Internetworking

Centillion addressed the complexity issue by adapting the store-and-forward technique used in many Ethernet switches. Packets arriving at the switch are stored in two sets of buffers. At the incoming switch port, the address of each packet is read before it is forwarded to the appropriate outgoing port. Then, at the outgoing port, the packet is held until the token on the destination ring has returned to the switch, enabling the switch to forward that traffic.

WHY IT'S HOT

Makes it easy to set up and administer virtual LANs

The one drawback to using a store-and-forward architecture is that the Centillion switch introduces higher and more variable levels of delay compared with the so-called cut-through switches now being sold by some Ethernet switch vendors. According to Centillion, Speed Switch 100 takes a little over 1 millisecond to process a 1-kbyte packet; that delay increases proportionately with packet size. In contrast, cut-through switches typically add only 45 microseconds of delay, and that delay remains constant regardless of packet size.

The delay factor means the Centillion product isn't as adept at handling delay-sensitive traffic like interactive multimedia and voice as its cut-through cousins. According to Centillion, it couldn't use cut-through switching in its switch because of token ring's token passing scheme.

PROTOCOL PROTECTION

Speed Switch 100's ability to filter broadcast packets is especially important for larger internetworks that carry Netbios traffic. The Centillion switch can handle three different schemes for directing packets to their destination: transparent bridging, source route bridging (SRB), and source routing transparent (SRT) bridging. Transparent bridging operates at the media access control (MAC) layer. SRB is an algorithm developed by IBM specifically for token ring internetworks. SRT bridging is a standard that defines how source routing workstations can communicate with transparent bridging workstations.

Devices implementing SRB and SRT bridging broadcast "explorer" packets to discover the optimal route for packets. Token ring nodes running Netbios also send out broadcasts to discover the location of other devices on the LAN. In larger networks, either type of broadcast can have a crippling effect on network throughput; when both are present on the same network, things can get ugly really quickly.

Speed Switch 100's filtering mechanism prevents this from happening. Each time it sees a packet from a new node, the switch opens up that packet and reads its source routing and Netbios information fields. The switch then stores this data in a memory cache; when it receives subsequent source route or Netbios discovery packets, it sends those packets only to their destination nodes rather than broadcast those packets to the entire network.

"The ability to firewall broadcast frames is the switch's most important feature," says Steve Toce, an engineering consultant at Travtech (Hartford, Conn.), which is responsible for assessing and providing networking technology to Travelers Corp. After beta-testing two of Centillion's switches at the insurance giant, Toce expects Speed Switch 100 to eliminate more than half the broadcast traffic on the Travelers net. He adds that broadcast packets typically account for about 50 percent of overall bandwidth at the insurer.

Centillion is not the only vendor shipping a token ring switch. The Elite Switchinghub from Standard Microsystems Corp. (SMC, Hauppauge, N.Y.) can switch traffic between up to 20 token ring LANs. But the SMC product is more expensive ($3,150 per port), it doesn't automatically control Netbios broadcasts, and it doesn't yet support ATM.

One shortcoming of Speed Switch 100 is that it does not accommodate full-duplex token ring switching. Full-duplex switching effectively doubles the bandwidth available for each token ring port, to 32 Mbit/s. Centillion says a full-duplex facility is now in the works.

—Stephen Saunders

Centillion Networks; 415-969-6700

Circle No. 372

Network Translation's PIX

IP Addresses: Easing the Crunch

Setting up a corporate TCP/IP network is a big enough challenge without having to worry whether there'll be enough unique IP addresses for each and every device. Network Translation Inc. (Palo Alto, Calif.) says save the worry beads for something really important (like color-coordinating adapter cards): Its Private Internet Exchange (PIX) is the first-ever NAT (network address translator).

PIX sits at the boundary of a corporate network and the Internet. Simply put, it allows a few unique IP addresses to be shared among thousands of TCP/IP hosts (much as a PBX shares a few telco lines among thousands of extensions).

Sounds simple, but with PIX in place corporate networkers are free to expand and reconfigure their TCP/IP networks without agonizing over the much-publicized IP addressing crunch. It also spares them from having to upgrade all their host and router software to run IP version 6 (see "Doubts About IPng Could Create TCP/IP Chaos," November 1994). What's more, the router-size translator box boosts security and offers unprecedented freedom when it comes to configuring networks.

WHY IT'S HOT

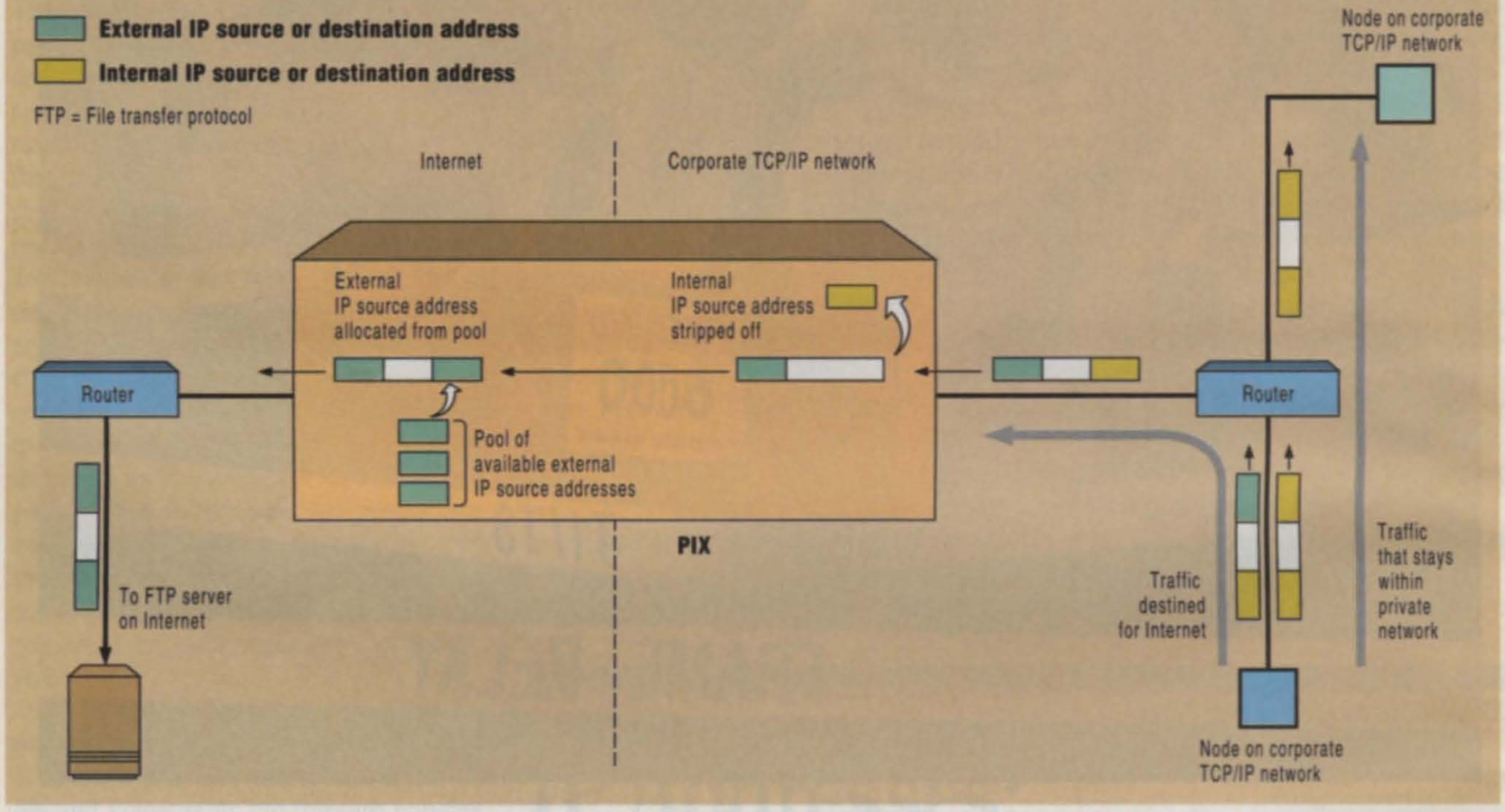
First-ever network address translator

PLAYING POST OFFICE

To understand what PIX does, it helps to take a quick look at the problem it solves. IP addresses are allocated by Internic (Internet Network Information Center). Class A and Class B addresses,

PIX Plays Post Office

When a packet destined for the Internet is routed through PIX, the translator box strips off the internal source address. The external source address that replaces it is assigned to the corporate node for the duration of the application session. When the session is finished, PIX returns the external address to the pool.


🟩 External IP source or destination address
🟨 Internal IP source or destination address
FTP = File transfer protocol
Internet
Corporate TCP/IP network
External IP source address allocated from pool
Internal IP source address stripped off
Pool of available external IP source addresses
PIX
Router
Router
To FTP server on Internet
Node on corporate TCP/IP network
Node on corporate TCP/IP network
Traffic destined for Internet
Traffic that stays within private network

which can accommodate 16.3 million and 65,500 hosts, respectively, are virtually impossible to get. Class C addresses support up to 256 hosts. They're still available, but they're not large enough for the typical corporate network. Thus, net managers are forced to set up and connect several Class C nets with routers, which translates into unnecessary effort and expense.

It gets trickier. An IP host on the Internet cannot have the same address as any other device. If IP addresses are duplicated, the Internet's backbone routers won't be able to distinguish between devices and will refuse to route the packet. And that means end-users attached to hosts with duplicate addresses can't be reached. Just as bad, end-users on hosts with doubled-up IP addresses can't establish FTP (file transfer protocol) sessions (among others): They can reach the target file server without trouble, but when the server attempts to contact the user and set up the session, the backbone routers once again can't determine which host should receive the packet.

Of course, net managers only have to worry about this sort of duplication if their networks are attached to the Internet. If that's not the case, they're free to use any IP addresses they choose (as long as they don't repeat them on the corporate net). But if they ever want to establish an Internet connection, all of the company's IP hosts will have to be assigned unique IP addresses—no easy task. That's why most corporate networkers go to Internic right from the start.

PIX AND CHOOSE

PIX provides a straightforward solution to all this addressing agony by dividing IP addresses into different types and translating between them. External addresses must remain globally unique (no other device on the Internet can use them); internal addresses must follow IP conventions within the organization.

The net manager configures the translator with one or more Class C addresses. From the Internet's point of view, the corporate network consists only of those addresses, which PIX allocates on demand to hosts that need to communicate with the outside world (see the figure).

When a host on the corporate network wants to communicate with a device on the Internet, packets from the originating device are routed to PIX. PIX strips the internal source address from each packet and replaces it with one of the Class C addresses. The packet thus travels over the Internet carrying a valid (unique) source address.

PIX keeps track of which address has been allocated to which device. An external (Class C) address belongs to a device for as long as the application session is running; if the device is retrieving information via FTP, for instance, PIX ensures that the address remains allocated for the duration of the session. Once the device finishes with its application session, its external address is returned to the pool of available addresses.

While PIX may be the next best thing to a chill pill for overstressed network managers, there's one problem it can't solve. If a net manager accidentally configures a host on the corporate network with an address that's in use on the Internet, the company's routers may not be able to direct packets properly because they are unable to determine the correct destination (ironically, this is a scaled-down version of the problem that PIX is intended to solve).

To prevent this from happening, the IETF (Internet Engineering Task Force) has set aside one Class A, 16 Class B, and 255 Class C addresses that will never be used on the Internet. Network managers do not need agency approval to use these addresses, as long as they are kept strictly off the Internet. (For a listing of these addresses, consult RFC 1597 on the server ds.internic.net.)

THE MADDING CROWD

Since there are more devices on the corporate network than there are Class C addresses, if every device on the corporate net tried to reach the Internet simultaneously, some devices would be denied external addresses. That's an unlikely scenario, however. According to John Mayes, the founder and president of Network Translation, only one Class C address is needed for every four to 10 devices (depending on usage patterns). It's important to understand that Class C addresses cannot be used by more than one device at a time.

PIX also increases network security. Since there's no way for anyone on the Internet to know which machine on the corporate network is using a Class C address at any given time, it's impossible to establish a telnet or FTP session with any particular device.

And what about hosts that *should* be recognizable from the Internet, such as mail servers?

These either can be directly attached to the Internet and assigned a public address or can be attached through PIX. In the latter case, the translator is configured to map one of the external addresses to the device not just for the duration of an application session but on a permanent basis.

Pricing for PIX ranges from $7,995 to $23,995, depending on the number of users. *—Johna Till Johnson*

Network Translation; 415-494-6387

Circle No. 373

Proteon's DLSw Software

One Giant Step Toward Integrated Networks

Data Comm MAGAZINE *Hot Products*

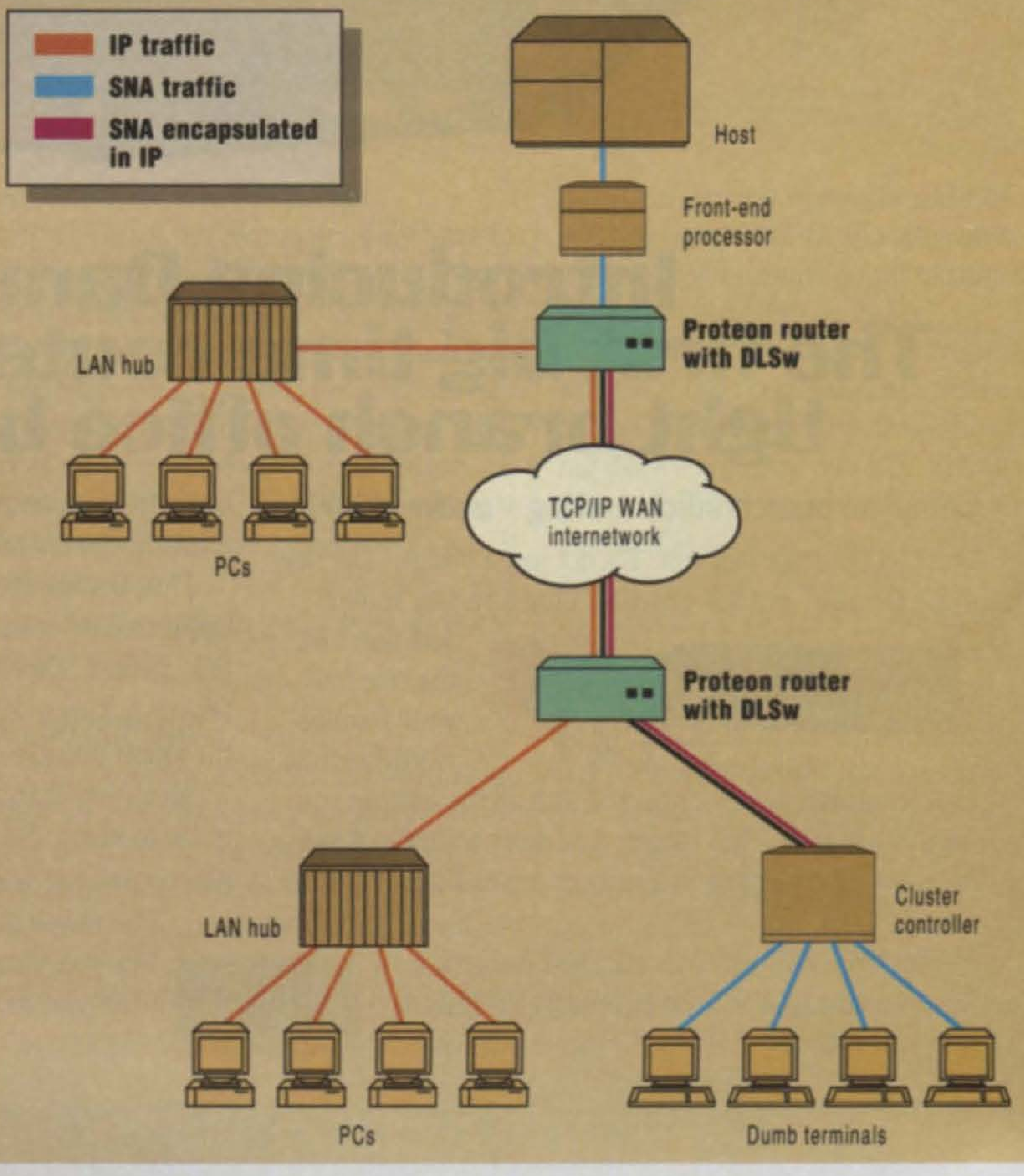
After years of waiting for vendors to pull the trigger, net managers finally have a standard mechanism for bringing SNA traffic into TCP/IP LAN internetworks. That standard, of course, is Data Link Switching, and the vendor that's done the best job of implementing DLSw in its routers is Proteon Inc.

Proteon's success with DLSw comes as a mild surprise considering the technology originally was developed by IBM. But even Big Blue has tacitly acknowledged Proteon's preeminence by licensing Proteon's DLSw code for the IBM 2210 router.

Proteon (Westborough, Mass.) was one of the first router vendors to offer a standard implementation of DLSw, as defined by the Internet Engineering Task

Different Worlds, Same Backbone

Data Link Switching (DLSw) software residing in Proteon routers encapsulates SNA traffic in IP, eliminating the need to have separate backbones for SNA and LAN traffic.


IP traffic
SNA traffic
SNA encapsulated in IP
Host
Front-end processor
LAN hub
Proteon router with DLSw
PCs
TCP/IP WAN internetwork
Proteon router with DLSw
LAN hub
Cluster controller
PCs
Dumb terminals