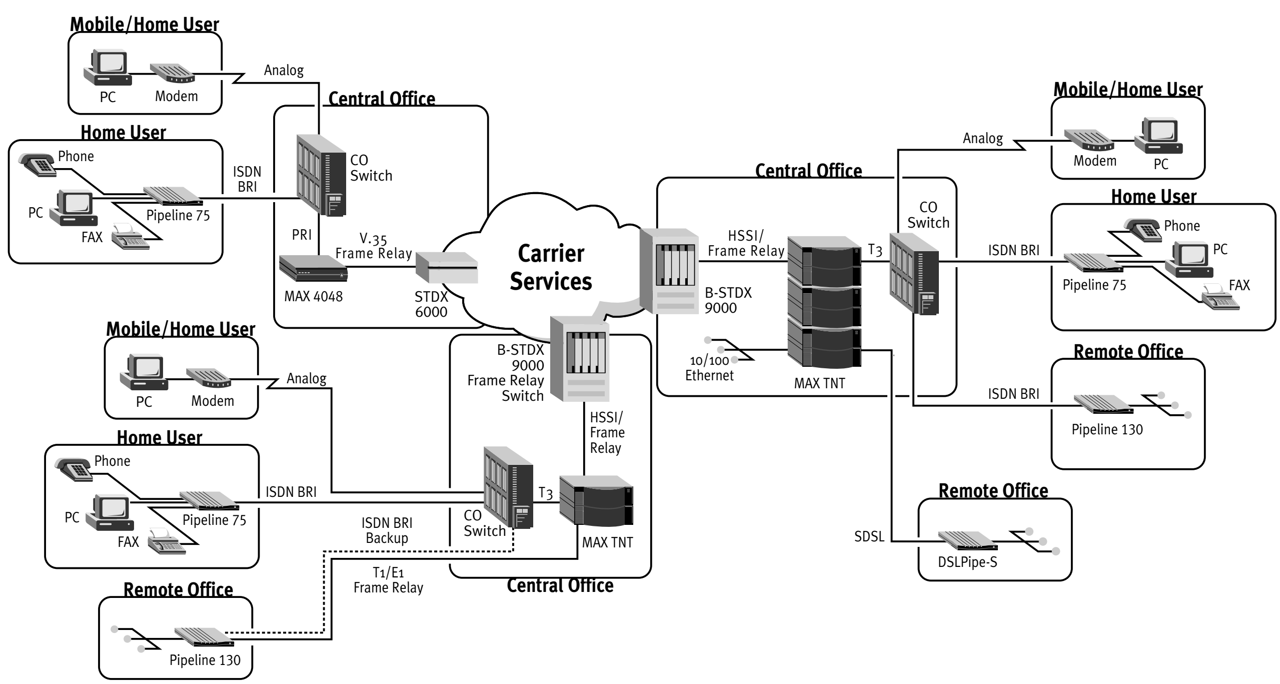

Figure 5 – This scenario shows a carrier network using MAX TNT units, MAX 4000 access switches, Ascend STDX 6000 and B-STDX 9000 Frame Relay switches.

Corporate Applications

The MAX TNT is well suited for corporate networking because of the high level of security, scalability and investment protection it provides and the range of access technologies that it supports.

To provide bullet-proof security for your corporate network the MAX TNT offers an optional, integrated dynamic firewall. This same firewall technology is available on the full line of Ascend branch office routers so local offices can also be well protected and easily integrated into your future Virtual Private Networks (VPNs). To cover a corporation's need to scale to support dozens of branch offices and hundreds or even thousands of dial-in workers with a range of access technologies, the MAX TNT system was designed to start with a single moderate-density MAX TNT system and scale up to large, multi-chassis access capacities. Companies can start with analog and Frame Relay access for their telecommuters and branch offices respectively, and easily migrate to new higher speed technologies like IDSL and RADSL as the need for greater speeds arises. Best of all, you don't need to purchase entirely new products or learn new network management software, and you can incrementally upgrade your capacity with affordable modules that allow you to do inexpensive trials of the technology before you roll it out to the entire company. At the appropriate time you can then add the required software to create a cost-effective and secure VPN using a combination of private Frame Relay circuits and the public Internet. Support for RADIUS, TACACS+, and Token-based security provide industry standard levels of network access protection, while the optional advanced dynamic firewalls and VPN software provide the highest possible levels of security.

In addition to supporting the latest evolving WAN/LAN and WAN standards, the MAX TNT smoothly integrates into your existing network environment with comprehensive SNMP support and full compliance with virtually all relevant LAN and WAN standards. The MAX TNT offers complete SNMP management of all its features and while you are free to use your existing Generic SNMP network management platform, Ascend also has the powerful NavisAccess network management software that provides simple and direct GUI management down to the individual modem level as well as expanded support for a broad range of third-party WAN devices.

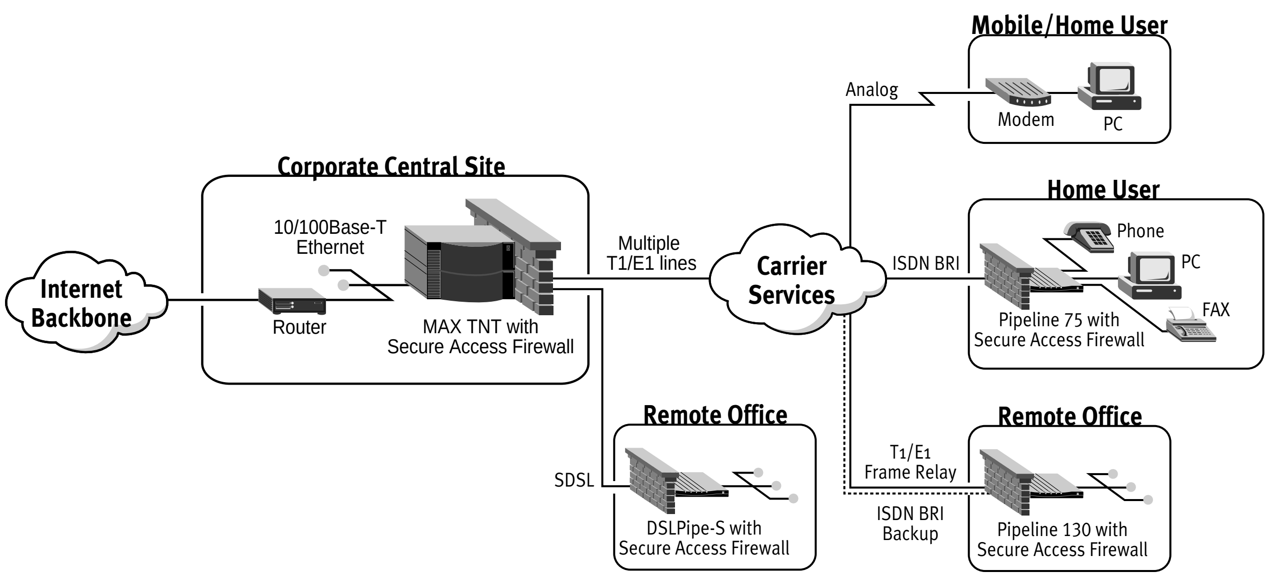

Figure 6 – The MAX TNT and Pipeline products provide complete corporate Internet access, telecommuting and remote office support.

3. Architectural Overview

Chassis

The MAX TNT chassis is a powerful, compact system that has been designed to allow Network Service Providers (NSPs), carriers and corporations to aggregate a broad array of access media in the limited space in network points of presence (POPs). The MAX TNT eliminates the need for miscellaneous access equipment from a multitude of vendors and allows a single, expandable and easy-to-manage MAX TNT shelf to provide a complete offering of network access services.

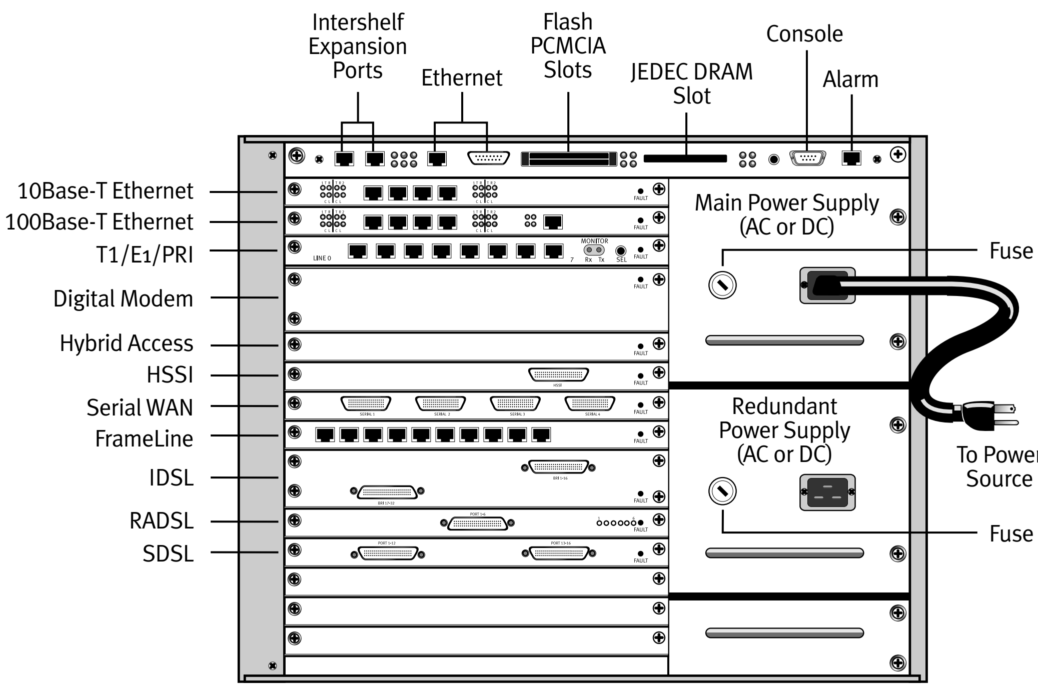

Figure 7 – The MAX TNT supports virtually all access standards in a single compact chassis.

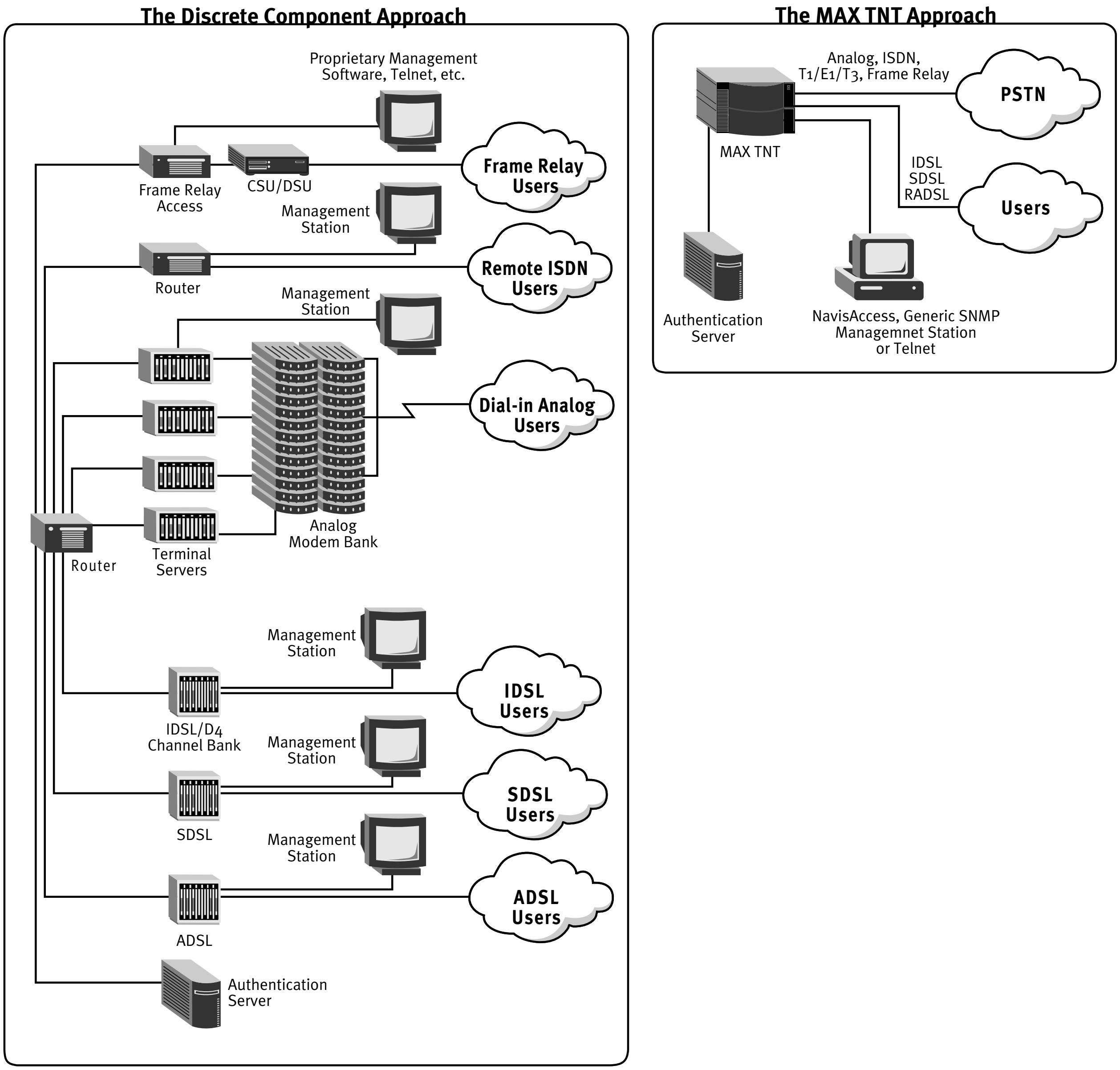

Figure 8 – Multi-access Network without MAX TNT compared to one with MAX TNT. The historic approach of using discrete components to address your access needs results in an expensive, complex WAN access network.

The Ascend Architectural Benefits:

1. Cost effectiveness, due to access line consolidation and access technology integration
2. Reduced network management overhead due to simpler, integrated WAN network and single standardized management interface
3. Reduced network support costs due to simplicity of WAN access solution
4. Increased responsiveness to user needs due to simple, incremental additions to WAN capacity via modular design
5. Increased network security due to optionally integrated firewall, fewer points of network access and simplified WAN network design

Every MAX TNT has a shelf controller module preinstalled and 16 option slots that can be populated with any of the available MAX TNT expansion modules. All expansion modules are treated as peers, making the MAX TNT equally powerful in either a data switch application (for example switching Frame Relay PVC data) or in access routing.

The MAX TNT has been designed for NEBS (Network Equipment-Building System) Level-3 compliance and can be placed in central office sites or standard telephone closets. Standard 19 inch (or optional 23 inch) rack mount ears can be used to accommodate your rack mount closet standard.

For power, the MAX TNT chassis can be outfitted with single, or dual power supplies of either AC or DC voltage. These hot swappable and load-sharing power supplies provide the redundant power option that the highest availability sites need.

The MAX TNT provides the broadest array of expansion cards in the industry; it accommodates existing access standards such as 10/100Base-T, HSSI, analog, ISDN and Frame Relay, while also addressing the increasingly number of new access standards such as IDSL, SDSL and RADSL. Each expansion module incorporates its own high-performance RISC processor so that the MAX TNT system resources scale as you expand the functionality. By simply adding new expansion modules you can quickly and seamlessly support new services and new technologies; obviating the need for additional external equipment and training, while avoiding potential integration challenges.

Backplane

For maximum performance the MAX TNT incorporates three buses in its backplane design and interconnects these buses on each chassis with inter-shelf links that run between the shelf controllers on each of MAX TNT shelves. Each bus is optimized for a specific type of data traffic and provides a high-throughput architecture for simultaneous control, TDM and packet data.

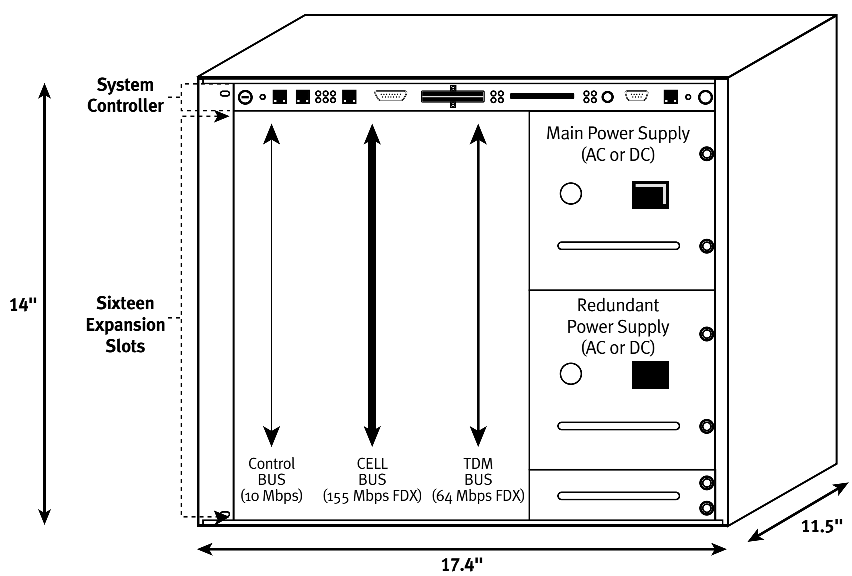

Figure 9 – Physical representation of a MAX TNT shelf

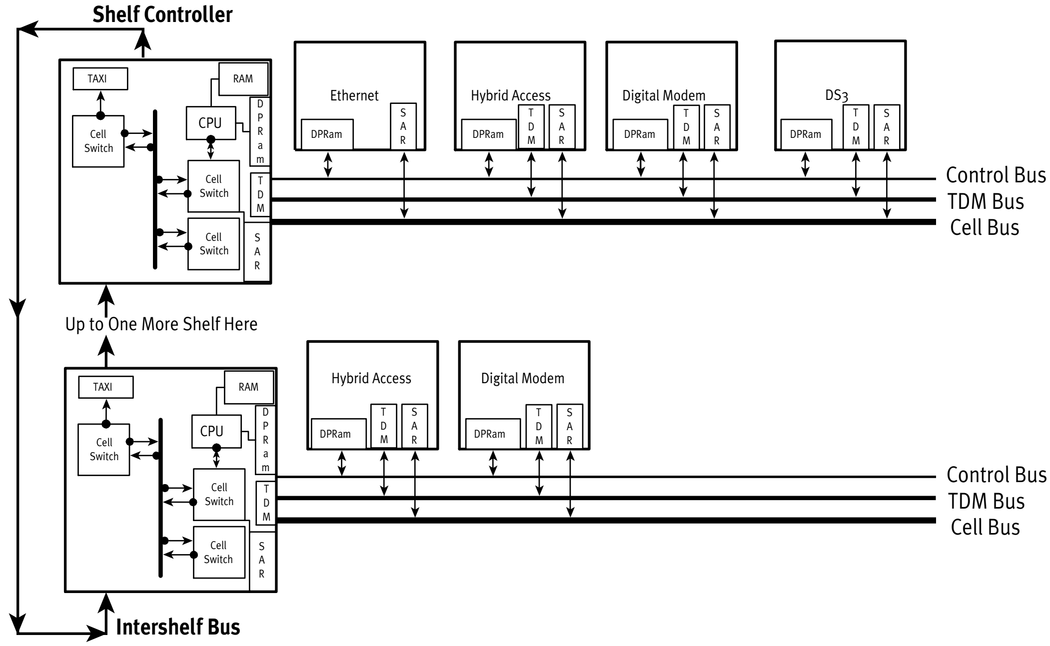

Figure 10 – Logical representation of MAX TNT Intra-shelf and Inter-shelf Buses

Control Bus

The control bus is a 10 Mbps module-to-module communications link that is used for exchange of control and configuration information between the shelf controller and expansion modules. It is also the channel for distribution of software (or image files) from the shelf controller to each of the expansion modules. The control bus is a dual-ported memory access channel which allows rapid and direct full-duplex communications between the CPU on the Shelf Controller and the CPUs on all the MAX TNT expansion modules. The Control bus connects the Shelf Controller to the expansion modules in a virtual star configuration so there is never any bus contention. Whenever a MAX TNT chassis is powered up the Shelf controller module communicates across this bus to determine what expansion modules are in the MAX TNT chassis and whether each of the modules in the MAX TNT chassis has the correct operating software and configuration information. If new operating software or configuration information is needed, it can be quickly downloaded from the shelf-controller to the appropriate modules over this bus.

The control bus is also used by the Shelf controller module to monitor the status of, and provide operating instructions to, all the other modules in the MAX TNT chassis in real-time. For example, as calls to the digital modem cards end, the shelf controller is notified over the control bus so it knows that it can reassign incoming modem calls to that modem.

The Control bus is comprised of two discrete segments; the Intrashelf bus (within the MAX TNT chassis) and Intershelf bus (between the MAX TNT chassis'). While most communications over the control bus will take place on a given shelf's intrashelf control bus, there are also on-going communications between the Master shelf controller and the other shelf controllers and expansion modules in the other shelves. This inter-shelf communication is accomplished by muxing the information over the high-speed intershelf cell bus that links up to three MAX TNT shelves.

TDM Bus

The MAX TNT TDM Bus is a 64 Mbps bus for circuit-switched WAN data. The TDM bus was designed for rapid transfer of inbound or outbound WAN traffic directly to, or from, other expansion modules. This approach maximizes throughput by avoiding the data format conversion and transfer delay that many WAN access switches have. The TDM bus supports 1024 full-duplex 64 Kbps time slots (or subrates of 64 Kbps) and can switch DS0 channels independent of data origination.

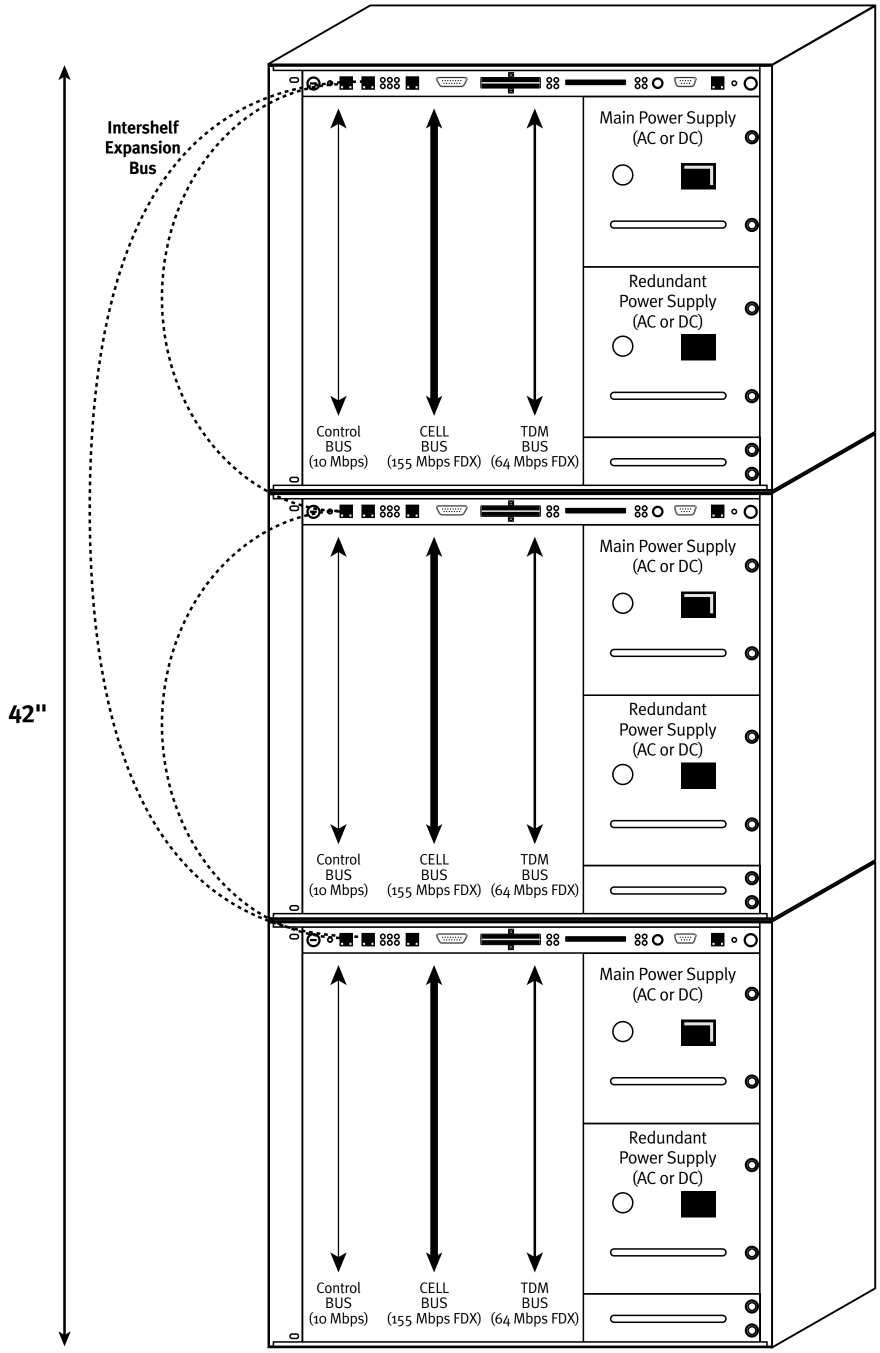

Figure 11 – The control Bus, Cell Bus and TDM Bus are extended between shelves via the Intershelf Bus.

As with all the MAX TNT buses, there are two implementations of the TDM bus; the Intra-shelf TDM bus, and the Inter-Shelf TDM bus. The Inter-Shelf bus is implemented via the Shelf Controller modules, provides a full 64 Mbps data path and is implemented using the TAXI (Transmit and Receive Interface) Cell technology. The Intershelf TDM bus transfers data over the twisted pair cable going between each of the Shelf controllers. The Intershelf bus provides full redundancy/backup protection because of it's closed loop design; each MAX TNT shelf provides a default with cut-through relays to insure that a non-communicative shelf does not interrupt communications between any of the other shelves.

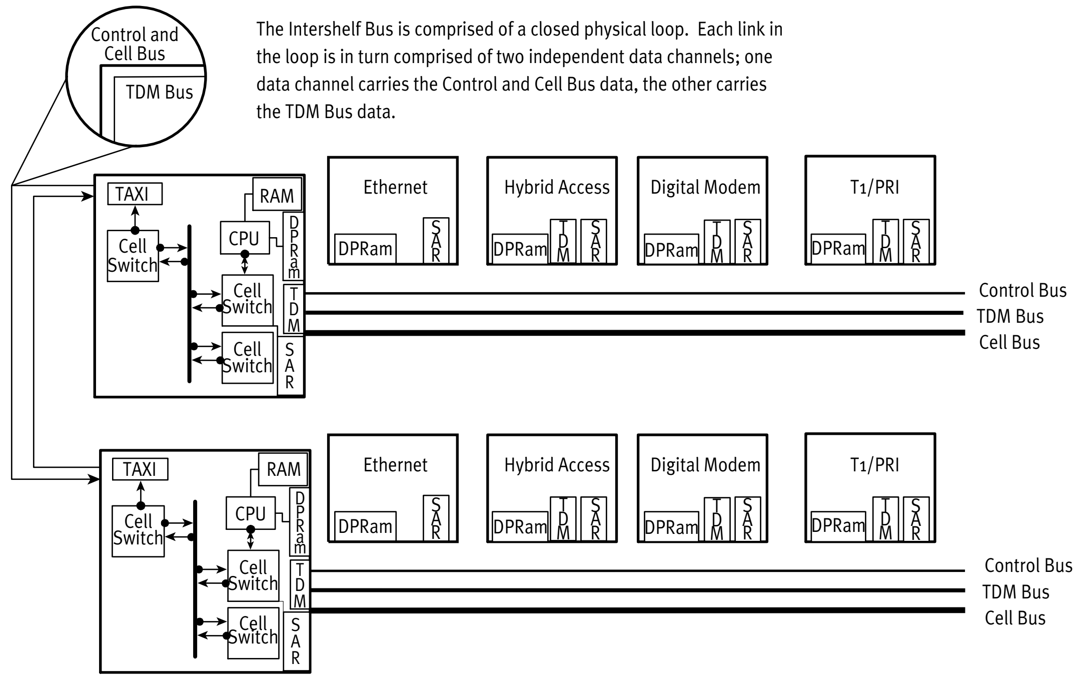

Figure 12 – Intershelf Bus

The TDM intershelf bus is incorporated within a single custom twisted pair cable with the other intershelf buses and must be part of a closed physical loop that passes through all the Shelf controllers in the two or three shelf MAX TNT system (see figure 13).

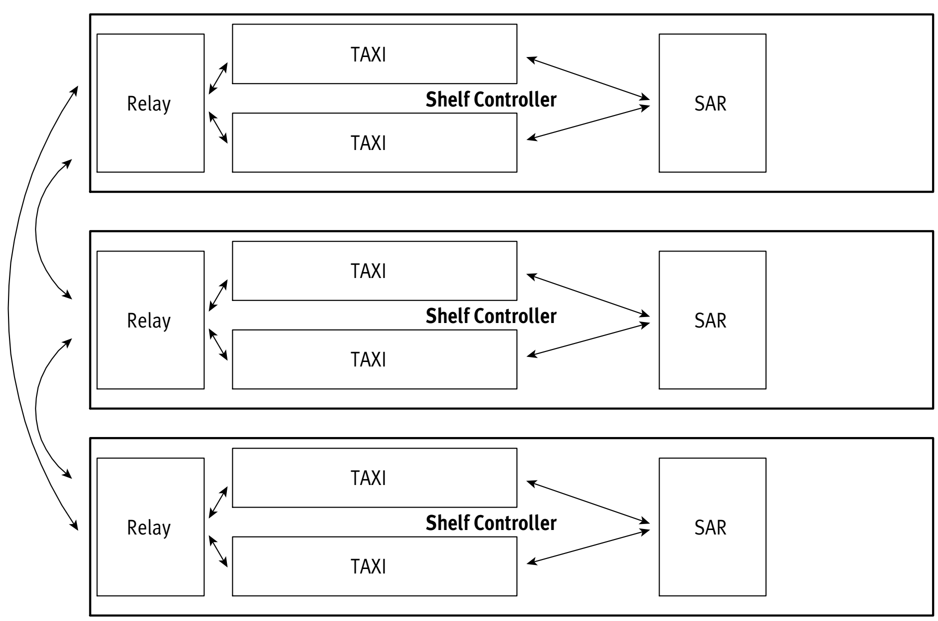

Figure 13 – Intershelf Bus – Cut-through relays improve reliability.

Cell Bus

The 155 Mbps cell bus is a high-speed, full-duplex, non-blocking, non-collision based path between the MAX TNT modules. Whenever data from any of the expansion modules (DS3, T1/E1, etc.) needs to be routed across the backplane in packet form, that data is transported over the Cell bus. Multiple shelves in a MAX TNT system can operate logically as a single large system. There is no delay penalty for switching data between modules in different shelves as compared with switching data between modules in the same MAX TNT shelf.

To communicate on the cell bus each MAX TNT expansion module has a Segmentation And Re-assembly (SAR) chip that breaks IP (or other Layer-3 protocol) packets or reassemble incoming packets into cells and forward them to their destination on the cell bus. Each shelf controller has a Transparent Asynchronous TX/RX Interface (TAXI) driver circuit that drives the intershelf cell bus in a redundant loop interface (see above Figure 13).

Every shelf controller has three high-speed Cell switches that direct these Cells at 155 Mbps speeds to their destinations – either on the local cell bus or over the intershelf link to one of the other MAX TNT shelves.

4. Software Overview

Call and Route Management

The MAX TNT system uses an advanced route management system to maintain a high level of throughput at all load levels. Each expansion module automatically caches routes locally as they are learned by the shelf controller. The shelf controller maintains the main routing table for the MAX TNT shelf and manages the route cache that exists on each of the expansion modules. As new routes are learned the route cache in the expansion modules are automatically updated and older unused or lesser used routes are deleted in a route table “aging” process. The shelf controller acts as a back-up routing engine for those instances when packet destinations don’t match the cached route.

Route Management/Route Caching

Route caches enable expansion modules to route IP packets to another MAX TNT module, reducing the route-processing overhead on the shelf-controller and eliminating routing delays. While the shelf-controller is still responsible for managing routing protocols and the route caches themselves each expansion module is able to check a local route cache and route packets to a destination slot. When a slot card receives an IP packet for which it has no cache entry, it forwards that packet to the shelf-controller, which routes it to the proper expansion module and writes a cache entry that is downloaded to the route cache of all slot cards via the control bus.

Route caches are enabled by default although you can turn them off. The default operation of the route cache sets no limit on the size of the cache. Router cache is normally only limited by the available memory on the individual expansion module which in turn is dependent upon the memory footprint of the code in that software release. In most applications, the vast majority of traffic is routed directly to the destination expansion module thereby maximizing system routing performance.

The following example describes how the first packet of a data flow through the MAX TNT in a non-route cached manner. After this first packet has been routed through the MAX TNT the data flow is then based on a “cached route”. In this example you can see that an incoming IP packet from a T1/E1 line is destined for the Ethernet module. The following steps take place in this example:

1. Incoming T1/E1 data is striped of its D4 Framing (For E1 data is stripped from a G.704 frame)
2. The data is forwarded to the SAR chip where it is broken up into 53 byte cells and forwarded over the Cell Bus to the Shelf Controller for IP routing.
3. The Shelf Controller’s SAR chip reassembles the IP packet, and forwards the IP packet to the CPU where the header is read for the destination, and the packet then placed back on the cell bus destined for the correct port on the Ethernet module.
4. The SAR chip on the Ethernet module again reassembles the IP packet and forwards them to the appropriate interface.

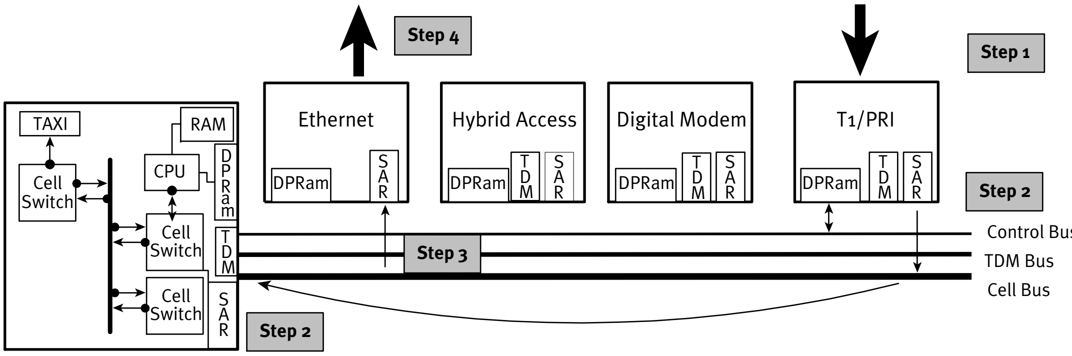

Figure 14 – Data flow example after authentication and before route caching

The T1 module communicates directly over the control bus to the Ethernet module to regulate the transfer of data over the Cell bus between the two modules.

By comparison, the route cache works as follows:

1. One main routing table is maintained in the Shelf controller.
2. The routing table identifies destination IP address, MAX TNT expansion module and port number.
3. When ever a packet that must be routed comes into the shelf controller the packet is routed, and then the routing cache on the expansion modules is updated with the correct route for a packet with that destination.
4. When additional packets come into an expansion module with the same destination as the aforementioned packet, the route cache identifies the other expansion module to which they should be forwarded, and the packet is immediately sent over the cell bus to the next expansion module.
5. When the expansion module cache becomes full the oldest unused, or least used, routes are discarded.

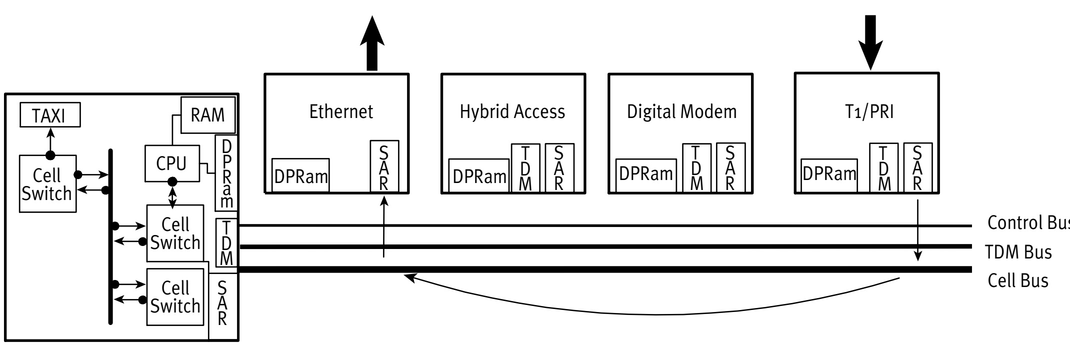

Figure 15 – Data flow example after route caching

Call Routing

Call routing takes place in a MAX TNT whenever a circuit is terminated on a MAX TNT expansion module and incoming or outgoing data needs to be forwarded to another expansion module. A general overview of the call routing process can be summarized as follows:

1. A call (or circuit) is terminated at the appropriate slot card (typically a T1/PRI or DS3 expansion module)
2. The Expansion module notifies the Shelf Controller of the incoming call (and details about it) via the control bus and the shelf controller responds with information on where to route the call.
3. The data from the card is passed on to the next module either for intermediate processing (for example in the case of an HDLC or Analog call, or a call which requires IP routing using the shelf controller routing engine), or directly to the ultimate destination card such as the Ethernet card using the route cache on the local card to determine the destination.

Calls are always received and placed on network ports (A MAX TNT network port is defined as a T1/E1/PRI or T3 channel). In some cases, the MAX TNT may forward a call to a Frame Relay switch or to a network host without processing the call or handling its encapsulation. In all other cases when the MAX TNT receives a call it must first be routed to a host port for encapsulation processing before being forwarded to the router or terminal server software. A MAX TNT host port is defined as an High-level Data Link Control (HDLC) channel or a digital modem.

HDLC processing removes encapsulation from high-speed incoming data calls such as those from ISDN terminal adapters. The Hybrid Access module (also referred to as the HDLC module) removes the call's link encapsulation and then passes the data stream to the router on the shelf controller. One 192-channel HDLC card supports all switched channels on an eight-port T1 card. The 10-port Frameline module incorporates both the T1 termination circuitry as well as the HDLC processors thereby eliminating the need for the additional Hybrid access module for HDLC processing.

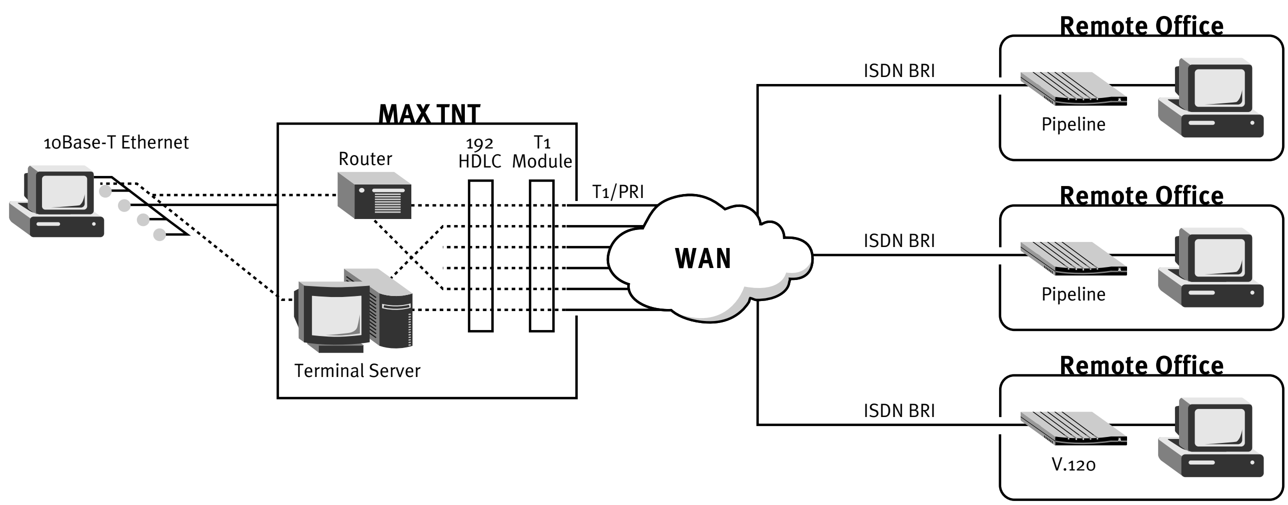

Figure 16 – Call routing with ISDN calls.

Digital modems in the MAX TNT handle the asynchronous data calls initiated by analog modems. A digital modem accepts an incoming call as a Pulse Coded Modulation (PCM) encoded digital stream, which contains a digitized version of the analog data sent by a modem. The digital modem also converts outgoing data to be sent across the WAN to an analog modem. Because asynchronous calls have a lower bit-rate, PPP encapsulation can be removed by the modem module's processor and further HDLC processing is not needed.

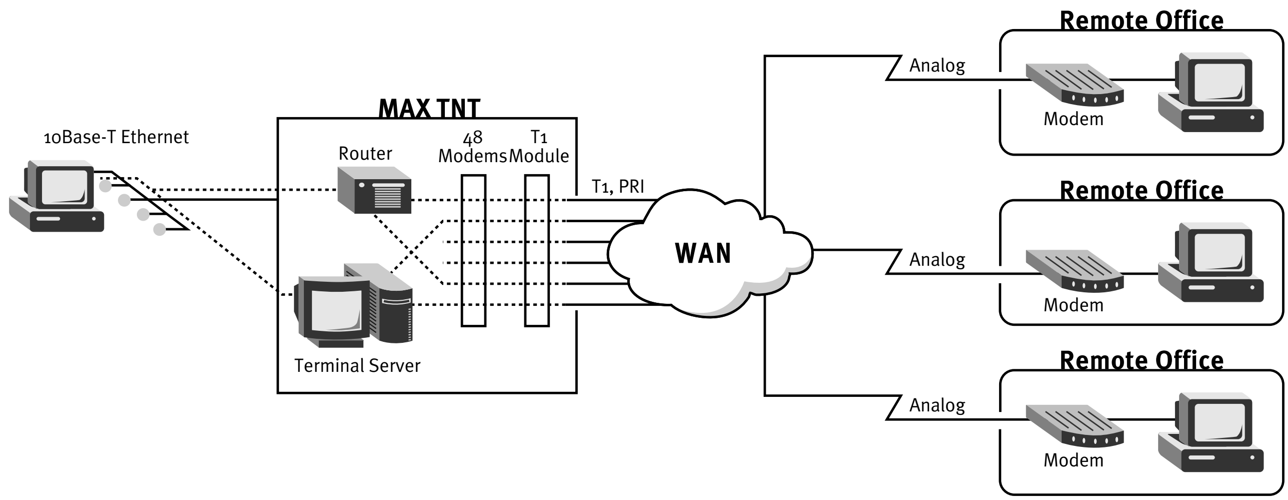

Figure 17 – Call routing with analog calls

Detailed Call routing

While call routing will vary by type of circuit or call the following description is representative of how a typical call type is routed in the MAX TNT. In this example a synchronous digital ISDN call is terminated in a MAX TNT via an ISDN PRI circuit on a T1/PRI expansion module. The caller (a Pipeline® 50 in this example) will be sending TCP/IP packets which are destined for a host available through the Ethernet slot card.

Each T1/PRI expansion module terminates the ISDN PRI circuits to which it is connected, and is responsible for all of the PRI signaling to the telephone company's switch for those circuits.

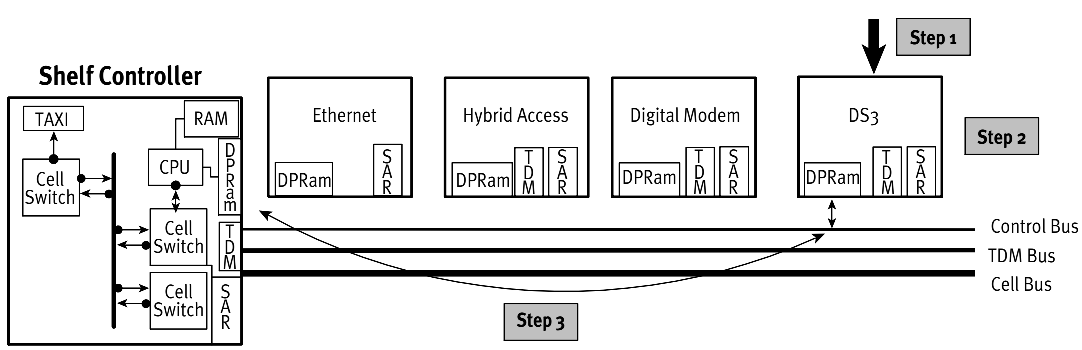

Figure 18 – DS3 module communicates with shelf controller to determine call routing.

Step 1. On an incoming call, synchronous digital PPP in this case, the telephone company switch notifies the T1 expansion module via the D-channel of the impending call.

Step 2. On receipt of notification of an incoming call, the T1 module notifies the shelf controller of the details of call – e.g. digital, 64 Kbps – and requests assignment of a TDM bus channel.

Step 3. The shelf controller refers to its call routing database to determine an appropriate expansion module to route the data to. It also identifies and allocates an available TDM channel for the call. Then, via the control bus, it directs the T1 module to route the data over the identified expansion module and TDM bus channel.

Step 4. The T1 module strips off the incoming bit stream of ISDN signaling information, and forwards the data over the assigned slot as an HDLC byte stream, including HDLC header, and HDLC payload (the IP packet).

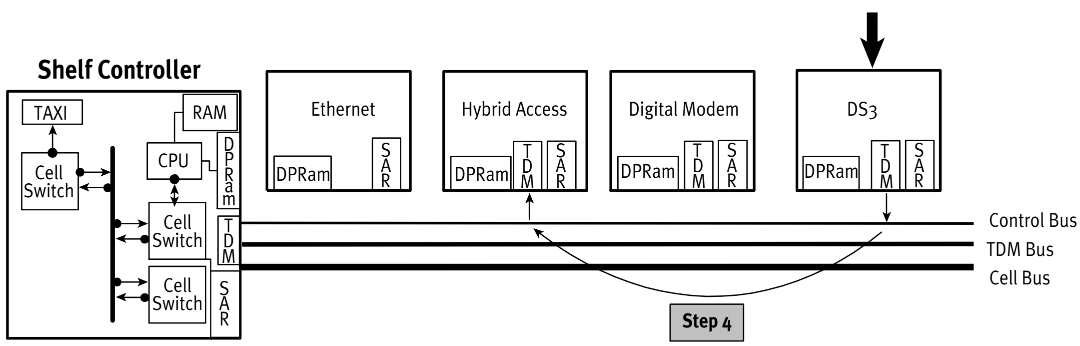

Figure 19 – The data packet is forwarded to the Hybrid Access module.

In this example the target module for that byte stream is the Hybrid Access (or HDLC processor) module. The T1 module forwards the incoming HDLC byte stream, byte for byte, over the TDM bus to the Hybrid Access module.

On receipt of the HDLC frames, the Hybrid Access module strips the HDLC headers and assembles a complete IP packet.

Once a complete IP packet is assembled, the Hybrid Access module is ready to forward that packet over the Cell bus to the appropriate expansion module.

The Hybrid Access module compares the destination IP address of the IP packet to destinations listed in the IP route cache. A cache ‘hit’ is the result of a successful comparison. A cache ‘miss’ is the result of an unsuccessful comparison.

Step 5. On a cache hit, the Hybrid Access module is able to forward the IP packet directly over the Cell bus to the appropriate expansion module.

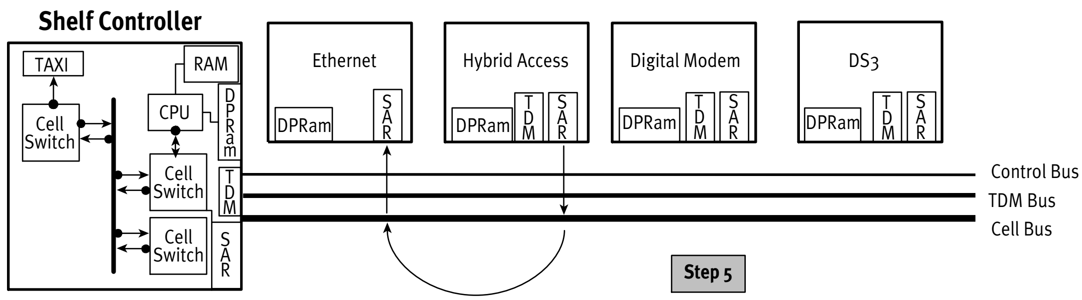

Figure 20 – A cache hit results in immediate packet forwarding.

Step 6. On a cache miss, the HDLC card must forward the destination of the IP packet, via the control bus, to the shelf controller for an IP route table lookup.

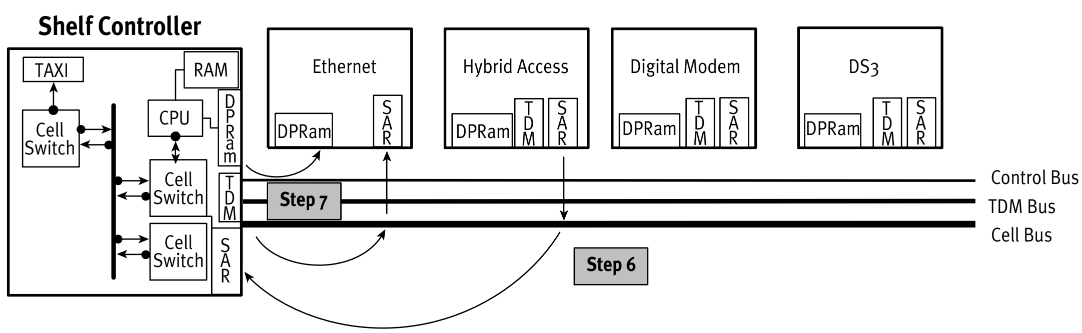

Figure 21 – A cache miss results in route lookup.

Step 7. The shelf controller performs the lookup, and returns, via the control bus, the appropriate target expansion module and port for the packet so as to update the route cache. At the same time the shelf forwards the packet on to its destination over the Cell bus.

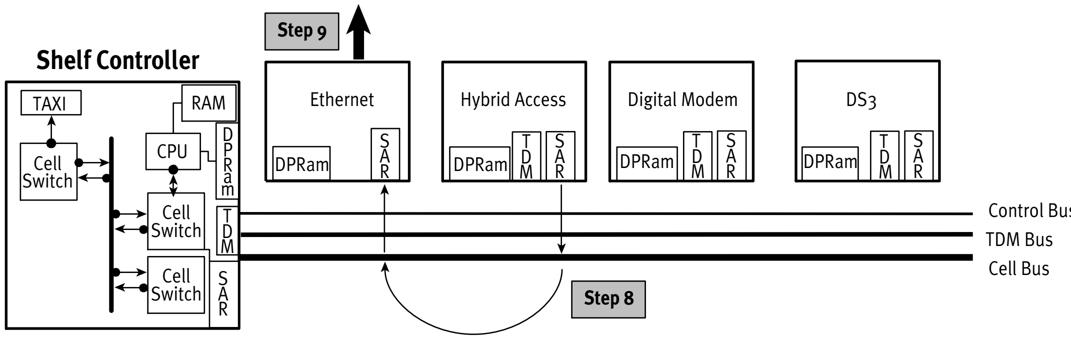

Figure 22 – Step 8, route cached, data forwarded.

Step 8. In either case, once the HDLC card has learned the target destination slot card and port for the IP packet, the Hybrid Access module's SAR chip frames the IP packet in cells for forwarding on the Cell bus.

Assuming that the target slot card is the Ethernet card, the HDLC SAR then targets the cells for the Ethernet card.

Step 9. The SAR chip on the Ethernet card re-assembles a complete IP packet from the cells received from Hybrid Access module. Once a complete IP packet is re-assembled, it frames the IP packet for transmission on the Ethernet.

Routing Support

The Ascend MAX TNT provides routing support for IP, IPX and AppleTalk protocols. However, it differs from a traditional backbone router in several key ways.

A traditional backbone router (such as those manufactured by Cisco Systems, Bay Networks, and 3Com) is specifically designed for a relatively low number of low to moderate speed fixed point-to-point connections. These traditional routers support dozen of protocols and have a few expensive ports to support digital leased lines and LAN-to-LAN connections. But they have very little switched circuit intelligence. They provide little in the way of switched WAN management, and are frequently not certified to connect to the world's switched digital services.

The MAX TNT, on the other hand, was designed specifically for very large numbers of switched and leased connections and as such can be defined as a Network Access Switch (NAS). It supports the few key protocols widely used for internetworking – IP, IPX and AppleTalk. Moreover, its ports are designed to support the lower speeds of analog and ISDN dial-in connections in addition to the higher speed LAN to LAN standards, so its per-port cost is much less than a traditional backbone router. The MAX TNT is "smart" about switched WANs, and provides comprehensive switched circuit management and security capabilities. Furthermore, it is certified to connect to the world's switched digital services. The MAX TNT supports switched dial-in ISDN and modem connections as well as Frame Relay. The MAX TNT's Frame Relay or Serial port option modules can be used to interconnect the NSP's remote POPs to the central POP to create a high-speed Frame Relay backbone.

While the MAX TNT and traditional backbone routers both support LAN to LAN and LAN to WAN routing and bridging, they are designed for different purposes and as such coexist on the backbone network. Increasingly, however, we are seeing a trend in the Internet towards high speed IP Switches such as the Ascend GRF replacing traditional backbone routers. In applications where the traffic is entirely IP-based, and the highest possible throughput is needed, IP switches are the products of choice.

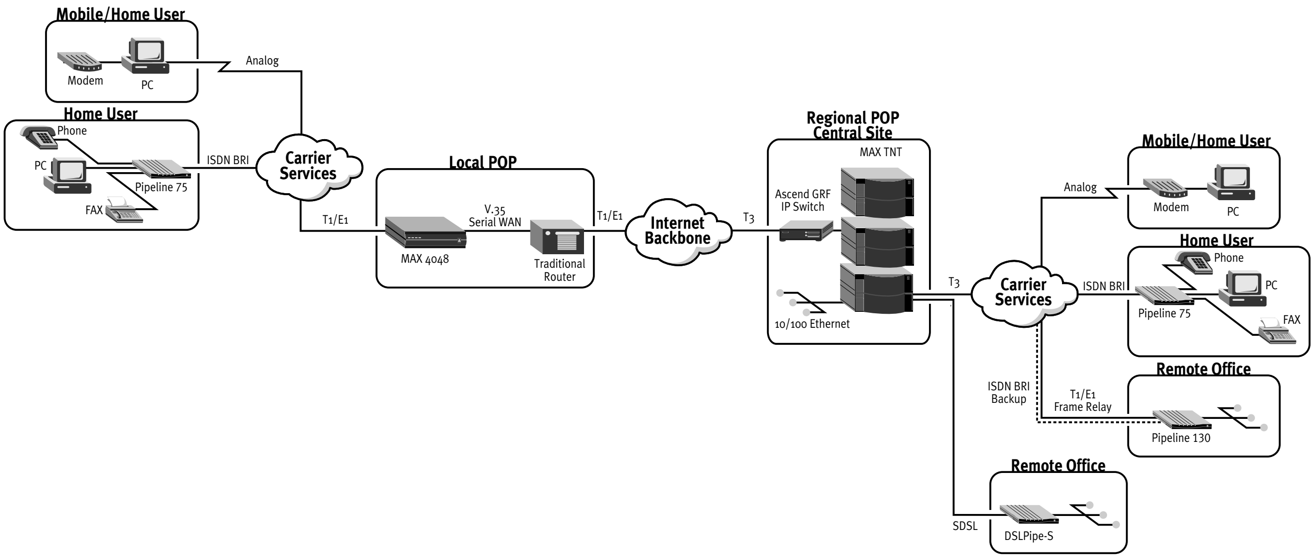

Figure 23 – Access Switches like the MAX TNT co-exist with traditional backbone routers and high-performance IP Switches.

IP Routing Support

The MAX TNT supports a comprehensive range of IP Routing protocols including Routing Information Protocol (RIPv1), RIPv2, Open Shortest Path First (OSPF), and IGMP V1,2 forwarding as defined in RFCs 1058, 1388, 1131 and 1112, respectively.

The MAX TNT also supports IP routing over Point to Point Protocol (PPP), Multilink Protocol (MP), Multilink Protocol Plus™ (MP+), Bandwidth Allocation Control Protocol (BACP), TCP-CLEAR, and Frame Relay connections and is fully interoperable with non-Ascend products that conform to the TCP/IP protocol suite and associated RFCs. IP routing connections have a level of built-in authentication, because the MAX TNT matches the IP address of a Connection Profile to the source IP address of a caller. However, for most sites this level of security is not enough and PAP or CHAP authentication are used as well, and optional dynamic firewall protection is available for even greater security.

IP routing can be configured along with protocol-independent IPX and AppleTalk routing in any combination.

RIP

The MAX TNT supports Routing Information Protocol Versions 1 and 2 (RIP-1 and RIP-2). You can configure the MAX TNT to send, receive, or send and receive, RIP-1 or RIP-2 on the Ethernet port or any WAN interface. Within RIP the user may decide, on a per-interface basis, whether updates are sent and received on the interface, and whether the interface is filtered from transmitted updates.

You can use a RADIUS server’s Framed-Routing attribute to indicate whether each user sends packets, receives RIP packets, or both.

Many sites turn off RIP on the WAN interface in order to avoid storing very large local routing tables and to conserve bandwidth. If you turn off RIP, the MAX TNT does not listen to RIP updates across the connection. To route to other networks through that connection, the MAX TNT must rely on static routes specified in a special connection profile.

If RIP is enabled to both send and receive RIP updates on the WAN interface, the MAX TNT broadcasts its routing table to the remote network and listens for RIP updates from that network. Gradually, all routers on both networks have consistent routing tables (all of which may become quite large).

RIP-2

RIP version 2, the enhanced version of RIP that is supported in the MAX TNT, greatly benefits NSPs. It allows Class C address blocks to be broken into subnets for assignment to multiple business customers. In addition, "leftover" addresses from different Class C blocks can be combined into a common subnet. RIP-2 enables more efficient address usage, which reduces administrative overhead and costs.

RIP-2 includes the following improvements to RIP-1:

- Subnet routing – RIP-1 recognized subnet information only within the subnet and purposely did not advertise netmasks to other routers. There was no way to distinguish between a subnet and a host entry except to routers directly connected to the subnet. When a RIP-1 router receives an IP address, it assumes the default subnet mask. RIP-2 passes the netmask in parallel with the address. This enables support not only of reliable subnet routing, but also of variable length masks within the same network and Classless Inter-Domain Routing (CIDR). If a RIP-1 router receives a RIP-2 update that includes netmasks, it ignores the subnet information.
- Authentication – RIP-1 provided no way of authenticating its routing advertisements. Any program that transmitted packets on UDP port 520 was considered a router with valid distance vectors. RIP-2 packets include an authentication field that can contain a simple password. If a RIP-1 router receives a RIP-2 packet that contains a password, it ignores the field.
- Routing domains – To enable multiple networks to share a common backbone, RIP-2 uses a routing domain number that enables routers to recognize packets bound for a particular one of the router's networks.
- Multicasting – RIP-1 uses a broadcast address for sending updates, so its tables are received not only by routers but by all hosts on the cable as well. RIP-2 uses an IP multicast address for periodic multicasts to RIP-2 routers only.

OSPF

OSPF addresses RIP's shortcomings and is better suited to today's large, dynamic networks. Following are some advantages of OSPF over RIP:

- Fast, Loopless convergence – RIP creates a routing table and then propagates it throughout the internet of routers, hop by hop. The time it takes for all routers to receive information about a topology change is called "convergence." A slow convergence can result in routing loops and errors. A RIP router broadcasts its entire routing table every 30 seconds. On a 15-hop network, convergence can be as high as 7.5 minutes. In addition, a large table may require multiple broadcasts for each updates, which consumes a lot of bandwidth. OSPF uses a topological database of the network and propagates only changes to the database. Instead of sending the entire routing table every 30 seconds, OSPF routers send link information every 30 minutes. Additionally, with OSPF small update messages (usually less than 75 bytes) are sent whenever changes in the network are detected. Fewer routing updates provide better performance
- Support for subdivisions of larger networks – OSPF areas, logical subdivisions of an OSPF network, address the issue of slow convergence in large networks. ISPs that use OSPF can structure their networks into many areas, such as local POPs, regions, or other administrative domains, to ensure high quality service. OSPF routers exchange messages only with routers in their area, which reduces the number of updates that flow through the network and the size of topology databases. OSPF areas are connected by a backbone, which is also considered to be a defined area. Special backbone routers, called area border routers, maintain a topology database for multiple areas. With areas, the convergence of the routing tables is faster than with RIP.
- Support for more precise metrics, and if needed, multiple metrics – RIP is a distance-vector protocol, which uses a hop count to select the shortest route to a destination network. RIP always uses the lowest hop count, regard-

less of the speed or reliability of a link. OSPF is a link-state protocol, which means that OSPF can take into account a variety of link conditions, such as the reliability or speed of the link, when determining the best path to a destination network.

- Support for multiple paths to a destination – OSPF supports the ability to have multiple paths to a destination for traffic. This feature can result in lower delays and lower delay variance than if all traffic is queued over a single path. Additionally, because of the potential for multiple paths, only a fraction of the traffic will have to be rerouted after a link failure, and the overall pattern will be much smoother. RIP only supports a single path.
- Separate representation of external routes – A network is generally connected through one or several “external gateways” to one or several “transit networks.” OSPF allows “gateway link state records” that lead to better performance for the link state algorithm due to more precise metrics and easier computations.

RIP is used within OSPF networks as an end-station-to-router protocol. As a result, OSPF addresses the deficiencies of RIP without affecting connectivity to RIP-based networks. With a good network design, OSPF lets networks scale to very large topologies, while maintaining high levels of availability and performance. Because of these advantages, OSPF has quickly become widely employed. The MAX TNT’s support of OSPF allows for smooth integration into existing networks whether they are RIP or OSPF based.

IGMP Multicast Forwarding

The MAX TNT’s support for Multicast standards allows for much better utilization of the Internet in broadcast (especially multimedia broadcast) applications by forwarding only one copy of a given packet over a link even if the information contained in that packet is destined for a number of downstream clients. Instead of forwarding multiple copies of the same packet as has traditionally been done in IP unicast routing, multicast supporting routers take the responsibility of distributing and replicating the multicast data to their destinations. The MAX TNT supports the Internet Group Membership Protocol (IGMP) version-1 and version-2 standards, along with configuration options that enable the MAX TNT to communicate with the multicast routers and forward multicast traffic for the groups it maintains.

IGMP Protocol Overview

IGMP, documented in Appendix I of RFC 1112, allows Internet hosts to participate in IP multicasting. RFC 1112 describes the basic of multicasting IP traffic, including the format of multicast IP addresses, multicast Ethernet encapsulation, and the concept of a host group. For more information on the Multicast protocols please refer to RFC 1112.

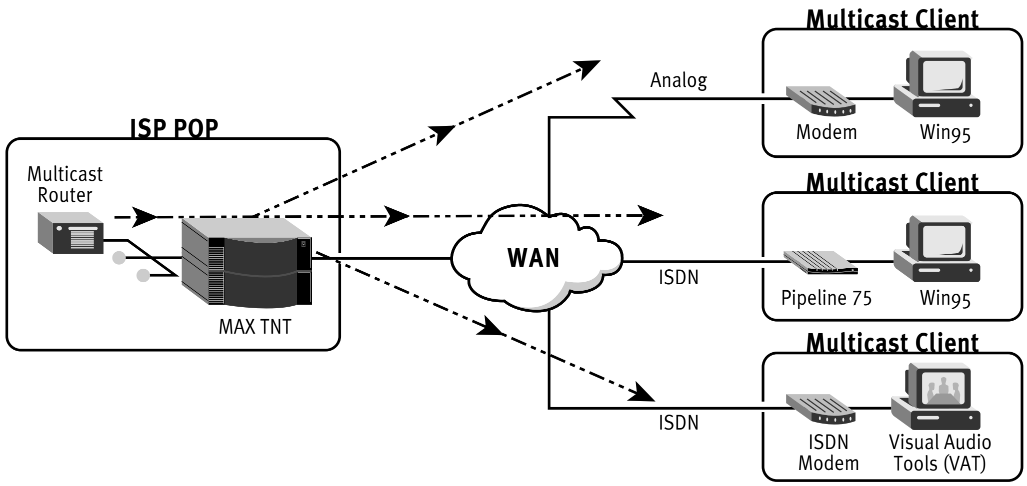

Figure 24 – The MAX TNT communicates with a multicast router on its Ethernet interface and forwards multicast traffic to dial-in multicast clients.

To communicate with a IP Multicast (or Multicast Backbone – MBONE) router, the MAX TNT acts as a multicast client; it receives queries from the router and responds to them using IGMP. The multicast router may reside on its Ethernet interface or across a WAN link. If the router is accessed across the WAN, the MAX TNT can respond to multicast clients on its Ethernet interface as well as across WAN links.

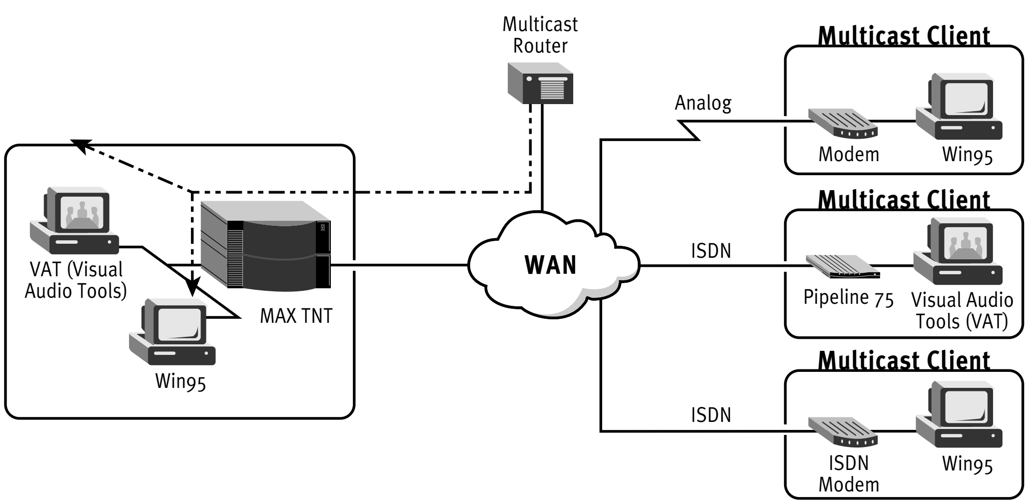

Figure 25 – MAX TNT acting as a multicast forwarder on Ethernet

To communicate with multicast clients, the MAX TNT sends the clients IGMP queries every 60 seconds, receives responses, and forwards multicast traffic. To the clients it looks like a multicast router, although in fact the MAX TNT is forwarding multicast packets based on group memberships. When multicasting is enabled in the MAX TNT, it builds a multicast forwarding table. Based on IGMP messages it exchanges, the MAX TNT creates new group memberships or refreshes existing ones in its multicast forwarding table. When the MAX TNT receives IP multicast packets from its MBONE interface, it checks its multicast forwarding table and forwards the packets to its multicast clients according to group membership. When it creates a new group membership, it sends a JOIN message on its MBONE interface. When the last member of a group is no longer active, if the MBONE interface supports a multicast router running IGMP, the MAX TNT sends a LEAVE message.

In the MAX TNT implementation of multicast routing support, the "Forward multicast trace packets" feature has been implemented. This feature allows multicast clients to MTRACE (multicast trace) the path taken by multicast traffic. The MAX TNT can pass IGMP MTRACE packets from multicast clients to MBONE and MTRACE RESPONSE packets back to clients from MBONE.

Static Routes

The MAX TNT fully supports static routing. A static route is a predefined path from one network to another, which specifies the destination network and the router to use to get to that network. For routes that must be reliable, the administrator often configures more than one path (a secondary route), in which case the MAX TNT chooses the primary route based on an assigned metric. In contrast, a dynamic route is a path to another network that is "learned" dynamically rather than configured in a profile. Static routes do not "age," as do routes that are learned through a protocol like RIP.

Static routes are supported through connection profiles in the MAX TNT configuration software. Each static route may be optionally filtered from or included in routing protocol updates. This allows custom static routes on a per user basis thereby providing a very high level of customization as needed for individuals or groups of users.

Interface-based Routing

The MAX TNT implements what is referred to as system-based or box-based routing. With system-based routing, the entire MAX TNT is addressed with a single IP address. For systems that have a single backbone connection system-based routing is by far the simplest form of routing from both a configuration and trouble-shooting perspective.

The alternative form of routing is referred to as interface-based routing. With interface-based routing, each physical or logical interface on the product has its own IP address. For a product such as a MAX TNT it would potentially be required to assign hundreds of IP addresses.

However, there are some applications that the MAX is used for in which it might be useful to "number" some of the interfaces – so as to have the MAX TNT operate as a partially system-based router and partially as an interface-based router. Reasons for using numbered interfaces include trouble-shooting leased point-to-point connections and forcing routing decisions between two links going to the same final destination. More generally, the interface-based routing option allows the MAX TNT to operate more closely to the way a multi-homed Internet host behaves.

Novell IPX

Ascend's IPX implementation includes full support for IPX spoofing and dial-in or LAN-to-LAN routing. This support can be used either natively or over IP tunnels (i.e. Virtual Private Networks).

IPX support includes the ability to:

- Establish IPX routing
- Forward IPX packets
- Generate RIP and SAP packets
- Interpret incoming RIP and SAP packets
- Filter incoming RIP and SAP packets

Tunneling IPX across the Internet

Ascend Tunnel Management Protocol (ATMP) tunnels enable remote NetWare clients to log into corporate IPX networks across the Internet by using a local ISP connection. This new technology allows very cost-effective remote networking for corporations, and an important value-added service opportunity for Network Service Providers. See the Virtual Private Network section of this paper for additional information.

AppleTalk

Ascend's AppleTalk implementation includes support for dial-in access for ARA 1.0 and 2.0 as well as AppleTalk native routing. AppleTalk Remote Access (ARA) connections rely on AppleTalk, and a basic AppleTalk stack has been added to the MAX TNT for ARA support. The stack includes an Name Binding Protocol (NBP) network visible entity and an AppleTalk Echo Protocol (AEP) echo responder, which allows the administrator to use standard AppleTalk management and diagnostic tools such as InterPoll (Apple Computer) to obtain information. Native AppleTalk routing allows the interconnection to two AppleTalk LANs using the standard AppleTalk (as opposed to ARA).

ARA connections for IP access

The MAX TNT is able to act as a DDP-IP gateway, encapsulating outbound IP packets in DDP for transmission via ARA and stripping off DDP headers from inbound IP packets. For the remote Macintosh to communicate with IP hosts on an ARA connection, it must be running both ARA software and TCP/IP software such as MacTCP or Open Transport.

5. WAN Access Line Types

Today's leased and switched services are accessed from your location through a network access line. Ascend MAX TNT systems integrate a dynamic mix of network access lines:

- IDSL
- ISDN PRI
- T1, E1 (G.703), and Fractional T1 (FT1) access lines
- T3 access lines

IDSL Access

Ascend now offers ISDN Digital Subscriber Line (IDSL) support via MAX TNT expansion modules that provide "always on" (nailed-up) digital data circuits. Ascend has announced that there will be a future software upgrade to support voice services over IDSL also. As with regular ISDN BRI services, these lines each contain two 64 Kbps data channels (B-channels) that can be used for data (or voice, Q4 '97) independently, and a single out-of-band signaling channel (D-channel).

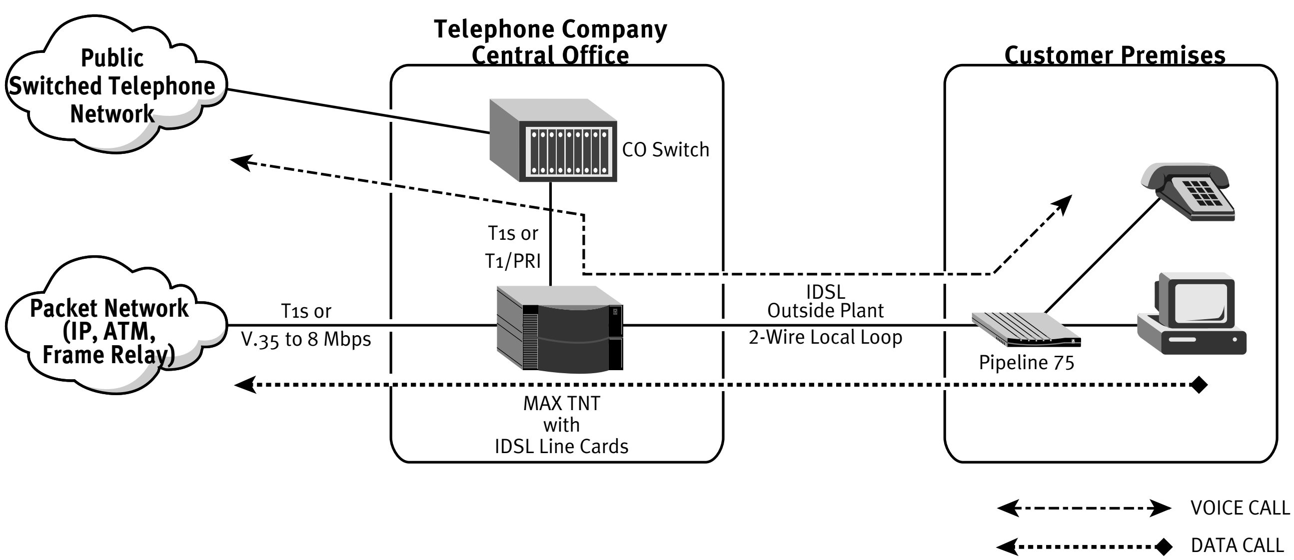

Figure 26 – IDSL addresses data and voice needs.

Unlike normal ISDN lines IDSL lines provide data services that do not burden the traditional telephone company central office switches, instead the packet data is directly routed to the data network and only the voice service are switched onto the traditional telephone switches. Because the IDSL card in the MAX TNT is splitting off the data before it reaches the central office switch, the MAX TNT must be co-located in the Telco's central office or can be used in a corporate building/high-rise or college campus environment where telephone wiring is available over significant distances and high-speed internetworking support is desired.

IDSL lines are an ideal addition to a ISP's or carrier's service offering as an inexpensive voice and data service. From an end-user standpoint IDSL is an ideal solution for the small office or medium-sized business that wants to host a Web server at its office, and have full-time Internet connectivity (and voice connectivity) at a reasonable cost.

The key benefits of Ascend's IDSL are:

1. Voice and data support over a single pair of wires without an expensive Central Office switch upgrade (voice to be a software upgrade to existing MAX TNT IDSL modules in the first half of 1998)
2. User-configurable data channel pre-emption for incoming voice calls (so as to allow important phone calls through even though B-channels may be busy with data transfer)
3. Up to 18,000 ft. transmission distance on standard local loop.
4. Transparency of "U" loop repeaters and Digital Loop Carriers (DLCs) to IDSL technology means that distances beyond 18,000 ft. are supported by using standard local loop extension devices.
5. Compatibility with any ISDN terminal adapter or router for IDSL circuits with data-only service.
6. 64 Kbps or 128 Kbps Frame Relay service over a single pair or wires saves the scarce and expensive resource – copper pair (traditional 56 Kbps and 128 Kbps Frame Relay services require 2 pairs of wires)
7. Protection of customers' investment in their existing ISDN CPE

IDSL lines work with all regular ISDN CPE equipment (such as the Ascend Pipeline series of bridge/routers and terminal adapters) without special configuration.

ISDN PRI Access Lines (in North America, Japan, and Korea)

Primary Rate Interface (PRI) lines – Each consist of 23 64 Kbps channels (B-channels) and a single 64 Kbps out-of-band signaling channel (D-channel). They can connect to standard voice, ISDN Multirate, Switched 1536, Switched 384, Switched 64, or Switched 56 services.

ISDN PRI Access Lines (Outside of North America, Japan and Korea)

These lines each contain 30 64 Kbps channels (B-channels) and two 64 Kbps out-of-band signaling channels (D-channels) for a total throughput of 2.048 Kbps. They are based on the CEPT G.703 (E1) standard. They can connect to standard voice, ISDN Multirate, Switched 1536, Switched 384, Switched 64, or Switched 56 services.

E1-R2 Access Lines

E1 access lines are available throughout Asia, Eastern Europe, China and Latin America. These lines support 30 data channels and one signaling channel.

T1 Access Lines

T1 access lines are 1.544 Mbps lines (1.536 Mbps actual user bandwidth plus 8K of framing bits) which have 24 channels, each with 56 Kbps of user bandwidth and 8 Kbps of in-band signaling. Each of these channels can be used to access the standard voice network, the Switched 56 data network, or routed as non-switched leased circuits between two points. Ascend MAX TNT systems can connect to T1 access lines to provide access to switched 56 services or dedicated circuits (such as leased 56, fractional T1, or full T1).

E1 (G.703) Access Lines

E1 is used in Europe like T1 line is used in the United States. Instead of 24 channels combined on a 1. 536 Mbps link, E1 time division multiplexes 32 channels of 64 Kbps for a combined bandwidth of 2.048 Mbps. One of the 32 channels is used for signaling and one for frame alignment, and the remaining 30 are used for actual user bandwidth.

Fractional T1 (FT1) Access Lines

Also called subrate T1, these lines utilize a T1 circuit, but the bandwidth that you have access to is a fraction (for example 128 Kbps, 384 or 756 Kbps) of the full T1 Speed. Fractional T1 is delivered over a standard T1 access line that has been channelized to provide the fractional rate that you have contracted for and uses a standard T1 DSU/CSU.

T3 Access Lines

T3 circuits, provide approximately 45 Mbps of user bandwidth, or up to 28 T1 circuits. Ascend's MAX TNT DS3 module fully supports fractional T3 rates in any increment of DS0 rates.

Hybrid Access

Hybrid Access is an optional hardware feature that gives users flexible digital access via the T1/E1 or ISDN/PRI interface. With this hardware option the MAX TNT supports HDLC processing for those circuits that need it; such as ISDN PRI signaling, Frame Relay etc. NSPs and corporations must frequently expand their capabilities to meet new user requirements. Hybrid Access allows just this type of evolution for analog-focused sites.

PPP-FR Gateway, Frame-Relay Direct

An important application for Frame Relay connections is to link the MAX TNT to Frame Relay switches. A Frame Relay gateway connection supports routing to and from the switch across a nailed connection. A Frame Relay redirect connection allows incoming switched connections that use IP routing to be redirected out through the MAX TNT to the Frame Relay switch.

A configuration profile in the MAX TNT defines a logical link to an end-point reached through a Frame Relay switch. There are two different ways to configure these links:

Gateway Connections

A gateway connection is a bridging or routing link between the MAX TNT and a remote site via a Frame Relay switch. When the MAX TNT receives IP packets destined for that site, it encapsulates the packets in Frame Relay (RFC 1490) and forwards the data stream out to the Frame Relay switch using the specified Data Link Connection Identifier (DLCI). The Frame Relay switch uses the DLCI to route the frames to the right destination.

Redirect Connections

A redirect connection is designed only for forwarding incoming switched calls that use IP routing, such as a regular PPP or MP+ call. When the MAX TNT receives IP packets from a caller that has a redirect specified in its Connection Profile, it simply forwards the data stream out to the Frame Relay switch using the specified DLCI effectively passing on the responsibility of routing those packets to a later hop on the Frame Relay network.

6. MAX TNT Management

The Ascend MAX TNT supports several sophisticated management mechanisms, including integrated SNMP management applications, as well as the more traditional management approaches such as VT100 and Telnet.

NavisAccess

NavisAccess™ is a powerful new SNMP network management application from Ascend that can be used to manage not only Ascend equipment, but also other SNMP-manageable devices in an ISP, carrier or corporate WAN network. NavisAccess comes with an array of common MIBs for immediate compilation and use in management of most common routers and switches on a WAN network. Additionally, full GUI management tools are included (including active backpanel views) for the Cisco 2000, 3000, 4000 and 7000 series of routers.

NavisAccess' key benefits to Ascend customers are:

1. Comprehensive management support of all Ascend access switches
2. Integrated support for third-party SNMP devices such as non-Ascend routers, switches and hubs
3. Network access lines and interface management (e.g., T1/E1, T3, ISDN, xDSL etc.)
4. Management of network services such as Frame Relay, ISDN and ATM
5. Management of elements by grouping into logical entities
6. Individual modem level management for MAX TNT Digital modems

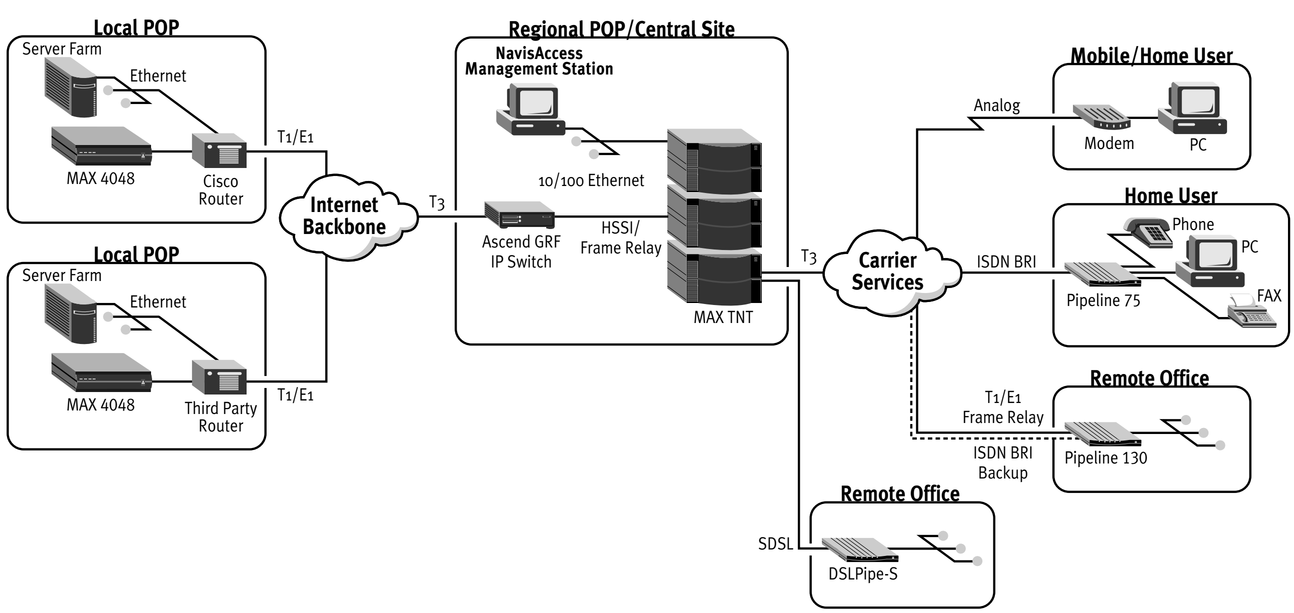

Figure 27 – Use NavisAccess to manage your Ascend and third party WAN equipment.

NavisAccess has been designed to support the most popular management platforms and operating systems. NavisAccess is available as a fully integrated application that runs under HP OpenView 4.1 on Solaris 2.5 and HP OpenView 4.1 on HP UX 10.0 and NavisAccess is also available as a standalone application that runs on UNIX (Solaris) or NT workstations.

VT100

A VT100 (or a PC running a VT100 terminal emulation program) can be used to control the MAX TNT. The windowed user interface displays all functions and status screens and can be used to control remote MAX TNTs.

The MAX TNT VT100 interface provides the following administrative features:

Security Profiles – The MAX TNT has password security to protect the box itself from unauthorized access.

System administration commands – The MAX TNT provides commands for rebooting the device, saving or restoring configuration information, and performing other administrative functions. The MAX TNT enables software upgrades in the field without opening the unit or changing memory chips, a process that also makes use of the configuration management commands.

“**DO**” **commands** – Pressing Ctrl-D in the VT100 interface displays the “DO” menu, which contains commands for changing security levels in the MAX TNT, or manually dialing or clearing a call. When full access (or another appropriate security level) has been activated, you can perform all DO commands as well as other administrative operations.

Terminal server command-line interface – The MAX TNT’s command-line interface provides commands for testing a connection, checking routing tables and other configuration parameters, or configuring far-end Ascend units across the WAN. Many of these commands are related to system administration.

MIF interface – Machine Interface Format (MIF) is an Ascend-specific scripting language that provides an alternative configuration interface for Ascend units. You can use a command-line or write a MIF program that sets Ascend parameters rather than use the configuration menus to change one parameter after another. MIF programs provide a batch-processing method of changing a configuration or performing a series of actions. You can also use MIF to program asynchronous traps to capture Call Detail Reporting (CDR) data, which otherwise records call events in the order in which they occur in real-time without saving the data.

Status windows – The status windows in the VT100 interface provide information about what is currently happening in the MAX TNT. For example, one status window displays up to 31 of the most recent system events that have occurred since the MAX TNT was powered up, and another displays statistics about the currently active session. You can also perform DO commands, for example, clear an active connection, using the status windows.

Interaction with syslog for ASCII log files – If a Windows or UNIX host on the local network is running the Syslog daemon, you can configure the MAX TNT to write log messages to an ASCII file on that host.

SNMP Management

The MAX TNT completely supports the SNMP management standard for all its management functions; every command that you can manipulate via the Telnet interface can also be managed via SNMP commands. By implementing standard and enterprise SNMP MIBs within the MAX TNT, Ascend provides the ability to manage MAX TNTs along with your other SNMP devices from a central generic SNMP management platform (for example NavisAccess by Ascend, SUN Microsystem’s SunNet Manager, Cabletron’s Spectrum, or HP OpenView).

MAX TNT systems support SNMP MIB II, the T1 MIB, and the Ascend Enterprise MIB. Ascend’s SNMP implementation also supports SNMP traps, allowing MAX TNT units to send alarms, call detail reporting, and other management information directly to an SNMP management station without being polled.

Ascend’s SNMP management feature allows true integration of MAX TNT units into the ISP internetwork, by providing the means to manage the Ascend equipment as easily as any other bridge, router, or other SNMP-managed equipment on the network.

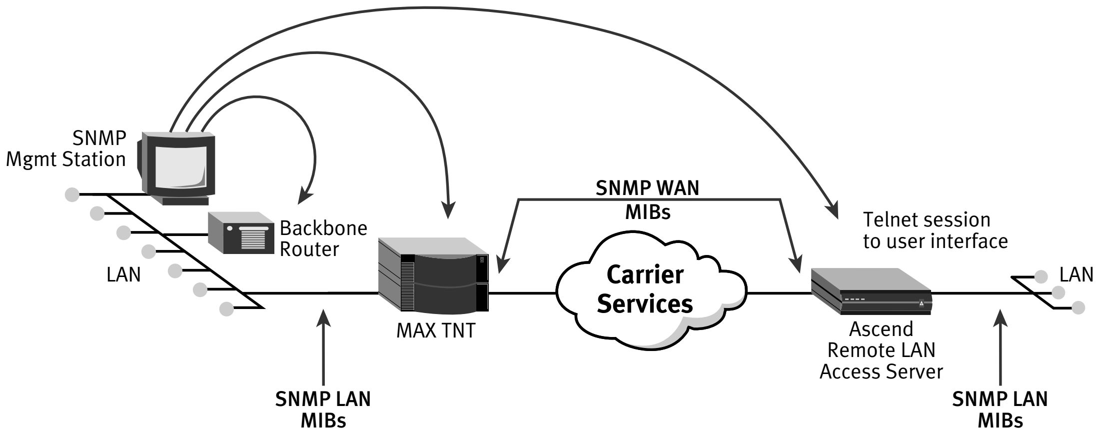

Figure 28 – SNMP management

TCP/Telnet Management

Ascend MAX TNTs can be remotely managed by establishing a Telnet session to the remote unit from any Telnet workstation on the network and viewing the MAX TNT user interface on a Telnet VT100 window. A network administrator at a management station connected to the Internet (or LAN) can use this feature to manage the MAX TNT from a local or remote computer. You can also use it to manage remote Ascend units, such as Pipeline routers, at a remote office or home office. From a Telnet session you can perform all of the configuration, diagnostic, management, and other functions that could be performed from a computer directly connected to the MAX TNT or Pipeline Control port.

FLASH Memory/Remote Software Upgrades

All Ascend MAX TNTs are based on FLASH EEPROM technology. The FLASH EEPROM provides the ability to perform software upgrades in the field without opening the unit or changing memory chips.

All MAX TNTs may be upgraded through the serial control port of the unit. This can be performed locally or through the dial-in modem. Note that remote software upgrades cannot be performed over the WAN interface due to the conflict between running the WAN and reprogramming the software.

Annex D Frame Relay Link Monitoring

The Ascend MAX TNT supports the Frame Relay ANSI Annex D link management specification (RFC 1490) for status monitoring of Frame Relay links. Specifically supported is the specification for ANSI T1.617/Annex D (and the corresponding CCITT Q.933/Annex A) for Local Management Interface as well as LEI Revision 1. This feature helps network managers understand the detailed performance and usage characteristics of a company's Frame Relay network.

From the viewpoint of the MAX TNT, a Frame Relay switch is an endpoint for all DLCIs (Data Link Connection Indicators) connecting to it. A DLCI identifies a Connection Profile as a logical link. The Frame Relay switch connects the endpoints of the DLCIs to each other to make a virtual permanent circuit to which users can connect. The circuit acts like a wire between two endpoints with a fixed maximum bandwidth (though this may be flexible in the case of the Frame Relay link).

Annex D specifies the link management protocol used between the MAX TNT and the Frame Relay switch to which the MAX TNT Frame Relay circuit is terminated. The Annex D standard specifies the procedures for user-network signaling for ISDN support of Frame Relay calls. You can display LMI (Link Management Information) for each link activated by a Frame Relay switch. (Please refer to the Annex D specification for a full definition of each of the fields reported.)

Call Detail Reporting

ISPs and Corporate MIS departments frequently need detailed information on usage of their WAN networks. Most ISP subscribers use dial-up services to access the Internet, and the ISP requires detailed information about bandwidth usage patterns for billing and planning purposes. Corporate MIS departments frequently need very similar information for allocation of expenses to the departments and users that are dialing in. Because users are frequently billed by the network carrier for bandwidth on an as-used basis, information that helps ISPs and MIS departments understand and manage their bandwidth usage is invaluable. Additionally, since inverse multiplexing sessions are made up of multiple individual connections, each of which is billed independently by the carrier, some means of understanding the cost of each inverse multiplexed session is required.

Ascend's Call Detail Reporting (CDR) feature provides a database of information about each network event. For each call, the date, time, duration, called number, calling number, call direction, service type, and associated inverse multiplexing session and port are provided.

This information can then be manipulated to create a wide range of different reports, including individual call costs (to be compared to carrier's billing data), inverse multiplexer-based WAN session costs, costs on an application-by-application basis, bandwidth usage patterns over specified time periods, and so on. Such information can be used to better understand bandwidth usage and, if necessary, make adjustments to the ratio of switched to dedicated bandwidth between network sites. Even more call reporting detail features are available with the Ascend Access Control™ RADIUS server software which provides an interface to ODBC compliant databases.

The MAX TNT includes the ability to specify a usage cap over a specified time period. This helps preclude unexpectedly large monthly bills.

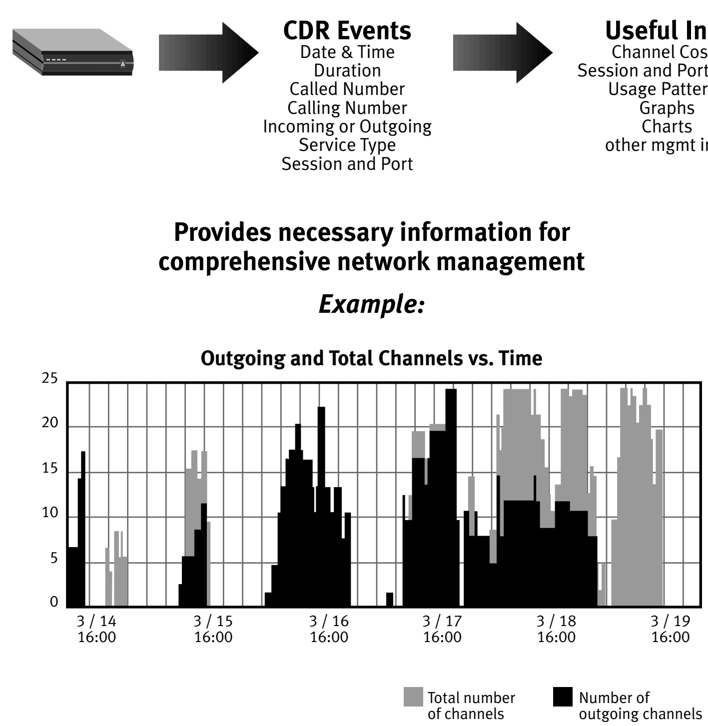

Figure 29 – CDR provides the information you need to manage your bandwidth expenses.

7. MAX TNT Dial-up Security

The MAX TNT provides full WAN security through callback, direct password, and secured password exchange. The security is achieved through a combination of the PPP-based security standards and Ascend WAN security extensions.

PPP provides two levels of authentication security: Password Authentication Protocol (PAP) and Challenge-Handshake Authentication Protocol (CHAP). Both of these are supported by the MAX TNT.

PAP: Password Authentication Protocol

PAP provides a simple method for a peer to establish its identity in a 2-way handshake. This is done only upon initial link establishment, and “in the clear.” PAP is not a particularly strong authentication method, although it does provide for baseline security when interoperating with non-Ascend equipment, and is frequently enough security for basic Internet access services.

CHAP and MS-CHAP: Challenge-Handshake Authentication Protocol

CHAP is used to periodically verify the identity of a peer using a three-way handshake. This is done upon initial link establishment, and may be repeated anytime after the link has been established.

CHAP is encrypted using a one-way hash function. CHAP provides protection against playback attack through the use of an incrementally changing identifier and a variable challenge value. The use of repeated challenges is intended to limit the time of exposure to any single attack. The MAX TNT controls the frequency and timing of the challenges.

Support for the Microsoft – Challenge Handshake Authentication Protocol (MS-CHAP) format supported by Windows NT systems has also been added to the MAX TNT.

Restricted Address

A MAX TNT may be configured with a list of IP networks and stations that are allowed to dial in. The MAX TNT can be configured to reject incoming calls from any unrecognized network. Restricting network access to the MAX TNT provides a high level of secure control and management of the network and its topology.

Callback Security

Using the restricted address list described above, a MAX TNT can be configured to force a callback to any dial-in MAX TNT. The callback number is registered in the MAX TNT and is associated with the address and name of the dial-in MAX TNT. Callback security provides the highest level of confidence in the control and security of the network and its topology.

Security Servers

As large communities of dial-in sites are built, it becomes impractical to store all relevant security and access parameters in a single piece of equipment. It is instead preferable to set up a host application database that maintains current user lists, passwords, and permissions. This database is then accessed by a MAX TNT when users attempt to connect, on an on-demand as-needed basis. Thus one database serves many potential users and MAX TNT switches, and security management may be more effectively audited and controlled. This one database typically provides all necessary data for user authentication, authorization and accounting.

To make this possible, the MAX TNT systems communicate with the security databases by a real-time protocol, specifically RADIUS, TACACS or TACACS+.

RADIUS Security Servers

Remote Access Dial In User Server (RADIUS) is a more robust protocol that can provide greater flexibility than TACACS. In a RADIUS query, the MAX TNT systems provide the user ID and password to the server, and in return receive a complete profile, which supplies routing, packet filtering, destination specific static routes, and usage restrictions specific to that user (see Figure 20).

In addition to providing the configuration and filters for incoming calls, the MAX TNT can use the same data in the RADIUS database to create and advertise static routes and to place outbound calls based on the routing information in the RADIUS database.

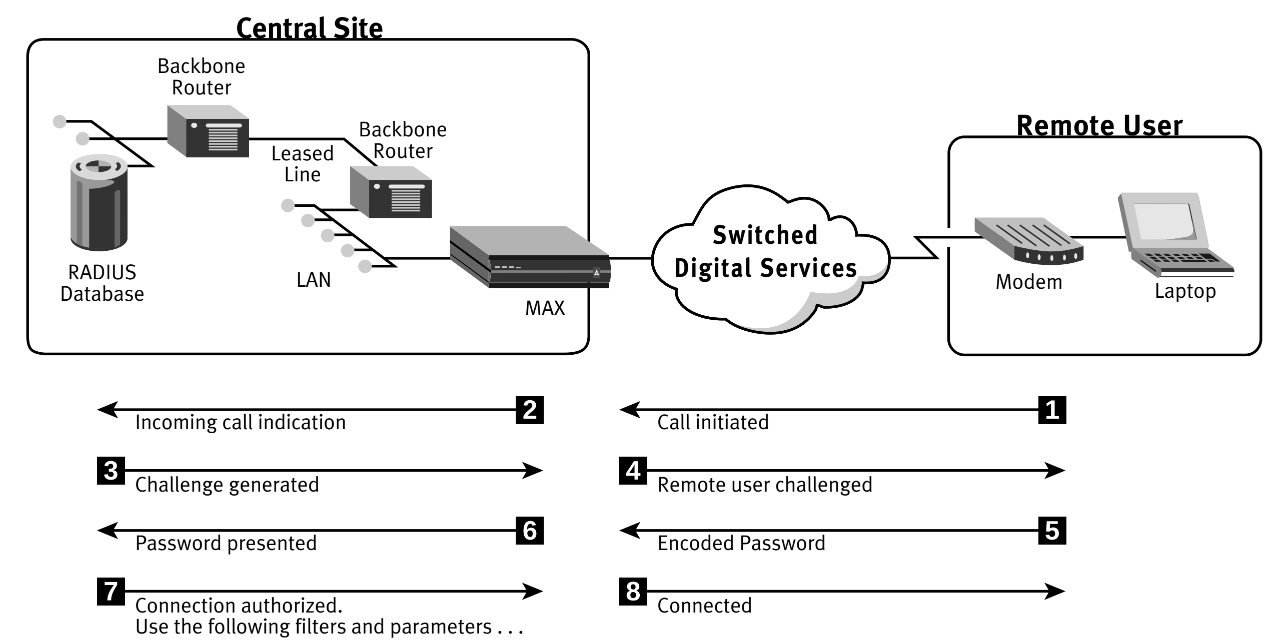

Figure 30 – A RADIUS access query.

Access Control RADIUS Security Servers

Ascend Access Control™ is a comprehensive network-wide security, authorization and accounting management system (sold as a software product that is independent from the MAX TNT). Using Ascend Access Control administrators can identify legitimate callers, perform authentication and authorization, monitor access to network resources and compile extensive billing and accounting details. Ascend Access Control works with any RADIUS-compliant network access server such as MAX TNT, and it supports all of the popular protocols, authentication methods, token cards and database servers. Additionally, Access control fully supports ODBC databases for support of call profiles and CDRs allowing you to have maintain a single database for all your core record keeping and thereby simplifying customer/user management and billing.

Ascend Access Control is also the ideal solution for handling the dial-up traffic on Virtual Private Networks (VPNs) offered by ISPs or corporate Intranets. Administrators can supervise the network activities of thousands of remote callers using Access Control Manager-a Java-based application with a point-and-click interface. When used in conjunction with Ascend's Secure Access™ products, Ascend Access Control delivers a robust, single-vendor solution for protecting the entire network. For more information on Ascend Access Control see the Ascend Access Control data sheet. Ascend Access Control is available for a variety of platforms including UNIX variations and NT.

TACACS and TACACS+ Security Servers

Terminal Access Concentrator Access Control Server (TACACS) is a very simple query/response protocol that allows MAX TNT systems to check a user's password and either enable or prevent access based upon that check. TACACS servers will only support basic password exchanges used in the PPP PAP protocol. They do not support CHAP. Additionally, TACACS+ authentication, authorization, and accounting is supported on all Ascend platforms that currently support RADIUS accounting. TACACS+ is a server from Cisco Systems, Inc.

Multi-level User-access Password Security

The MAX TNT provides multi-level password security to allow different levels of access to different users. Access security for MAX TNT is defined by what are called "Security Profiles". Security Profiles are the means by which access to crucial MAX TNT operations is limited, while leaving other less critical operations more broadly available.

Calling Line ID (CLID)

The Calling-line ID (CLID) feature applies only to ISDN and allows you to authenticate incoming calls by checking the calling-party's phone number. Because the caller's phone number is included in the information sent over the D-channel as part of a call initiation, the MAX TNT can perform CLID authentication before answering an incoming call. The calling party's phone number must match the Calling # parameter (or the equivalent value in a RADIUS entry). If the device cannot authenticate the call when CLID authentication is required, the call is rejected.

Expect Callback

Expected Callback, also called D-channel callback, is when an MAX TNT initiates an ISDN call and the call is identified on the receiving end by CLID information passed over the D-channel, but the call is rejected by the receiving end. The called machine on the client side then immediately initiates a call back to the original caller (callback). To the MAX TNT (the initiating side), it appears as if the first call never got through at all. This feature can be useful in providing on-demand web access services to customers who want to host their web servers at their corporate site, yet do not want to pay for a full-time communications link with the ISP due to low traffic demands. In this manner the telecommunications charges are still incurred by the corporate customer and bill-backs for telephone connect services do not have to take place.

PPP Callback

You can specify that the MAX TNT call back any user dialing into it. The callback number is registered in the MAX TNT and is associated with the address and name of the dial-in MAX TNT. Callback security provides the highest level of confidence in the control and security of the network and its topology.

Encrypted Token Card

The MAX TNT supports hand-held personal security cards, such as those provided by Security Dynamics and Secure Computing's Enigma Logic division. These cards have dynamic passwords that provide a higher level of security than traditional static password methods. Support for dynamic passwords requires the use of a RADIUS server that has access to an authentication server, such as an Security Dynamics ACE or Enigma Logic SafeWord AS authentication server.

Logging

The MAX TNT supports two important tools for logging information on the activity of your MAX TNT to help monitor and ensure high levels of security; Syslog and RADIUS.

Syslog is an IP protocol that sends system status messages to a host computer, known as the syslog host. This host is specified by the Log Host parameter in the Ethernet Profile. The log host saves the system status messages in a syslog file. These messages are derived from two sources-the Message Log display and the CDR display. See the UNIX man pages on logger(1), syslog(3), syslog.conf(5), and syslogd(8) for details on the syslog daemon.

The MAX TNT can be configured to send detailed warning, notice, and CDR records from the system logs to the Syslog host. CDR is a feature that provides a database of information about each call, including date, time, duration, called number, calling number, call direction, service type, and associated inverse multiplexing session and port. Alarms and detailed access information can therefore be tracked to monitor any potential breach of security.

RADIUS servers, as mentioned above, are powerful authentication, authorization and accounting databases that can also log detailed information to enhance your understanding of any efforts to breach your network's security. MAX TNT supports both the public domain version of RADIUS which is available from the Ascend FTP server, as well as the sophisticated Ascend Access Control RADIUS server that is sold by Ascend. Detailed information on both these servers is available on the Ascend web site.

Telnet Password Verification Failure Trap

This feature adds the IP address of the Telnet client to the existing security violation message indicating the maximum number of Telnet login attempts to a MAX TNT has been exceeded.

Static Packet Filtering

The MAX TNT provides standard packet filtering mechanisms that enables you to set up basic levels of security in your dial-up networking environment. You can define filters that will exclude certain packets from reaching your network or from going out to the WAN.

Each filter consists of an ordered list of conditions based on either IP-specific or protocol-independent information. For an IP filter, you can filter data based on addresses, protocols, port numbers, and other packet conditions. For a generic filter, you can specify data values within packets.

Properly incorporating and using filtering provides security within a dial-up internetworking environment. The filtering within the MAX TNT allows for independent filters on a per-interface and per-connection for:

- Call establishment
- Call clearing (idle timer filter)
- Transmit data
- Receive data

Each filter associated with an interface consists of an ordered list of allow/deny parameters based on IP-specific or protocol-independent parameters. For IP specific filters, any combination of:

- Source/destination address
- Protocol discriminator
- Source/destination port
- Established/Not Established TCP sessions

For protocol independent filters, any combination of data comparisons and masks may be used to allow/deny packet traffic.

Dynamic Firewall – Secure Access

Ascend Secure Access Firewall is a software option that provides firewall security protection to ISP networks, corporate LANs, remote offices, and telecommuters. Secure Access Firewall offers a fully integrated, single-vendor dynamic firewall solution that cost-effectively protects a company's entire network against intruders, as shown in Figure 31.

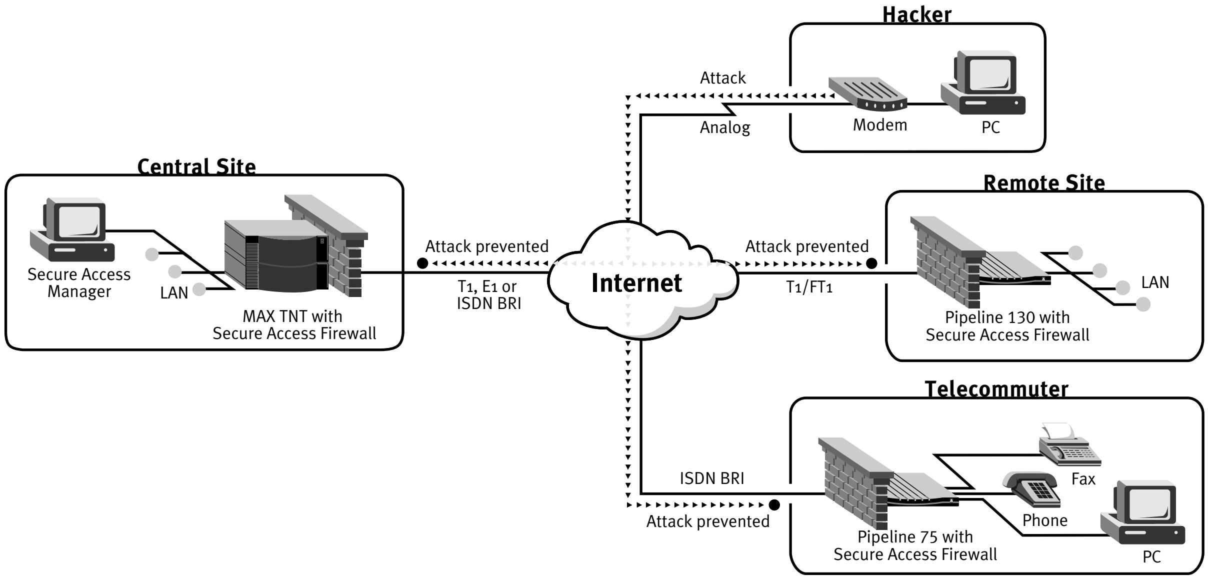

Figure 31 – Secure Access Firewall protects networks from unauthorized access by public network users.

Although companies are obligated to protect their network from unauthorized access, many companies are unable or unwilling to assume the responsibility of maintaining a firewall. In the past, firewalls have been expensive and often hard to configure or maintain. This creates opportunities for ISPs to attract and maintain large corporate clients. ISPs can provide a value-added service to their corporate clients by installing and maintaining their firewalls for them.

With Secure Access Firewall, the firewall and router are integrated into the MAX TNT and Pipeline product families. Other firewall solutions require a standalone hardware and software network appliance that connects to a router on one side and a corporate LAN on another. Because Secure Access Firewall resides on the same device that provides remote access, this scalable solution is less costly and easier to manage than other vendors' products.

The Windows-based Secure Access Manager lets the ISP manage remote firewall agents from a central site, which eliminates the need for separate management workstations. Centralized control also reduces ongoing operating expenses by simplifying security management. Security administrators simply point-and-click to configure Secure Access Firewall for authorizing traffic.

Secure Access Firewall is dynamic, which means incoming traffic can be screened by network address, host name, application, protocol, source and destination port, and TCP header bits. Ports can opened and closed based on triggered events in transmitted packets. For example, with static packet filtering, when an FTP session request is received, many ports are opened in anticipation of the request. This makes the server vulnerable to attack by an intruder. With the dynamic firewall technology dynamic packet filtering (only dynamic firewall technology) used by Secure Access Firewall, however, the request triggers a dynamic rule change so that only one port is opened and packets are filtered so they are recognizably part of the correct data stream.

In addition, Secure Access Firewall provides comprehensive monitoring and logging capabilities, including:

- Customizable reporting of activities
- Audit trail on would-be intruders
- Centralized reporting of firewall activity

Secure Access Firewall is also appropriate for intranet use. By configuring the Secure Access Firewall to permit access only for authorized remote users and only for specific applications, an intranet can be extended through the Internet to include remote offices.

Dynamic Firewall Technology

Secure Access Firewall uses a dynamic firewall technology. This means that incoming traffic can be screened by:

- Network address
- Host name
- Application, such as TFTP, FTP, WWW, SMTP, POP Mail, SATAN probe, Source Routing, Anti-Spoofing IP Spoofing, Telnet, nntp, Talk/Chat (IRC, Talk, Ntalk), archie, finger, whois, etc.
- Protocol, including UDP, TCP, and ICMP
- Source and destination port
- Direction, including send and receive
- TCP session state, such as start, acknowledgment, reset, establish, and end

Ports can opened and closed based on triggered events in transmitted packets. For example, with static packet filtering, when an FTP session request is received, many ports are opened in anticipation of the request because the servers negotiate the data port separately, without knowledge of the router. Static packet filtering does not contain the intelligence to selectively open and close ports; it can either open all the high-numbered ports (1024-65535) or close all the ports. This makes the server vulnerable to attack by a knowledgeable intruder.

With the dynamic packet filtering used by Secure Access Firewall, however, the request triggers a dynamic rule change so that only one port is opened and packets are filtered so they are recognizably part of the correct data stream. It dynamically adapts to traffic. When a legitimate session is initiated, dynamic packet filtering monitors requests to open ports between the two computers. It opens only those ports and keeps other ports closed. When the session ends, it immediately closes the ports. No security holes are left for intruders to enter.

Virtual Private Networks, Tunneling and Mobile Nodes

The MAX TNT's extensive protocol support and Access Control RADIUS software allow ISPs to offer businesses a multi-protocol Virtual Private Network (VPN) over the Internet by using tunneling protocols such as Point to Point Tunneling Protocol (PPTP) and Ascend Tunnel Management Protocol (ATMP). VPNs use these secure tunneling protocols and the Internet to replace expensive leased lines and Frame Relay networks that companies have traditionally used to interconnect branch offices and corporate sites.

These VPNs enable corporate clients to reduce long-distance charges, to eliminate mesh networks, and to outsource the management and security responsibilities of maintaining private WANs. Through the use of VPNs companies can achieve savings up to 60% over traditional private networks and because of these efficiencies VPNs are expected to be a major profit opportunity for ISPs/NSPs over the coming years. To take advantage of the this market for VPNs, ISPs must select POP equipment and RADIUS servers that support tunneling, as well as authentication and encryption.

Ascend provides the following features for secure VPNs:

- PPTP and ATMP tunneling are available today, and Ascend is committed to supporting L2TP (Layer-2 Tunneling Protocol) soon after the standard is finalized.
- Access Control's Extended RADIUS capabilities for support of Proxy RADIUS, and necessary tunneling protocols
- Remotely manageable perimeter firewall security

In addition to the basic technologies necessary to implement VPNs, Ascend has integrated a number of important performance enhancements that provide maximized bandwidth utilization. These enhancements include:

- IP Multicast support for multi-point data broadcast applications
- Frame Relay Direct to channel tunnels through virtual circuits in the ISP/NSP's Frame Relay backbone, rather than route traffic unnecessarily as IP packets.
- CPE (such as the Pipeline 130 series) with integral PSTN-based dial backup and overflow provisions.
- ISDN bandwidth-on-demand with the Multilink Protocol (MP) and the Multilink Protocol Plus (MP+)

Tunneling encapsulates IP, IPX, AppleTalk, NetBIOS, and NetBEUI packets within IP packets for transmission over the Internet. At the receiving end, the encapsulation is removed, leaving the original packets intact. This process is automatic and transparent to users. As shown in Figure 32, tunneling ensures the privacy of data packets while they traverse a public network.

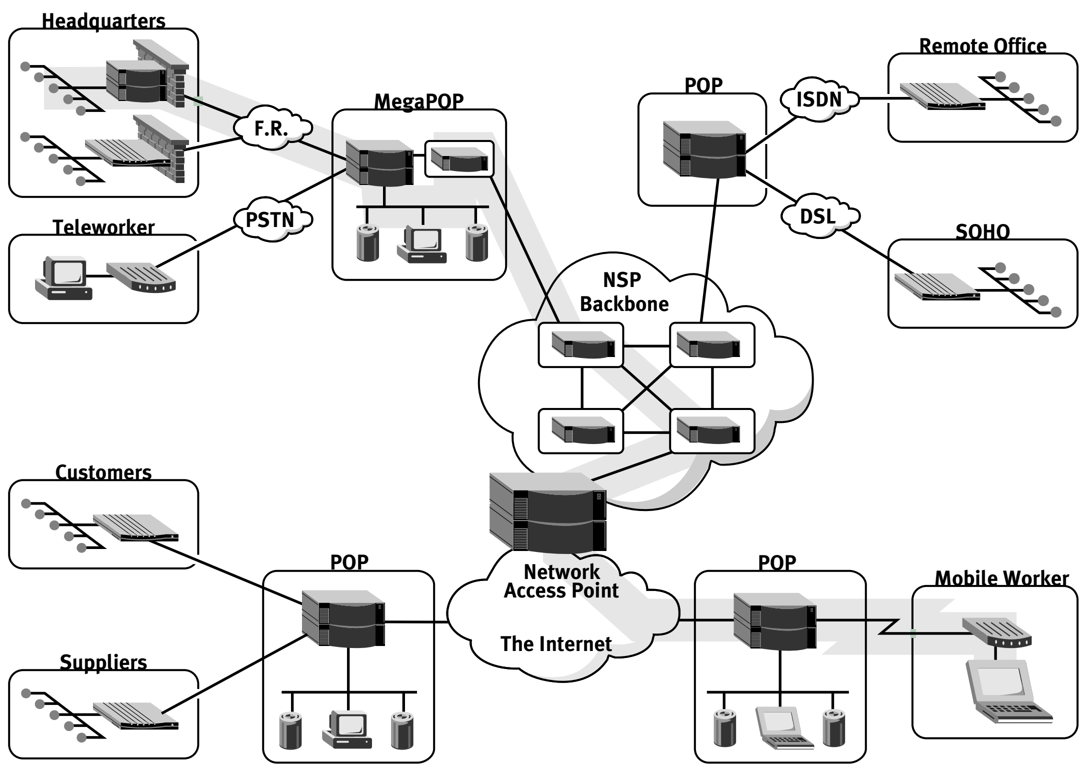

Figure 32 – Tunneling keeps data private on a public network.

Ascend uses its own ATMP for tunneling from one MAX TNT or Pipeline to another within the ISP site. This protocol dynamically manages Generic Routing Encapsulation (GRE) protocol tunnels over the Internet. ATMP has the ability to route Novell IPX and private IP packets over the Internet. Some advantages of ATMP over other tunnel protocols include:

- Multi-protocol support (IP, IPX, and AppleTalk)
- No special client software required on the mobile node
- Simple to use
- Uses the standard GRE protocol (RFC 1701)

ATMP is a UDP/IP-based protocol that provides a cross-Internet tunneling mechanism using standard GRE between two Ascend units. The Ascend units can be from the MAX TNT or Pipeline product families.

ATMP tunneling enables mobile nodes to connect to the home network. The node can move from one network or subnetwork to another and might not maintain the same node address. The secure “tunnel” has a MAX TNT unit at each end. The mobile user connects to a remote MAX TNT through a PPP session. At the other end of the tunnel is an MAX TNT assigned to the home network. Each MAX TNT tracks the location information of the mobile node and encapsulates packets for transmission to and from the node. The MAX TNT at the home network can either route packets it receives from the remote MAX TNT or forward the packet to a pre-determined WAN connection, called router mode and gateway mode, respectively. (See Figure 33.) To ensure the proper security, a RADIUS database server must be present. The home MAX TNT requires password authentication through the Message Digest (MD5) algorithm before it accepts a tunnel connection.

ATMP tunnels enable a mobile node to access a home network through two Ascend devices – a foreign agent and a home agent – across the Internet. Typically the mobile node is a dial-in user. If the home network is an IP network ATMP can also enable LAN-to-LAN connectivity through the tunnel.

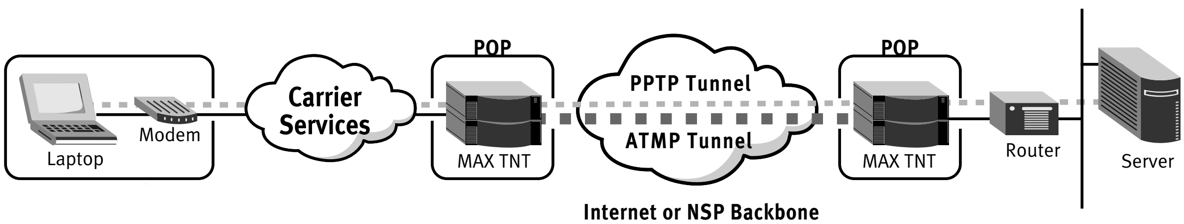

Figure 33 – Tunnels originate and terminate in different places, depending on the location of the home and foreign agents. This example demonstrates POP-to-POP tunneling with ATMP, and client -to-server tunneling.

Ascend also supports the Point-to-Point Tunneling Protocol (PPTP), which was developed by Microsoft and Ascend and is available with the Microsoft NT RAS 4.0 operating system. PPTP requires that a Windows NT server be present as the termination point of the tunnel on the customer's LAN. By contrast, ATMP is platform-independent and lets the originating caller engage in a session with any TCP/IP or IPX server. PPTP can route IP, IPX, NetBIOS, and NetBEUI packets.

Authentication and Encryption

Robust and comprehensive authentication support is important to ISPs and corporations because it helps prevent unauthorized network access. The MAX TNT supports RADIUS, TACACS and TACACS+ protocols that are used for authentication.

Encryption is also important to ISPs because it enhances the security of your own network, and allows ISPs to target the corporate market with new services that meet corporate needs for security. Ascend currently supports password encryption using the Ascend Access Control RADIUS software. Ascend will also implement the IPSec encryption standard to provide packet-level security.

Ascend's Access Control RADIUS software application is the industry's most complete authentication, accounting and access control application available. For more information on this product please refer directly to the related product literature.

8. MAX TNT Diagnostics

Power-on Self-tests

When turned on, the MAX TNT runs a complete set of diagnostic tests. If a problem is observed, it will notify the user through the terminal interface or alternatively by blinking an error code using its front panel LEDs.

Continuous Statistics Collection

The MAX TNT collects statistics concerning connections: number of transmitted and received packets, error conditions, and so on. These statistics are kept in memory, available for retrieval from a local or remote management station.

ISDN Event Log

The MAX TNT keeps track of events that occur on the ISDN access line. A log is kept of events such as incoming call, link down, link up, outgoing call failure, and so on. These events can be forwarded to a central collection point for later analysis. The most recent 15 or 20 events are kept in MAX TNT memory for review.

Loopback

For diagnosing problems with a wide-area connection, loopback facilities are invaluable. The Ascend MAX TNT allows a call to be placed to itself over the WAN, and to send a user-determined number of packets over the connection. This tests the MAX TNT's ability to send and receive calls, as well as the digital access line, and the WAN.

PPP Link Quality Monitoring (LQM)

The MAX TNT implements standard PPP LQM to monitor the quality of the link and take action if the link is not of sufficient quality to allow adequate throughput. LQM counts the number of packets sent across the link and periodically asks the far end how many packets have been received. Discrepancies are evidence of packet loss, indicating link quality problems. The MAX TNT can tear down and reestablish a call if the threshold exceeds a user settable limit.

Modem Monitoring

The lanModemGroup in the Ascend Enterprise MIB is a feature/ MIB extension that allows you to monitor the digital modem usage for analog calls on individual modems either directly via the Ascend console or from any generic SNMP management station. Detailed information is available on the location and ID of the modems, the number of accepted and placed calls, the number of times the modem has been used in a given period, and any failures that have occurred with the modem. This feature is valuable when troubleshooting a user's connection when he or she is having connection problems, and can help in identification of the particular problem area.

Digital Modem Quiescence

A debug monitor command lets you gracefully disable digital modems in the MAX TNT, without disrupting existing connections. This is accomplished by making all channels that are not active busy; as calls are cleared, individual channels are also made busy. Another command brings the modems back into service. This feature enables you to quietly take modems out of service for maintenance without affecting users. If all modems are on the disabled list, incoming callers receive a busy signal until the modems have been restored for service.

9. Bandwidth Management

The MAX TNT offers a number of features that make it easier for ISPs to manage bandwidth.

Multicarrier Gateway for Carrier Diversity

For increased reliability and lower bandwidth costs, ISPs may choose more than a single carrier for their data networks. For reliability purposes, if one carrier's facilities suffer an outage, data can be routed over an alternate carrier's facilities until the faulty facilities are restored. For cost saving purposes, data can be routed over whichever carrier offers the least cost transmission path. Furthermore, for international purposes, some carriers offer service to countries not served by other carriers, and it is advantageous to be able to select a carrier's facilities on a call-by-call basis depending on the destination country.

Ascend's Multicarrier Gateway feature allows a single MAX TNT unit to connect to multiple carriers and route data traffic over selected facilities. The selection may be made by a specified dial plan, list, or prioritized alternate paths chosen based on availability and time of day.

For example, a system administrator may set up an MAX TNT to place a call over AT&T by first dialing 9, or MCI by first dialing 8, or Sprint by first dialing 7. On the other hand, the selection of carrier may by made transparently to the caller, based upon which carrier offers a path to the destination at the lowest cost for that time of day. Of course, if one network should fail or be congested, the MAX TNT can choose to place the call using an alternate carrier, based upon a predetermined priority list. For support of Multicarrier Gateway features outside of the U.S., consult your Ascend representative.

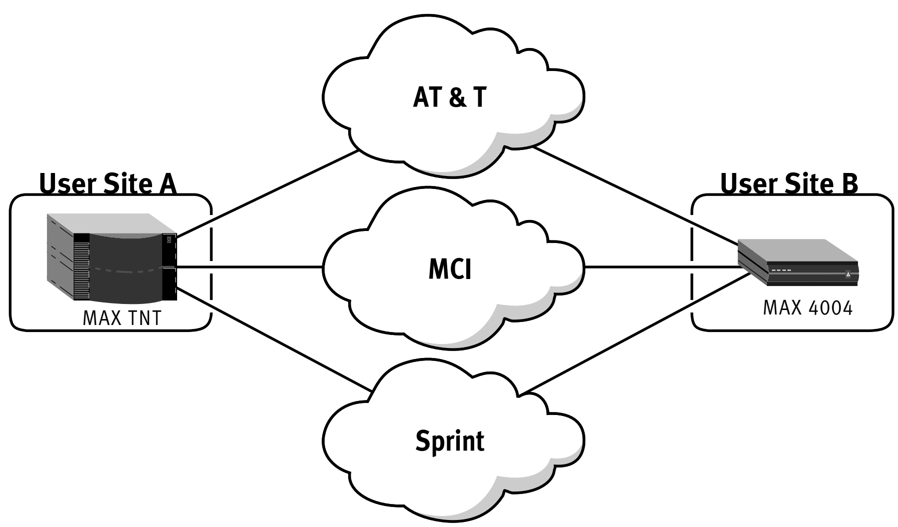

Figure 34 – Multicarrier gateway

NFAS

Non-Facility Associated Signaling (NFAS) enables the D-channel on one PRI interface to control the B-channels on another PRI interface that does not have a D-channel. This means that all 24 channels of bandwidth on the second (and third and fourth) PRI interface can be utilized for B-channel data communications. If implemented, it is important that more than a single D-channel be available to service connections to avoid a single point of failure.

With MAX TNT T1/PRI expansion module you can have up to 8 PRI lines. Each T1 interface has 24 B-channels and a D-channel. Utilizing NFAS signaling a single D-channel can service all the 8 PRI lines.

Each MAX TNT DS3 expansion module supports up to 28 T1/PRI circuits. However the NFAS standard limits single D-channel signaling support to 20 PRI circuits.

10. Terminal Server

A traditional terminal server allows asynchronous terminals or personal computers emulating asynchronous terminals to have VT100 or equivalent access to hosts on a network through an RS-232 interface. With the addition of modems at the terminal server and at the personal computer, dial-up terminal access is provided. Through the use of optional digital modems, the MAX TNT supports asynchronous terminal users at raw data rates up to 115 Kbps, with compression for even greater throughput.

The MAX TNT supports all the common capabilities of standard terminal servers, including Telnet, Domain Name Services (DNS), login and password control, call detail reporting and authentication services. A local terminal server session takes place when a terminal (or a computer emulating a terminal) is connected to the MAX TNT unit's Control port, or when you open a Telnet connection to the MAX TNT from an IP host on the local network. Remote terminal server sessions take place through a digital modem or through a V.110 or V.120 connection to the MAX TNT.

An incoming terminal server connection can be directed in several ways. The remote user can be allowed access to the command-line interface, from which the user can contact hosts on the local network via PPP, SLIP, TCP, Rlogin, or Telnet sessions. Or, the login can be directed immediately to a local host via Telnet, TCP, or Rlogin.

Enhanced Dial-up Networking through Terminal Servers

Newer PC software allows personal computers to gain access to more than just simple terminal services on the network. This software provides a full PPP or SLIP implementation and includes applications software for electronic mail, file and database sharing, as well as most other services available locally on a network. Such PC software is compatible with standards-based V.32bis modems, including compression and error control with V.42/V.42bis.

A traditional terminal server with only asynchronous terminal support doesn't provide the services required for proper operation of such PC software. A terminal server must not only support a full range of control mechanisms, but must also support asynchronous PPP, SLIP, C-SLIP, dynamic IP addressing, and single node host routing.

The MAX TNT combines the capabilities of a terminal server with a wide range of digital dial-up internetworking features, and therefore supports all of the requirements of the latest PC software applications.

Appendix One: WAN Services and Standards Compatibility

WAN Carrier Services

WAN carrier services are offered by the Interexchange Carriers (IXCs), such as AT&T, MCI, and Sprint and the Local Exchange Carriers (LECs). Not all services are offered by all carriers. Check to determine which services are offered by your local carrier.

The Ascend MAX TNT is fully certified to operate over all the following available services:

Switched 56

Switched 56 is the most commonly-used North American switched digital service. It is also available in some European and Pacific Rim locations for purposes of North American compatibility. Switched 56 services use the 64 Kbps architecture of the network for transport, but allocates one bit out of every 8 for signaling purposes. This is known as in-band signaling, or “robbed-bit” signaling. Switched 56 is the “highest common denominator” service because virtually all types of access lines can connect to it.

Switched 64

Switched 64 is universally available in Europe and the Pacific Rim, and becoming more available in North America. It’s similar to Switched 56 except that it uses all 8 bits of each octet for data, since its signaling information is sent along an independent path. This is called out-of-band signaling. To access Switched 64 service, you must use either an ISDN BRI or ISDN PRI line, because these access lines have an out-of-band signaling channel, known as the D-channel.

Switched 384

Switched 384 (also known as ISDN Ho) is currently available in North America and Japan. This service takes six 64 Kbps network channels and provides them to the user as a single 384 Kbps call. You must use an ISDN PRI line to access Switched 384.

Switched 1536

Switched 1536 (also known as ISDN H11) is also currently available in North America and Japan. This service takes 24 64 Kbps network channels and provides them to the user as a single 1536 Kbps call. Two ISDN PRI lines must be used to access Switched 1536. One line carries the full 1536 Kbps data stream, and the other line contains the signaling D-channel (and excess bandwidth for other uses).

Switched Nx64 (ISDN Multirate)

Switched Nx64 (also known as ISDN Multirate) has been approved by standards bodies and has been rolled out by selected carriers. It allows end users to specify the bandwidth of a call to be any 64 Kbps multiple. For example, a user can dial a first call at 384 Kbps (6 x 64 Kbps), and later dial a second call at 512 Kbps (8 x 64 Kbps). An ISDN PRI line is required to access ISDN Multirate.

Frame Relay Service

Frame Relay is an HDLC-based packet protocol that allows data to be sent to its destination through Frame Relay switches that reside within either a private network or a public carrier’s network. Typically, access to Frame Relay service is obtained over dedicated synchronous circuits between the user location and the central office or POP. A virtual point-to-point connection is established between connection end points, called a Permanent Virtual Circuit (PVC). Multiple PVCs, connecting to multiple locations, can be run over a single access line.

Frame Relay can be run over synchronous dialup circuits (such as ISDN) as well as dedicated circuits, but requires that the network service provider allows for such dialup connections. To date, most Frame Relay providers have not allowed users to establish Switched Virtual Circuits (SVCs).

Frame Relay can be run over most types of transparent synchronous circuits. For telecommuters, this is usually a 56 or 64 Kbps line. For sites with larger bandwidth requirements, this will likely be a T1 access line (1.536 Mbps) or the newer SDSL. Some Frame Relay service providers allow Frame Relay to be run over subrate T1, or fractional T1, circuits. The MAX TNT supports RFC 1490 encapsulation over Frame Relay circuits, as well as PPP and MP+ over Frame Relay.

Optional Frame Relay software integrates incoming Frame Relay traffic from other Frame Relay access devices (such as the Ascend Pipeline 130 family), with analog and digital dial-in traffic. High-speed synchronous V.35 ports on the MAX TNT Serial card supports direct connections to a Frame Relay switch at up to 8 Mbps and even higher speed links are possible with the HSSI module.

The MAX TNT products also route data to multiple Frame Relay PVCs over single or multiple interfaces, and offer:

- Support for up to 4096 PVCs with RADIUS authentication software
- Frame Relay forum UNI and NNI interface support
- Dial-in PPP to Frame Relay gateway function with PVC selectable on a per user basis
- RFC 1490 encapsulation
- ANSI Annex D and ITU Annex A management
- PVC switching
- Dial Access Signaling Interface (DASI)

As a Frame Relay concentrator, the MAX TNT can support a high number of low-speed Frame Relay connections and concentrate them into one or more high-speed connections to a Frame Relay switch using either the serial WAN interface or T1/E1 lines.

Interoperability of Switched Digital Services and Access Lines

A common misconception about digital dial-up services is that there is an inherent lack of interoperability between ISDN and non-ISDN, between T1 access lines and Switched 56 access lines, and so on.

In fact there is full interoperability between all types of digital access lines. To better understand how this is so, it should be understood that digital service access lines are simply that: access lines used to access digital services within the network cloud.

Different types of access lines can access different services (see Figure 35). For example, T1 access lines and Switched 56 access lines can only access Switched 56 service. On the other hand, an ISDN PRI line can access all of the available types of network services, including Switched 56, whereas an ISDN BRI line can access both Switched 56 and Switched 64 services.

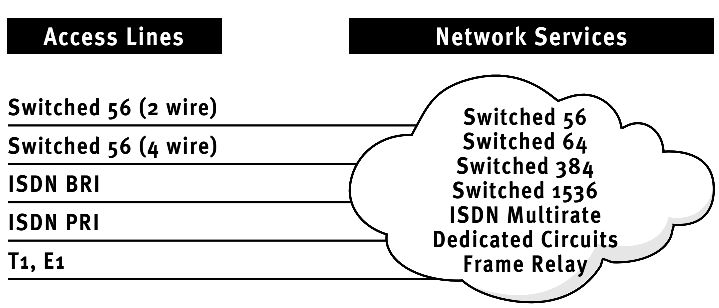

Figure 35 – Access lines provide access to network services.

Therefore, by using Switched 56 service as a common denominator, all types of access lines can interoperate at either 56 Kbps or, using inverse multiplexing, at an integral multiple of 56 Kbps, or Nx56 (see Figure 36).

Access	SW56	ISDN BRI	T1	ISDN PRI
SW 56	56	56	56	56
ISDN BRI	56	56, 64	56	56, 64
T1	56	56	56	56
ISDN PRI	56	56, 64	56	56, 64, 384, 1536, Multirate

Figure 36 – By using switched 56, ISDN interoperated with non-ISDN.

Ascend MAX TNT systems are available with all types of access line interfaces, to allow interoperability between all sites, regardless of what type of access line is available.

Interoperability of Leased and Dialed Services

A single access line can be used to connect to a combination of leased, Frame Relay, and dialed services (see Figure 37). A T1 access line contains 24 individual 56 Kbps channels, and an ISDN PRI access line contains 23 individual 64 Kbps channels. These lines can be provisioned so that some of the channels support leased point-to-point connections (routed directly to the other end point or to a Frame Relay switching node within a private or public network), while others support dialed (switched) connections.

Note: For information about capabilities offered by carriers outside of North America, consult your local Ascend representative.

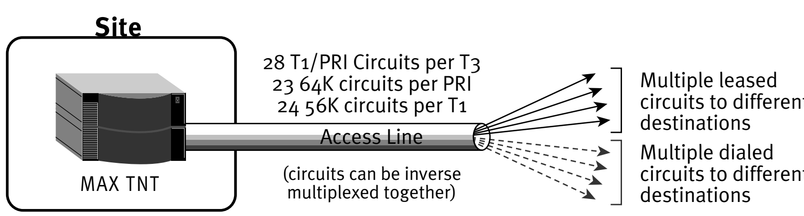

Figure 37 – Multiple leased and dialed circuits can be carried over a single access line.

Ascend MAX TNT systems can create connections using leased or switched (dialed) circuits, or both. Access line costs are kept to a minimum because separate access devices and lines are not required for leased and switched circuits and because of the economies of buying higher speed circuits instead of large numbers of lower speed circuits (e.g. One T1 line is typically much more cost-effective than 24 analog lines).

In addition, MAX TNT systems can combine both leased and switched circuits as part of the same connection by using inverse multiplexing techniques (see Figure 38). A connection built of leased and dialed circuits can be expanded or contracted in real time by adding or subtracting switched circuits. This allows the bandwidth of connections to be expanded in times of greater bandwidth demand, and reduced as traffic decreases.

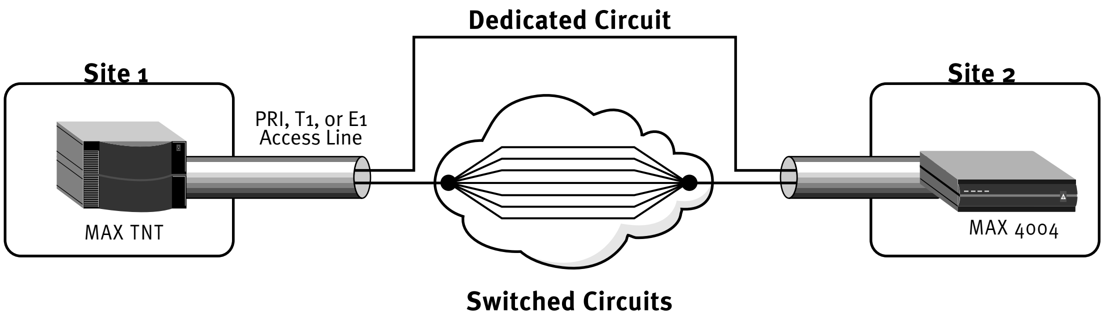

Figure 38 – Leased and dialed circuits combined using inverse multiplexing

Inverse Multiplexing

There are two types of inverse multiplexing: packet-level and circuit-level (also called bit-level). An inverse multiplexer allows the packets or bits being transferred on individually dialed channels across a network to be combined into a single, higher-speed data stream. For example, one site might have three ISDN BRI lines connected to an inverse multiplexer (or "mux"). Another site might have a T1 access line connected to an inverse multiplexer. The user at the first site can place a 336 Kbps call to the second site using inverse multiplexing. Because each BRI line has two 64 Kbps channels, six individual calls are placed by the inverse multiplexer over switched 56 service to the answering T1-based inverse multiplexer. The two inverse muxes combine the six independent calls into a single data stream, and the two sites are now communicating at 336 Kbps (6 x 56).

For most internetworking applications, MAX TNT systems use packet-level inverse multiplexing, using the MP, MP+ and BACP (Bandwidth Allocation Control Protocol) protocols.

Packet-level Inverse Multiplexing

This type of inverse multiplexing performs the inverse multiplexing function at the packet level; that is, one data packet is sent out over the first circuit, the next data packet is sent out over the second circuit, the next data packet is sent out over the third circuit, and so forth, spreading the data packets out over the available circuits. At the receiving end, the data packets are received, adjusted for network-induced delay, and reassembled in their proper order. This inverse multiplexing technique is often referred to as load balancing, and is the method of inverse multiplexing used with internetworking applications.

Multilink Protocol (MP)

MP stands for Multilink Protocol (also referred to as Multilink PPP) and is a standard for inverse-multiplexing multiple dialup channels to form a single aggregate session. MP is an extension to PPP supporting ordering of the payload (but with no error control) across multiple channels. MP is based on RFC 1717.

Multilink Protocol Plus (MP+)

MP+ stands for Ascend's Multilink Protocol Plus™. MP+ is an extension to MP that supports the inverse multiplexing, session management, and bandwidth management capabilities that are required to support combined leased and switched circuits, backup and overflow capabilities, and wide area network resource and phone number management. MP+ allows up to 30 individual calls or channels to be combined into a single high-speed virtual connection. MP+ consists of two components: a low-level channel identification and error monitoring and recovery mechanism, and a session management level for supporting bandwidth modifications and diagnostics. MP+ allows the addition or removal of dialed channels from a connection in a real-time fashion to create Dynamic Bandwidth Allocation (DBA). MP+ is based on RFC 1934.

Bandwidth Allocation Control Protocol (BACP)

Ascend has recently worked with other industry members to come up a new protocol that is an Internet standard and which allow multiple calls to be inverse multiplexed on a number of different media types – including ISDN BRI B-channels and analog links. Like MP+ this new protocol provide the ability to do dynamic inverse multiplexing across multiple links, and to add or subtract mutiplexed circuits as needed (based upon demand).

As part of the standards effort, two new protocols were defined; the Bandwidth Allocation Protocol (BAP), as well as its associated control protocol, the Bandwidth Allocation Control Protocol (BACP). BAP can be used to manage the number of links in a multilink bundle. BAP defines datagrams to co-ordinate adding and removing individual links in a multilink group, as well as specifying which peer is responsible for which decisions regarding managing bandwidth during a multilink connection.

The leading companies in the access switch market began to implement support for BAP and BACP in their NASs (Network Access Switches) in early 1997. BACP is defined in RFC 2125.

Dynamic Bandwidth Allocation

Certain inverse multiplexing protocols, such as MP+ and BACP, allow dialed circuits to be added or subtracted from an inverse multiplexed connection without terminating the connection. Adding or subtracting bandwidth from a connection in real time is called Dynamic Bandwidth Allocation™.

For example, if a circuit between two locations is continuously used to its capacity 24 hours per day, it's generally more cost effective to use a leased line for the connection. But if the circuit is only needed sporadically, or is at times underutilized, then it often makes more sense to lease a smaller amount of bandwidth and supplement that leased bandwidth with additional dialed bandwidth as traffic requirements dictate.

Furthermore, some connections (especially internetworking connections) will only be established when there is data to be transferred. Low traffic levels can be transmitted over a single circuit. However, if traffic levels saturate the single circuit (such as during a large file transfer), additional switched circuits can be automatically added to the connection to increase the bandwidth and therefore performance. When traffic levels subside (specifically, when the file transfer is complete), the additional circuits can be removed from the connection and the bandwidth (and connection cost) reduced.

Figure 39 shows a 56 Kbps leased circuit between a MAX TNT and a MAX 4000. As WAN traffic exceeds a predetermined threshold, additional dial-up 56 Kbps circuits are added to supplement the original leased or switched circuit. As data loads decrease, some or all of the dialed circuits are removed, reducing the bandwidth. Sufficient bandwidth is made available to accommodate peak loads without degrading performance, which avoids the expense of paying for excessive bandwidth during periods of reduced traffic. Bandwidth is provided (and paid for) only as it's needed, as shown by the usage graph in Figure 40.

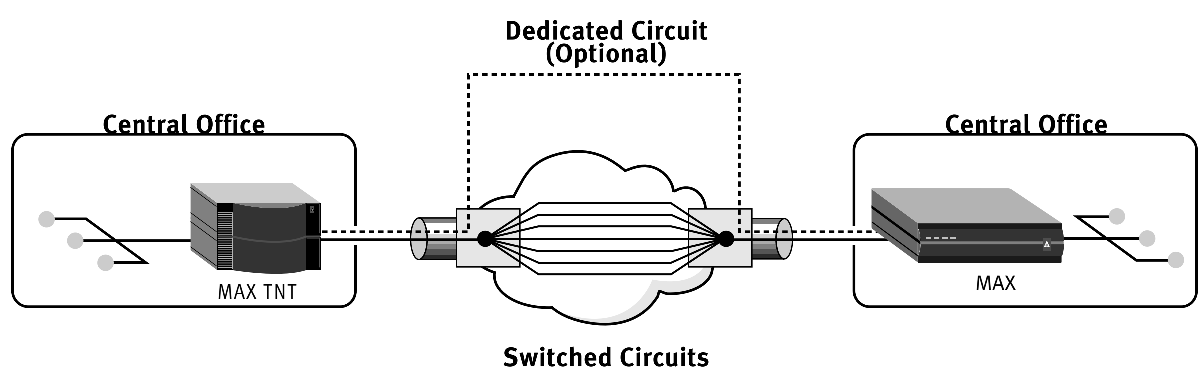

Figure 39 – Dynamic Bandwidth Allocation: Dedicated and switched bandwidth combined into a single data stream

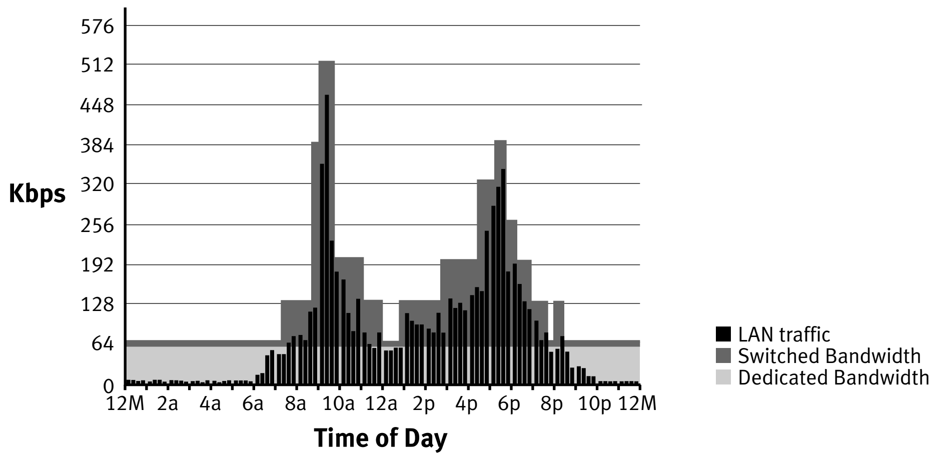

Figure 40 – Dynamic Bandwidth Allocation: Changing bandwidth over time to accommodate real time traffic patterns

Controlling Dynamic Bandwidth Allocation

Dynamic Bandwidth Allocation is automatically controlled by the Ascend MAX TNT. The MAX TNT determines if and when additional bandwidth should be added or subtracted from a connection based upon a set of user-defined parameters usually defined by a given bandwidth utilization level over a given period of time.

The MAX TNT monitors the data stream and measures the data density. Figure 41 shows a connection with a relatively small amount of traffic. In this scenario, the MAX TNT would likely reduce the bandwidth between the two locations to lower bandwidth costs.

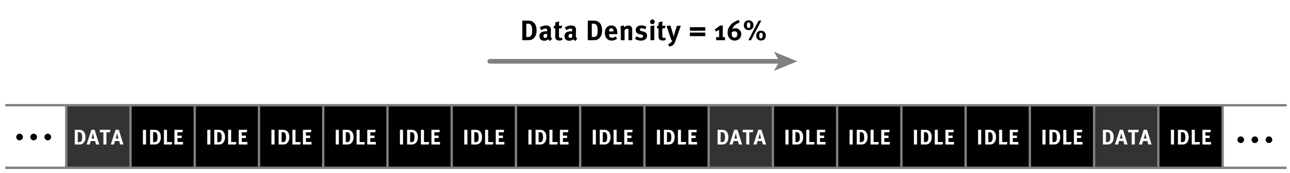

Figure 41 – Low density data stream

Figure 42 shows what the connection looks like as more data is transmitted, for example during a large file transfer. When this occurs, the MAX TNT detects the increased data density and increases the bandwidth between the two locations to improve performance. At the conclusion of the file transfer, the data density would be reduced and the MAX TNT would reduce the bandwidth to lower bandwidth costs.

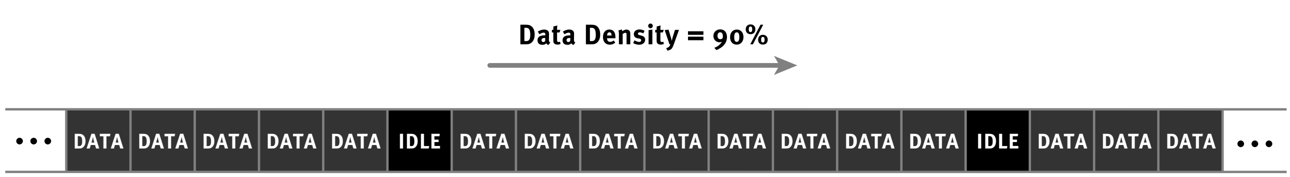

Figure 42 – High density data stream

The user is able to specify a set of parameters to control the decision process that the MAX TNT uses to add or subtract bandwidth. For example, the user can specify such parameters as target line-utilization percentage, the minimum and maximum bandwidth boundaries for the connection, the time period over which to average the data-density measurements, time-of-day considerations, and so on.

WAN Encapsulation Protocols

The MAX TNT is compatible with a long list of WAN encapsulation protocols including: PPP, MP, MP+, BACP, SLIP/C-SLIP, X.25 encapsulation, Frame Relay encapsulation (RFC 1490) and Combinet encapsulation. Virtual Private Networking (VPN) encapsulation protocols include PPTP, ATMP and GRE, with L2TP shortly after the standard is finalized. ARA and TCP-CLEAR are also supported.

On incoming calls, the WAN encapsulation mechanism is automatically detected by the MAX TNT. For outgoing calls, the WAN encapsulation mechanism is specified by the user in the MAX TNT's connection profile, a list of parameters used by the MAX TNT for outgoing calls. Automatic fallback on outbound calls from MP+ to MP or PPP is also performed.

PPP

The Point to Point Protocol (PPP) is the standard wide area network protocol for interoperability of routers and bridges today. PPP is also supported in workstations and personal computers, allowing direct dial-up access from a single computer to a corporate or public Internet. PPP is a constantly growing and evolving standard supporting new capabilities. Newer capabilities in PPP include Compression Control Protocol (CCP) to support standard and negotiated payload compression. The MAX TNT supports all of PPP's optional features, including all security header compression and payload compression features. On a per-interface basis, you may enable or disable any of the optional features.

MP, MP+ and BACP

The MAX TNT product line offers complete support for the MP and MP+ connections, which use PPP encapsulation and support up to 30 inverse multiplexed, multi-channel calls. Standard PPP calls use only a single channel, so the key benefit of MP+ is dynamically allocated increased bandwidth when traffic levels dictate such a need. MP+ calls are typically network-to-network calls involving an IP, IPX, or other type of networking connection. BACP offers much the same functionality of MP+ but in an Internet-standard configuration for compatibility with third-party equipment.

SLIP/C-SLIP

The Serial Line Internet Protocol (SLIP) is another standard for transmitting IP packets over an asynchronous serial link, such as a dial-up or leased line. Compressed SLIP (C-SLIP) is also supported by the MAX TNT product line (RFC 1144). In general, PPP is preferable to SLIP, since SLIP does not include a protocol identifier field (so it can be used only with IP), has no initial negotiation to ensure interoperability, does not support error detection or correction and supports only asynchronous data communication. SLIP is defined in RFC 1055.

Frame Relay RFC 1490

The MAX TNT provides for encapsulation as defined in RFC 1490 over Frame Relay links. This means that a Frame Relay PVC may be provisioned between the MAX TNT and another node and the MAX TNT will encapsulate data for transmission over the link using RFC 1490 encapsulation.

ATMP, GRE and PPTP

The MAX TNT product line fully supports GRE tunneling, PPTP, and AMTP. ATMP is a UDP/IP-based protocol that provides a cross-Internet tunneling mechanism using standard GRE between two Ascend products. GRE is a protocol for encapsulation of one network layer protocol over another network layer protocol and is described in RFC 1701. The encapsulation provides secure transmission of packet contents and enables transmission of packets that would otherwise be unacceptable on the Internet, such as IP packets that use unregistered addresses or IPX packets from roaming clients.

Ascend has its own tunnel management protocol (ATMP) that creates and tears down the tunnel between two Ascend units. In effect, the tunnel collapses the Internet cloud and provides what looks like direct access to a home network. Packets received through the tunnel must be routed within the MAX TNT, so ATMP applies only to IP, IPX or AppleTalk networks at this time.

ARA

AppleTalk Remote Access (ARA) connects a Macintosh to an AppleTalk or TCP/IP network over an asynchronous modem. ARA provides its own authentication method, as well as a maximum ARA connection time. If the ARA encapsulates IP packets, IP routing is supported. ARA connections are single-channel connections. Ascend's AppleTalk implementation includes support for ARA dial-in access for ARA 1.0 and 2.0.

TCP-CLEAR

A TCP-CLEAR connection is a TCP connection that does not use PPP encapsulation. For example, America Online customers who log in from an ISDN device typically use this type connection to allow their own proprietary encapsulation method across the connection.

Other WAN Protocols

Data Compression

The MAX TNT product line support a broad array of different data compression standards, making it one of the most compatible products on the market. Ascend's Data compression support includes:

- Stac Data compression – including the Ascend, Microsoft Stac, and Stac V9 and Hi/fn variations of that standard.
- VJ header compression for TCP/IP connections
- Combinet compression for Combinet calls
- V.42 compression for modem calls
- Compressed SLIP for user SLIP (Serial Line IP) sessions

Stac compression refers to the Stacker LZS compression algorithm, developed by Stac Electronics, Inc., which modifies the standard LZS compression algorithm to optimize for speed (as opposed to optimizing for compression). Stac compression is one of the parameters negotiated when setting up a PPP connection. The Ascend MAX TNT product line implements Stac compression in hardware for maximum performance. MS-Stac refers to Microsoft LZS compression for Windows 95 (also referred to as MS-Stac, or simply as MS Compression). This is a proprietary compression scheme for Windows 95 only (not for Windows NT).

VJ header compression applies only to packets in TCP applications, such as Telnet. When you turn it on, the MAX TNT applies TCP/IP header compression for both ends of the link.

Compression is often a source of confusion when comparing ISDN and modem throughput and performance. Modems are sometimes claimed to support speeds of up to 115 Kbps (with the newer 56 Kbps modem standards). However, this data rate assumes the use of data compression on specific types of data. Since MAX TNT products include compression for their digital interfaces, an “apples-to-apples” comparison is possible. Assuming full compression and an optimal uncompressed data source, Ascend MAX TNTs can achieve throughputs of up to four times the raw bandwidth of the connection. For example, using a single 64 Kbps ISDN B-channel, data throughput of up to 256 Kbps can be achieved. Inverse multiplexing two 64 Kbps ISDN channels together allows up to 512 Kbps data throughput. Data compression requires that both sides of a connection support a given compression protocol (e.g. Stac data compression protocol) to function.

HDLC and Hybrid Access

High-Level Data Link Control (HDLC) is an ISO communications standard for bit oriented protocols – this standard corresponds to Layer 2 (the Data Link Layer) of the ISO 7-layered architecture. It is responsible for the error-free movement of data between network nodes and such protocols as LAPB, LAPD, LAPF, V.120 and SS7 data link layer are all based upon HDLC. The job of the HDLC layer is to ensure that data passed up to the next layer has been received exactly as transmitted (i.e. error free, without loss and in the correct order). Another important job is flow control, which ensures that data is transmitted only as fast as the receiver can receive it.

HDLC processing support is either built into, or available as an option, in all the MAX TNT modules to support circuits that are based on HDLC (such as ISDN, X.25, Frame Relay, etc.). With these types of circuits the HDLC frame must be assembled or disassembled at high speed; a processor intensive process that is usually accomplished by specialized hardware to avoid unnecessary load on the CPU. When configuring a MAX TNT product that will be using HDLC-based communications lines be sure that the MAX TNT has sufficient HDLC processing power (via the standard support, or optional expansion modules) to support all the circuits. HDLC processing is incorporated in the Hybrid Access module, the FrameLine (Frame Relay) module and the IDSL module. If you are to be using Frame Relay circuits you will also need the Frame Relay software option for the MAX TNT.

V.110

This standard specifies how Data Terminal Equipment (DTEs) can operate on an ISDN network. The MAX TNT can both accept incoming V.110 calls and also make outgoing calls to a V.110 terminal adapter using the PPP protocol. This feature also supports the call-back feature for the MAX TNT Link Client software product.

You can configure the MAX TNT to direct terminal server calls to its own administrative command- line, or to a Telnet host or TCP host on the local IP network. After the V.110 (or V.120) encapsulation has been removed, if the data is PPP-encapsulated as well, the terminal server connection can support IP or IPX access.

A MAX TNT V.110 card provides eight V.110 modems, each of which enables the MAX TNT to communicate with an asynchronous device over synchronous digital lines. An Async device such as an ISDN modem encapsulates its data in V.110. The V.110 module in the MAX TNT removes the encapsulation and enables an Async session (a terminal server session).

V.120

This is a protocol specification for encapsulating transmitted data so that DTEs, with synchronous or asynchronous serial interfaces, can operate on an ISDN network.

V.120 is used with ISDN terminal adapters (also known as ISDN modems) such as the Ascend Pipeline 15 for asynchronous calls with CCITT V.120 encapsulation. The MAX TNT handles V.120 encapsulation in software, so it does not require installed devices to process these calls. After removing the link encapsulation, it forwards these calls to its terminal server software. The terminal server either displays one of its interfaces to the caller or forwards the call to a Telnet or TCP host on the local network, depending on how it is configured. Or, if it detects PPP encapsulation, it can forward the call to the bridge/router software for an asynchronous PPP session.

D4 and ESF Framing (T1)

The MAX TNT T1 module fully meets the D4 Framing standard used in T1 line transmissions. D4 specifies the D4 format, also known as the SuperFrame format, for framing data at the physical layer. The MAX TNT also supports the Extended SuperFrame (ESF) standard, a T-1 carrier framing format that provides 64 Kbps clear channel capability.

Switch types

The network switch that provides an T1/PRI line to MAX TNT and connects the line to the WAN can either:

1. AT&T 5ESS
2. NTI (Northern Telecom Inc., now Nortel, Inc.) DMS 100

G.703/G.732 Framing (E1)

An E1 line consists of 32 64 Kbps channels with a total throughput of 2.048 Mbps. It uses 30 B-channels for user data, one 64 Kbps D-channel for ISDN signaling, and one framing channel. This type of communications line is a standard in Europe and Asia called CEPT G.703/G.704. R2 signaling is also supported.

Switch types

The network switch that provides an E1/PRI line to MAX TNT and connects the line to the WAN can be any one of the following:

- Net 5 (the default)

Net 5 is the switch type for European ISDN services in Belgium, Netherlands, Switzerland,

Sweden, Denmark, and Singapore.

- DASS 2

DASS 2 is available for installations in the U.K. only.

- ISDX
- ISLX
- MERCURY

ISDX, ISLX, and MERCURY are varieties of DPNSS.

- Australian
- NTI (Northern Telecom, Inc.)
- French (VN3 ISDN PRI)
- German (1TR6)

Framing mode

The physical layer can use one of the following methods of framing data:

- G.703 (a standard framing mode used by most E1 ISDN providers and by DASS 2).
- 2DS (a variant of G.703 required by most E1 DPNSS providers in the U.K).

Frame Relay

The MAX TNT supports Frame Relay via any of the standard network interfaces, and can serve as a Frame Relay switch interfacing to Frame Relay concentrators. A common use of the MAX TNT serial expansion module's Frame Relay interface is to interconnect the ISP remote POPs to the central POP, which creates a high-speed Frame Relay backbone.

The MAX TNT provides for encapsulation as defined in RFC 1490 over Frame Relay links. This means that a Frame Relay Permanent Virtual Circuit (PVC) may be provisioned between the MAX TNT and another node, and the MAX TNT will encapsulate data for transmission over the link using RFC 1490 encapsulation.

The Ascend MAX TNT supports two of the standard Frame Relay interface types: UNI (User to Network Interface) and NNI (Network to Network Interface). In a Frame Relay backbone, every access line must connect directly to a Frame Relay switch. In the past, most connections to the Frame Relay network were relatively high speed (full T1 lines). Frame Relay switches such as those from Cascade are designed around high performance T1 speed or higher interface connections.

With the decreases in Frame Relay pricing offered by Regional Bell Operating Companies (RBOCs) it may be lower in cost to run low speed 56K or 64 K leased Frame Relay connections in place of analog or even ISDN dial-up connections. However, with the traditional UNI interface a Frame Relay port that is designed for the high speed connections must be used for the 56K or 64K link.

With NNI interface support, the MAX TNT can be configured so that each DS-0 on a T1/E1 line is a separate Frame Relay connection from a low-speed Frame Relay user (for example a remote office with a Pipeline 130 with the 56K Frame Relay port in use). Up to 4096 such low-speed Frame Relay connections can be concentrated into a single MAX TNT. This makes the MAX TNT a very cost-effective Frame Relay concentrator for ISPs addressing the business market or in corporate sites with a high number of distributed regional or local offices.

As a Frame Relay concentrator, the MAX can support many low-speed Frame Relay connections and concentrate them into one or more high-speed connections to a Frame Relay switch using either the serial WAN interface or T1/E1 lines.

In a frame-relay backbone, every access line connects directly to a Frame Relay switch. In the past, most connections to the Frame Relay network were relatively high speed, such as full T1 or E1 lines. With recent changes in Frame Relay pricing, many sites now want to concentrate many low-speed dial-in connections into one high-speed nailed connection to a Frame Relay switch. When the MAX TNT is configured as a Frame Relay concentrator, it accepts incoming dial-in connections as usual and forwards them out to a Frame Relay switch.

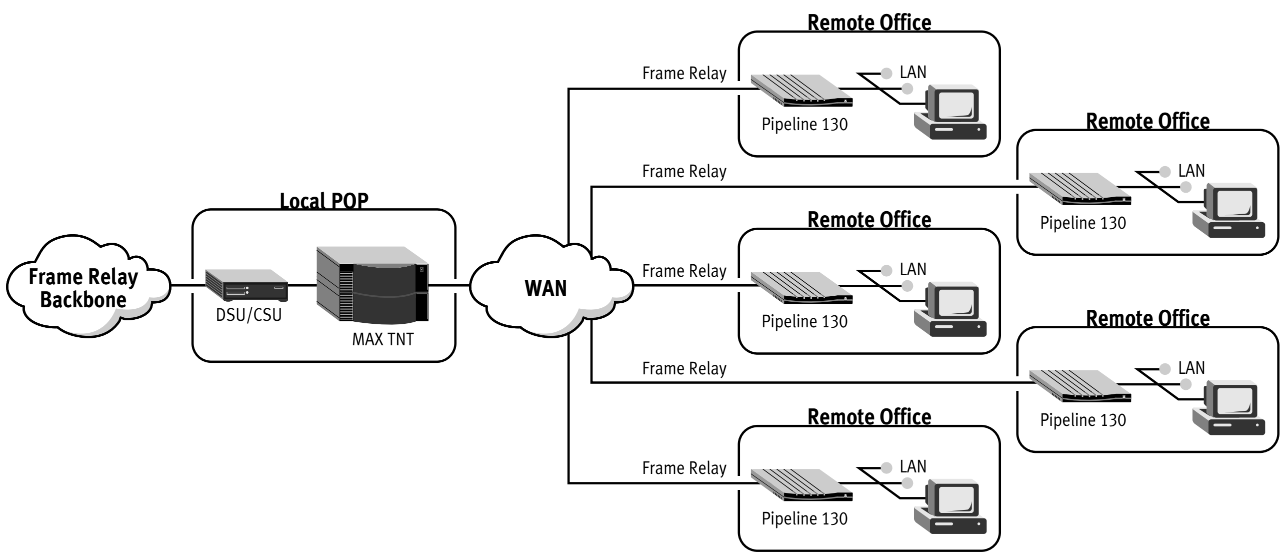

Figure 43 – MAX TNT Frame Relay support

Appendix Two: Digital Modem Overview and Standards Support

Digital Modem Concept

The Ascend MAX TNT can accept incoming data calls from the network either as pure digital data streams, or as Pulse Coded Modulation (PCM) encoded digital streams which contain digitized analog waveforms from modem-based callers. Calls from modem users, sent to the network over analog lines, are presented to MAX TNT systems as digitized analog waveforms. The MAX TNT then converts the digitized PCM stream into the original analog waveform and performs the necessary demodulation. Likewise, MAX TNTs can modulate outgoing data into analog waveforms, convert these waveforms to PCM, and send them to the network over digital facilities. The information is presented to the receiving modem by the network over analog facilities, as it would have been if the information had originated at an analog line-based sending modem.

There are several advantages to digital modems. The main advantage is that a MAX TNT can connect to the network over digital lines (such as ISDN BRI, PRI, T1 or E1) and still communicate with both digital- and analog-based stations. This allows support for both modem and digital dial-up users, as well as providing a smooth migration path as more and more users move to digital access lines.

In addition, by bringing the digitized modem signals from the network to the MAX TNT over digital lines instead of analog lines, a significant increase in noise immunity is obtained for each incoming call. This means that there is less likelihood of data errors or prematurely terminated calls due to noise picked up on the access line between the carrier's central office and the central site where the MAX TNT is located.

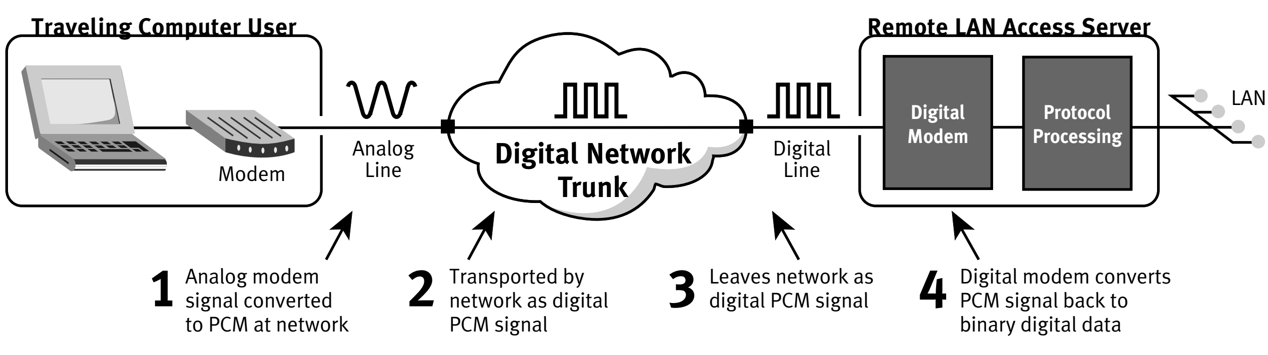

Figure 44 – The analog modem to digital modem communications process.

Furthermore, by integrating digital modems into the Ascend MAX TNT, full visibility of the digital modems can be had through SNMP-based network management systems or Telnet access. Advanced management support of the modems provides such features as modem-by-modem performance analysis, and the ability to gracefully take modems out of service without disrupting user sessions. Additionally, the MAX TNT's digital modems perform automatic load balancing across the pool of modems so as to maximize performance and improve system reliability by distributing the load over all available modems.

The Ascend digital modems have DSP-based Hierarchical Data Processing and Software-Upgradable Modem/Bit-Pump Code. Extensive SNMP Management support make the modems easy to manage either through Ascend network management applications or via any generic SNMP management station.

The High-Speed, Upgradable Digital Modem

Higher Bandwidth Modem Protocols

The lowest level of modem communications is referred to as the modulation scheme. Examples of modulation schemes include the V.34 and V.32 families. It is these modulation schemes that define the raw bit rate at which the modems communicate. (For example, V.34 defines bit rates of up to 33.6 Kbps.)

The modem modulation bit rate includes neither data rate increases due to data compression nor the overhead associated with error control. The most common data compression and error control protocol in use with modems is the V.42 family. With optimum data characteristics, the 33.6 Kbps raw data rate represented by V.34 could be leveraged to over 100 Kbps.

Until now, all of the modem modulation schemes have been designed with the assumption that at least two segments in the end-to-end modem call are analog. With this assumption, it is not possible to achieve a bit rate greater than 33.6 Kbps. However, with the introduction of the Series56™ Digital Modem module, there may be only one analog segment. Assuming a single analog segment, the maximum achievable bit rate can be re-evaluated.

Ascend, in conjunction with several leading modem manufacturers that together represent approximately 70% of the analog modem market, has developed the K56flex modem modulation scheme. The K56flex modulation scheme dynamically determines if there is only one analog segment in the end-to-end call. If it recognizes this optimum configuration and there is a K56flex-compatible modem at the far end, transmit bit rates as high as 56 Kbps[1] can be achieved from the digital end; full standard V.34 bit rates are still achieved transmitting from the end connected to the analog segment. If there is more than one analog segment or if the quality of the single analog segment is insufficient, K56flex falls back to V.34 bit rates.

Flexibility

There are two primary levels of operation associated with a modem: bit-pump and control. The bit pump is the direct implementation of the modulation scheme: translating the voice-band data from the telephone network into a digital bit stream and vice versa.

The control functions include the error control, compression and higher level call control functions.

Standards defining the control functions of a modem can change very frequently. Introduction of new control protocols and refinement of existing standards is an ongoing process. For this reason, all Ascend digital modem products have always supported fully field-upgradable control functions.

Until recently, evolution of the bit pump functionality has been slow. In the past, manufacturers did not consider it to be possible to communicate at modem speeds greater than V.34. Therefore, there was no reason to support field-upgradable bit pumps.

Figure 45 below depicts the software configuration of a system with traditional digital modems.

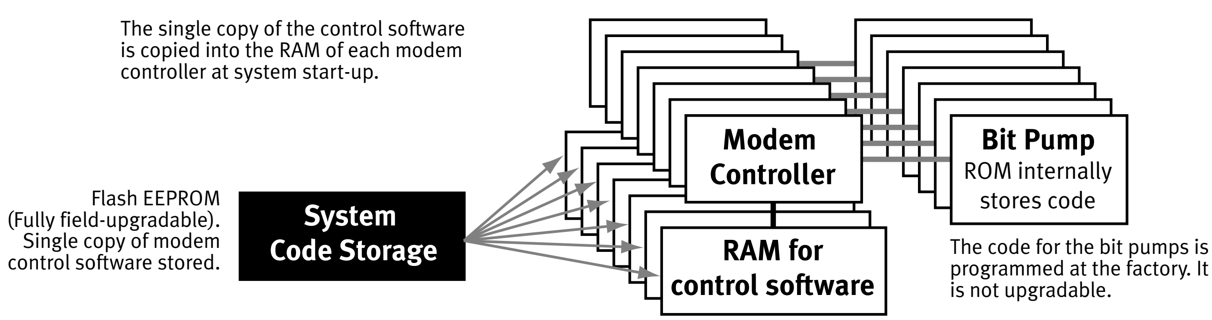

Figure 45 – Traditional software configuration of a system

[1]*Current FCC restrictions, line conditions and other external factors will reduce data transmission rates and may reduce them significantly.*

With the new support of K56flex, and the foresight into the ongoing changes expected as the 56K standards evolve, the Series56 Digital Modem supports not only field-upgradable controller software but also field-upgradable bit pump software.

The code for the bit pumps is now stored in the system flash along with the controller software. Figure 46 depicts the change in code storage.

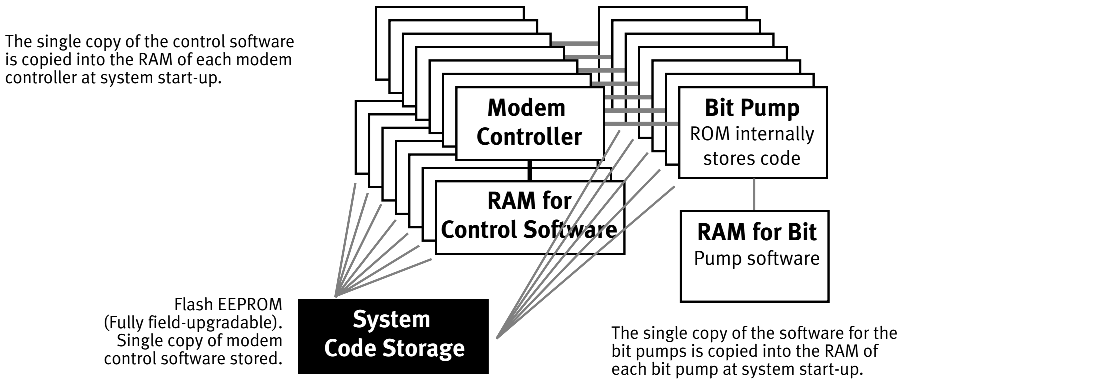

Figure 46 – Series56 Digital Modem software configuration

With all of the components making up a digital modem now fully software programmable, the Series56 has the flexibility to support all current and future modulation schemes as well as control protocols without the need for any hardware upgrades.

Additionally, because of the general flexibility associated with the system software mechanism of the MAX TNT, the bit pump and modem controller software can be upgraded remotely even during system operation, without any real-time interruption of the system services.

In the previous sections, two levels of modem protocols were discussed: the modulation level and the error control/compression level. Though these are critical, they are only the first level of the data hierarchy. Figure 47 depicts the full data-processing hierarchy associated with a modem.

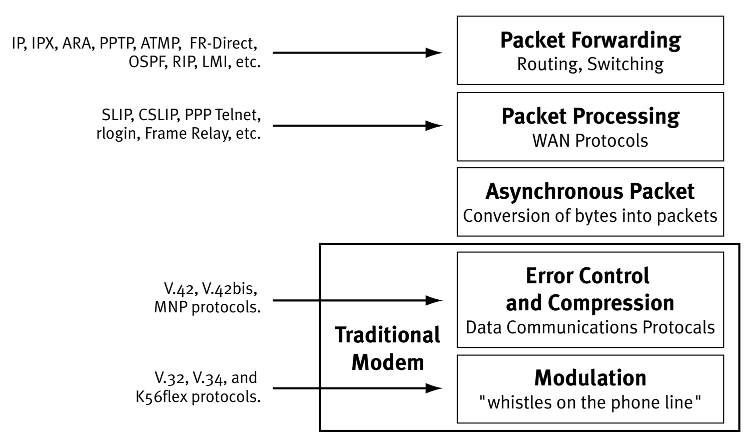

Figure 47 – Data processing hierarchy for a modem session

Traditional Processing Model Prior to the introduction of the Series56 Digital Modem, the three packet layers were implemented in a single central processor. The central processor was responsible for the three layers for all modems in a system. The processor hierarchy is depicted in Figure 48.

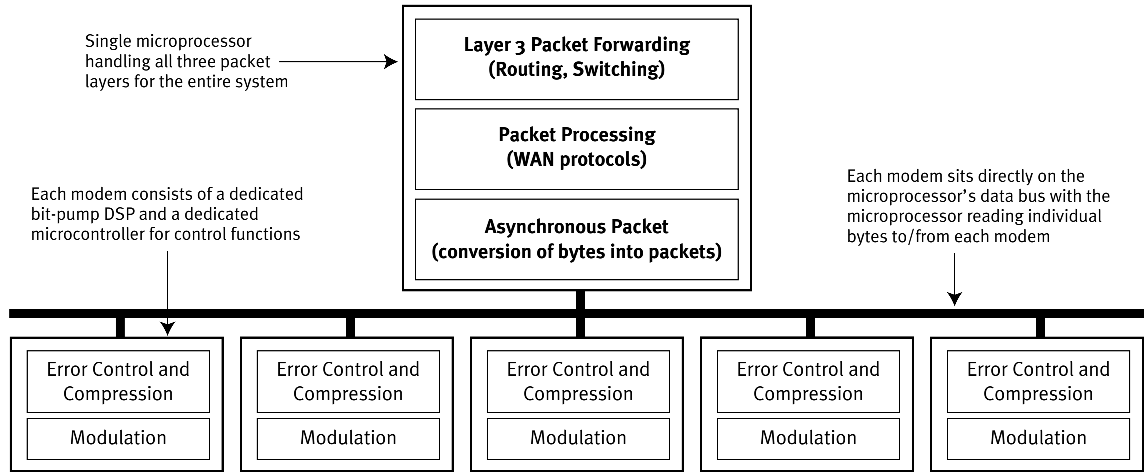

Figure 48 – Processor hierarchy in a traditional system

Series56 Processing Model Of the three packet processing levels, the Asynchronous Packet level is the most processor intensive: It must retrieve each individual byte from the modems and intelligently aggregate them for processing by the higher layer. Likewise, it must do the same in reverse: convert packets of data into individual bytes for processing by the modem.

With the increase in both available bandwidth and more demanding user applications, the Series56 processor hierarchy is enhanced to create a non-blocking system. Specifically, for each group of modems, a dedicated high performance processor is inserted to perform the asynchronous packet layer. The diagram below depicts the Series56 processor hierarchy.

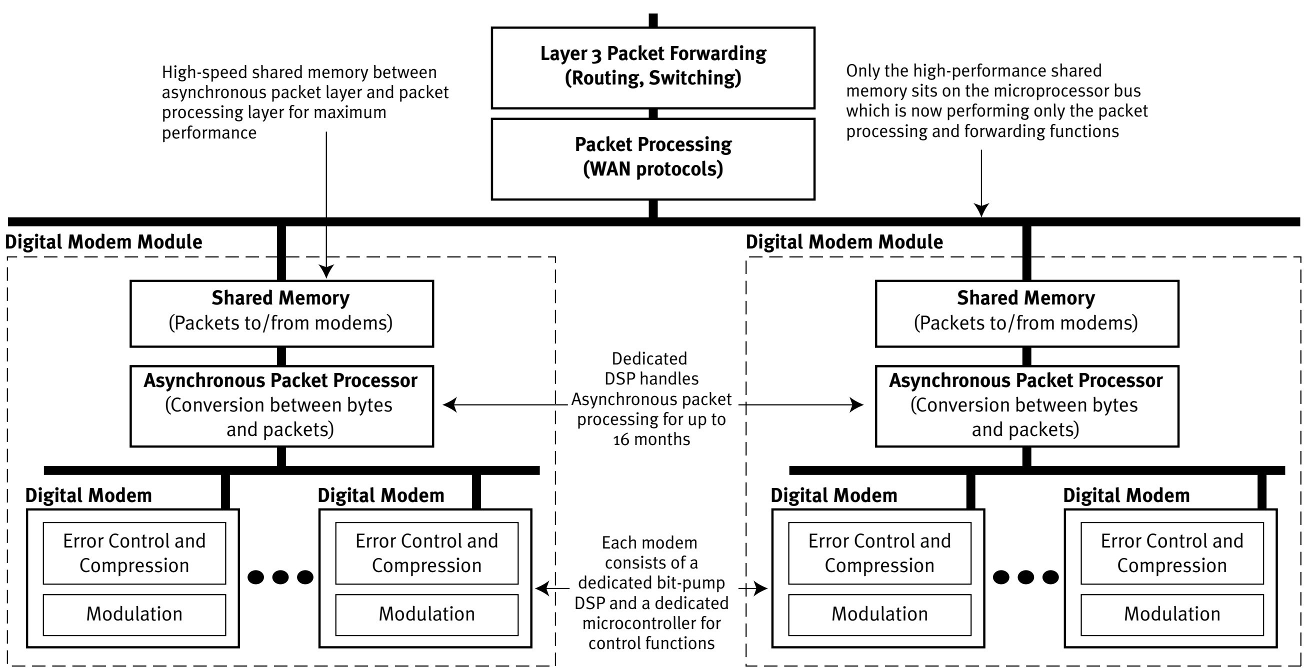

Figure 49 – Processor hierarchy in a Series56 system

The additional processing capability in Series56 modems separates the per-byte functions from the per-packet functions into separate processors. By making this separation, each processor is optimized for its specific task. The task optimization improves the system performance even beyond what might normally be expected by adding the additional processors.

The Series56 provides an processor architecture that supports extended duration full-bandwidth data flow from K56flex and future modems.

Modem Protocols

The MAX TNT digital modems supports all the standard modem protocols including:

- K56Flex
- MNP 10-EC for cellular modem support
- 33.6 Kbps (V.34)
- V.FC
- V.32 and V.32 bis
- V.22 and V.22 bis
- Bell 212A and Bell 103
- MNP and V.42 error correction for wired access
- V.42 bis data compression
- Fax modem send up to 14.4 Kbps (Group 3)
- V.17, V.29, V.27 ter, and V.21

Wireless and Cellular Communications

A popular WAN service that ISPs can provide is cellular communications and wireless remote access. The most robust way to support cellular subscribers is with the MNP10EC (Enhanced Cellular) standard provided with the Ascend MAX TNT. This standard enables subscribers to get wireline performance over cellular links – from 14.4 Kbps to 57.6 Kbps, with compression. The protocol automatically adjusts speed and packet size to match signal quality, and handles cell transitions and signal interruptions transparently. MNP10EC is backward compatible to MNP10 and interoperates with the Enhanced Throughput Cellular (ETC) and Throughput X-Celerator (TX-CEL) protocols.

MNP10EC offers the following advantages:

- ISPs can implement service innovations involving proactive information delivery (e.g. via “Push” technologies) and information requests carried out by an intelligent agent. Mobile users could receive updated information in real time or access stored information that is collected at their request.
- Customers will be free to access information anytime, anywhere. They can access the Internet or corporate intranets over wireless connections.

MNP10EC uses circuit-switched cellular (CSC) technology, which has the following benefits:

- Supports standard networking protocols
- Mimics dial-up access so no changes to existing off-the-shelf or proprietary applications are required
- Uses a common logon sequence and application interface for both wireline and wireless access
- Uses modems that support cellular protocols; these modems work over both cellular and wireline networks
- Uses per-minute pricing, which makes usage costs easier to predict and control for popular character-intensive, IP-based applications

Appendix Three: MAX TNT Expansion Modules

The MAX TNT has an array of expansion modules that allow you to customize your system with the features and benefits you need, when you need them. After you've got your initial system configured, you can easily upgrade your system with additional expansion modules that plug into your existing chassis, or into additional MAX TNT expansion chassis' that can be integrated seamlessly using the MAX TNT intra-shelf expansion bus.

While each MAX TNT expansion module provides unique features and benefits, they have been designed with several common design approaches that help to maximize overall system performance and reliability:

High-performance RISC CPU – Every expansion module incorporates a high-performance Intel i960 RISC processor that allows for distributed processing and scalable processing power as the system is filled with modules. In addition to the high performance CPU, there is significant DRAM on each module to allow for significant route caches, and ongoing enhancement of the feature set of the existing software that runs on each module.

Distributed Processing – Utilizing the high speed CPU, every module performs "Front-end Processing" of as much data as possible. For example, encapsulation processing of all data is handled as close to the physical line termination as possible; T1 cards handle T1 and ISDN signaling and framing, HDLC cards handle synchronous PPP framing and modem cards handle the asynchronous PPP framing. Frame Relay, ATMP and PPTP are all handled at the slot card that terminates the Frame Relay ATMP or PPTP connection. Additionally, each module does its own Route Caching and Call Processing thereby minimizing any impact on the shelf controller CPU and maximizing the scalability of the MAX TNT system.

Dual-port RAM – Each expansion module incorporates high-speed dual port RAM that allows simultaneous read/write commands directly between the shelf controller memory and the Expansion module CPU's memory. The dual-port RAM creates the interface for the control bus over which the Shelf Controller maintains constant communications with each of the expansion cards, and the cards with each other.

Cell-bus Interface – Each expansion bus incorporates a Cell bus interface for direct routing of data to other expansion modules, or to the shelf controller. Every expansion module incorporates the SAR interface circuitry that assembles or reassembles the data for transfer across the cell bus.

Steel Enclosure – The expansion module circuit boards are encased in a protective steel enclosure for maximum protection against physical shock, and isolation from electrical interference. Every expansion module is designed to comply with the rigorous NEBS (National Electronics Building Standards) level of certification for Telephone company central office use.

Shelf Controller

The MAX TNT was designed with the goal of merging the best elements of a distributed processing system and a centralized processing system so as to get the optimal balance of reliability, scalability and cost-effectiveness. Toward this aim the MAX TNT was designed with a shelf controller module that resides in each MAX TNT shelf that can provide the centralized management, communications, synchronization and routing functions for the entire system. The shelf controllers in the other shelves of a MAX TNT system are always sharing information and are available in hot-standby mode should the designated master shelf controller ever encounter problems.

The key components of the Shelf Controller are:

CPU – The shelf controller uses a high performance Intel RISC i960 Processor

Cell Switches – Three cell switches per shelf controller, for swift transfer of data over the intershelf and intrashelf buses for maximum performance. Each Cell switch has three ports – dual transmit and receive paths – so you can get data into the router and out of the router at the same time. The third port on the ATM switch goes to the Intershelf link.

SAR IC – provide the Segmentation And Reassembly (SAR) of the data sent over the cell bus

TAXI IC – The TAXI (Transparent Asynchronous Xmitter-Receiver Interface) integrated circuit drives the intershelf bus Intershelf Bus – The Intershelf bus is a physical and logical ring; the cabling must form a closed loop using the shelf controller Intershelf bus ports.

DRAM – The shelf controller has 8Mb of standard DRAM for the routing table and the shelf controller's executable code that handles the assignment of TDM channels and the over all chassis housekeeping of data structures. This memory can be upgraded at any time with the addition of DRAM using the DRAM/JEDEC (Joint Electron Device Engineering Council) expansion slot which allows up to 32Mb of additional DRAM to be added. Significant new software releases such as for BGP4 support and larger OSPF routing areas will require additional DRAM in the shelf controller. The MAX TNT administrator can query the MAX TNT via CLI (command line interface) commands and SNMP queries for information on system resource utilization.

On-Board FLASH – where store compressed executable code for upgrade. Decompresses code out to DRAM. Motherboard's executable code is decompressed into mother board DRAM from FLASH. There is enough memory space on the board that the software can be decompressed and verified as operative before the active software is erased.

PC Card Slots – Each shelf controller has one Type III, or two type II PC Card slots (previously called PCMCIA card slots). These PC card slots can be used for additional FLASH memory cards that will be needed for the BGP4 code, and larger OSPF routing areas.

10Base-T/100Base-T Ethernet port – Provide basic network connectivity for the MAX TNT shelf.

Serial RS232 Port – Provides direct terminal or PC access to the shelf controller, or can be used to connect a modem for dial-up access to MAX TNT.

Shelf Controller ID – Factory set at "1," must be set to a unique number within at MAX TNT system group.

Alarm Relay – The MAX TNT is equipped with an alarm relay whose contacts are brought out on the back panel's alarm relay terminal block. The alarm relay contacts close during loss of power, during hardware failure, or whenever the MAX TNT is being reset, such as during its power-on self test. During normal operation, the alarm relay contacts remain open.

10Base-T Ethernet Module

The 10Base-T Ethernet module has four 10Base-T interfaces; each of which is a numbered interface with its own collision domain. The MAX TNT four-port Ethernet module provides multi-port Ethernet routing capabilities. Routing can be done between anyone of the 10Base-T interfaces to any WAN port, or any other LAN port on the MAX TNT.

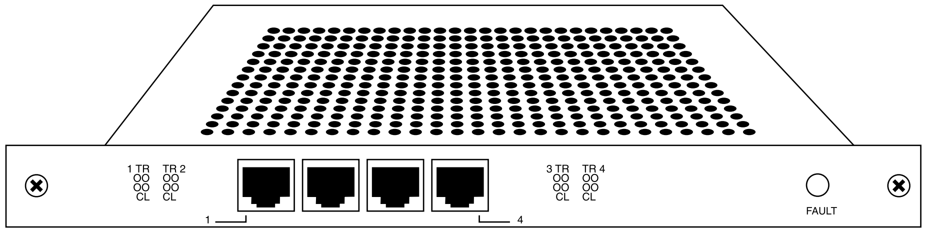

Figure 50 – 10Base-T Ethernet module

Up to four 10Base-T modules can be used in a three-shelf MAX TNT system for a total of up to 16 ports. This Ethernet module was designed to provide basic multi-segment LAN to WAN access.

Application Example:

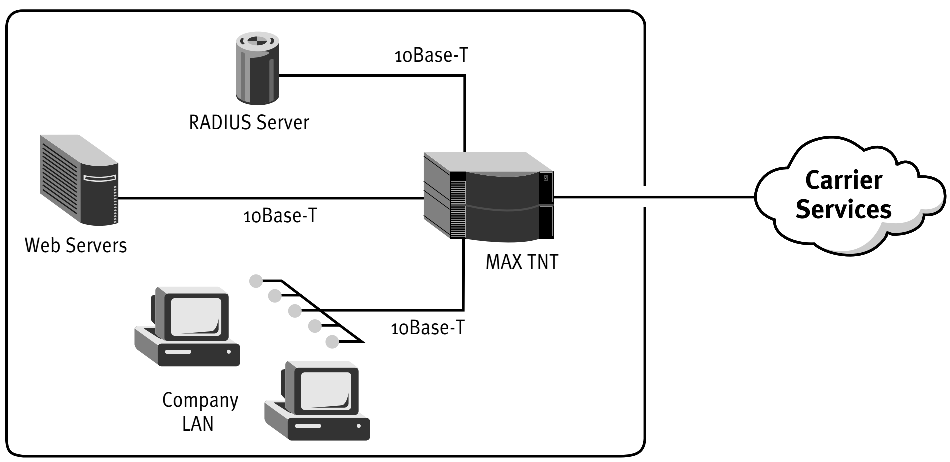

Figure 51 – Ethernet networks connecting to the MAX TNT using the 10Base-T Ethernet module

Module Summary

Module Type	10Base-T Ethernet
Module Model Number/Part Number	TNT-SL-E10
MAX TNT Slots Occupied	One
Transfer Rate	10 Mbps
Transmission Distance	100 Meters
Connector Requirements	RJ45
Module Weight	Approx. 3.9 lbs (1.77 kg)
Module Dimensions	8.8 in high x 10.6 in long (22.35 cm x 26.92 cm)
Hot-swap Capability	Yes
Operating Temperature	32° to 104° F (0° to 40° C)
Operating Humidity	10% to 90%, non-condensing
CPU Type/Speed	Intel i960 RISC Processor
Interfaces per module	4 X 10Base-T
Max. Number of modules per Shelf	4
Max. Number of modules per System*	4
Cable Requirements	Category 3 or Higher, Category 5 Recommended
Protocols Supported	RIP, RIPv2, OSPF, OSPF NSSA
Standards Compliance	802.3

** A system can be made up of up to 3 shelves. A single MAX TNT chassis is referred to as a shelf.*

10/100Base-T Ethernet Module

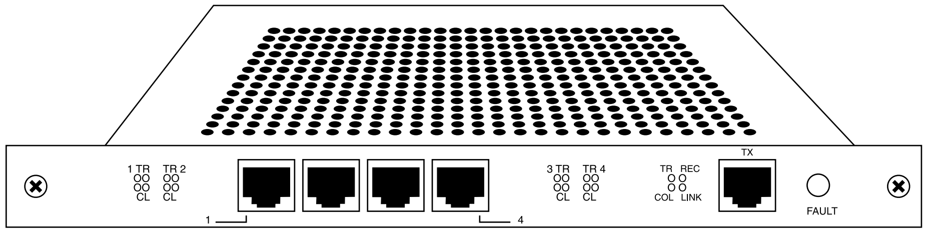

Figure 52 – 10/100Base-T Ethernet module

The 10/100 Ethernet module is identical to the 4-Port 10Base-T Ethernet module but has four routed 10Base-T interfaces and one 100Base-T interface. Up to four 10/100Base-T modules can be used in a three-shelf MAX TNT system for a total of up to 20 ports. This Ethernet module was designed to provide basic multi-segment LAN to WAN access.

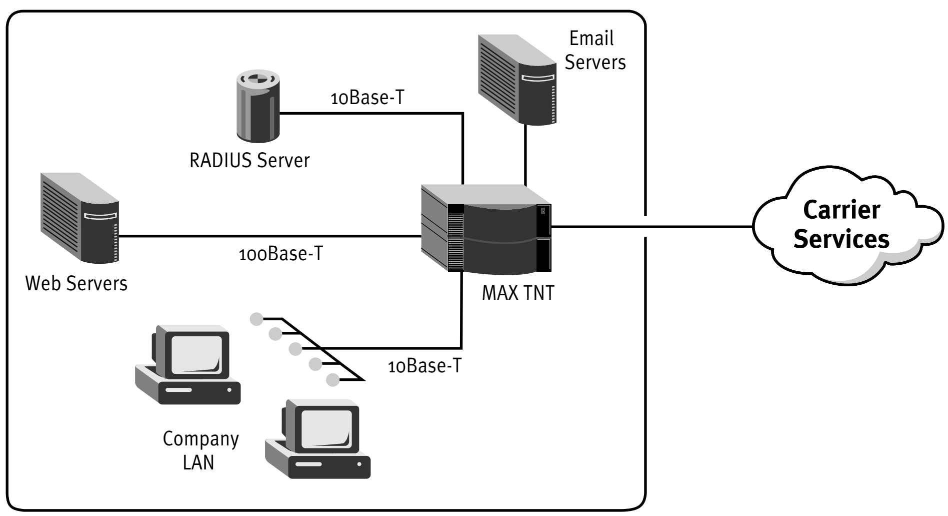

Figure 53 – Ethernet networks connecting to the MAX TNT via the 10/100Base-T Ethernet module

Module Summary

Module Type	10/100Base-T Ethernet
Module Model Number/Part Number	TNT-SL-E100-TX
MAX TNT Slots Occupied	One
Transfer Rate	10/100 Mbps
Transmission Distance	100 Meters
Connector Requirements	RJ45
Module Weight	Approx. 3.9 lbs (1.77 kg)
Module Dimensions	8.8 in high x 10.6 in long (22.35 cm x 26.92 cm)
Hot-swap Capability	Yes
Operating Temperature	32° to 104° F (0° to 40° C)
Operating Humidity	10% to 90%, non-condensing
CPU Type	Intel i960 RISC Processor
Interfaces per module	4 x 10Base-T, 1 x 100Base-T
Max. Number of modules per Shelf	4
Max. Number of modules per System*	4
Cable Requirements	Category 5
Protocols Supported	RIP, RIPv2, OSPF, OSPF NSSA
Standards Compliance	802.3, 802.3u

**A system can be made up of up to 3 shelves. A single MAX TNT chassis is referred to as a shelf.*

Serial WAN Module

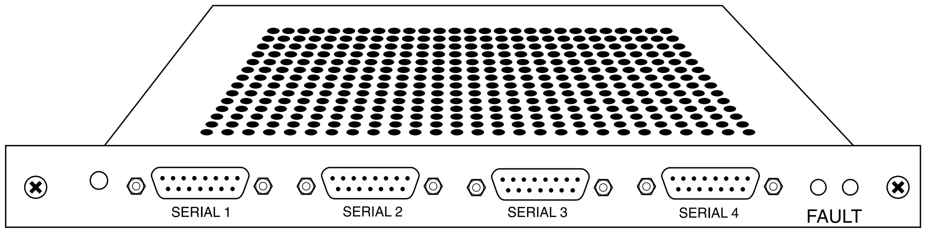

Figure 54 – Serial WAN module

The Serial WAN module has four high-speed V.35 ports, each of which supports data rates of up to 8 Mbps. This module is designed to provide direct connections to a Frame Relay or packet switch and is functionally equivalent to the WAN serial port on the MAX 4000 series product. Because there may be compression over the WAN serial interfaces, hardware-based STAC compression is included on this module. Up to six Serial modules can be used in a MAX TNT shelf for a total of up to 24 ports.

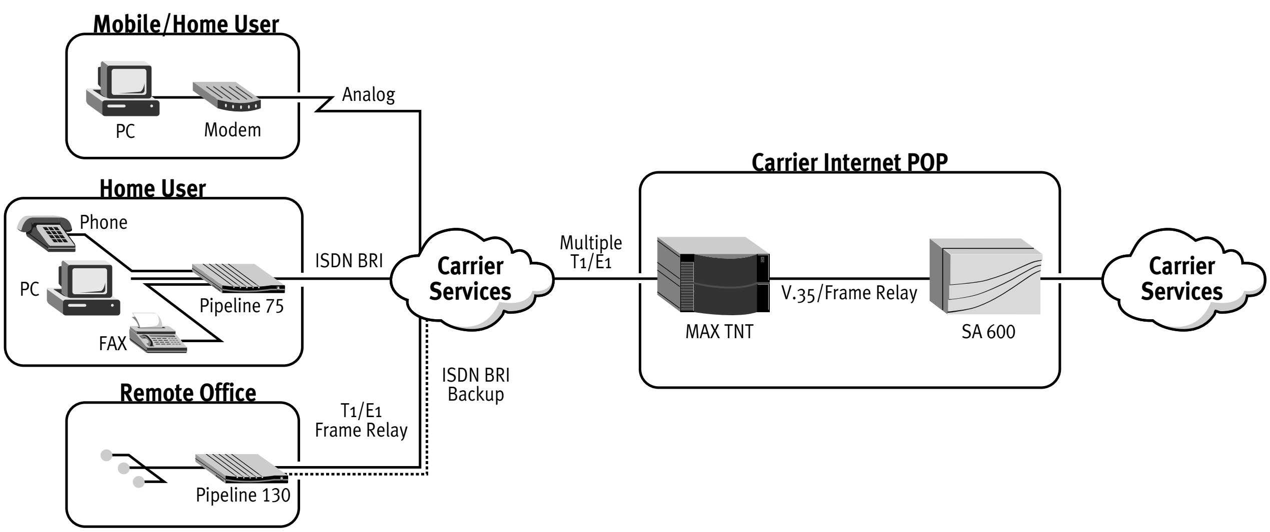

Figure 55 – Serial WAN module application – V.35/Frame Relay from MAX TNT to Ascend SA 600 Frame Relay switch

Module Summary

Module Type	Serial WAN module
Module Model Number/Part Number	TNT-SL-S8
MAX TNT Slots Occupied	One
Transfer Rate	Up to 8 Mbps
Module Weight	Approx. 3.9 lbs (1.77 kg)
Module Dimensions	8.8 in high x 10.6 in long (22.35 cm x 26.92 cm)
Hot-swap Capability	Yes
Operating Temperature	32° to 104° F (0° to 40° C)
Operating Humidity	10% to 90%, non-condensing
CPU Type/Speed	Intel i960 RISC Processor
Interfaces per module	4
Max. Number of modules per Shelf	6
Max. Number of modules per System*	18
Protocol Support	Frame Relay, PPP
Standards Compliance	RS-449/422 , V.35 , X.21
Other	Hardware STAC Data Compression (Hi/Fn) – supports STAC, Ascend and Microsoft compression.

**A system can be made up of up to 3 shelves. A single MAX TNT chassis is referred to as a shelf.*

HSSI Module

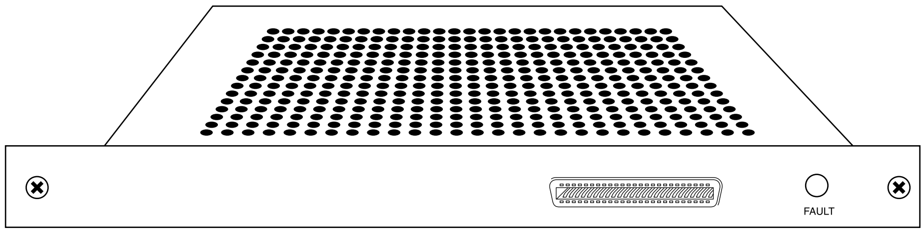

Figure 56 – HSSI module

The HSSI module has one high-speed serial interfaces that supports speeds of up to 52 Mbps. One HSSI module can be used per three-shelf MAX TNT system. Applications for the HSSI module include high-speed uplinks to a Frame Relay switch or router (such as to an Ascend/Cascade B-STDX, or Ascend GRF backbone router).

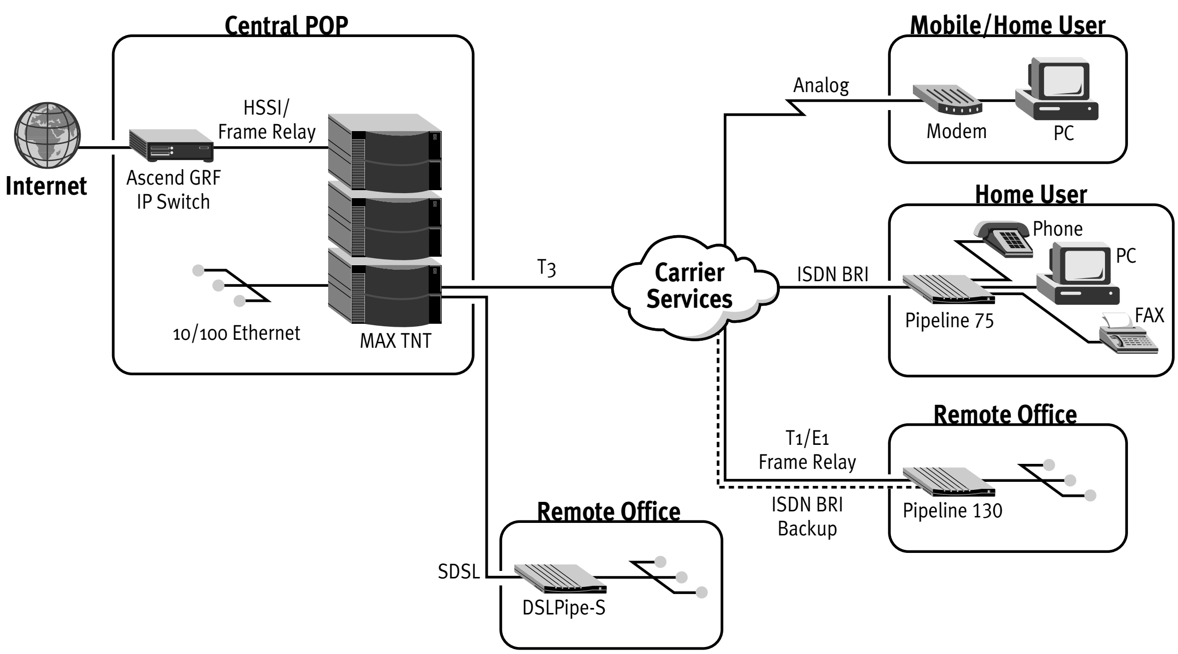

Figure 57 – HSSI module application: Ascend MAX TNT to Ascend GFR IP switch for high-speed Internet backbone access.

Module Summary

Module Type	HSSI module
Module Model Number/Part Number	TNT-SL-S50
MAX TNT Slots Occupied	One
Transfer Rate	Up to 52 Mbps
Module Weight	Approx. 3.9 lbs (1.77 kg)
Module Dimensions	8.8 in high x 10.6 in long (22.35 cm x 26.92 cm)
Hot-swap Capability	Yes
Operating Temperature	32° to 104° F (0° to 40° C)
Operating Humidity	10% to 90%, non-condensing
CPU Type/Speed	Intel i960 RISC Processor
Interfaces per module	1
Max. Number of modules per Shelf	3
Max. Number of modules per System*	3
Protocol Support	Frame Relay, PPP
Standards Compliance	EIA 613

**A system can be made up of up to 3 shelves. A single MAX TNT chassis is referred to as a shelf.*

T1/PRI/E1 Module

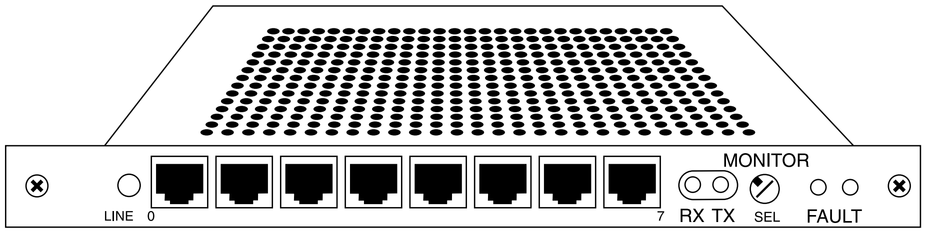

Figure 58 – T1/PRI module

The T1/PRI module has eight routed T1 interfaces with a built-in CSU for every port. Up to four T1 modules can be used in a single MAX TNT shelf for a total of up to 24 ports. The T1/PRI card does not do any data processing but forwards the raw DS0s/B-channels directly to the TDM bus for processing by the other expansion modules (i.e. the Digital Modem module or Hybrid Access/HDLC module).

The T1 card supports tone generation and detection on all interfaces, thereby supporting DNIS digits on a DS1 as well as on PRI interfaces.

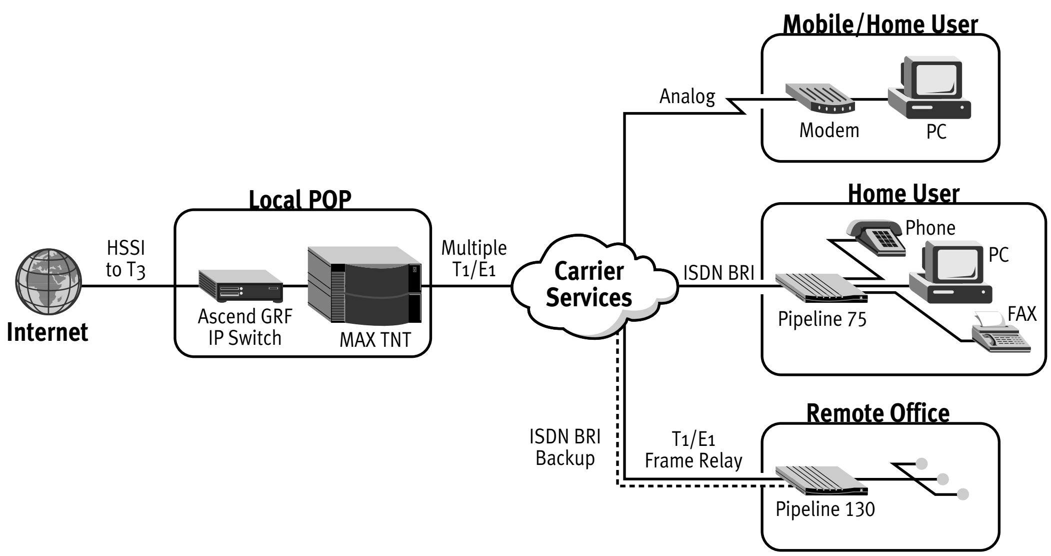

Figure 59 – Sample application of T1/E1/PRI module

Note: Due to phone company definitions of "Yellow Alarm" and the fact that D4 framing was initially designed with voice circuits in mind, when operating in D4 Framing mode the T1 module is limited to 23 channels of HDLC data to prevent false yellow alarm.

When using 56 Kbps modems with D4 Framing, you must use the 56 Kbps data setting (not the 64 Kbps setting) due to the one's density rule and robbed bit signaling must be turned off.

Module Summary

Module Type	T1/PRI module	Octal E1/PRI module
Module Model Number/Part Number	TNT-SL-CT1	TNT-SL-CE1
MAX TNT Slots Occupied	One	One
Transfer Rate	1.544 Mbps, 24 DS0s	2.048 Mbps, 32 DS0s
Connector Requirements	RJ45	120 Ohm RJ45, 75 Ohm Coax
Module Weight	Approx. 3.9 lbs (1.77 kg)	Approx. 3.9 lbs. (1.77 kg)
Module Dimensions	8.8 in high x 10.6 in long (22.35 cm x 26.92 cm)	8.8 in high x 10.6 in long (22.35 cm x 26.92 cm)
Hot-swap Capability	Yes	Yes
Operating Temperature	32° to 104° F (0° to 40° C)	32° to 104° F (0° to 40° C)
Operating Humidity	10% to 90%, non-condensing	10% to 90%, non-condensing
CPU Type/Speed	Motorola 68360	Motorola 68360
Clocking	Provide or Sync to existing clock	Provide or Sync to existing clock
Interfaces per module	8 X RJ45	8 X RJ45, 8 X BNC
Max. Number of modules per Shelf	4[2]	4[2]
Max. Number of modules per System*	4[2]	4[2]
Max. Number of Analog/Digital Sessions	184	240
Switch Type Support	AT&T, NTI, NI-1	ITR6, Australian, NET5, R2, VN3, DPNSS, DASS2, CAS
Framing Support	AMI, B8ZS	B8ZS
Line Encoding Support/Frame Type	D4, ESF	G703/G704, 2DS, D4, ESF
Signaling Support	In-band, ISDN, NFAS	ISDN, DPNSS/DASS2, R2
Other	Integrated CSU on each port	No Integrated CSUs

**A system can be made up of up to 3 shelves. A single MAX TNT chassis is referred to as a shelf.*

[2]*Maximum of 28 T1s/E1s per MAX TNT system (672/720 DS0s respectively).*

DS3 WAN Module

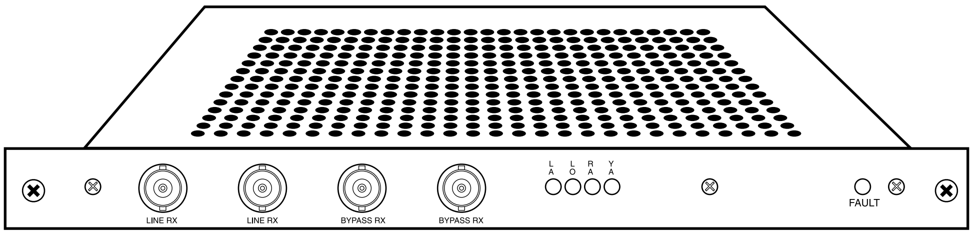

Figure 60 – DS3 WAN module

The DS3 card is a dual-slot module that provides full access and control of the channelized data to the DS0 level. One DS-3 module, with a single backup module, can be supported in a MAX TNT shelf, or MAX TNT system (of up to three shelves).

The DS3 card has four BNC interfaces; two for the active circuit and two to offer a passthrough connection down to a second DS3 card as a backup should the first DS3 card become inactive for any reason.

The DS3 module is designed for applications of bandwidth aggregation where a large percent of the potential DS3 bandwidth will be used and it is therefore cost-effective over terminating a large number of T1/PRI circuits. The DS3 card fully supports fractional DS3 rates so can be used to terminate sub-DS3 rate circuits.

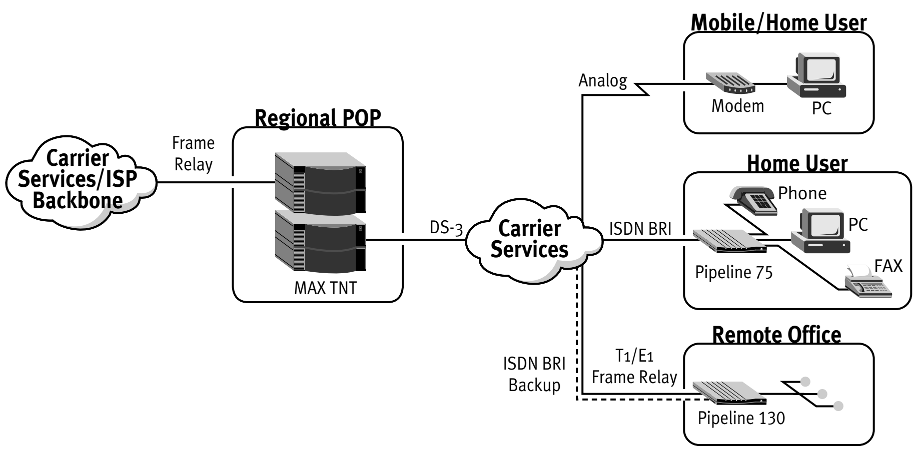

Figure 61 – Typical application for DS3 module

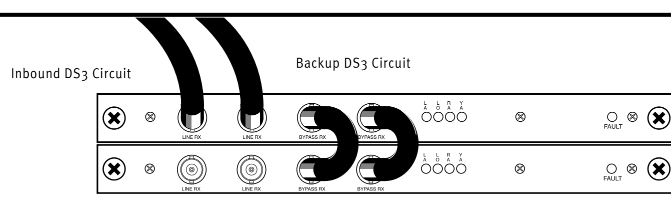

Figure 62 – In a redundant DS3 Module application, the DS3 circuit will be automatically switched to the backup module in the event of a failure of the primary DS3 Module.

Module Summary

Module Type	DS3 WAN module
Module Model Number/Part Number	TNT-SL-CT3
MAX TNT Slots Occupied	One
Transfer Rate	45 Mbps
Data Service	64 Kbps to 43008 Kbps
Connector Requirements	4 – 75 Ohm BNC/DS3
Module Weight	Approx. 3.9 lbs (1.77 kg)
Module Dimensions	8.8 in high x 10.6 in long (22.35 cm x 26.92 cm)
Hot-swap Capability	Yes
Operating Temperature	32° to 104° F (0° to 40° C)
Operating Humidity	10% to 90%, non-condensing
CPU Type	Intel i960 RISC Processor
Interfaces per module	2 BNC Connectors, 2 Backup BNC Connectors
Max. Number of modules per Shelf	2 (1 active, 1 Backup)
Max. Number of modules per System*	2 (1 active, 1 Backup)
Switch Type Support	AT&T, NTI, NI-1
Framing Support	AMI, B8ZS
Line Encoding Support	D4, ESF
Signaling Support	In-band, ISDN, NFAS
Management	Annex D, T1.617D
Circuit Type Support	Switched, Nailed
Other	Provide or Accept Clocking

**A system can be made up of up to 3 shelves. A single MAX TNT chassis is referred to as a shelf.*

Hybrid Access/HDLC Module

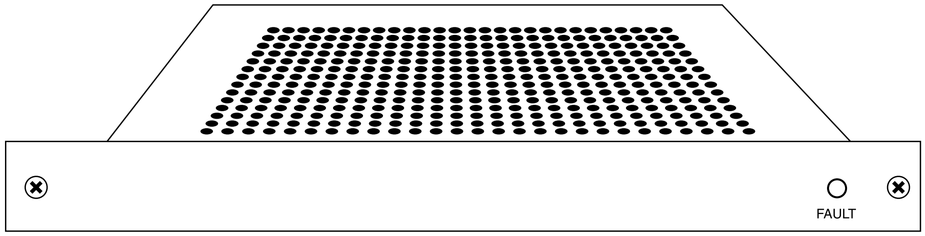

Figure 63 – Hybrid Access/HDLC module

The Hybrid Access module is a single-slot expansion module that is similar to the digital modem card but which houses HDLC controllers for processing HDLC data encapsulation from inbound or outbound ISDN calls. Each Hybrid Access module supports up to 192 active sessions. The Hybrid Access module is also required for support of Frame Relay on the channelized T1 module.

Up to 4 modules can be used in a single MAX TNT shelf and a total of up to 4 in a three-shelf system.

Module Summary

Module Type	Hybrid Access (HDLC)
Module Model Number/Part Number	TNT-SL-HA
MAX TNT Slots Occupied	One
Module Weight	Approx. 3.9 lbs (1.77 kg)
Module Dimensions	8.8 in high x 10.6 in long (22.35 cm x 26.92 cm)
Hot-swap Capability	Yes
Operating Temperature	32˚ to 104˚ F (0˚ to 40˚ C)
Operating Humidity	10% to 90%, non-condensing
CPU Type/Speed	Intel i960 RISC Processor
Interfaces per module	No External Interfaces
Max. Number of modules per Shelf	4
Max. Number of modules per System*	4
Protocol Support	HDLC
Other	Supports ISDN Call Routing, Hardware STAC Data Compression (Hi/Fn) – supports STAC, Ascend and Microsoft compression.
Applications	Required for Frame Relay support of channelized T1

*A system can be made up of up to 3 shelves. A single MAX TNT chassis is referred to as a shelf.

FrameLine (Frame Relay) Module

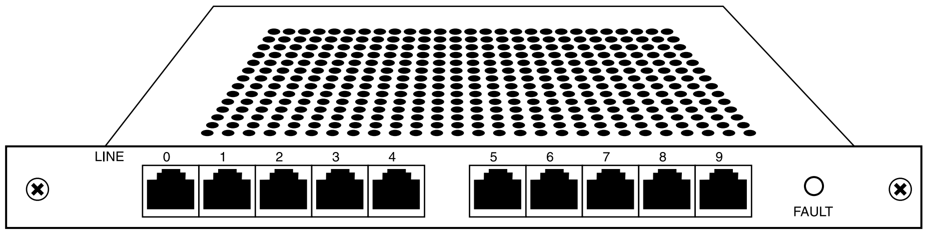

Figure 64 – FrameLine (Frame Relay) module

The Frameline module has 10 unchannelized T1 interfaces and integrated HDLC controllers so that it can provide the complete Frame Relay solution in a single module. To utilize this module you need the Frame Relay software option for the MAX TNT (Note: only one instance of the Frame Relay software option is needed for support of any number of Frameline modules.)

You manage the T1 ports on the FrameLine card similar to the T1 ports on the existing eight-port T1 card. The FrameLine card can only be used for nailed Frame Relay or PPP links.

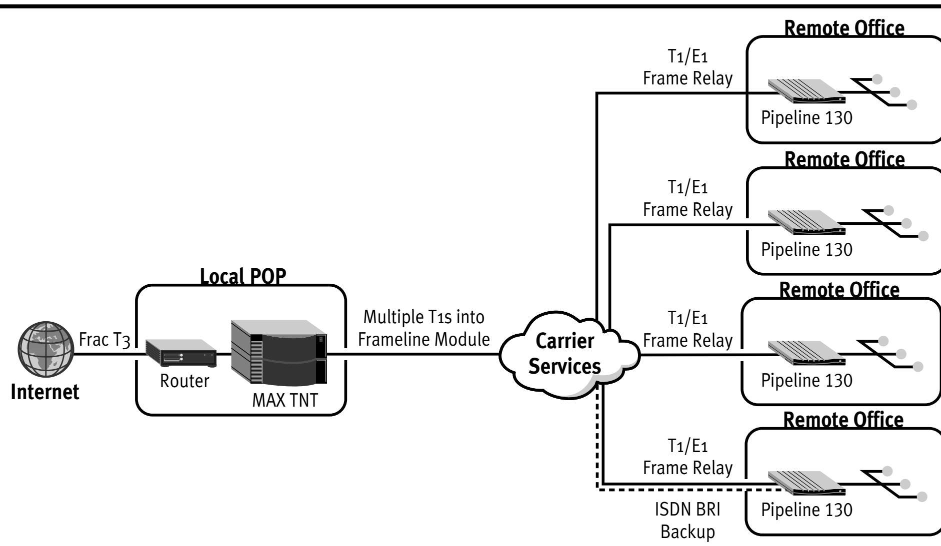

Figure 65 – The Frameline module is ideal for high-density T1 Frame Relay services.

PPP support

Bandwidth per session is 1-24 DS0 channels and the channels need not be contiguous.

Frame Relay support

Bandwidth per link is 1-24 DS0 channels. Channels need not be contiguous. Up to 120 DLCIs are supported per card.

Note: Due to phone company definitions of “Yellow Alarm” and the fact that D4 framing was initially designed with voice circuits in mind, when operating in D4 Framing mode the T1 module is limited to 23 channels of HDLC data to prevent false yellow alarm.

When using 56 Kbps modems with D4 Framing, you must use the 56 Kbps data setting (not the 64 Kbps setting) due to the one’s density rule and robbed bit signaling must be turned off.

Module Summary

Card Type	Frameline
Card Model Number	TNT-SL-FL10
MAX TNT Slots Occupied	One
Transfer Rate	1.544 Mbps +/- 32ppm
Transmission Distance	Standard
Connector Requirements	RJ45
Module Weight	Approx. 3.9 lbs (1.77 kg)
Module Dimensions	8.8 in high x 10.6 in long (22.35 cm x 26.92 cm)
Hot-swap Capability	Yes
Operating Temperature	32° to 104° F (0° to 40° C)
Operating Humidity	10% to 90%, non-condensing
CPU Type/Speed	Intel i960 RISC Processor
Interfaces per Card	10 RJ45 (100 ohm line)
Max. Number of modules per Shelf	2[2]
Max. Number of modules per System*	2[2]
Protocol Support	Frame Relay, PPP, HDLC
DLCIs Supported	120
PVCs per module/System	10/956
Electrical	DSX-1 per ANSI T1.102 (DSX) DS1 per ANSI T1.403, Pub 62411 (CSU)
Line Build Out	0dB, -7.5db, -15db, -22.5db (CSU) 0-133 ft, 133-266 ft, 266-399 ft, 399-533 ft, 533-655 ft (DSX)
Line Code	AMI, B8ZS
Frame Format	Per ANSI T1.107a (M23 or C-Bit Parity)
LED	Single LED, which functions identically to the LED for the eight-port T1 card
Alarm Signaling	Red Alarm, yellow signal
Other	Integral CSUs, Integral HDLC Processors, also called Serial Communications Adapter (SCA)

**A system can be made up of up to 3 shelves. A single MAX TNT chassis is referred to as a shelf.*

[2]*Maximum of 28 T1s/E1s per MAX TNT system (672/720 DS0s respectively).*

Analog Module

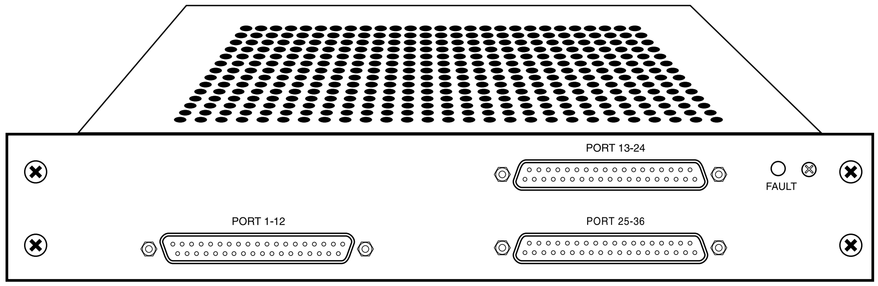

Figure 66 – Analog module

The 36 Port Analog module is a two-slot analog modem module that supports a total of 36 analog ports directly for application in areas where digital trunk lines are not yet available.

Up to 6 modules can be used in a single shelf, or 18 in a three-shelf MAX TNT system for a total of up to 672 ports. This analog modem module was designed for locations where digital trunk lines are not yet available.

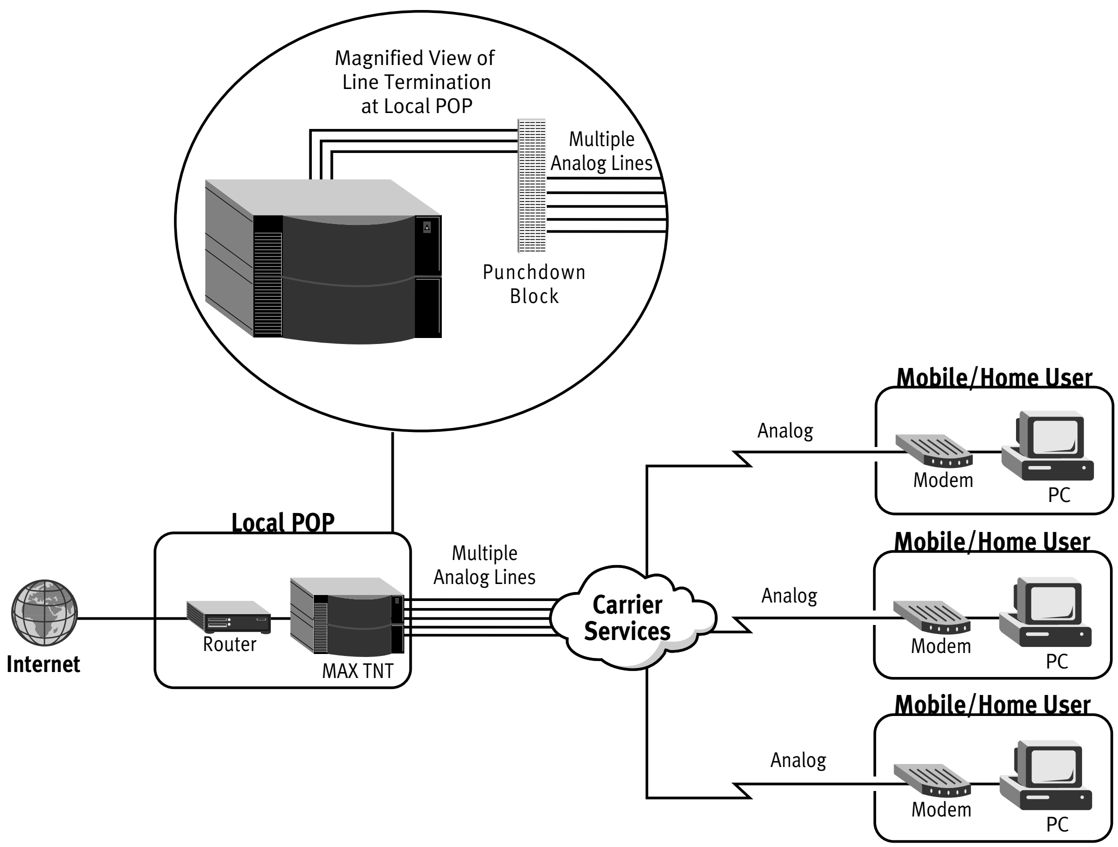

Figure 67 – Analog modem module application.

Module Summary

Module Type	Analog module
Module Model Number/Part Number	TNT-SL-AM36
MAX TNT Slots Occupied	Two
Transfer Rate	Analog – 33.6 Kbps
Module Weight	Approx. 5.6 lbs (2.55 kg)
Module Dimensions	8.8 in high x 10.6 in long (22.35 cm x 26.92 cm)
Hot-swap Capability	Yes
Operating Temperature	32° to 104° F (0° to 40° C)
Operating Humidity	10% to 90%, non-condensing
CPU Type/Speed	Intel i960 RISC CPU
Interfaces per Card	36 via pigtail cables (included)
Max. Number of modules per Shelf	6
Max. Number of modules per System*	18
Standards Compliance	V.32, V.22, V.21, etc.
Compression Support	V.42, STAC
Cellular/FAX Support	MNP 10/Class 3

**A system can be made up of up to 3 shelves. A single MAX TNT chassis is referred to as a shelf.*

Digital Modem 48/S56 Module

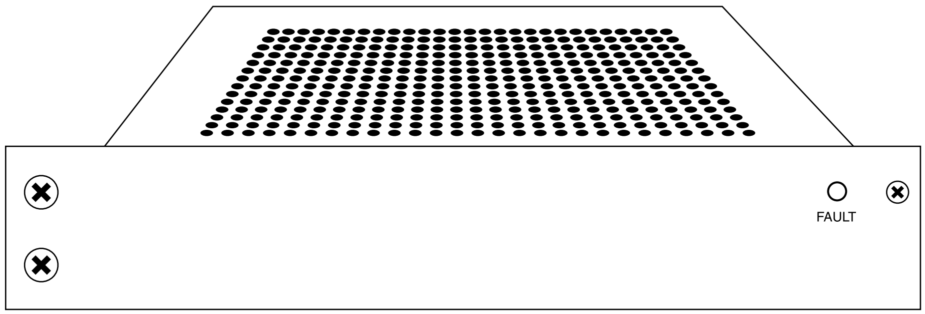

Figure 68 – Digital Modem module

Each MAX TNT Digital Modem module provides forty-eight V.34 Digital Modems, which can receive or place analog and digital calls. The module can support analog or cellular connections at speeds of up to 56 Kbps. It enables remote users with a modem and an analog or cellular line can dial into the MAX TNT via T1 access lines. The K56Flex Digital Modem module is dual-height, meaning that it occupies two MAX TNT expansion slots. You can install a maximum of 7 Digital Modem modules in a single MAX TNT shelf.

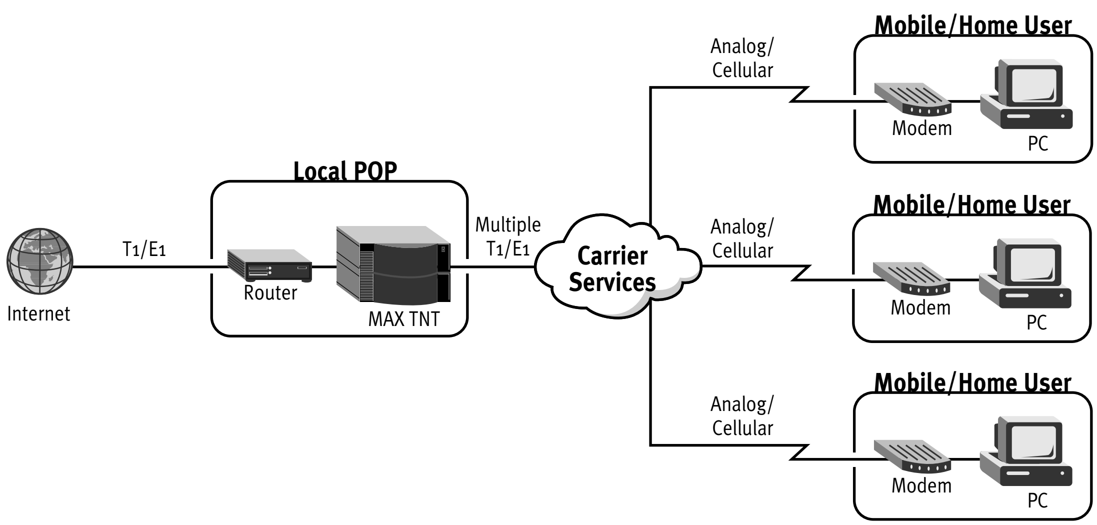

Figure 69 – Typical MAX TNT with Digital Modems application

Module Summary

Module Type	Digital Modem (Flex56K)
Module Model Number/Part Number	TNT-SL-DM
MAX TNT Slots Occupied	Two
Module Weight	Approx. 5.6 lbs (2.55 kg)
Module Dimensions	8.8 in high x 10.6 in long (22.35 cm x 26.92 cm)
Hot-swap Capability	Yes
Operating Temperature	32° to 104° F (0° to 40° C)
Operating Humidity	10% to 90%, non-condensing
CPU Type/Speed	Intel i960 RISC Processor
Interfaces per Card	No External Interfaces, 48 Modems supported on each module
Max. Number of modules per Shelf	7
Max. Number of modules per System*	14
Standards Compliance	K56 Flex upgradable to ITU-T 56K, 33.6, V.34, V.32, V.32 bis, V.22 A/B, V.23, V.21, Bell 212A and 103
Internal Error Correction and Data Compression	V.42 LAPM, MNP 2-4, MNP 10
V.42 bis, MNP 5	
FAX Modem Support	Send/Receive to 14.4 Kbps, V.33, V.17, V.29, V.27ter, V.21 Channel 2 Group 3, T-30 and Class 1, 2
Other	MNP 10 EC Enhanced Cellular Performance

**A system can be made up of up to 3 shelves. A single MAX TNT chassis is referred to as a shelf.*

Ascend's MultiDSL Solutions

Unlike other vendors of xDSL equipment that require you to purchase an entirely new hardware and management system, and add yet another layer of complexity to your network, Ascend allows you to seamlessly integrate xDSL technologies into your existing MAX TNT access solution to provide a complete and compact, manageable, and familiar operating environment. The MAX TNT's xDSL module support allows you to upgrade incrementally with only the card density that you need, when you need it. With the MAX TNT these new access technologies are just one more expansion card option and there is no new learning curve that your NOC needs to learn how to support; if you are familiar with the Ascend products already then implementation and support of xDSL expansion modules will be simple and quick.

Every xDSL module leverages off the Ascend core operating system that is currently used in most of the top 30 Internet service providers.

As everyone who runs a network knows, the upfront equipment costs are only a small part of the total cost of a network. Ongoing support, maintenance and line costs can quickly exceed the original investment and become the majority of the network expenditure. Ascend has focused on minimizing the total cost of ownership by providing a complete platform for both the hardware and management software so that when you buy an Ascend product you are getting an important part of an integrated solution. By comparison, most other vendors will sell just one piece of a puzzle; forcing the bulk of the integration and management costs onto you and quickly eliminating any potential savings that may have been expected.

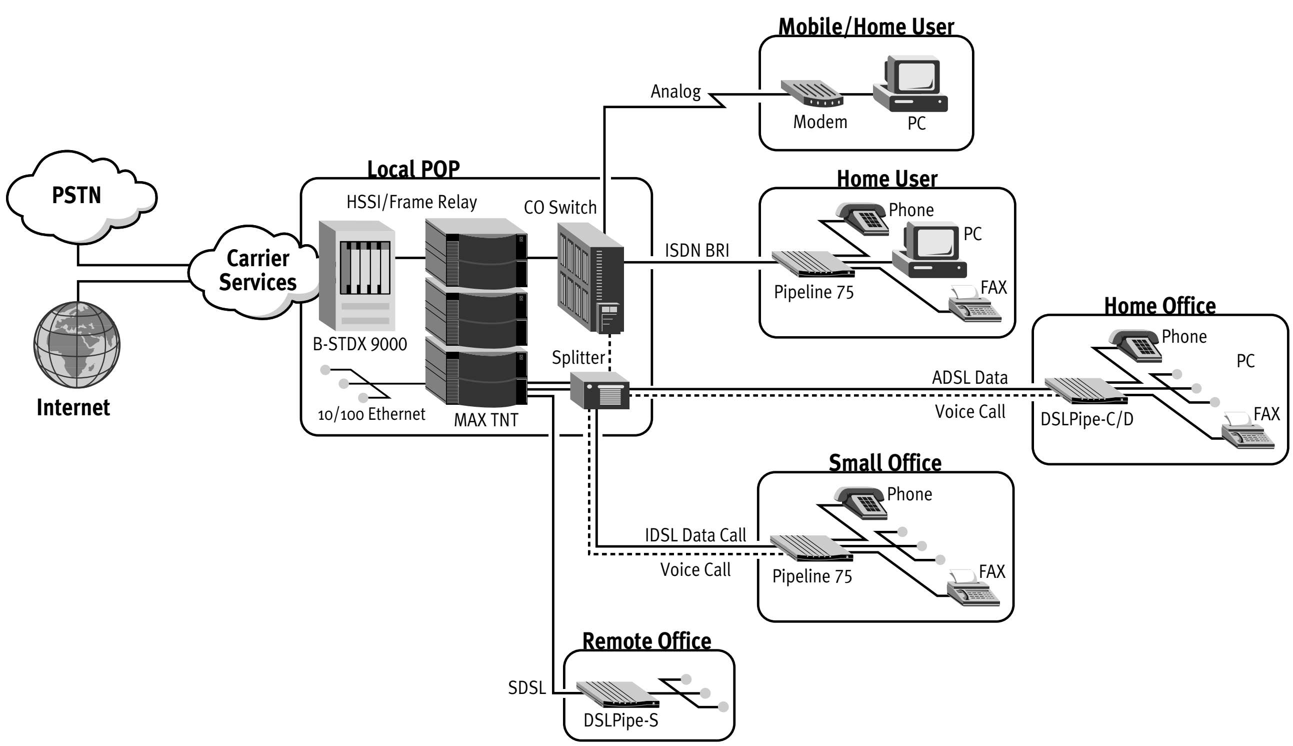

Figure 70 – Carrier/competitive access provider xDSL application example.

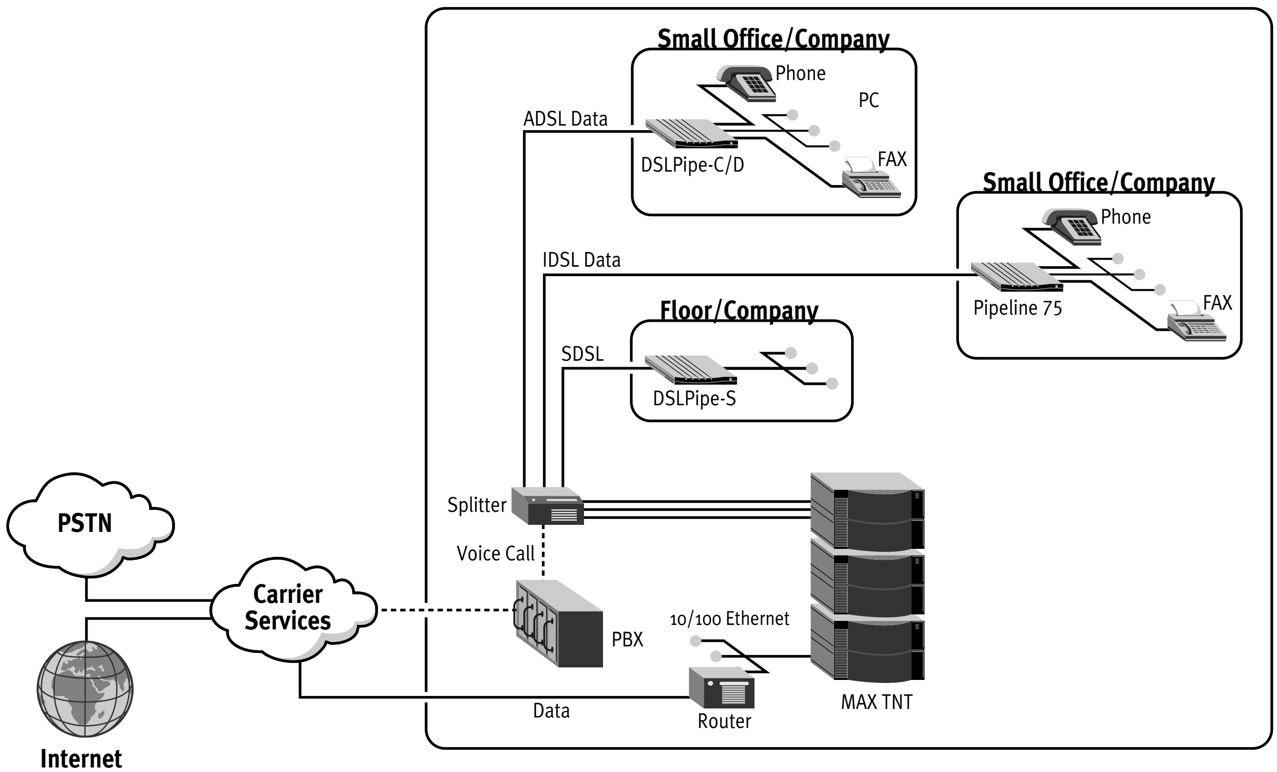

Figure 71 – Office tower/corporate campus application example.

Benefits of the Ascend approach with MultiDSL:

- Leverages proven remote access technology and expertise from Ascend – the MAX TNT based on a core OS, authentication and user validation software, and accounting and billing.
- ISPs/Carriers/CAPs can immediately enter the DSL market with IDSL
- IDSL alleviates the PSTN network congestion
- Multi-service platform provides smooth migration (Analog to ISDN, IDSL, SDSL, RADSL-CAP, RADSL-DMT)
- Ascend has end-to-end CPE and COE products for turn-key solution
- Delivers high-speed remote access for corporate customers
- Comprehensive support for network management, User and Accounting
- Virtual Private Network Support – PPTP, ATMP, Frame Relay and IP Direct – L2TP shortly after standards are agreed to.

IDSL Module

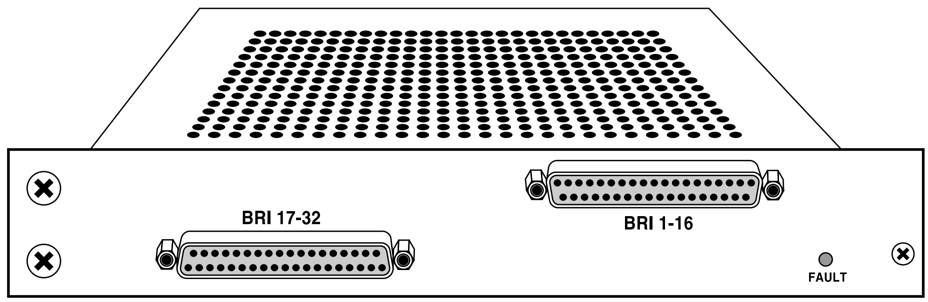

Figure 72 – IDSL module

The IDSL module has thirty two (32) IDSL interfaces and is ideal for moderate to low speed data access to a central network or the Internet. IDSL supports a single 128 Kbps full-time data circuit and avoids the common problem of losing valuable central office switched circuits to long data connections. Voice support for the IDSL module will be a software-only upgrade available in the future. IDSL is an Ascend innovation that provides simple high-speed data networking over a local loop of up to 18,000 ft. In IDSL installations the MAX TNT is installed in central office sites and directly terminates the ISDL data circuit – by-passing the switched telephone network.

IDSL is fully compatible with any standard ISDN BRI Terminal Adapter, Bridge or Router which means that customers and users can easily upgrade to this service with a minimal of hassle. The ISDL line accepts the standard AT&T 5ESS "data-only" configuration parameters that are commonly supported in ISDN data equipment and can be in the same binder group as any other standard T1, SDSL or RADSL lines.

The ISDL card supports standard 2B1Q line encoding for transparent operation through "U" loop repeaters and Digital Loop Carrier systems (DLCs). HDLC controllers are built into the ISDL card eliminating the need for any additional HDLC processing of the incoming IDSL data. ISDL line cards are simple to operate, easy to install, and provide a cost-effective alternative to switched or leased 56 Kbps line as well as full-time ISDN circuits.

The IDSL card is a dual-slot card and up to 3 of them can be used in any MAX TNT shelf, for a total of 224 IDSL ports in any MAX TNT system. The ISDL module is ideal for low to moderate bit-rate applications that require full-time connectivity; some typical application scenarios would be Internet links for small- to medium-sized businesses that want to host a web site in their corporate office and also use the full-time Internet connectivity for employee Internet access.

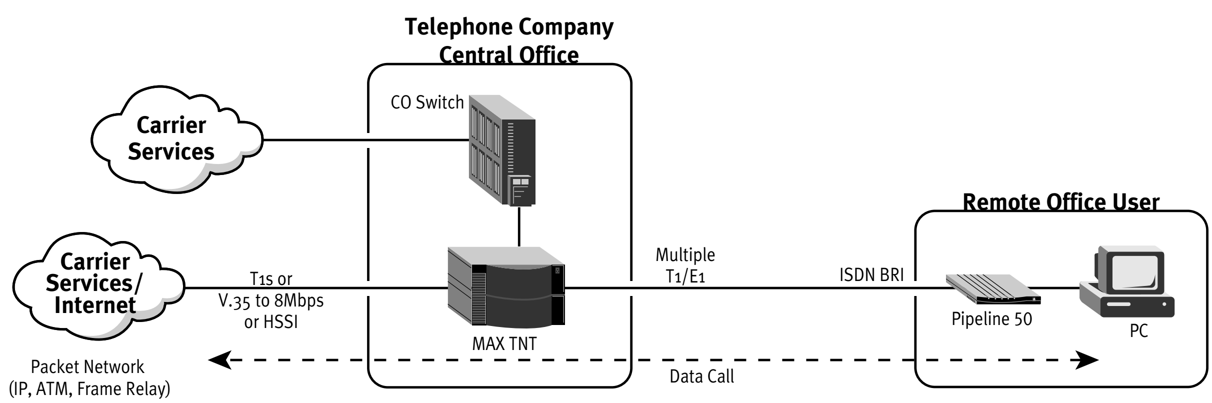

Figure 73 – End-to-end connectivity using IDSL

Module Summary

Module Type	IDSL
Module Model Number/Serial Number	TNT-SL-IDSL
MAX TNT Slots Occupied	Two
Transfer Rate	128 Kbps symmetric data service
Transmission Distance	18,000 ft.
Data/Voice Support	Data available now, Voice support to be a software upgrade in future
Module Weight	Approx. 5.6 lbs (2.55 kg)
Module Dimensions	8.8 in high x 10.6 in long (22.35 cm x 26.92 cm)
Hot-swap Capability	Yes
Operating Temperature	32° to 104° F (0° to 40° C)
Operating Humidity	10% to 90%, non-condensing
CPU Type/Speed	Intel i960 RISC CPU
Interfaces per Card	2 DB37 connectors, each providing 16 IDSL sessions for a total of 32 (DB37 to 50-pin telco pigtail cables included)
Connectors	Must meet JIS C 5973 standards
Max. Number of modules per Shelf	7
Max. Number of modules per System*	7
Protocols Supported	PPP, MP, MP+, Frame Relay
Switch Configuration	AT&T Point to Point
Line Signaling Support	2B1Q
Compatibility	Compatible with any standard ISDN BRI CPE (ISDN TA/Modem, Bridge or Router), Transparent operation through U-loop repeaters.

**A system can be made up of up to 3 shelves. A single MAX TNT chassis is referred to as a shelf.*

SDSL Module

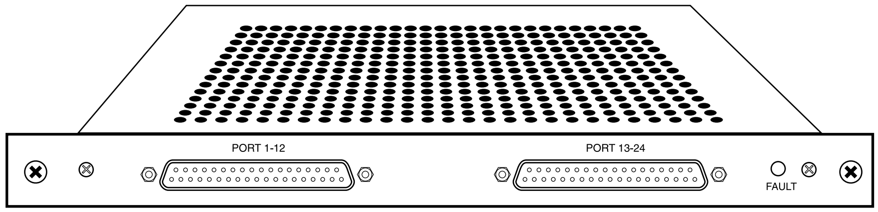

Figure 74 – SDSL module

The Single-pair high-speed Digitial Subscriber Line (SDSL) module has 16 interfaces via two connectors and is ideal for moderate to high-speed corporate data network or Internet connectivity. SDSL supports a 768 Kbps symmetric data rate, and a local loop of up to 12,000 feet.

Ascend's SDSL solution offers standard 2B1Q line encoding, integrated line monitoring and diagnostics, and integrates smoothly with the Ascend DSLPipe-S CPE router that functions just as the current Ascend Pipeline routers but with the addition of an SDSL interface. Just as with the Pipeline ISDN routers, the DSLPipe-S router incorporates IP, IPX and AppleTalk routing and a standard Ethernet interface for LAN connectivity.

Up to 6 SDSL cards can be supported in any one MAX TNT shelf, for a total of 240 ports in any 3-shelf MAX TNT system. The ISDL circuit is a simple process to configure, with no user-configurable parameters at the CPE equipment, and the SDSL line can be in the same binder group as any other standard T1, SDSL or RADSL lines.

This MultiDSL module was designed to high-speed corporate network or Internet access to any company or individual requiring full-time data services. It is a cost-effective alternative to traditional T1 services or lower speed switched services.

Module Summary

Module Type	SDSL
Module Model Number/Part Number	TNT-SL-SDSL
MAX TNT Slots Occupied	One
Transfer Rate	768 Kbps symmetric data service
Transmission Distance	12,000 ft. (3.7 km)
Connector Requirements	DB37 connector, providing 16 SDSL sessions (DB37 to 50-pin telco pigtail cable included)
Module Weight	Approx. 3.9 lbs (1.77 kg)
Module Dimensions	8.8 in high x 10.6 in long (22.35 cm x 26.92 cm)
Hot-swap Capability	Yes
Operating Temperature	32° to 104° F (0° to 40° C)
Operating Humidity	10% to 90%, non-condensing
CPU Type/Speed	Intel i960 RISC CPU
Interfaces per Card	16
Max. Number of modules per Shelf	15
Max. Number of modules per System*	15
Line Encoding	2B1Q
Protocols Supported	PPP, Frame Relay
CPE Compatibility	Ascend DSLPipe-S
Other	Pigtail cables included with module

**A system can be made up of up to 3 shelves. A single MAX TNT chassis is referred to as a shelf.*

RADSL Module (Rate Adaptive DSL)

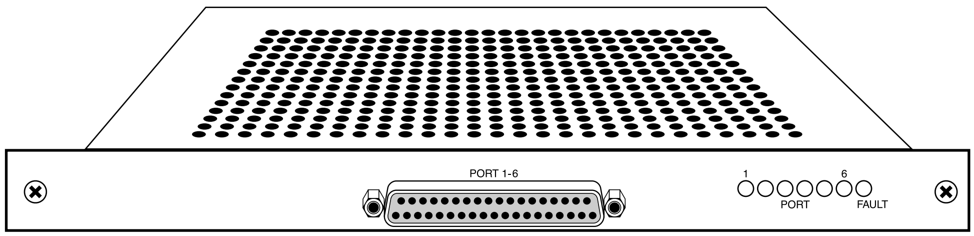

Figure 75 – RADSL module

The MAX TNT RADSL-CAP module has 6 RADSL interfaces that supports up to 7 Mbps downstream and 1 Mbps upstream up to 12,000 ft from the central office, and 640 Kbps downstream and 544 Kbps upstream up to 17,000 ft. from the central office. The Ascend RADSL-CAP solution is designed for full-time data connectivity as well as life-line POTS support, and the DSLPipe-C/D router that acts as CPE equipment acts much like the traditional Ascend Pipeline 75 ISDN router with POTS except with only a single analog phone port.

Rate Adaptive Digital Subscriber Line (RADSL) allows the MAX TNT to detect the noise level on the line and automatically adjust the data transfer rate for optimum performance.

Up to 6 RADSL-CAP modules can be used in a shelf, and up to 15 modules in a three-shelf MAX TNT system for a total of up to 90 ports of RADSL-CAP connectivity.

The RADSL module was designed for high-speed corporate network or Internet access for an individual requiring high-speed data services. It is a cost-effective alternative to traditional lower-speed switched or full-time services and provides the downstream throughput that is necessary for effective professional Telecommuting based on the Internet and Intranets.

RADSL-DMT

Ascend has announced support for DMT-based RADSL and while the basic functionality will be the same as the RADSL-CAP products, the precise specifications will differ slightly. The Ascend RADSL-DMT solution will support 640 Kbps upstream and 6.14 Mbps downstream at a 12,000 foot local loop, and 176 Kbps upstream and 1.54 Mbps downstream at an 18,000 foot local loop. RADSL-DMT will also support lifeline POTS. Availability: Q4 '97.

Module Summary

Module Type	RADSL-CAP
Module Model Number/Part Number	TNT-SL-ADSLC6
MAX TNT Slots Occupied	One
Transfer Rates – Downstream/Upstream Rates at X Distance:	7.168 Mbps/1.088 Mbps up to 10,000 feet (3.05 km) 2.560 Mbps/1.088 Kbps up to 12,000 feet (3.7 km) 640 Kbps/544 Kbps up to 17,000 feet (5.18 km)
Connector Requirements	DB37 to 50-pin telco connectors
Module Weight	Approx. 3.9 lbs (1.77 kg)
Module Dimensions	8.8 in high x 10.6 in long (22.35 cm x 26.92 cm)
Hot-swap Capability	Yes
Operating Temperature	32° to 104° F (0° to 40° C)
Operating Humidity	10% to 90%, non-condensing
CPU Type/Speed	Intel i960 RISC Processor
Interfaces per Card	6
Max. Number of modules per Shelf	15
Max. Number of modules per System*	15
Line Encoding	CAP (Carrierless Amplitude Phase)
Protocols Supported	IP, IPX, PPP, Frame Relay
CPE Support	Ascend DSLPipe-C/D
Other	Lifeline POTS service,

**A system can be made up of up to 3 shelves. A single MAX TNT chassis is referred to as a shelf.*

Worldwide and North American Headquarters
One Ascend Plaza
1701 Harbor Bay Parkway
Alameda, CA 94502, United States
Tel: 510.769.6001
Fax: 510.747.2300
E-mail: info@ascend.com
Toll Free: 800.621.9578
Fax Server: 415.688.4343
Web Site: http://www.ascend.com

European Headquarters
Rosemount House
Rosemount Avenue
West Byfleet
Surrey KT14 6NP, United Kingdom
Tel: +44 (0) 1932.350.115
Fax: +44 (0) 1932.350.199

Japan Headquarters
Level 19 Shinjuku Daiichi-Seimei Bldg.
2-7-1 Nishi-Shinjuku
Shinjuku-ku, Tokyo 163-07, Japan
Tel: +81.3.5325.7397
Fax: +81.3.5325.7399
Web Site: http://www.ascend.co.jp

Asia-Pacific Headquarters
Suite 1419, Central Building
1 Pedder Street
Central, Hong Kong
Tel: +852.2844.7600
Fax: +852.2810.0298

Latin, South America and the Caribbean Headquarters
One Ascend Plaza
1701 Harbor Bay Parkway
Alameda, CA 94502, United States
Tel: 510.769.6001
Fax: 510.747.2669

ASCEND

05-31
10/97