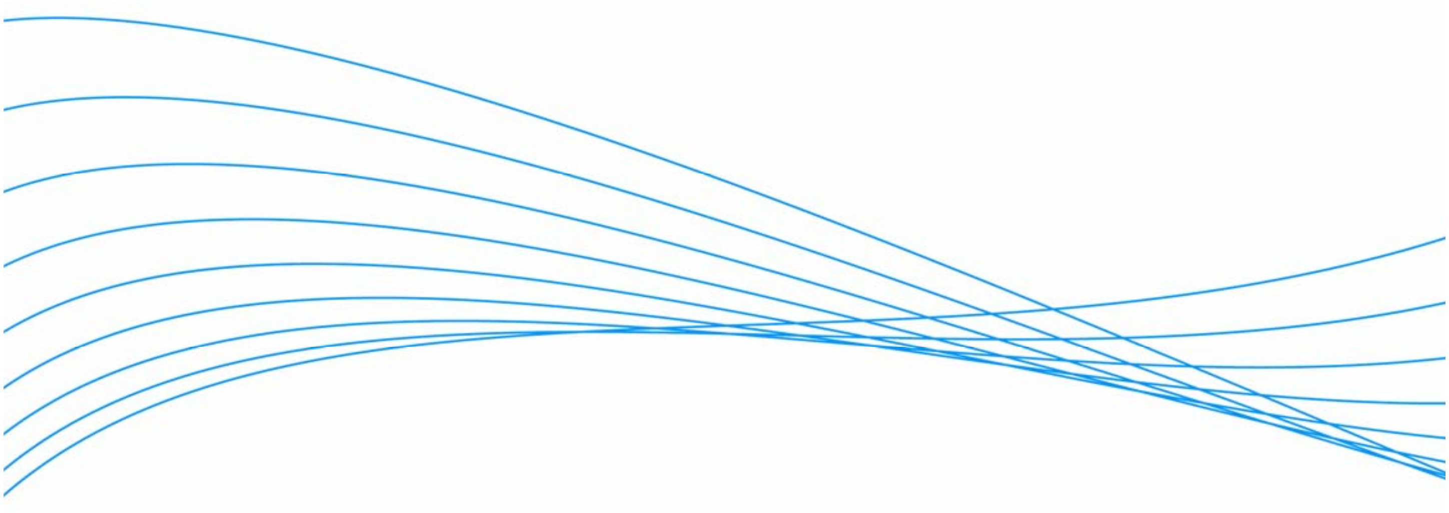
ProCurve Networking by HP

WAN Design Guide

The Lower Layers

August 2005



Introduction

Since the dawn of time we have had the need to communicate at a distance. From the fleet-footed messenger running between small villages to the dawn of the telegraph and telephone the goals have been the same. Bring the message from point “A” to point “B” as quickly as possible, with accuracy in transmission. Later requirements often included cost, but it is not much of a stretch to believe that villages didn’t like loosing fast runners to injury either!

The messages between point “A” and point “B” may have changed and become more sophisticated but the ideas are the same. Today companies that have multiple offices need a cost-effective, efficient means to exchange data between those offices. Many companies have created intranets or extranets, which enable customers at different locations to view information and to upload and download information.

Security is also an issue because often times today the customer’s intranet (internal network) must be connected to the Internet in order to conduct business outside their own company and allow the resources of the Internet in. The various customer location connected through the Internet must be protected by firewalls.

With these considerations to serve us, this paper will stay focused on what are the basic requirements are for the transmission of data and site to site communication. At times we will discuss cost considerations but only at a high level. Reference text books are mentioned in the back of this guide for those requiring further information. We will introduce various example networks to consider using the ProCurve Secure Router 7000dl series.

The intended audience for this guide is the technical consultant, with moderate experience in wide area networking, familiar with the lower four layers of the OSI model, yet who may not be familiar with the ProCurve Secure Router 7000dl series or an expert in WAN technologies. In short the consultant who has been focused on LAN networking but has limited experience with WAN. Even though this is the audience focus, this guide will still be useful at many points even for the most experienced, as it does contain some configuration comparisons between some of the ProCurve and Cisco routers and other relevant information for those more experienced.

This guide will also focus most of its attention on the traditional WAN layers, the physical and data link layers. There are sections discussing the network layer and Internet connectivity, yet considerations at this point will be limited to technology overviews, and configuration examples, with a focus on the ProCurve Secure Router 7000dl series. Design considerations for IP addressing, or consideration of the implications of one dynamic routing protocol over another will not be a major focus of this paper. Never the less there will be references to direct the reader to further information.

Given this scope the main body of this guide will investigate two major domains of wide area network design; Designing the Physical and Data Link Layers, Designing the Network Layer and Internet.

Other highlights within each section are:

- Overview of Technologies
- Summary of Major Points
- How The Technology is Used
- Advantages and Disadvantages
- What to Determine During Planning or for Implementation
- Solution Configuration Examples

Secure WAN Design Overview

Understanding the Customer Requirement

How does one progress from conception to reality in designing their network? This is as difficult to find a single best answer for as if one were to try determining the best earth-bound route to go from Bannock to Frankfurt. No single right answer would be given. But knowing this should not keep you from gathering enough information to make intelligent choices and concessions.

In all cases the reader must remember to work toward a wide area network that is as fast as possible, within any understood constraints, that handles the data accurately and securely, for a reasonable cost. To accomplish this we need to ask some basic questions. Below are some suggested questions to help you get started:

- Is this a new installation or replacing an existing?
- If existing, what problems does the customer currently face that they would like corrected?
- What are the requirements?
- What is the rate of data transfer?
- Must the network be high speed in both directions or only one?

By answering some of these we might determine performance and reliability requirements. Other questions would be:

- What levels of security need to be in place?
- If this customer wants these routers hooked to the Internet then they need to have designed for the stateful firewall and access policies to be in place.
- What would be the areas we could compromise?
- Is high performance is priority at all locations or only at some.
- Are there areas that are not "top priority?"

Other questions would be:

- Is this for data only or is this a combined data and voice solution?
- Is the voice solution traditional TDM voice or Voice over IP?
- Does the customer need a strategy for redundancy?
- If yes then consider, through risk assessment, what should be redundant the WAN links, the carrier or ISP, the routers themselves, the modules in the routers?
- How much monthly cost do I tolerate for one day of downtime?
- Then what would be the best possible network design?
- In order to answer this question the previous questions need to be addressed and then combined with what is available in the locations of the customer locations. Your best possible design will be a combination of requirements aligned with the technologies and services available to accomplish them.

These are just a few of the questions one would need to answer before designing the network.

Finally, as mentioned previously, there are many good reference texts available for your use. If the reader requires further guidance there is a reference section at the end of this paper along with a brief description of the publication to help you determine if you want to purchase the reference or not. There are times when smaller networks and upgrades can be designed with estimates, at other times a much more systematic approach is required. Some would argue as Robert Cahn who writes, "It is not possible to design networks at any scale without algorithms". Yet he also admits, "… Design problems are much too hard to be solved exactly". So although this paper does agree that their needs to be objective analysis and design utilizing tools that are available, its philosophy holds that solid understanding of network communications, along with knowing the basic infrastructure and cost, a designer can come up with a reasonably good design without dependency upon algorithms in every design. To those who have been competent in LAN design can learn WAN technologies and adapt many of them to their current understanding.

This paper will equip the technical consultant with the major tools required for designing wide area networks, with knowledge of the technologies, and understanding of how those technologies may be implemented.

Overview of WAN Environments

In the sphere of wide area networking there are two basic environments or domains; the public domain and the private domain. Consideration for public or private, and surrounding security, must be evaluated at all levels of networking. For example, most would consider the local connection between a private facility, the customer site, and the carrier, to be private. But even this private line is carried in a public domain to some extent. That means we need to consider, at all levels, the risks for security and redundancy. Copper wire can be "tapped"; but copper is the most common local connection, or "local loop", media. If one were to use a wireless connection the problem is more readily seen. "Consideration" does not necessarily mean "implementation" but does still indicate that a consultant perform a risk assessment.

Using public carrier network infrastructure can be more cost effective than using privately owned infrastructure, but this is all dependent upon the customer's relationship with the carrier and what they already have negotiated and may currently be using. In general, public carrier networks allow many subscribers to share the costs of installing, managing, and maintaining the carrier infrastructure so that often times they are lower in cost to each customer using that infrastructure.

Often times the two domains, public and private, are combined to gain the best of both. For example, a customer may want to consider some redundancy between sites. This redundancy could take the form of a primary private network that is backed up by the public Internet. The configuration could be such that the private network is the primary route and the public Internet is secondary.

What is a WAN?

In the most general sense, a Wide Area Network (WAN) is a geographically dispersed telecommunications network. For the purposes of this paper a WAN is generally defined as a network created to connect two or more Local Area Networks (LANs). WAN discussion could include the interconnection between carriers, but this is beyond the scope of this paper.

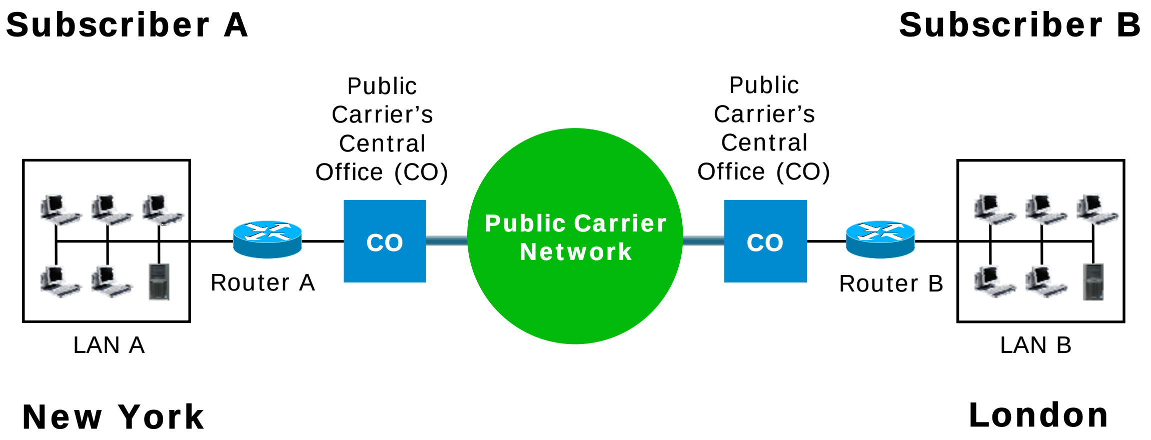


Figure 1: General Carrier Supported WAN in N.A. Needs figure title

WAN connections can connect LANs located in the same city or around the world. A public "carrier" network is commonly used to create WAN connections between LANs in different parts of the world. In most regions it is the Public Telephone and Telegraph (PTT) companies, which serve Mexico, Europe, Asia, South America, and other parts of the world.

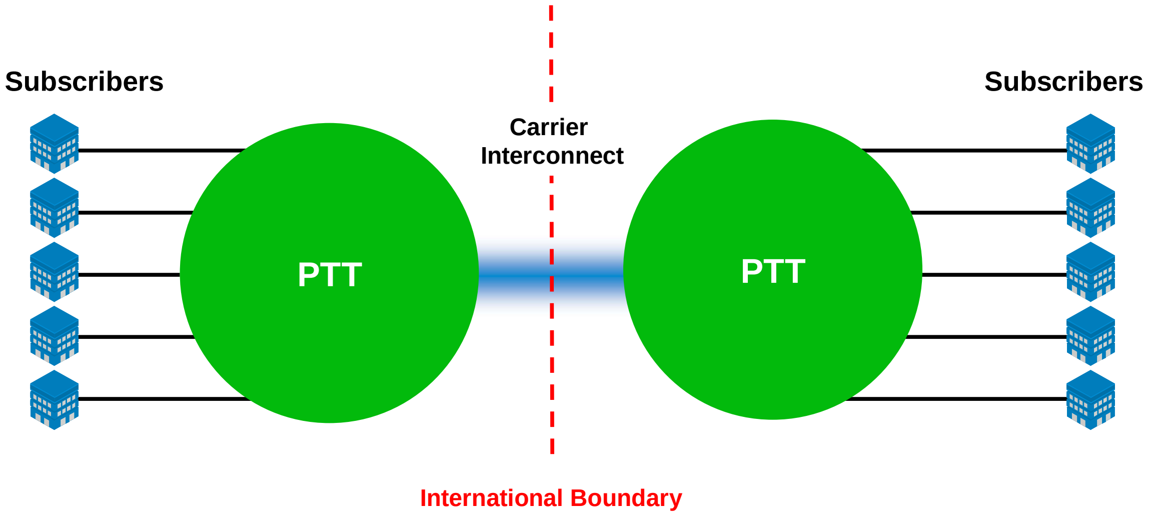


Figure 2: Basic Infrastructure in Most Regions

In Canada and the United States the public carrier networks include what are called "Public Switched Telephone Network (PSTN)".

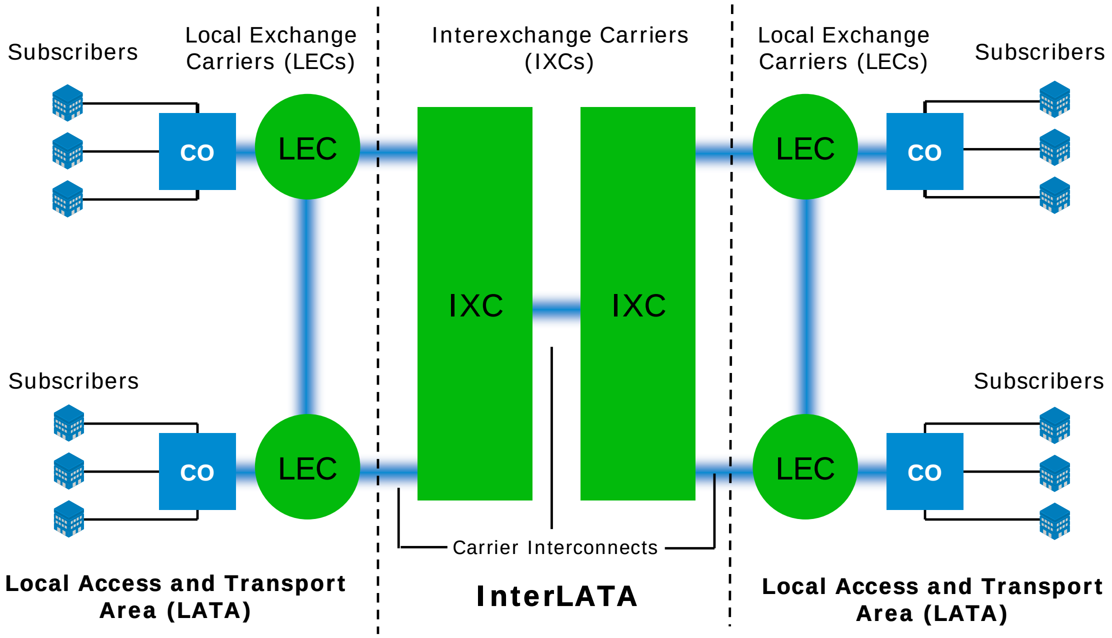

Subscribers
Local Exchange Carriers (LECs)
Interexchange Carriers (IXCs)
Local Exchange Carriers (LECs)
Subscribers
CO
LEC
LEC
CO
IXC
IXC
Subscribers
Subscribers
CO
LEC
LEC
CO
Carrier Interconnects
Local Access and Transport Area (LATA)
InterLATA
Local Access and Transport Area (LATA)

Figure 3: Basic Infrastructure of North America

Over time, through the advent of the Internet and those companies providing services, the "carrier" who previously may only have been connecting the lowest layers, have taken on the name of "Service Provider". Today the terms "carrier" and "service provider" or "Internet Service Provider" (ISP) are sometimes used interchangeably. The ISP can provide basic local connectivity to them, and then further connectivity into the Internet.

Over the past few years there has also been a blending of terms to the point that some technologies once considered MAN (Metropolitan Area Network) are now included in some WAN discussions. This paper focuses on the traditional and historical use of the acronym and therefore deals with the lower speed local loop technologies (If one can rightly call ADSL2+ at 25Mbps a lower speed technology!) and does not discuss SONET/SDH. This cross over, or blending, often occurs from the fact that the WAN needs a WAN as well. The WAN of choice between carriers must of necessity be of much greater speed and capacity since it serves as the "core" of all the customer networks. This is the realm of the telecommunications providers and is beyond the scope of discussion for this paper.

How is LAN different from WAN?

Those familiar with LANs should not abandon all knowledge about them during their quest to understand WAN design. Generally speaking a WAN differs from a LAN in areas regarding reoccurring costs (price), performance, and span:

- Price, since there is often a recurring cost to building a WAN. A LAN is typically installed and the customer owns the wire and underlying switches. In a WAN you work with a vendor (carrier or service provider) and pay them "rent"; the customer leases the lines and services required to get from point "A" to point "B".
- Performance, since there are many differences at the physical layer, distances traveled, and connection setup. LANs today are primarily Ethernet. There is no longer a major change between Layer 1 on LAN such as from FDDI to Token Ring. LANs today are Ethernet. WANs are not there yet. There are many flavors of Layer 2 used in the WAN. Therefore there will be a need to convert Layer 2 and Layer 1, introducing latency. There will continue to be some difference between the transmission speeds on a WAN also because WANs cover great distance, and LAN which are often only 1000 meters from point "A" to point "B". Even if a service provider can provision some flavor of Ethernet, there will still be latency since the distances are much greater. It is also impractical to use broadcast mechanisms for large distances. Additionally WAN technologies must also handle connections, which often are brought up only when needed, keeping costs lower but increasing the time for the first packet to arrive at its destination.
- Span, since WANs connect across vast distances that have no other end-points between point "A" and point "B" and often cross oceans to bring point "A" and point "B" together. Span means more than distance it means population density. A LAN has a dense population of end-nodes on a LAN. A WAN is really a network of point to point, coterminous linkages, whether physical or virtual.

Further consideration for the WAN environment is that data is not transmitted until there is a connection. WAN connections are established at either layer 1 or layer 2 or both. In a LAN the remote end station is always considered to be there. This led to the "send and pray" phrase that meant you could send data but not always know if it got there. Obviously Layer 4 protocols such as TCP would accommodate this, but others such as UDP would not. The main reason connections must be established for a WAN is because no one wants to send data at great distance, pay for the travel charges, and then not have the data be received. Imagine yourself attempting to travel from Singapore to Sydney, arranging the travel, traveling, arriving, going to the final destination hotel, and it was shut down due to reconstruction. Quite the expense with no results! At least you wouldn't be dropped by the destination! Of course there are many "permanent" linkage options in WANs, but you will pay for the privilege of having the link "always connected".

Types of WAN Circuits

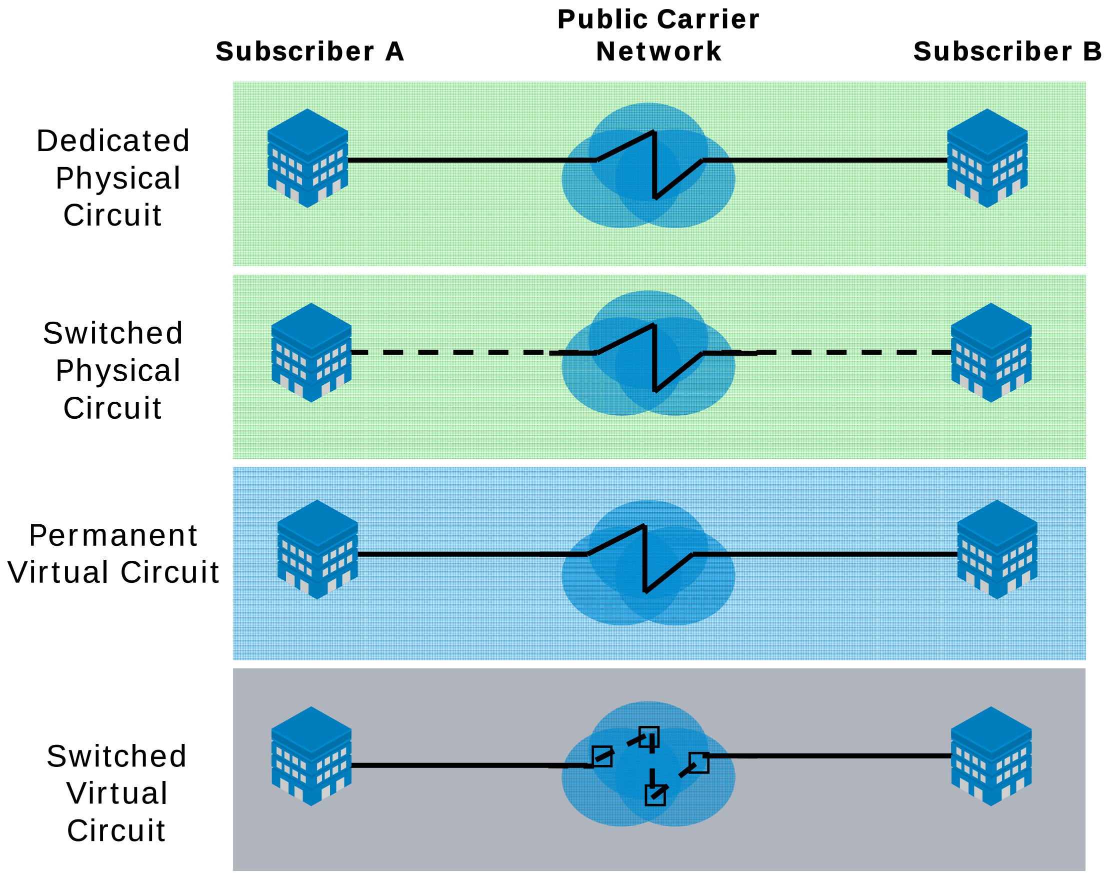

Public Carrier Network
Subscriber A
Subscriber B
Dedicated Physical Circuit
Switched Physical Circuit
Permanent Virtual Circuit
Switched Virtual Circuit

Figure 4: Types of WAN Circuits Illustrated

As the figure above shows, there are four types of circuits used in creating WAN connections when considering both the physical and data link layers:

- Dedicated physical circuits
- Switched physical circuits
- Permanent Virtual Circuits (PVCs)
- Switched Virtual Circuits (SVCs)

Dedicated Physical Circuits

Dedicated circuits are permanent circuits dedicated to a single subscriber. The connection is always active. The subscriber purchases dedicated time slots, or channels, that provide a specific amount of bandwidth that is always available for the subscriber to use. The channels in a dedicated circuit are created using time division multiplexing (TDM), which is discussed later in this section. In addition to providing guaranteed bandwidth at all times, dedicated circuits provide the most secure and reliable WAN connections available.

Switched Physical Circuits

Switched physical circuits are connected upon proper signaling exchange; for example, a phone call. These circuits are “switched” on or “connected” between customers as the call routing demands. The connection is active until one side or the other hangs up. (Next time you are troubleshooting a call duration problem between routers you could just say the other router got angry with you and hung up!).

Seriously though, analog modems and ISDN circuits operate like this. The subscriber purchases the ability to use the circuit but does not pay for the call duration time unless connected. This is what makes these types of circuits useful for backup links.

Permanent Virtual Circuits (PVCs)

PVCs are also permanent circuits dedicated to a single subscriber. The connection is always active. However, because multiple virtual circuits share a physical circuit, there is no guarantee that any specific amount of bandwidth will be available at any specific time. Sometimes there may not be any bandwidth available on the physical circuit because the physical circuit is saturated.

When the physical circuit is saturated, the traffic is temporarily stored at a switching point until bandwidth becomes available. When bandwidth becomes available, the stored traffic is forwarded to its destination. This process is referred to as store-and-forward processing, or packet switching, which is the same processing method used on LANs.

PVCs provide an average bandwidth guarantee. The average bandwidth guarantee is accomplished through statistical multiplexing (STM), which underlies packet switching technology. Because PVCs are more cost effective for the public carrier, PVCs are usually less expensive for the subscriber than dedicated circuits. PVCs are commonly used for Frame Relay, which is explained in detail in Frame Relay section.

Switched Virtual Circuits (SVCs)

SVCs are identical to PVCs in all respects, except that they are temporary physical circuits. SVCs are activated when a subscriber initiates a connection to transmit data. When all data have been transmitted, the connection is deactivated, and the physical circuit resources are made available to other subscribers.

Because of these considerations the WAN is typically built up of many point to point connections, at both layer 1 and layer 2. This can make it difficult for the designer to consider connectivity. To make the routing most efficient the layer 2 network must often be fully meshed, to reduce the number of hops between sites. (A full mesh is one where all sites are completely connected to every other site.) If all traffic goes back and forth from central site to remote, there is little problem. When all sites have to share information equally the number of interfaces required per site, physical or virtual, will be N-1=interfaces, where N equals the number of sites.

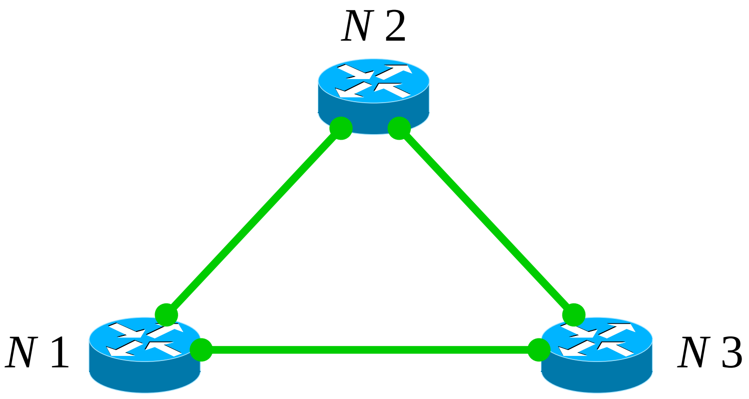


Figure 5: Simplified WAN Physical Layer Connection Paths

This is a simplified look at a private WAN physical layer possibility. Virtual circuits, such as created with Frame Relay, will add another layer of complexity to this and will add connection points if you want a “full mesh” as described with the physical layer example. Notice the example with Frame Relay. Even though there is only one physical connection there are two arrow points at each physical connection. In essence the same formula applies. It is just that you will need to consider both the “raw” physical bandwidth available on a physical single link and then the committed information rate for the two virtual links.

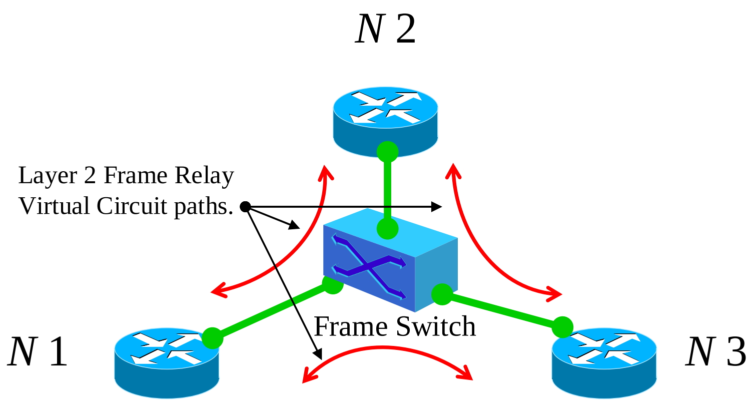


Figure 6: Frame Relay Connection Paths

How is LAN similar to WAN?

Generally speaking a WAN and LAN are similar when considering resource placement. One needs to analyze the traffic flow regarding client to server communication. Some of these things can be estimated (which is required for new installations), sometimes measurement tools should be put in place, but this is not always possible as with a brand new installation. A good discussion with the customer will help determine where the resources are and how often they are accessed by the clients. You will need to understand the customer's use of the following:

- Network protocols and interconnection architectures in general such as Bridging, IP, TCP, and UDP.
- How certain services and infrastructure work such as their Web Server or email.
- What are their requirements for security?
- The topological layout of the WAN – how you want locations to interconnect.
- The cost and performance offerings from various service providers and/or carriers. The logistics and planning for deployment.

You should also consider how the customer network might change over the next months and years in an attempt to allow for that in your planning. It is not possible to predict this with complete accuracy, but will allow you to consider the options.

Note: This paper discusses the standard local loop technologies and the specified bandwidth available for these technologies. Although physical layer bandwidth cannot be increased on an E1 or T1, or exceed certain limits with technologies such as ADSL, there are more than these physical standards that are available to the designer. On the ProCurve Secure Routers 7102dl and 7203dl one can use other link technologies and the 10Mbps serial interface module to connect to "special" modems. Some parts of the world offer wireless transmissions that could run close to 10Mbps. Other parts of the world offer dark fiber to their modems to connect to the serial port. Bandwidth can also be increased though the use of multilink protocols such as Multilink PPP or Multilink Frame Relay, more on those later.

With all of this in mind let's stick with the focus of our paper first. Other considerations can be made later. At this point let's consider performance, getting the data from point "A" to point "B". One simple illustration of this might be seen as the current bandwidth requirement at the central site is only 2Mbps with four remotes feeding it at about 500Kbps each, but you have asked the right questions to determine the four will double to eight in the next six months. You should plan on a minimum of 4Mbps at the central site, and even that may be a little short sighted if you truly double every six months!

We could give you plenty of information in order to help you make the intelligent choice for the network you are designing. The better solution, at least in our estimation, would be to couple the right amount of information with a few examples. Ultimately you need to adapt these to your given situation.

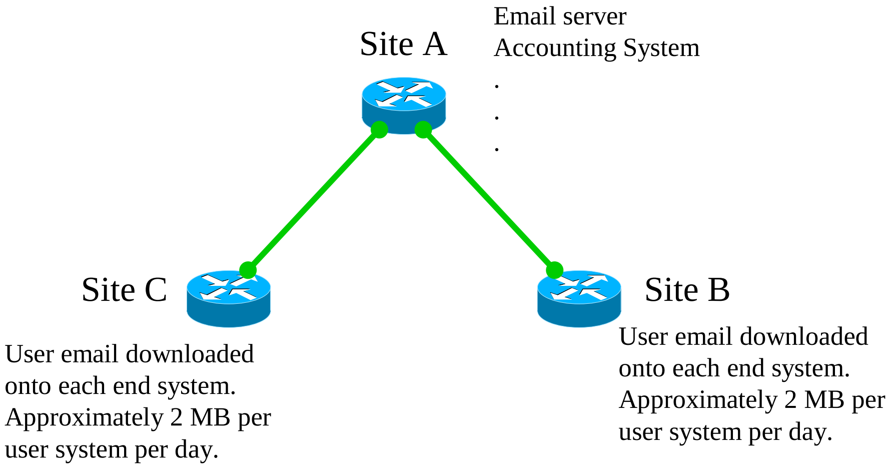


Figure 7: Overly Simplified Sketch of Customer Requirements

A simple approach is to take the customer requirements and begin to sketch them out so that you can see the big picture. In this overly simplified sketch we see that at minimum Site A and Site B will require 2 Mbytes of data in one direction per day per person. Downloading email over an eight hour period that would become:

(2,000,000 bytes * 8 bits/byte) / 8 hours * 60 minutes/hour * 60 seconds/minute = 556 bits/second.

If you have 100 users you can see this is 55.6 Kbps. That is, as you will learn later in this paper, about 1 DS0 on an E1 or T1 channel.

But of course nothing is as simple as we design guide writers stipulate! So with this simple example we have assumed that email is downloaded over the entire 8 hours evenly, but it never is. That is where you come in and adjust up the required bandwidth for bursts and other traffic. It is more likely that between 8:30 and 8:45 AM that at least half of the email is downloaded for the entire day. All of a sudden our 8 hour window is compressed into 15 minutes and must handle 1 Mbyte per user at that time. When you do that same equation you find:

(1,000,000 bytes * 8 bits/byte) / 15 minutes * 60 seconds/minute * 100 users = 889 K bits/second

Now the requirement is nearly a full megabit! But the rest of the day they need very little bandwidth. One thing to note here, this is a simplified and hypothetical example. There are other factors that will shave performance from the raw numbers. One should typically plan for at least a 30% hit simply from packet headers and protocol handshaking. That now means that our requirement of 889 K bps is really a full T1 of at least 1.544 Mbps. 1.544 Mbps less 30% is about 1 Mbps which if rounding is close enough for this type of design to 889 Kbps.

Familiarity with the technologies will allow the consultant to help the customer make decisions about the physical and data link layer requirements. Let’s now look at those lower layer technologies.

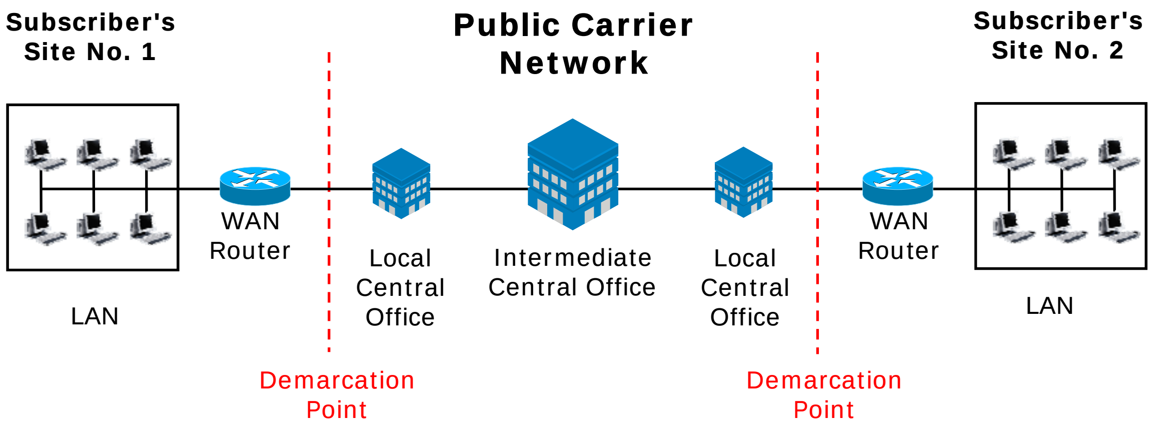


Figure 8: Basic Representation of WAN Path between Sites

At this point we should consider that there are always two sides to every story. Up to this point we have not discussed that there are two sides to every conversation and that the two sites involved in the conversation are subject to a myriad of considerations for performance between them. Some of the things to observe and consider in the figure showing the basic representation of WAN path between sites are:

- What is the number of clients or servers on site one that need access to site two?
- What is the raw bit rate of the traffic flow from site one to site two?
- Is this transmission rate different when sending from site one to two compared to reception? Some technologies, such as ADSL which we'll cover later, are asymmetrical.
- Is the full bit rate available for data or do the sites under consideration allow for some channels of the T1 or E1 link to be used for telephony?
- Is site one primarily comprised of a single VPN client that requires access to site two?

This final question is an interesting one to consider more closely. For example, is site one primarily comprised of a single VPN client that requires access to site two? In this case the client VPN perspective is just as important as the router side. The multitude of connection points between client and router in this case is an ominous factor. Considering all points in the path between point “A” and point “B” are essential in properly explaining the real performance potential of this path. What bandwidth is available to the VPN client of site one?

Considering the single VPN client on a home or small business network it doesn't matter too much what the link speed from the client to the router is, but the limiting factor would be the WAN link. That client is going to get all the bandwidth to the router to use for their transmission. They share with only one person so they get 100% of available LAN bandwidth. On the other hand, if there are many clients funneling data through that router, then the link to the router is technically “shared” by all the users even though it may be coming from a link on a switch! Regarding the aspect of sharing the data path we see that WAN links are similar. The WAN link is shared by all others require data through it.

Another characteristic differentiating WAN from LAN is that the upper layer protocols, more specifically the dynamic routing protocols, should be constructed to run efficiently. Responsiveness to routing changes can come at the expense of delivering critical data traffic. Advances in Ethernet throughput in LAN technology over the past few years has dramatically reduced the need to consider congestion, since switched Ethernet congestion (which is no longer really Ethernet as we once knew) caused by running at 0.1, 1, and 10Gbps speeds is not typically congested at the physical and data link layers. We have grown accustomed to so much speed that there was little need to consider congestion on a link! This is different for WAN. Dynamic routing protocols can consume valuable bandwidth unless properly architected and since the customer will always pay for “renting” or “leasing” of WAN links, they will always pay a price for dynamic routing protocol overhead. Techniques such as route summarization and proper use of OSPF or BGP can effectively control the potential problem.

Designing the Physical and Data Link Layers

An Overview of the Local Loop (The Transmission Technologies)

Executive Summary

The local loop is the connection from the customer site to the service provider or carrier. They typically work across 2 or 4 wire copper links, though fiber is also used. They are fixed bandwidth (T1, E1, ISDN, and some types of DSL), or are variable bandwidth such as ADSL. Usable bandwidth for T1 is up to 1.536 Mbps, E1 is 1.92 Mbps, and ADSL up to 25Mbps downstream but is quite dependant upon distance and link conditions and that is only in one direction.

Costs for these general transmission technologies vary globally. Without cost as a consideration the choice will be for using guaranteed fixed bandwidth. These are typically T1 or E1 circuits. When cost is a consideration, often ADSL or ISDN will be the link of choice. Some parts of the world can only get ISDN so the question is answered “by default” for those areas.

Overview

All WAN connections consist of three basic elements:

- The physical transmission media.
- Electrical signaling specifications for generating, transmitting, and receiving signals through various transmission media.
- Data-link–layer protocols that provide logical flow control for moving data between peers in the WAN. (Peers are the devices at either end of a WAN connection.)

Note: This is a brief overview. If you need further information please see the references at the end of this paper.

The physical transmission media and electrical specifications are part of the physical layer (layer one) of the Open Systems Interconnection (OSI) model, and data-link–layer protocols are part of the data-link layer (layer two). They are used to create WAN connections into and through public carrier networks.

The connection between a subscriber’s premises and the public carrier’s nearest central office (CO) is referred to as the local loop. The local loop includes the entire telecommunications infrastructure—such as repeaters, switches, cable, and connectors—required to connect a subscriber’s premises to the CO.

Public carrier networks were originally designed to carry analog voice calls. Therefore, copper wire is the most common physical transmission media used on the local loop. Because of the limits in the signal-carrying capacity of copper wire, local loops that use copper wire are the slowest, least capable component of a WAN connection. Public carriers are beginning to install coaxial and fiber optic cable in local loops to meet ever-increasing bandwidth demands.

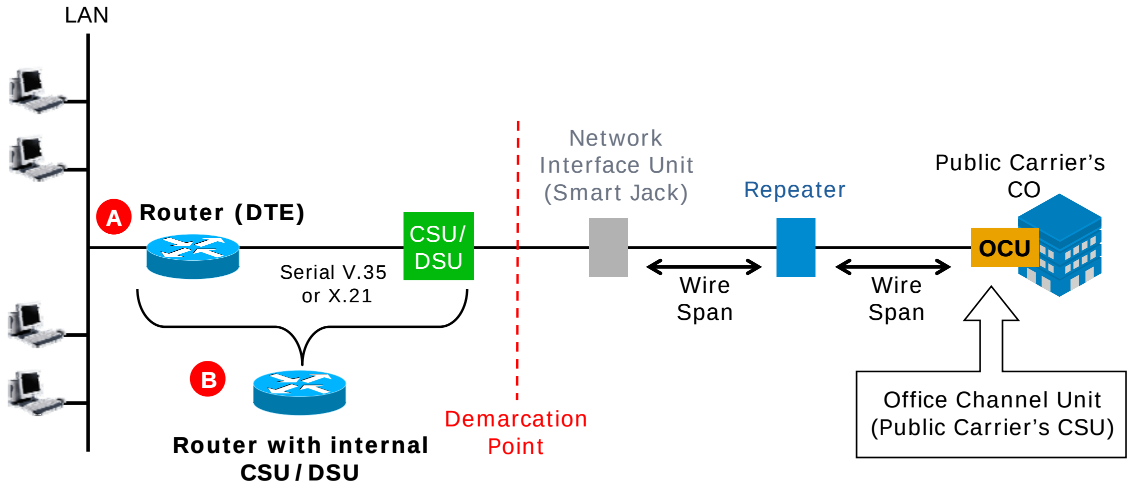


Figure 9: Infrastructure Common to Carrier Local Loops

T1 and E1 Technologies

T1 and E1 are basically defined as series of DC pulses that are generated at the rate of 1,544,000 pulses per second for T1, or 2,048,000 pulses per second for E1. At the time of the introduction of T1 many decades ago, it was designed to utilize the existing cable infrastructure in North America. The T1 "bit" rate was determined due to the degradation of the signal across the two pair cables (TX-RX). The design engineers determined that a 1.544 Mbps signal rate was the highest they could regenerate at 6000 ft. (the distance between manhole covers in a typical U.S. city). These pulses could then be grouped together and "Channelized" through Time Division Multiplexer techniques to carry 24 separate channels. E1 differs from T1 primarily because it has 32 channels, a different encoding scheme, and different framing.

Depending on the particular use of T1 or E1, you may see differing rates published. For example you may only have 30 or 31 64Kbps channels available on an E1 circuit since some of the channels may be used for "signaling". An E1 bit rate of 2.048Mbps is still valid, but the bit rate is not equivalent to usable bandwidth since encoding, framing and signaling overhead are factors detracting from the raw bit rate available. More on this later.

A carrier WAN T1 or E1 connection provides a permanent, dedicated, point-to-point, fixed-bandwidth link between two endpoints. Unless the service provider changes the path, the data sent between the two endpoints in a carrier line WAN connection always flow along the same physical path.

The bandwidth for each connection is guaranteed across all parts of the path, because each connection is allocated dedicated time slots, end-to-end. If there is no traffic to transmit, the time slots for that connection go unused.

Note: T1 and T3 carrier lines are used primarily in Canada and the United States. In Europe and other Sector locations that follow the ITU Telecommunications Standardization (ITU-T) standards, the comparable dedicated, high-speed WAN connections are E1 and E3 carrier lines. J1 and J3 carrier lines were defined for use in Japan.

T-carrier WAN connections are based on the American National Standards Institute (ANSI) T1.102 and T.107 specifications. A T1 WAN connection provides twenty-four 64Kbps DS0 channels for a total of 1.544 Mbps as a data rate. After this point, dependant upon the framing and formatting chosen, the available data rate can fall as low as 1.344Mbps (AMI encoding), or more typically today 1.536 (B8ZS encoding). The loss of 8Kbps is formatting overhead. ProCurve Secure Routers default to B8ZS.

A full T1 connection uses all 24 DS0s. Fractional T1 connections, which use fewer than 24 DS0s, are also available. The channels in a T1 connection can be used for voice traffic, data traffic, or a combination of the two, but all traffic moving through the connection is in digital form.

Note: In North America, a subscriber's site is connected to the central office (CO) of a local exchange carrier (LEC) that provides the T1 WAN connection. T1 WAN connections can also be created through multiple LECs and interexchange carriers (IXCs), as needed, to link two subscribers' premises together.

E-carrier lines are based on a range of specifications from the ITU from G.703 to G.822. An E1 WAN connection provides thirty-two 64Kbps DS0 channels with 2.048 Mbps in total bit rate.

The bit rate of an E1 WAN connection is greater than that of a T1 WAN connection simply because there are more DS0 channels (64K channels) available for data. There are differences in framing and encoding, but collectively the E1 DS0s provide 32 times 64Kbps or 2.048Mbps. These 32 DS0s are collectively referred to as bandwidth, yet the precise amount available as "raw" bandwidth is dependent upon the usage for the circuit. An E1 effectively provides either a total of 1.984Mbps or 1.920Mbps, or 31 and 30 channels respectively, dependant upon whether the design requires use of channel 16 for signaling. Some of this potential overhead comes from the use of channel 16 for signaling. Channel 16 signaling is referred to as TS16 (Time Slot 16) signaling. So a full E1 carrier WAN connection uses either 30 or 31 DS0s. Fractional E1-carrier WAN connections, which use fewer than 30 channels, are also available. The channels in an E1 WAN connection can be used for voice traffic, data traffic, or a combination of the two, but all traffic moving through the connection is in digital form.

E1 is available in balanced (120 Ohm with BNC connectors) or in unbalanced mode (75 Ohm with RJ45 connector).

J-carrier WAN connections are a closely related variant of T-carrier WAN connections.[i]

Please use the reference material listed at the end of this paper for further information about T-carrier, E-carrier, and J-carrier technologies.

Summary of Major Points

- Actual bit rate for T1 is 1.544 Mbps, E1 is 2.048 Mbps. Usable bit rate that can be considered "bandwidth" is as low as 1.344 for T1 and 1.920 for E1 yet these numbers vary with use model and implementation.
- Both are fixed bandwidth.
- The links are always active by default – a permanent circuit.

How This Technology is Used

- To connect from customer site routers to carrier or ISP.
- It can carry both data and traditional voice conversations.
- Multiple T1 or E1 links may be combined to make one larger logical interface through the use of layer 2 protocols like Multi Link Frame Relay and Multi Link PPP.

Advantages

The advantages to the T and E carrier technologies are because of fixed bandwidth, dependant upon the technology. Bandwidth is constant and is available symmetrically. These technologies are well established and interoperability should rarely be a concern once the proper encoding and framing are set on both ends of the link.

Disadvantages

Speed relative to ADSL. See ADSL discussion following this section. ADSL can, under proper conditions, deliver many times the performance of E1 or T1 but only asymmetrically.

What to Determine During Planning or for Implementation

- Cost for given distance covered on each link
- Channels available for your data, all 24, or 30, or some fraction?
- Frame Type? For T1 the ProCurve Secure Router 7000dl series supports D4 (SF) or ESF. For E1 the ProCurve Secure Router 7000dl series supports FAS with optional CRC-4.

- Will voice services also be carried on this link?
- Encoding type? For T1 the ProCurve Secure Router 7000dl series supports AMI or B8ZS. For E1 the ProCurve Secure Router 7000dl series supports AMI or HDB3.
- The ProCurve Secure Router 7000dl series currently supports the RJ45 connector for E1.

ADSL Technology:

ADSL, and xDSL technologies in general, provide high-speed WAN connections over existing local loops. To increase the amount of data that can be transmitted over the local loop (which is typically comprised of plain copper wires), xDSL technologies employ advanced modulation techniques.

ADSL, in particular, was developed to alleviate a critical problem facing public carriers—congestion in the public carrier network. With the increasing popularity of the Internet, more and more businesses and residential customers began to connect to the Internet through the public carrier network. Because the public carrier network was designed to handle random, short-term phone calls, carrying the traffic created by numerous, lengthy Internet connections began to overwhelm the voice switches in the public carrier network.

ADSL is only one of many types of DSL technology. Historically, as DSL technologies developed, the collective group were often referred to as “xDSL” where the “x” is replaced with a letter that represents a particular type of DSL, such as ADSL (Asymmetric DSL), HDSL (High bit rate DSL), and Very high bit rate DSL (VDSL). The various types of xDSL provide different speeds, and the speed necessarily determines how each type of xDSL is used. Over time the “xDSL” reference has changed and is simply now referred to as “DSL” when discussing the collective group of technologies.

Because DSL works over existing local loops, it is a cost-effective WAN technology for both public carriers and customers. By performing minimal adjustments to the existing copper lines that are used for most local loops, public carriers can offer customers a high-speed broadband connection. In addition, DSL does not require repeaters as T1 or E1, so it is less costly to implement than other traditional local loop technologies. DSL is also an attractive solution for a wide range of customers, from residential customers to large corporations.

With DSL the connection is always on. For customers who have used dial-up connections, this is a distinct advantage—saving time because there is no dial-up process and eliminating the frustrations (such as busy signals and disconnections) often associated with dial-up connections.

DSL has some disadvantages, however. For example, in the past, DSL has suffered from a lack of standards, or better put, a lack of agreement on which standards to implement. Equipment was often proprietary and did not interoperate. This is changing as standards groups further refine specifications for various types of DSL.

In addition, DSL is not available in all areas because it is a distance-sensitive technology. If a company or home is too far away from the public carrier’s central office (CO), DSL is not an option. The distance between the company or home and the CO also dictates DSL transmission rates. The greater the distance, the slower the rate.

DSL WAN connections can be either symmetric or asymmetric, depending on how data is transmitted upstream and downstream. Downstream refers to the traffic being sent from the service provider or public carrier to the customer’s premises. Upstream refers to the traffic being sent from the customer’s premises to the service provider or public carrier.

If a DSL technology is symmetric, data is transmitted at the same speed both upstream and downstream. This is sometimes called duplexed DSL. To avoid confusion with the more mainstream use of duplexing (bidirectional transmissions), the term duplexed DSL is not used in this paper. Companies should select a symmetric DSL solution for environments such as the following:

- The DSL WAN connection is linking two office sites and equal amounts of data are transmitted to each site.

- Companies need to provide high-speed access to their network or web servers. In this case, the upstream transmission speed would affect customers' ability to access and download information from the companies' servers.

If a DSL technology is asymmetric, it provides different transmission speeds for upstream and downstream. The transmission speed for downstream is higher than the transmission speed for upstream. This makes asymmetric DSL ideal for Internet use because customers typically download more data from the Internet then they upload. Below are tables of both asymmetrical and symmetrical DSL technologies with their typical speeds, distances, and usages.

DSL Technology	Speed	Distance	Usage
IDSL	Up to 144 Kbps	5.49 km (18,000 ft.)	Internet access, video, telephony, IP telephony
HDSL	1.544 Mbps (T1) 2.048 Mbps (E1)	2 pairs of wire; 3.66–4.57 km (12,000–15,000 ft.)	T1/E1 local loop, WAN connection for businesses
HDSL2	1.544 Mbps (T1) 2.048 Mbps (E1)	2 pairs of wire; 3.66–4.57 km (12,000–15,000 ft.)	T1/E1 local loop, WAN connection for businesses
SDSL	1.544 Mbps (T1) 2.048 Mbps (E1)	3.05 km (10,000 ft.)	T1/E1 local loop, WAN connection for businesses
SHDSL	2.3 Mbps	1 pair of wire; 5.49 km (18,000 ft.)	WAN connection, video, multimedia
VDSL*	Up to 34 Mbps	.305–1.37 km (1,000–4,500 ft.)	Multimedia, HDT
* Can be either symmetric or asymmetric; usually asymmetric			

Table 1: Table of Asymmetrical DSL Technologies

DSL Technology	Speed	Distance	Usage
ADSL	Downstream: 1.5 to 8 Mbps	3.66 – 5.49 km	Internet access, remote, LAN access, VPNs, VOIP
	Upstream: Up to 1.544 Mbps	(12,000–18,000 ft.)	
ADSL Lite (G.Lite)	Downstream: 1 Mbps	5.49 km (18,000 ft.)	Internet access, video telephony, IP telephony
	Upstream: 512 Kbps		
RADSL	Downstream: 1.5 to 8 Mbps	3.66 – 5.49 km	Internet access, remote, LAN access, VPNs, VOIP
	Upstream: Up to 1.544 Mbps	(12,000–18,000 ft.)	

DSL Technology	Speed	Distance	Usage
ADSL2	Downstream: 12 Mbps	3.84 – 5.67 km	Internet access, video, remote LAN access, VPNs
	Upstream: Up to 1.544 Mbps	(12,600–18,600 ft.)	
ADSL2+	Downstream: Up to 25 Mbps	1.52 km (5,000 ft.)	Internet access, video, remote LAN access, VPNs
	Upstream: Up to 1.544 Mbps		
VDSL*	Downstream: 13 – 52 Mbps	.305 – 1.37 km	Multimedia, HDTV
	Upstream: 1.5 – 2.3 Mbps	(1,000 – 4,500 ft.)	
* Can be either symmetric or asymmetric; usually asymmetric			

Table 2: Table of Symmetrical DSL Technologies

ADSL is arguably the most standardized type of DSL available. ADSL also supports analog voice on the local loop. This gives ADSL a clear advantage over DSL technologies because customers do not need a separate pair of wires to transmit analog voice. Their existing telephone equipment can continue to send voice traffic over the same pair of wires that carry ADSL traffic. In the ADSL standards, support for analog voice is called ADSL over Plain Old Telephone Service (POTS), or ADSL Annex A.

In addition to supporting analog voice, ADSL supports ISDN traffic. Customers who have ISDN equipment such as telephones and fax machines can continue using this equipment while moving their Internet or WAN connection to ADSL. Support for ISDN is called ADSL over ISDN, or ADSL Annex B, and is common in countries such as Germany where ISDN is widely implemented.

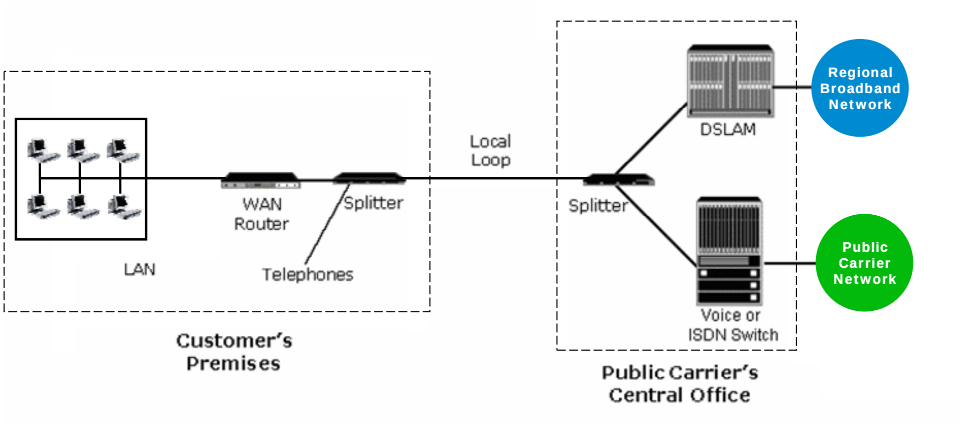


Figure 10: Typical Infrastructure of ADSL WAN

This figure illustrates a company's ADSL WAN connection. The WAN router functions as an ADSL transceiver, performing the modulation required to send data at ADSL speeds across the local loop to the public carrier's CO. At the CO, the DSLAM (Digital Subscriber Line Access Multiplexer) aggregates ADSL connections from multiple customers and creates one high-capacity connection to the regional broadband network. This regional broadband network provides the backbone to connect DSLAMs from multiple public carriers and connects each DSLAM to the Internet.

Because ADSL supports analog voice or ISDN traffic, the local loop is a shared medium. In an ADSL Annex A environment, telephones send analog voice over the local loop, and the WAN router sends digital data. At the CO, the analog voice must be transmitted to the voice switch and then routed over the public carrier network. The digital data, on the other hand, must be transmitted to the DSLAM and then routed over the regional broadband network. At the customer's premises, the analog voice must be sent to the telephones, and the digital data must be sent to the WAN router.

To separate the analog voice from the ADSL data, a POTS splitter is installed at both the customer's premises and the public carrier's CO. The POTS splitter filters the traffic at both ends of the local loop and ensures that the analog voice and the ADSL traffic are sent to the appropriate device at each location.

In an ADSL Annex B or Annex C environment, ISDN equipment and the WAN router transmit data over the local loop. At the CO, the ISDN traffic must be transmitted to the ISDN switch and then routed over the public carrier network. The ADSL data must be transmitted to the DSLAM and then routed over the regional broadband network. At the customer's premises, the ISDN data must be sent to the ISDN equipment, and the ADSL data must be sent to the WAN router.

To separate the ISDN data from the ADSL data, an ISDN splitter is installed at both the customer's premises and the CO. This splitter ensures that each type of traffic is transmitted to the appropriate device at each location.

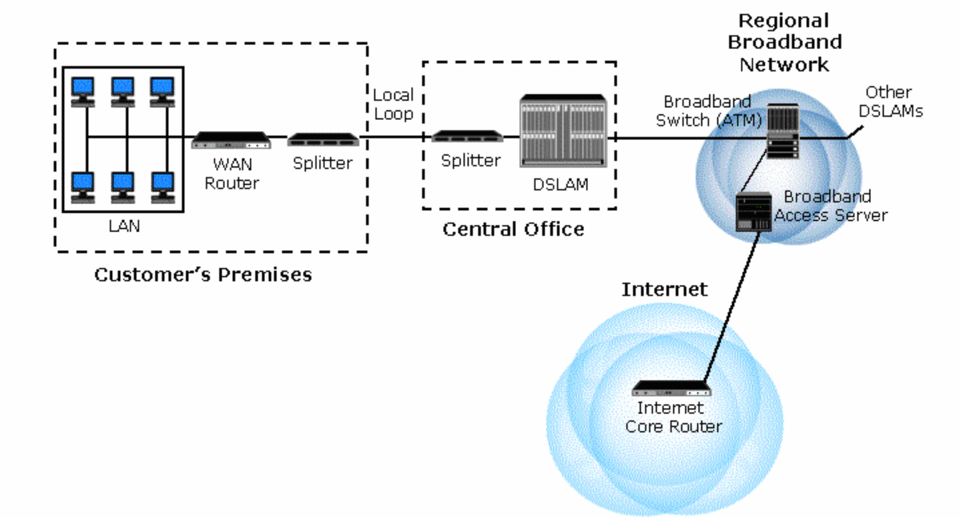


Figure 11: ADSL Internet Connection

As mentioned earlier, ADSL is ideal for Internet access. To enable this Internet access, the regional broadband network must be connected to the Internet. In this figure, the DSLAM connects directly to a broadband switch, which is connected directly to a broadband access server. The broadband access server then connects directly to a core Internet router. As the name suggests, the broadband access server authenticates customers accessing the Internet through the broadband access network.

This figure shows one possible way to connect the DSLAM to the Internet. The exact configuration varies, depending on factors such as the following:

- The capabilities provided by the DSLAM
- The broadband network equipment that the public carrier owns
- The technology used to create the broadband network

In addition to aggregating multiple DSL connections, new DSLAMs provide advanced capabilities such as ATM switching. In this case, the DSLAM may be connected directly to the broadband access server or even to a core Internet router. The DSLAM may also be connected directly to the core Internet switch if the public carrier owns that switch.

Finally, the public carrier must configure the DSLAM to support the technology used to create the broadband network. Because DSL was originally developed for use with ATM-based broadband networks, this is still the most common architecture. In fact, when ADSL Lite is implemented without splitters, ATM is required: ATM cells must be included within the ADSL Lite frames.

Despite this ATM legacy, some public carriers and DSL vendors are investigating and implementing other technologies for the broadband network. For example, the broadband network could be an Ethernet-aggregation network linked together by a group of high-capacity switches.

Proponents of Ethernet-aggregation networks point to benefits such as lower costs, enhanced scalability, enhanced support for services such as multimedia, more quality of service (QoS) features, and greater resilience. Public carriers in Asia have already begun implementing Ethernet-aggregation networks.

Even if a majority of public carriers begin to migrate their broadband networks to Ethernet-aggregation networks, ATM will have an ongoing role in DSL networks for some time. There is a large installed base of ATM-based broadband networks, and because DSL was designed to work with ATM, ATM protocols are often exchanged between the DSL transceiver and the DSLAM.

Finally there are many different Annex specifications for DSL technologies. Two of primary importance for ADSL are Annex A which is ADSL over POTS and the other, Annex B, which is ADSL over ISDN. Below is a simple table comparison of the two supported standards:

Annex A – ADSL over POTS	Annex B – ADSL over ISDN
Connector RJ-11C	Connector RJ-11C (some countries use an RJ-45 connector. Germany is one example)
ADSL2 - ITU G992.3	G.DMT – ITU G992.1
ADSL2+ - ITU G992.5	Multi-Mode – Auto detect mode
G.DMT - ITU G992.1	
G.LITE - ITU G992.2	
Multi-Mode - Auto detect mode	
READSL2 - ITU G992.3 Annex L	
ATM Multiple Protocol over AAL5 (RFC2684)	ATM Multiple Protocol over AAL5 (RFC2684)
ATM Forum UNI 3.1/4.0 PVC	ATM Forum UNI 3.1/4.0 PVC
ATM Class of Service (UBR)	ATM Class of Service (UBR)
PPP over ATM (RFC2364)	PPP over ATM (RFC2364)
PPP over Ethernet (RFC2516)	PPP over Ethernet (RFC2516)
ATM F5 OAM	ATM F5 OAM

Table 3: ADSL Annex A and Annex B Comparison

Summary of Major Points for ADSL

- Speeds for different types of ADSL
- Always on.
- Asymmetrical bandwidth.
- Different Annex for ISDN.

How This Technology is Used

- To connect from customer site routers to ISP.
- It can carry data while allowing traditional voice conversations on existing voice equipment.

Advantages

Because ADSL works over existing local loops, it is a cost-effective WAN technology for both public carriers and customers. By performing minimal adjustments to the existing copper lines that are used for most local loops, public carriers can offer customers a high-speed broadband connection. In addition, ADSL does not require repeaters, so it is less costly to implement than other local loop technologies. ADSL is also an attractive solution for a wide range of customers, from residential customers to large corporations.

Customers, on the other hand, get a high-speed connection at a relatively low cost. For example, ADSL is less costly than T1- or E1-carrier lines.

With ADSL, the connection is always on. For customers who have used dial-up connections, this is a distinct advantage—saving time because there is no dial-up process and eliminating the frustrations (such as busy signals and disconnections) often associated with dial-up connections.

Disadvantages

ADSL is not available in all areas because it is a distance-sensitive technology. If a company or home is too far away from the public carrier's central office (CO), ADSL is not an option.

The distance between the company or home and the CO also dictates ADSL transmission rates; the greater the distance, the slower the rate. This makes if very difficult to plan for bandwidth.

This author has not heard of committed information rates with ADSL and Internet connectivity. There is no guarantee of bandwidth.

What to Determine During Planning

- How far are my sites from the carrier's central office?
- Do the local carriers supply ADSL to that location?
- Can the design allow for asymmetrical bandwidth? Is most of the traffic flow in one direction?
- Will the customer site connect through to the carrier's IP packet network to be routed over the Internet or into an ATM network for a private WAN?

The ProCurve Secure Router 7000dl series currently support ADSL2+ in both Annex A and Annex B.

Current Support for Annex A	Current Support for Annex B
ITU G.992.1 – Annex A (G.dmt)	ITU G.992.1 – Annex B (G.dmt)
ITU G.992.2 – Annex A (G.lite)	ITU G.992.3 – Annex B ADSL2 (G.dmt.bis)
ITU G.992.3 – Annex A ADSL2 (G.dmt.bis)	ITU G.992.5 – Annex B ADSL2+
ITU G.992.3 – Annex L READSL2	
ITU G.992.5 – Annex A ADSL2+	
ANSI T1.413 Issue 2	

Table 4: Current ProCurve Support Capabilities

ISDN

ISDN is a dial-up or, switched circuit, technology for WAN connections that was originally intended to support voice, data, fax, and video services over standard telephone lines. Although ISDN is a multipurpose solution, its core strength today is the ability to dial for connection before data transmission. This relatively high-speed dial capability makes it suitable for backup link scenarios.

In North America, ISDN appears to have a dwindling role as a primary WAN connection. Other parts of the world use it more frequently. Many public carriers are promoting Digital Subscriber Line (DSL) connections, rather than ISDN. There are at least two reasons for this trend: First, DSL transmits data faster than ISDN does. Second, DSL does not overload the switches that handle voice traffic through the public carrier network. Instead, public carriers use data switches and routers to transmit DSL data. For more information about DSL please see the section above or the references at the back of this paper.

However, there is at least one region where ISDN is still frequently used as a primary WAN connection. In Europe, many public carriers actively sell ISDN as a primary WAN connection. Because these public carriers have replaced their analog switches with digital switches, they have the capacity to provide ISDN.

Note: In most regions, however, companies are implementing ISDN as a cost-effective backup to a carrier line WAN connection. If the carrier line WAN connection is unavailable, the WAN router can use the ISDN WAN connection to send data.

In addition to these traditional implementations, some public carriers are offering a special ISDN implementation for retail business that need to get approval on customers' credit cards. This special implementation is discussed in more depth in later in this module.

ISDN provides an end-to-end digital connection between the source device and the destination device. Because ISDN is a digital connection, it is not limited to the 56 Kbps maximum dial-up speed of an analog connection. Instead, ISDN provides transmission speeds of 64 Kbps and above. The exact transmission speed depends on the type of ISDN service and the region in which the service is delivered.

Public carriers offer two ISDN services:

- Basic Rate Interface (BRI)
- Primary Rate Interface (PRI)

BRI ISDN provides a transmission rate of 64 Kbps or 128 Kbps, while PRI ISDN provides a transmission rate of 1.544 Mbps or 2.048 Mbps. (The next sections describe these services in more depth.) BRI ISDN is provided across the twisted-pair cable that is used for ordinary telephones. PRI is provided as a T1 connection in North America and Japan, or as an E1 connection in Europe and Asia.

On the local loop, ISDN requires at least Category-3 (CAT-3) unshielded twisted pair (UTP). The number of wires required depends on the ISDN service that you purchase: BRI ISDN requires two wires, or one twisted pair. PRI ISDN requires four wires, or two twisted pairs.

When ISDN is implemented, the local loop is set up for BRI or PRI service. At the public carrier's central office (CO), the office channel unit (OCU) multiplexes and de-multiplexes channels on the twisted pair wiring of the local loop. Like the channels for carrier lines, ISDN channels are based on DS0 or E0 and created through time division multiplexing (TDM). With BRI ISDN, the OCU multiplexes three channels. With PRI ISDN, the OCU multiplexes 24 or 32 channels, depending on the region.

Because ISDN is a dial-up connection, it establishes a switched virtual circuit (SVC) when the subscriber initiates or receives a call. For the duration of the call, the physical path through the public carrier network is fixed. However, when the call is terminated and a new call is made, ISDN establishes another physical path through the public carrier network.

A separate signaling channel is used called D-channel to setup and release a data channel (B-channel). The network layer of the D-channel has not been defined in such details as the lower layers, therefore different protocol implementations exist which are sometimes referred to as “switch types”.

ISDN Equipment at the Subscriber's Premises

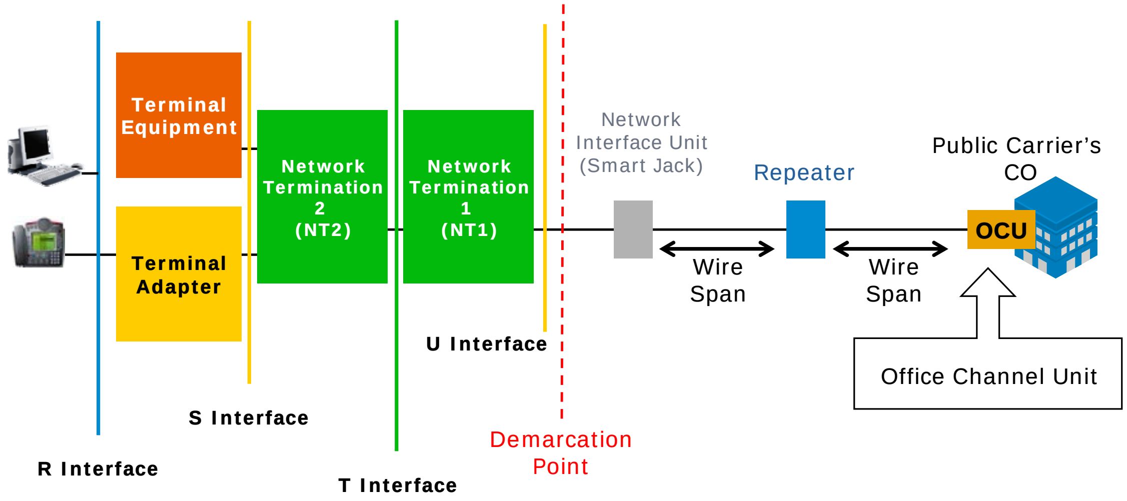


Figure 12: ISDN Equipment at the Subscriber's Premises

The equipment required on the subscriber's side of the loop varies, depending on the region and the public carrier that is providing the ISDN service. This section explains the equipment that is generally used in an ISDN network.

Network Termination 1

On the subscriber's side of the local loop, the Network Termination 1 (NT1) provides the physical and electrical termination for the ISDN line. The NT1 monitors the line, maintains timing, and provides power to the ISDN line.

In Europe and Asia, the public carriers supply the NT1 device. In North America, however, the subscriber provides the NT1 device. Many vendors are now building the NT1 directly into ISDN equipment such as routers.

PRI ISDN also requires a Network Termination 2 (NT2) device. NT2 provides switching functions and data concentration for managing traffic across the multiple B-channels.

In many regions, NT1 and NT2 are combined into a single device. In ISDN terminology, the device that combines these functions is called an NT12 (NT-one-two) or just NT.

Terminal Equipment

Any device—such as a telephone, fax machine, or router—that connects to an ISDN line is called terminal equipment. Two types of terminal equipment are associated with an ISDN connection:

- Terminal equipment 1 (TE1)
- Terminal equipment 2 (TE2)

TE1 devices are ISDN ready and can be connected directly to the NT1 or the NT2. TE1 devices include routers, digital phones, and digital fax machines.

TE2 devices do not natively support ISDN and cannot connect directly to an ISDN network. TE2 devices require a terminal adapter (TA) to convert the analog signals produced by the TE2 device into digital signals that can be transmitted over an ISDN connection. TE2 devices include analog telephones and analog fax machines.

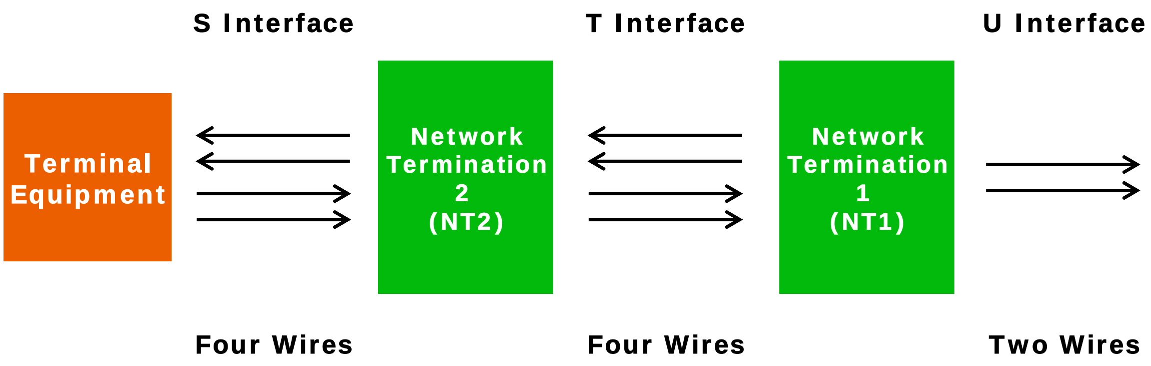


Figure 13: ISDN Interfaces

Equipment can be at any of the four interface points on the subscriber's side of an ISDN WAN connection:

- U interface
- T interface
- S interface
- R interface

These interfaces define the mechanical connectors, the electrical signals, and the protocols used for connections between the ISDN equipment.

U Interface

The U interface provides the connection between the local loop and NT1. For BRI ISDN, the U interface is one twisted pair. For PRI ISDN, the U interface is two twisted pairs.

Because public carriers in Europe and Asia provide the NT1, these regions do not use the U interface. In regions that support the U interface, there can be only one U interface on the ISDN network.

T Interface

The T interface is used to connect the NT1 to the NT2. This interface is a four-wire connection, or two twisted pair. Each pair handles the traffic sent in one direction (see the figure above).

In the United States and Canada, the T interface—along with the NT1 and NT2—is frequently built into a circuit board in an ISDN device such as a router. In other regions, the T interface is the first interface at the subscriber's premises.

S Interface

The S interface is used to connect the NT2 to the TE1 or TA. This interface is also a four-wire connection, or two twisted pair.

On a BRI ISDN, the S interface is mostly implemented as a passive bus, allowing you to connect multiple TEs and TAs to the ISDN WAN connection. If you use a passive bus configuration, that bus is a shared medium. The TEs or TAs connected to the passive bus must take turns transmitting, and they must be able to detect collisions. PRI ISDN does not support multiple TEs at the S interface.

The S and T interfaces are often combined as the S/T interface.

R Interface

The R interface is used to connect TE2 to the TA. Because there are no standards for the R interface, the vendor providing the TA determines how the TA connects and interacts with the TE2.

Connectors

The public carrier typically installs an RJ-45 jack to connect the subscriber's premises to the local loop. ISDN supports RJ-11 connectors, but an RJ-45 connector is recommended.

The following lists the advantages and disadvantages of ISDN:

Summary of Major Points

- Switched circuit technology
- Data or, “B” channels, each use a DS0
- North America uses a “U” interface
- The rest of the world uses an “S/T” interface
- A BRI is two “B” channels of 64K each.
- A PRI is same bit rates as T1 and E1

How This Technology is Used

- To back up IP routed network primary links.

Advantages

- ISDN takes advantage of existing copper wiring, and setup requirements are not extensive or expensive.
- ISDN can be used for both voice and data transmissions, and bandwidth can be regulated according to your needs.
- Because ISDN is a dial-up service, you do not pay for idle connection time. Paying only when the line is in use is beneficial for infrequent calls.

Disadvantages

- Because you pay for ISDN when the line is in use, it can be costly if the connection is maintained for long periods of time
- There is a lack of interoperability between ISDN devices from different vendors.

What to Determine During Planning

	Options
Switch Type	Euro-ISDN (sometimes called NET3 or DSS1), AT&T 5ESS, Northern Telecom DMS-100, or National ISDN-1
Channel Usage	Voice, data, or both voice and data
Line Number 1 (or sometimes more specifically for ISDN it is called MSN, Multiple Subscriber Number)	Telephone number ex: 64 000 00000
Line Number 2 (or sometimes more specifically for ISDN it is called MSN, Multiple Subscriber Number)	Telephone number ex: 64 111 11111
SPID 1 (North America Only)	Telephone number + numerals ex: 64 000 00000 11
SPID 2 (North America Only)	Telephone number + numerals ex: 64 111 11111 00
TEI	Assigned by public carrier and can be either dynamically or statically configured

Table 5: Table of Information Needed for ISDN

Data Link Layer Protocols in the WAN (The Transport Technologies)

Executive Summary

The Data Link protocols are used to ensure reliable data transmission of variable length packages called “frames”. The frame is the first basic structure required to transport the upper layer protocols such as IP. In the WAN routing process the “frame” and lower physical layer are exchanged at each network interface. This is the essence of pure routing. WAN routers must not only reconstruct the lower layers to forward layer 3 protocol but may have to re-establish connection before forwarding such as with any switched circuit at either layer 1 or 2.

PPP and Frame Relay can also take advantage of “link aggregation” where as HDLC cannot. Link aggregation is the combining of two or more physical links (interfaces) into one larger logical interface.

Overview

As mentioned previously all WAN connections consist of three basic elements:

1. The physical transmission media
2. Electrical signaling specifications for generating, transmitting, and receiving signals through various transmission media
3. Data-link–layer protocols that provide logical flow control for moving data between peers in the WAN

For each of the local loop connections, a customer can choose among several data link layer protocols such as HDLC, PPP, Frame Relay, or ATM; these are defined later in this paper. The Data Link protocols may span only the local loop, span across regions, or even go intercontinental. This is unlike the physical layer transmission technologies that are only concerned with moving electrical signals from customer location to the central office for processing.

Data link layer protocols are chosen for a variety of technical and business reasons. Typically they are chosen for the technology that allows the best communication between point “A” and point “B” expediently for the given requirement. PPP (Point to Point Protocol), HDLC (High Level Data Link Control), ATM (Asynchronous Transport Method), and Frame Relay are among the most common and interoperability is typically not an issue.

If the customer leases their lines between sites so that the carrier is not involved in Data Link layer switching or routing (other than simply allowing it to traverse the wires on their physical infrastructure), and they are building a private non-Internet based WAN, then PPP or HDLC is often chosen. If a more complex private WAN spanning many carriers is required then Frame Relay will likely be chosen.

If HDLC or PPP can be used there are two primary considerations: what the router on the other end of the link supports and if there is a requirement for security (particularly for authentication of the connection router). There are other minor factors but these are most prominent.

Some routers perform HDLC by default and the customer may not have required some basic security. In this situation it is acceptable to choose HDLC. If you are connecting site “A” and site “B” and the router at site “B” supports PPP, or PPP is already enabled, then choose PPP at site “A”. Often PPP is chosen to allow for authentication of link establishment. So PPP allows for security and HDLC does not.

PPP and Frame Relay can also take advantage of “link aggregation” while HDLC cannot. Link aggregation is the combining of two or more physical links (interfaces) into one larger logical interface.

HDLC

High-Level Data Link Control, also know as HDLC, is a bit oriented protocol. HDLC is one of the oldest data link layer protocols for the WAN. In fact, it predates the PC and was originally developed for mainframe environments. Because of this, HDLC was originally designed for use with primary and secondary devices, such as a mainframe with dumb terminals.

HDLC is a protocol developed by the International Organization for Standardization (ISO). It is used throughout the world and widely implemented because it supports both half duplex and full duplex communication lines, point to point, and multi-point networks, on both switched or non-switched links. HDLC is designed to permit synchronous, protocol transparent data transmission. HDLC also has many off shoots. Some of these are Synchronous Data Link Control (SDLC) and Link Access Procedure-Balanced (LAP-B), and PPP.

Summary of Major Points

- A point to point protocol
- No security

How This Technology is Used

- Site to site transport of upper layer network.
- Connection to Cisco routers.

Advantages

HDLC is a simple, effective, and well used standard for layer 2 point to point connections. Many, if not all, WAN devices should support this protocol.

Disadvantages

It does not support the authentication and many other features of PPP. There is no capability in HDLC or PPP to cross carrier boundaries. There is no NNI (network-to-network interface). These are advantages that are covered in the following technologies but unfortunately need mentioned here without previous reference.

What to Determine During Planning

- HDLC in the ProCurve Secure Router 7000dl series currently allow for the links to be "un-numbered". Un-numbered is a capability that allows for one of the link IP addresses to use the address of the Ethernet port. This special capability is useful to those conserving address space. In design determine if the customer needs to have the link run in un-numbered mode.
- Will this HDLC network require backup?

PPP

Point-to-Point Protocol (PPP) is the name of a single protocol, but most often "PPP" refers to the entire suite of protocols that are related to PPP. PPP is a layered protocol, starting with a Link Control Protocol (LCP) for link establishment, configuration and testing. Once the LCP is initialized, one or many of several Network Control Protocols (NCPs) can be used to transport traffic for a particular protocol suite. The IP Control Protocol (IPCP), documented in RFC 1332, permits the transport of IP packets over a PPP link.

PPP differs from HDLC primarily in that you can use some basic security methods with it. You can configure WAN routers (or other devices) to use optional protocols in the PPP suite. In addition, many protocols in the PPP suite, such as LCP, allow you to manually configure options.

When one of the peers in a PPP session has been configured to use protocols or options that are not used by default, the peers negotiate these options. They do so by exchanging configuration frames for the protocol in question.

Summary of Major Points

- Point-to-Point. One point to a single other point.
- Some security available through authentication.

How This Technology is Used

- Site to site, point to point, transport of upper layer protocol, IP for the ProCurve Secure Router 7000dl series, over a leased physical link.
- To establish an authenticated connection from router to ISP router over the physical connection when often this connection is ATM over ADSL, or Ethernet through an ADSL modem.

What to Determine During Planning

- The authentication method desired, typically CHAP or PAP.
- The passwords used during authentication.

Advantages

PPP allows for a wide range of features one of which is authentication of the other network device attempting to connect. This particular feature makes it extremely suitable for ADSL and Internet connectivity.

Disadvantages

There is no capability in HDLC or PPP to cross carrier boundaries. There is no network-to-network interface.

What to Determine During Planning

- The PPP attributes for the router at the other end of the connection.
- Determine if passwords and authentication methods are required (typically these are not needed in a private physical network).

Frame Relay

Frame Relay is a high-performance, packet-switching WAN technology. Frame Relay carrier networks use statistical multiplexing to allow multiple virtual connections to be multiplexed across a single physical link. This allows the Frame Relay network to better manage and use the available bit rate of the physical layer.

Frame Relay can carry multimedia traffic, such as voice or video, but it is not an ideal WAN technology for time sensitive applications. Frame Relay was designed for delay-tolerant traffic that may be "bursty" in nature. Additionally the carriers usually only offer a limited Quality of Service. So a customer with only data traffic is more likely to be satisfied when subscribing to Frame Relay than a customer requiring voice and/or video transport coupled with their data.

Although Layer 2 protocols are primarily concerned with reliable data transport, Frame Relay was designed when Layer 1 physical transmissions were growing in reliability. Frame Relay left out many of the unnecessary error correction (retransmission of data) up to the end-points, which speeds up overall data transmission. When an error is detected in a frame, it is simply "dropped". The end stations are responsible for detecting and retransmitting dropped frames. Frame relay allows data transmission in variable sized packages called frames. This is different than any "fixed" length size such as used in ATM or SONET/SDH.

With Frame Relay, a router at the customer's site is configured to communicate only with another router in a point-to-point connection. This connection is called a Virtual Circuit (VC). The Frame Relay standard allows for either a Permanent Virtual Circuit (PVC) or a Switched Virtual Circuit (SVC), but most customers only use PVCs. PVCs are established by using a carrier physical WAN connection or another form of permanent connection. LMI (Local Management Interface) circuit status messages provide communication and synchronization between Frame Relay DTE and DCE devices. These messages are used to periodically report on the status of PVC. There are different implementations of LMI.

Like carrier lines, Frame Relay is most frequently implemented through a public carrier network. The customer purchases a connection (E1 or T1) to a public carrier that provides Frame Relay service. The public carrier owns all of the Frame Relay equipment and the WAN infrastructure in the Frame Relay cloud.

When the customer purchases Frame Relay service, they negotiate a Service Level Agreement (SLA) that specifies the amount of bandwidth they will receive. This bandwidth is called a Committed Information Rate (CIR). The CIR can be considered a guaranteed amount of bandwidth. It is, however, contractually guaranteed, rather than physically guaranteed as it is with dedicated T and E carrier lines that use TDM. Frame Relay carriers usually rebate the customer if they do not provide the CIR commitment, so they are generally careful to meet it.

Frame Relay has the added benefit of both user to network (UNI) and network to network (NNI) interfaces. NNI allows transport between and through multiple carriers to go from point "A" to point "B". This does not affect the router configuration but allows the customer to understand what technology to use. PPP and HDLC are limited in the sense that they do not have termination within the carriers at layer 2 and do not have an NNI. If a customer wants to use HDLC or PPP spanning multiple carriers, then they must lease the physical connection between point "A" and point "B".

Frame Relay also has the ability to perform multilinking with the implementation agreement referred to as FRF.16. Multilink Frame Relay (MFR) allows the customer the ability to increase bandwidth by enabling multiple serial links to be aggregated, or trunked, to form a larger logical link of greater bandwidth. MFR allows for UNI and NNI Frame Relay networks.

The logical links formed are called “bundles”. Routers using MFR and their peer routers exchange link integrity control messages to determine which bundle links are active and to synchronize those bundle links that should be associated with each given bundle.

The bundle link interface's line protocol status is considered active and up when the peer router acknowledges that it will use the same link for the bundle. The line protocol remains up when the peer device acknowledges the hello messages from the local router.

MFR provides load balancing across the bundle links within a bundle. If a bundle link chosen for transmission happens to be busy transmitting a long packet, the load balancing mechanism can try another link, thus solving the problems seen when delay-sensitive packets have to wait.

MFR allows you to design a Frame Relay interface with more bandwidth than is available from any single physical interface. For example, many new network applications require more bandwidth than is available on a E1 or T1 line. Combining multiple E1 lines may be less costly than ordering a single E3 or T3.

MFR can also provide for high availability through the use of multiple physical interfaces, but is primarily a method for greater capacity.

Summary of Major Points

- Packet-switching technology
- Designed for delay-tolerant traffic that may be “bursty” in nature.
- Erred frames are dropped and the end stations are responsible for detecting and retransmitting dropped frames.
- Frame Relay uses Virtual Circuits (VC). PVCs are established by using a carrier physical WAN connection or another form of permanent connection.
- Statistically multiplexes many VCs onto a single physical link.
- SLAs are negotiated for bandwidth that is specified as the Committed Information Rate (CIR).
- Has a Network to Network Interface, NNI, that allows Frame Relay communication across carrier networks.
- MFR combines multiple physical links into one logical link called a bundle.

How This Technology is Used

- Interconnection of multiple sites through a minimum number of physical links required at each site.
- Especially used when crossing carrier or national boundaries.

Advantages

Frame Relay packet switching enables Frame Relay carriers to allocate network resources to active customers. Unlike Time Division Multiplexed (TDM) technologies, such as dedicated carrier lines and ISDN, packet-switching technologies do not ensure a constant bandwidth. However, LAN and WAN traffic is typically bursty, meaning large amounts of data are often transmitted at once, after which there may be no traffic whatsoever for a period of time. Thus with TDM, when the network is not transmitting, bandwidth is wasted; with packet-switching, when one network is not transmitting, another network can use the bandwidth. As a result, Frame Relay is more cost-effective for Frame Relay carriers, making it less expensive in many regions than dedicated carrier lines.

Frame Relay is also extremely flexible. Data in a Frame Relay network generally flows along the same physical path. However, that physical path is controlled simply by software in a switch, rather than any physical configurations. As a result, it is generally much easier to reroute traffic in the event of a switch or line failure.

Disadvantages

Although sharing resources among many circuits in a Frame Relay network provides many advantages, it also has one major drawback: Network throughput will be lower during peak hours if the Frame Relay network becomes congested. The customer may consider increasing their contracted CIR or add extra links.

PPP and other data-link–layer protocols, such as Frame Relay, establish a single point-to-point connection, which may not provide sufficient bandwidth to meet a business' requirements. Link-aggregation protocols such as Multilink Frame Relay address this limitation.

Theoretically, link aggregation is a simple idea: effectively double your available bandwidth by using two physical cables to connect your endpoints instead of only one, triple your bandwidth by using three cables, quadruple your bandwidth by using four cables, and so on. For example, you could aggregate two 1.544-Mbps T1 connections into a virtual single network connection with an underlying bandwidth of 3.088 Mbps.

However, to take advantage of multiple physical cables, data-link–layer protocols must be modified to fragment frames into smaller frames that can be passed simultaneously over separate cables and then reassembled by the receiving peer. Link-aggregation protocols, including Multilink PPP (MP) and Multilink Frame Relay (MFR), do exactly that.

What to Determine During Planning

- What is the minimum amount of bandwidth needed at the site under consideration? This yields the CIR?
- What is the LMI Type
- DLCI Numbers and how they are routed to other sites
- Does the customer need more bandwidth than a single E1 or T1?
- Does the carrier provide Multilink Frame Relay in the area under investigation?

ATM Technology

Asynchronous Transfer Mode, ATM, is the most frequently used backbone technology in the world. It was conceived as a "multi service" transport technology. It is a "standards based" transport technology that is deployed broadly within the core of the Internet and carrier networks. It is also used frequently at the edge of telecommunications systems to send data, voice and video.

ATM is best known for its integration with other technologies, and for its management features that allow carriers to offer quality of service (QoS) guarantees. ATM has historically been referred to as cell relay and uses short, "fixed length", packages called "cells" for transporting information that is either data or voice. This information is divided among these cells, transmitted and then reassembled at their final destination. This "cell based" technology is designed to work over any physical layer technology. ATM can be used in many applications. Customers can have flexible access to the network resources and can achieve a reasonable concession between performance and cost.

ATM technology consists of many layers. The first layer, the adaptation layer, holds the bulk of the transmission. This 48 byte payload divides the data into different types. The ATM layer contains five bytes of additional information, referred to as overhead. This header information allows the ATM switches to forward the cells to their destinations. Lastly, the physical layer attaches the electrical elements and network interfaces.

Service Categories

The ATM service categories are defined within the ITU-T, and specified in detail by the ATM Forum. ATM service categories make the technology suitable for an almost unlimited number of applications. ATM provides Virtual Path (VP) or Virtual Channel (VC) Connections with different levels of service. Each service level can be chosen to best meet the application requirement.

Most of the requirements that are specific to a given application may be resolved at the edges of an ATM network by choosing an appropriate ATM Adaptation Layer or AAL. It should also be noted that although the adaptation layer provides many services, they are not always required for all devices. Routers that offer QoS features at the upper layers can provide similar functionality. (There are many ways to solve any particular problem.)

The ATM layer behavior should not rely on the AAL protocols, since these are service specific, that is, the upper layers should define and use the services they need. In many cases the services are supported by the customer router. Given the presence of a heterogeneous traffic mix, and the need to adequately control the allocation of network resources for each traffic component, a much greater degree of flexibility, fairness and utilization of the network can be achieved by providing a selectable set of capabilities within the ATM layer itself. The Service Categories have been defined with this goal in mind.

Definitions

The following definitions address certain issues regarding Traffic Management and Congestion Control and are now stabilized standards managed by the ATM Forum. The ATM Forum forms a base to facilitate interoperability in multi-vendor implementations of these standards.

A first classification of these services and capabilities may be seen from a network resource allocation viewpoint here below:

- Constant (maximum) bandwidth allocation is called Constant Bit Rate (CBR) in the ATM Forum and Deterministic Bit Rate (DBR) by the ITU-T.
- Statistical (average) bandwidth allocation is called Variable Bit Rate (VBR) by the ATM Forum and Statistical Bit Rate (SBR) by the ITU-T.
- Further definition comes from ATM Forum as it groups VBR into real-time (rt-VBR) and non-real-time (nrt-VBR) classifications depending on the QoS requirements.
- Another division actually defines three VBR sub-classes depending on the conformance criteria adopted.
- Available Bit Rate (ABR) is used by both the ATM Forum and ITU-T. It is an "elastic" type of bandwidth allocation that occurs when the amount of reserved resources providing the bandwidth can vary with time, governed by network availability.
- One category that is considered only in the ATM Forum is the Unspecified Bit Rate (UBR). No explicit resource allocation is performed. There is no bandwidth or QoS objectives specified.
- One final category for consideration is within the ITU-T only. It is based on block (or burst) allocation and is called ATM Block Transfer (ABT). This class allows network resources to be negotiated and allocated on a per block basis rather than on a per connection basis.

Note: this paper will use the ATM Forum category designations since they seem to be more familiar and widely used in publications.

Services

ATM services use parameters and procedures for controlling traffic and congestion. These services are used to allow the network to achieve its performance goals. To meet these goals, services form the framework for managing and controlling network traffic.

Service categories are used on a per connection basis and formed during set up of the connection. Service categories work on both the Virtual Channel Connection, VCC, and the Virtual Path Connection, VPC.

Traffic Parameters

There are certain traffic parameters that describe characteristics of any given router using ATM. They are listed below for your reference and help with our understanding of Service Categories:

- Sustainable Cell Rate (SCR)
- Peak Cell Rate (PCR)
- Minimum Cell Rate (MCR)
- Maximum Burst Size (MBS)
- And finally there are QoS Parameters

Note: that these parameters are reasonably self descriptive. For further information you should seek out references listed at the end of this paper.

When QoS parameters are selected they relate to a given performance objective the customer has in the network. These parameters are listed below:

- Maximum Cell Transfer Delay (Max CTD)
- Cell Delay Variation (CDV)
- Cell Loss Ratio (CLR)
- Cell Error Ratio (CER)
- Severely Errored Cell Block Ratio (SECBR)
- Cell Mis-insertion Rate (CMR)

Service Categories

Constant Bit Rate (CBR)

CBR is used to set a fixed amount of bandwidth. It is characterized by the PCR value and is always available during the life of the connection. The router may send traffic at or below the PCR any time. This category is intended for real time applications that require tight control over jitter.

Key traffic parameters for this category are PCR, CTD, CDV, and CES. When the connection is established and the basic commitment is made by the network, the QoS negotiated is guaranteed to all cells conforming to the conformance tests. It is assumed that cells which are delayed beyond the value specified by CTD are less value to the application.

For example any data, text, or image transfer application that requires smooth traffic flow and response time from the other side should have a CBR channel. Examples are:

- Videoconferencing
- Interactive Audio such as with phone conversation.

Real-Time Variable Bit Rate (rt-VBR)

Real-Time Variable Bit Rate, rt-VBR, is for “time sensitive” applications. “Time sensitive” applications are those that require tight constraints on delay and variation in delay. Real-Time VBR serves voice and video applications well, especially when voice or video sources are expected to have a transmission rates that vary over time. Real-Time VBR would be useful to any application that could be characterized as “bursty”.

Key traffic parameters for this category are PCR, SCR, and MBS. Cells that are delayed beyond the CTD are assumed to be of lesser value to the given application. The rt-VBR service can also support statistical multiplexing from real time sources.

Non-Real-Time Variable Bit Rate (nrt-VBR)

The “non-real time VBR” service category is for applications that may still have “bursty” characteristics but do not have tight requirements for constraining variation in delay.

Key traffic parameters for this category are also PCR, SCR, and MBS. For the cells that are transferred within the contractual agreement, the application can expect a low CLR. For all other cells there are bounds on the CTD.

For example, VBR is suitable for any application for which the end system can benefit from statistical multiplexing, by sending information at a variable rate, and can tolerate or recover from a potentially small random loss of information.

Available Bit Rate (ABR)

ABR is a service category for sources that have the ability to increase or reduce their information rate when the supporting ATM network requires them to. This allows the sources sending traffic into the ATM network to take advantage of the changes in the ATM layer transfer characteristics (i.e., bandwidth availability) subsequent to connection establishment.

There are many applications having imprecise requirements for throughput and can utilize ranges of acceptable values; as with a minimum and maximum value rather than an average value. To do this an ABR connection is used and the source specifies the minimum and maximum bandwidth requirement.

Key traffic parameters for this category are PCR, MCR, CLR, and CDV. Although no specific QoS parameters are negotiated with ABR, it is expected that an end system adapts its traffic in accord with the feedback it receives with a low CLR. CDV is not controlled in this service, although cells sent from the source are not unnecessarily delayed. PCR and MCR are used to define the boundaries for the available bandwidth.

For example, any non time critical application running on the end systems that are capable of varying their emission rates can utilize the ABR service. This includes internetworking, such as one would have with an IP router. Though ABR can be used for IP routing, another service category is often chosen and described in the Unspecified Bit Rate.

Unspecified Bit Rate (UBR)

The Unspecified Bit Rate (UBR) category is best defined as delivering traffic on a "best effort" basis. It is for servicing non critical applications. (Not that IP data is "non critical" but when you consider that often TCP and IP are combined together this lower layer ATM service looks at it as "non critical" when compared with other applications.) UBR, from the ATM perspective, is for those applications that do not require tightly constrained delay and delay variation; or for that matter any particular level of QoS. UBR can be used by IP routers when QoS is furnished at the upper layers.

There are no key traffic parameters for this category since UBR does not give any guarantees for traffic. UBR provides an appropriate solution for less demanding applications. Most data applications such as file transfers are highly tolerant to delay and cell loss.

Typical Application	CBR	rt-VBR	nrt-VBR	ABR	UBR
LAN Interconnection	1	1	2	3	2
PABX Circuit emulation	3	2	N/R	N/R	N/R
POTS or ISDN Video Conferencing	3	N/R	N/R	N/R	N/R
Compressed Audio	1	3	2	2	1
Interactive Multimedia	3	3	2	2	1

Table 6: Typical Applications and Ratings for ATM service categories

Note: Recommended usage for the typical application of a service category are: good=1, better=2, best=3. The service categories that are not good for a given application are shown with a "not recommended" or "N/R".

Obviously , many of these categories are outside the scope of this paper, that is focused on WAN design with IP routers, but are put here for your reference and understanding.

Summary of Major Points

ATM service categories can be used in different ways and in many combinations. They are used within any VP or VC connection. These service help the customer gain the service level they require for the given application. Most often with IP based networks the chosen service category is UBR because QoS may be manageable with the upper layers.

- ATM connections offer QoS at the lowest layers.
- ATM works over any lower layer.

How This Technology is Used

- To connect from customer site routers to carrier or ISP.
- It can carry both data and traditional voice conversations.
- ATM is often combined with ADSL for IP routing.

Advantages

The real advantage for ATM is in its usage. For the customer requiring connection to the Internet, ADSL and ATM combine to build the best solution. ATM also is specified to provide QoS at the lowest layers.

Disadvantages

There are no real disadvantages in connecting to an ATM infrastructure.

What to Determine During Planning

- Since ATM and ADSL are often combined, many of these questions will be addressed below in a separate section.
- The PVC numbers that are available from the carrier.
- Customer name or ID and password for your connection that will be used in the PPPoE connection
- Encapsulation for ATM, either AAL5mux or AAL5snap
- Whether this is a PPPoE or PPPoA implementation
- VPI / VCI used by provider for ATM over ADSL connectivity
- Whether this is a PPPOE or PPPOA installation

Using ATM and DSL together

Probably the most used application with respect to IP branch office routing is the combination of ATM and DSL together. Used together, these two technologies can take the best qualities of each and provide an outstanding solution for customer interconnection to the Internet.

ATM is unique in its ability to work with DSL due to the number of services and applications it easily works with. It allows different types of traffic to be transported over the same network while supplying an unparalleled degree of QoS. DSL technologies use the ability of ATM to work over any lower layer technology to deliver the services needed by the customer wanting to hook to the Internet. Many DSL options are available with, as was discussed previously, ADSL being the most dominant currently.

ATM and ADSL are often combined. Below are some questions that should be addressed during planning and before implementation:

PPPoA (Point to Point Protocol over ATM) Planning Questions

What is the modulation; DMT or CAP?

What are the PVC numbers “VPI/VCI” values?

For authentication with PPP, what is the username and password required for your router to connect with?

If there is a static IP address assigned for your router, what is the public IP address and network mask?

If there is a static IP address assigned, what is the IP address of the provider’s default gateway?

PPPoE (Point to Point Protocol over Ethernet) Planning Questions

What is the modulation; DMT or CAP?

What are the PVC numbers “VPI/VCI” values?

Will an end-station such as a PC or the router be the PPPoE client?

What is the domain name of your provider?

For authentication with PPP, what is the username and password required for your end-station or router to connect with?

If there is a static IP address assigned for your router, what is the public IP address and network mask?

If there is a static IP address assigned, what is the IP address of the provider’s default gateway?

RFC 1483 Planning Questions

What is the modulation; DMT or CAP?

What are the PVC numbers “VPI/VCI” values?

If there is a static IP address assigned for your router, what is the public IP address and network mask?

If there is a static IP address assigned, what is the IP address of the provider's default gateway?

Further Information

For further information about layer 1, layer 2, and other networking protocols please see the references at the end of this paper.

Solution Examples for Layer 1 and 2

PPP Solution Example

The customer has the need to connect to multiple sites. The local cost for T1 or E1 is reasonable at their central location so multiple physical links are less expensive than other technologies. The remote sites are within the boundaries of the local carrier. The customer decides to lease the physical links to both sites. PPP is chosen at layer 2 but they could have used HDLC since there should not be any serious security issues on private leased lines. The Cisco router, a 2621XM supports PPP so there are no interoperability issues.

Note: Please note that these examples, and those in further sections, are given for your study and consideration only. They are to help you reach a better understanding of the fundamental concepts before configuring your own application. It will be necessary for you to modify these examples to match your own network design.

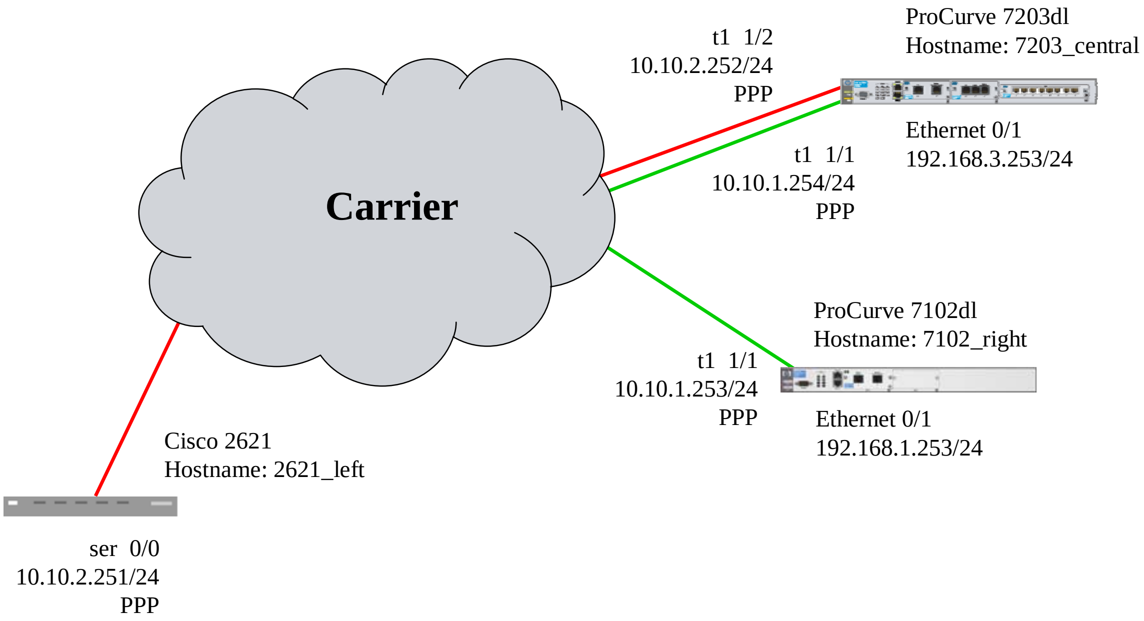


Figure 14: PPP Solution Example

ProCurve Secure Router 7102dl in PPP Network

```
!
!
hostname "7102_right"
enable password pnb
!
ip subnet-zero
ip classless
ip routing
!
event-history on
no logging forwarding
no logging email
logging email priority-level info
!
username "pnb" password "pnb"
!
!
interface eth 0/1
  ip address  192.168.1.253
255.255.255.0
  no shutdown
  no lldp send system-description
  lldp send management-address
!
interface eth 0/2
  no ip address
  shutdown
  no lldp send system-description
  lldp send management-address
!
!
!
interface t1 1/1
  tdm-group 1 timeslots 1-24 speed 64
  no shutdown
!
interface t1 1/2
  line-length 0
  shutdown
!
interface ppp 1
  ip address  10.10.1.253
255.255.255.0
  no lldp send system-description
  lldp send management-address
  no shutdown
  bind 1 t1 1/1 1 ppp 1
```

```
!
!
router rip
  redistribute connected
  network 10.10.1.0 255.255.255.0
  network 10.10.1.253 255.255.255.0
!
!
no ip tftp server
ip http server
ip http secure-server
ip snmp agent
no ip ftp agent
!
!
line con 0
  login
  password pnb
!
line telnet 0 4
  login
  password pnb
!
end
```

ProCurve Secure Router 7203dl in PPP Network

```
!
!
hostname "7203_central"
enable password pnb
!
ip subnet-zero
ip classless
ip routing
!
event-history on
no logging forwarding
no logging email
logging email priority-level info
!
customername "pnb" password "pnb"
!
!
!
```

```
interface eth 0/1
  ip address  192.168.3.253
255.255.255.0
  no shutdown
  no lldp send system-description
  lldp send management-address
!
interface eth 0/2
  no ip address
  shutdown
  no lldp send system-description
  lldp send management-address
!
!
!
interface t1 1/1
  tdm-group 1 timeslots 1-24 speed 64
  no shutdown
```

```
!
interface t1 1/2
  clock source through
  tdm-group 2 timeslots 1-24 speed 64
  no shutdown
!
!
interface ppp 1
  ip address  10.10.1.254
255.255.255.0
  no lldp send system-description
  no lldp send system-capabilities
  lldp send management-address
  no shutdown
  bind 1 t1 1/1 1 ppp 1
!
interface ppp 2
  ip address  10.10.2.252
255.255.255.0
  no lldp send system-description
  lldp send management-address
  no shutdown
  bind 2 t1 1/2 2 ppp 2
!
```

```
!
router rip
  redistribute connected
  network 10.10.1.254 255.255.255.0
  network 10.10.2.241 255.255.255.0
!
!
no ip tftp server
ip http server
ip http secure-server
ip snmp agent
no ip ftp agent
!
!
line con 0
  login local-customerlist
!
line telnet 0 4
  login local-customerlist
  password pnb
!
end
```

Cisco 2621xm in PPP Network

```
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 2621_left
!
boot-start-marker
boot-end-marker
!
!
no network-clock-participate slot 1
no network-clock-participate wic 0
no aaa new-model
ip subnet-zero
ip cef
!
!
```

```
ip audit po max-events 100
no ftp-server write-enable
!
!
interface FastEthernet0/0
 ip address 192.168.2.253
255.255.255.0
 ip rip send version 1
 ip rip receive version 1
 duplex auto
 speed auto
!
interface Serial0/0
 ip address 10.10.2.251 255.255.255.0
 ip rip send version 1
 ip rip receive version 1
 encapsulation ppp
!
!
```

```
interface FastEthernet0/1
 ip address 192.168.1.2 255.255.255.0
 shutdown
 duplex auto
 speed auto
!
router rip
 network 10.0.0.0
 network 192.168.2.0
!
ip classless
ip http server
no ip http secure-server
```

```
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
 password password
 login
!
!
end
```

MLPPP Solution Example

The customer has the need to connect but requires increased bandwidth beyond a single E1 or T1 link.

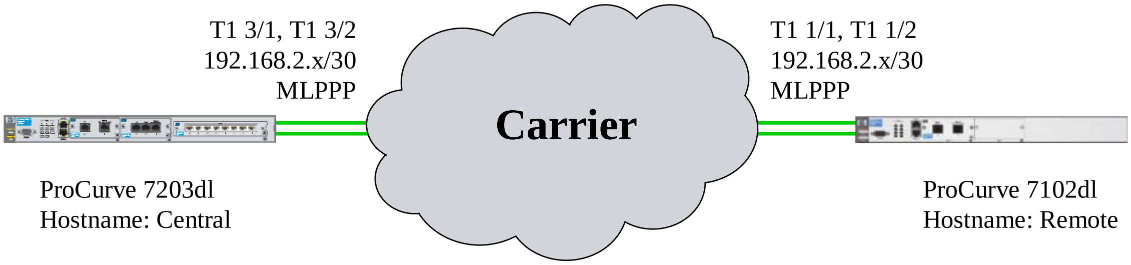


Figure 15: MLPPP Solution Example

ProCurve Secure Router 7203dl

```
!
!
hostname "Central"
no enable password
!
ip subnet-zero
ip classless
ip routing
!
event-history on
no logging forwarding
no logging email
logging email priority-level info
!
!
!
```

```
interface eth 0/1
  ip address  192.168.3.254  255.255.255.0
  no shutdown
!
interface eth 0/2
  no ip address
  shutdown
!
!
!
interface t1 3/1
  tdm-group 1 timeslots 1-24 speed 64
  no shutdown
!
interface t1 3/2
  tdm-group 2 timeslots 1-24 speed 64
  no shutdown
!
interface t1 3/3
  shutdown
!
interface t1 3/4
  shutdown
!
interface t1 3/5
  shutdown
!
interface t1 3/6
  shutdown
!
interface t1 3/7
  shutdown
!
interface t1 3/8
  shutdown
!
interface ppp 1
  ip address  192.168.2.2  255.255.255.252
  ppp multilink
  no shutdown
  bind 1 t1 3/1 1 ppp 1
  bind 2 t1 3/2 2 ppp 1
!
!
!
!
!
ip route 192.168.1.0 255.255.255.0 192.168.2.1
!
no ip tftp server
no ip http server
no ip http secure-server
no ip snmp agent
no ip ftp agent
!
!
!
!
!
!
!
line con 0
  no login
!
line telnet 0 4
  login
!
End
```

ProCurve Secure Router 7102dl

```
!
!
hostname "Remote"
no enable password
!
ip subnet-zero
ip classless
ip routing
!
event-history on
no logging forwarding
no logging email
logging email priority-level info
!
!
!
!
interface eth 0/1
  ip address  192.168.1.254  255.255.255.0
  no shutdown
!
interface eth 0/2
  no ip address
  shutdown
!
!
!
interface t1 1/1
  clock source internal
  tdm-group 1 timeslots 1-24 speed 64
  no shutdown
!
interface t1 1/2
  clock source internal
  tdm-group 2 timeslots 1-24 speed 64
  no shutdown
!
!
interface ppp 1
  ip address  192.168.2.1  255.255.255.252
  ppp multilink
  no shutdown
  bind 1 t1 1/1 1 ppp 1
  bind 2 t1 1/2 2 ppp 1
!
!
!
!
!
ip route 0.0.0.0 0.0.0.0 192.168.2.2
```

```
!
no ip tftp server
no ip http server
no ip http secure-server
no ip snmp agent
no ip ftp agent
!
!
!
line con 0
  no login
!
line telnet 0 4
  login
!
end
```

Frame Relay Solution Examples

The customer has the need to connect to multiple sites. Frame Relay provides connectivity across carrier boundaries and since customer traffic patterns are “bursty” yet normally low, they chose Frame Relay for cost reasons.

Frame Relay Solution Example 1

The customer has the need to connect to only a few sites but at great distance crossing carrier networks to do so. Frame Relay is a good choice for a true private network.

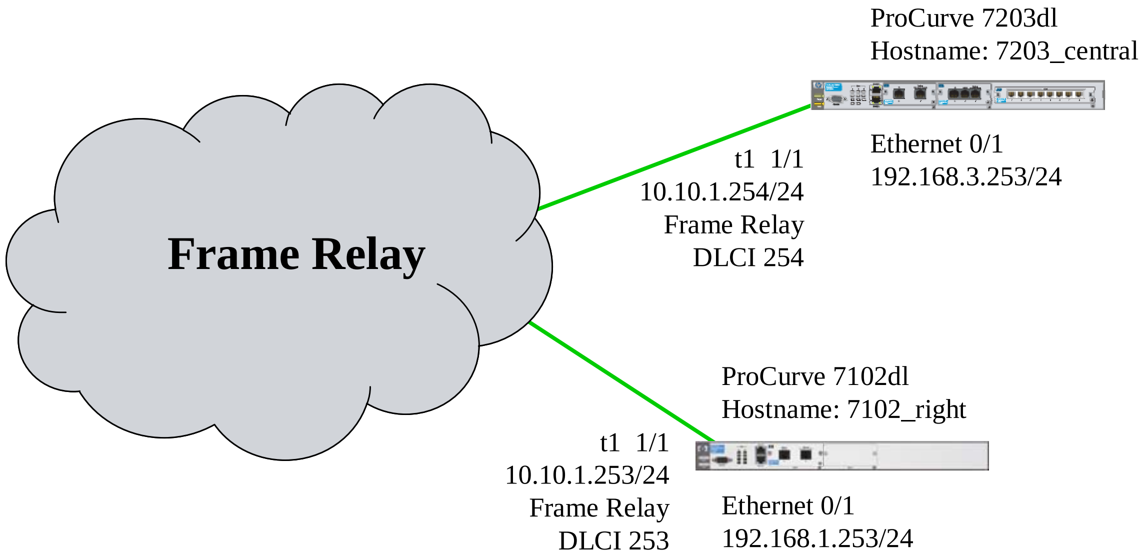


Figure 16: Frame Relay Solution Example 1

ProCurve Secure Router 7203dl

```
!
```

```
!
```

```
hostname "7203_central"
enable password pnb
!
ip subnet-zero
ip classless
ip routing
!
event-history on
no logging forwarding
no logging email
logging email priority-level info
!
username "pnb" password "pnb"
!
!
interface eth 0/1
  ip address  192.168.3.253
255.255.255.0
  no shutdown
  no lldp send system-description
  lldp send management-address
!
interface eth 0/2
  no ip address
  shutdown
  no lldp send system-description
  lldp send management-address
!
!
interface t1 1/1
  tdm-group 1 timeslots 1-24 speed 64
  no shutdown
!
interface t1 1/2
  clock source through
  shutdown
!
!
interface fr 1 point-to-point
  frame-relay lmi-type ansi
  no shutdown
  bind 1 t1 1/1 1 frame-relay 1
!
interface fr 1.254 point-to-point
  frame-relay interface-dlci 254
  ip address  10.10.1.254
255.255.255.0
  no lldp send system-description
  lldp send management-address
!
!
router rip
  redistribute connected
  network 10.10.1.254 255.255.255.0
!
!
no ip tftp server
ip http server
ip http secure-server
ip snmp agent
no ip ftp agent
!
!
!
line con 0
  login local-customerlist
!
line telnet 0 4
  login local-customerlist
  password pnb
!
end
```

ProCurve Secure Router 7102dl

```
!
!
hostname "7102_right"
enable password pnb
!
ip subnet-zero
ip classless
ip routing
!
event-history on
no logging forwarding
no logging email
```

```
logging email priority-level info
!
username "pnb" password "pnb"
!
!
interface eth 0/1
  ip address  192.168.1.253
255.255.255.0
  no shutdown
  no lldp send system-description
  lldp send management-address
!
interface eth 0/2
  no ip address
  shutdown
  no lldp send system-description
  lldp send management-address
!
!
interface t1 1/1
  tdm-group 1 timeslots 1-24 speed 64
  no shutdown
!
interface t1 1/2
  line-length 0
  shutdown
!
!
interface fr 1 point-to-point
  frame-relay lmi-type ansi
  no shutdown
  bind 1 t1 1/1 1 frame-relay 1
!
interface fr 1.253 point-to-point
  frame-relay interface-dlci 253
  ip address  10.10.1.253
255.255.255.0
  no lldp send system-description
  lldp send management-address
!
!
router rip
  redistribute static
  redistribute connected
  network 10.10.1.0 255.255.255.0
  network 10.10.1.253 255.255.255.0
!
!
!
no ip tftp server
ip http server
ip http secure-server
ip snmp agent
no ip ftp agent
!
line con 0
  login
  password pnb
!
line telnet 0 4
  login
  password pnb
!
end
```

Frame Relay Solution Example 2

The customer has the need to connect to only a few sites but at great distance crossing carrier networks to do so. Frame Relay is a good choice for a true private network. Multiple T1 links are shown to the central site. The customer may chose to do this for maximizing and equally distributing the bandwidth available for each site connection. Later they may chose to implement Multi Link Frame Relay.

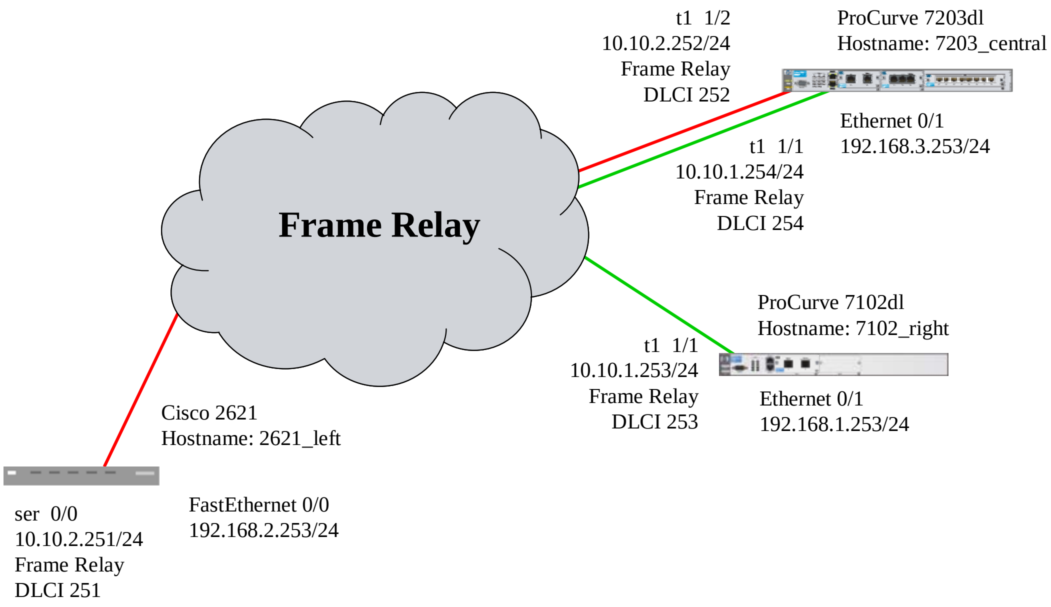


Figure 17: Frame Relay Solution Example 2

ProCurve Secure Router 7203dl

```
!
!
hostname "7203_central"
enable password pnb
!
ip subnet-zero
ip classless
ip routing
!
event-history on
no logging forwarding
no logging email
logging email priority-level info
!
username "pnb" password "pnb"
!
!
interface eth 0/1
  ip address  192.168.3.253
255.255.255.0
  no shutdown
  no lldp send system-description
  lldp send management-address
!
interface eth 0/2
  no ip address
  shutdown
  no lldp send system-description
  lldp send management-address
!
!
interface fr 1 point-to-point
  frame-relay lmi-type ansi
  no shutdown
  bind 1 t1 1/1 1 frame-relay 1
!
interface fr 1.254 point-to-point
  frame-relay interface-dlci 254
  ip address  10.10.1.254
255.255.255.0
  no lldp send system-description
  lldp send management-address
!
interface fr 2 point-to-point
  frame-relay lmi-type ansi
  no shutdown
  bind 2 t1 1/2 2 frame-relay 2
!
interface fr 2.252 point-to-point
  frame-relay interface-dlci 252
  ip address 10.10.2.252 255.255.255.0
  no llpd send system-description
  llpd send management-address
!
router rip
  redistribute connected
  network 10.10.1.254 255.255.255.0
  network 10.10.2.252 255.255.255.0
!
!
no ip tftp server
ip http server
ip http secure-server
```

```
ip snmp agent
no ip ftp agent
!
!
!
line con 0
  login local-customerlist
!
line telnet 0 4
  login local-customerlist
  password pnb
!
end
```

ProCurve Secure Router 7102dl

```
!
!
hostname "7102_right"
enable password pnb
!
ip subnet-zero
ip classless
ip routing
!
event-history on
no logging forwarding
no logging email
logging email priority-level info
!
username "pnb" password "pnb"
!
!
interface eth 0/1
  ip address  192.168.1.253
255.255.255.0
  no shutdown
  no lldp send system-description
  lldp send management-address
!
interface eth 0/2
  no ip address
  shutdown
  no lldp send system-description
  lldp send management-address
!
```

```
  !
  !
  interface t1 1/1
    tdm-group 1 timeslots 1-24 speed 64
    no shutdown
  !
  interface t1 1/2
    line-length 0
    shutdown
  !
  !
  interface fr 1 point-to-point
    frame-relay lmi-type ansi
    no shutdown
    bind 1 t1 1/1 1 frame-relay 1
  !
  interface fr 1.253 point-to-point
    frame-relay interface-dlci 253
    ip address  10.10.1.253
  255.255.255.0
    no lldp send system-description
    lldp send management-address
  !
  !
  router rip
    redistribute static
    redistribute connected
    network 10.10.1.0 255.255.255.0
    network 10.10.1.253 255.255.255.0
  !
```

```
!
no ip tftp server
ip http server
ip http secure-server
ip snmp agent
no ip ftp agent
!
!
line con 0
  login
  password pnb
!
line telnet 0 4
  login
  password pnb
!
end
```

Cisco 2621xm

```
!
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 2621_left
!
boot-start-marker
boot-end-marker
!
!
no network-clock-participate slot 1
no network-clock-participate wic 0
no aaa new-model
ip subnet-zero
ip cef
!
ip audit po max-events 100
no ftp-server write-enable
!
!
!
interface FastEthernet0/0
 ip address 192.168.2.253 255.255.255.0
 ip rip send version 1
 ip rip receive version 1
 duplex auto
 speed auto
!
interface Serial0/0
 ip address 10.10.2.251 255.255.255.0
 ip rip send version 1
 ip rip receive version 1
 encapsulation frame-relay IETF
 frame-relay lmi-type ansi
!
!
interface FastEthernet0/1
 ip address 192.168.1.2 255.255.255.0
 shutdown
 duplex auto
 speed auto
!
router rip
 network 10.0.0.0
 network 192.168.2.0
!
ip classless
ip http server
no ip http secure-server
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
 password password
 login
!
!
!
end
```

Frame Relay Solution Example 3

This example shows that true statistical multiplexing can be done across the central site link. The central site has only one physical link. It may have been determined that both sites only have about 50% of a T1 requirement or that each of them required access into the central site at different hours.

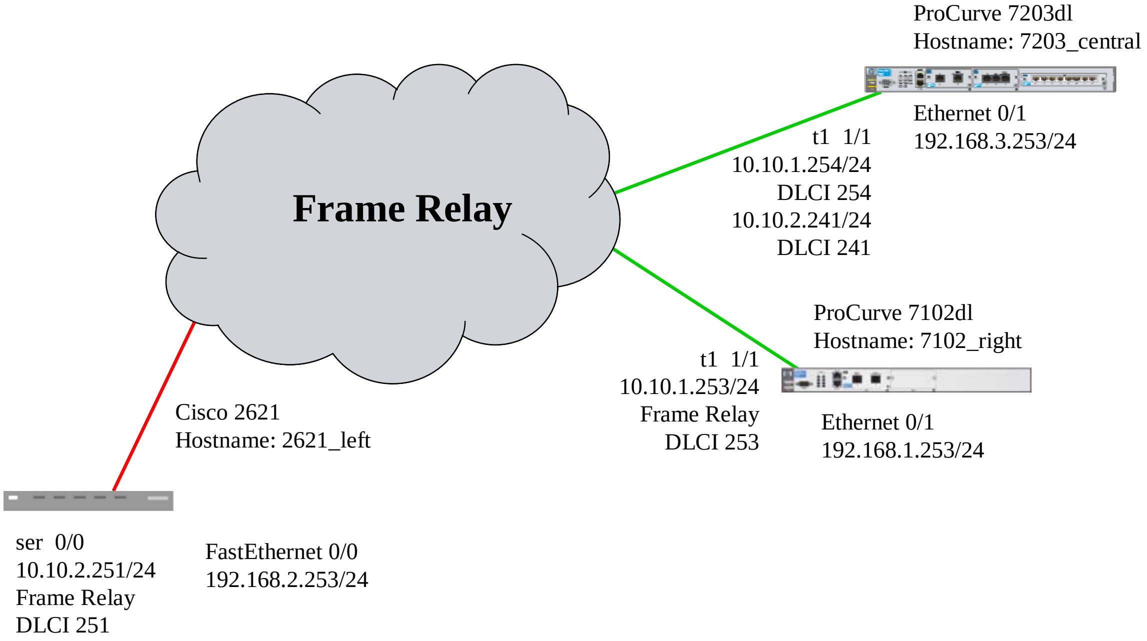


Figure 18: Frame Relay Solution Example 3

ProCurve Secure Router 7203dl

```
!
!
hostname "7203_central"
enable password pnb
!
ip subnet-zero
ip classless
ip routing
!
event-history on
no logging forwarding
no logging email
logging email priority-level info
!
username "pnb" password "pnb"
!
!
interface eth 0/1
  ip address  192.168.3.253
255.255.255.0
  no shutdown
  no lldp send system-description
  lldp send management-address
!
interface eth 0/2
  no ip address
  shutdown
  no lldp send system-description
  no lldp send system-
capabilities
  lldp send management-address
!
!
!
interface t1 1/1
  tdm-group 1 timeslots 1-24
speed 64
  no shutdown
!
interface t1 1/2
  clock source through
  tdm-group 2 timeslots 1-24
speed 64
  no shutdown
!
!
!
interface fr 1 point-to-point
  frame-relay lmi-type ansi
  no shutdown
  bind 1 t1 1/1 1 frame-relay 1
!
interface fr 1.241 point-to-point
  frame-relay interface-dlci 241
  ip address  10.10.2.241
255.255.255.0
  no lldp send system-description
  lldp send management-address
!
interface fr 1.254 point-to-point
  frame-relay interface-dlci 254
  ip address  10.10.1.254
255.255.255.0
  no lldp send system-description
  lldp send management-address
!
!
router rip
  redistribute connected
  network 10.10.1.254
255.255.255.0
  network 10.10.2.241
255.255.255.0
!
!
no ip tftp server
ip http server
ip http secure-server
ip snmp agent
no ip ftp agent
!
!
line con 0
  login local-customerlist
!
line telnet 0 4
  login local-customerlist
  password pnb
!
end
```

ProCurve Secure Router 7102dl

```
!
!
hostname "7102_right"
enable password pnb
!
ip subnet-zero
ip classless
ip routing
!
event-history on
no logging forwarding
no logging email
logging email priority-level info
!
username "pnb" password "pnb"
!
!
!
interface eth 0/1
  ip address  192.168.1.253
255.255.255.0
  no shutdown
  no lldp send system-description
  lldp send management-address
!
interface eth 0/2
  no ip address
  shutdown
  no lldp send system-description
  lldp send management-address
!
!
!
interface t1 1/1
  tdm-group 1 timeslots 1-24
speed 64
  no shutdown
!
interface t1 1/2
  line-length 0
  shutdown
!
!
!
interface fr 1 point-to-point
  frame-relay lmi-type ansi
  no shutdown
  bind 1 t1 1/1 1 frame-relay 1
!
interface fr 1.253 point-to-point
  frame-relay interface-dlci 253
  ip address  10.10.1.253
255.255.255.0
  no lldp send system-description
  lldp send management-address
!
```

```
!
router rip
  redistribute static
  redistribute connected
  network 10.10.1.0 255.255.255.0
  network 10.10.1.253 255.255.255.0
!
no ip tftp server
ip http server
ip http secure-server
ip snmp agent
no ip ftp agent
!
!
line con 0
  login
  password pnb
!
line telnet 0 4
  login
  password pnb
!
end
```

Cisco 2621xm

```
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 2621_left
!
boot-start-marker
boot-end-marker
!
!
no network-clock-participate slot 1
no network-clock-participate wic 0
no aaa new-model
ip subnet-zero
ip cef
!
!
ip audit po max-events 100
no ftp-server write-enable
!
!
interface FastEthernet0/0
 ip address 192.168.2.253 255.255.255.0
 ip rip send version 1
 ip rip receive version 1
 duplex auto
 speed auto
!
interface Serial0/0
 ip address 10.10.2.251 255.255.255.0
 ip rip send version 1
 ip rip receive version 1
 encapsulation frame-relay IETF
 frame-relay lmi-type ansi
!
!
interface FastEthernet0/1
 ip address 192.168.1.2 255.255.255.0
 shutdown
 duplex auto
 speed auto
!
router rip
 network 10.0.0.0
 network 192.168.2.0
!
ip classless
ip http server
no ip http secure-server
!
!
control-plane
!
!
!
line con 0
line aux 0
line vty 0 4
 password password
 login
!
!
!
end
```

Multilink Frame Relay Solution Example

This example shows interoperability for Multilink Frame Relay with Cisco 1841.

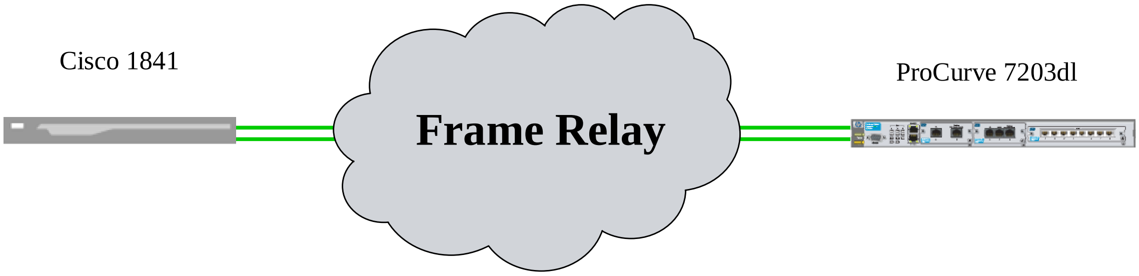


Figure 19: Multilink Frame Relay setup between a Cisco 1841 and ProCurve SR 7203dl

Cisco 1841

```
Cisco1841#sh run
Building configuration...

Current configuration : 1381 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Cisco1841
!
boot-start-marker
boot-end-marker
!
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
no aaa new-model
ip subnet-zero
ip cef
!
!
!
!
frame-relay switching
no ftp-server write-enable
!
!
!
controller T1 0/0/0
 framing esf
 clock source internal
 linecode b8zs
 channel-group 0 timeslots 1-24 speed 64
!
controller T1 0/0/1
 framing esf
 linecode b8zs
 channel-group 0 timeslots 1-24 speed 64
!
!
interface MFR1
 no ip address
 encapsulation frame-relay IETF
 frame-relay multilink bid Cisco1841
 frame-relay lmi-type ansi
 frame-relay intf-type dce
!
interface MFR1.16 point-to-point
 ip address 12.1.1.2 255.255.255.0
 frame-relay interface-dlci 16
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0:0
 no ip address
 encapsulation frame-relay MFR1
 no arp frame-relay
 frame-relay multilink lid Link1-to-7203
!
interface Serial0/0/1:0
 no ip address
 encapsulation frame-relay MFR1
 no arp frame-relay
 frame-relay multilink lid Link2-to-7203
```

```
!
ip classless
ip http server
!
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

ProCurve Secure Router 7203dl

```
ProCurveSR7102dl#sh run
Building configuration...
!
!
hostname "ProCurveSR7102dl"
no enable password
!
ip subnet-zero
ip classless
ip routing
!
event-history on
no logging forwarding
no logging email
logging email priority-level info
!
!
interface eth 0/1
  no ip address
  shutdown
!
interface eth 0/2
  no ip address
  shutdown
!
!
!
interface t1 1/1
  tdm-group 1 timeslots 1-24 speed 64
  no shutdown
!
interface t1 1/2
  clock source through
  tdm-group 2 timeslots 1-24 speed 64
  no shutdown
!
!
interface fr 1 point-to-point
  frame-relay lmi-type ansi
  frame-relay multilink
  no shutdown
  bind 1 t1 1/1 1 frame-relay 1
  bind 2 t1 1/2 2 frame-relay 1
!
interface fr 1.16 point-to-point
  frame-relay interface-dlci 16
  ip address  12.1.1.1  255.255.255.0
!

!
!
no ip tftp server
no ip http server
no ip http secure-server
no ip snmp agent
no ip ftp agent
!
!
line con 0
  no login
!
line telnet 0 4
  login
!
end
```

ADSL Solution Example

Note: Please note that these examples, and those in further sections, are given for your study and consideration only. They are to help you reach a better understanding of the fundamental concepts before configuring your own application. It will be necessary for you to modify these examples to match your own network design.

ADSL Solution Example

The customer needs to access the Internet through the ADSL modules.

ADSL Solution Example with PPPoE over ATM over ADSL

This example shows the customer needs basic connectivity to the Internet and the Service Provider has a packet routing core. PPPoE establishes a connection to that router over the carrier’s ADSL link and ATM layer 2.

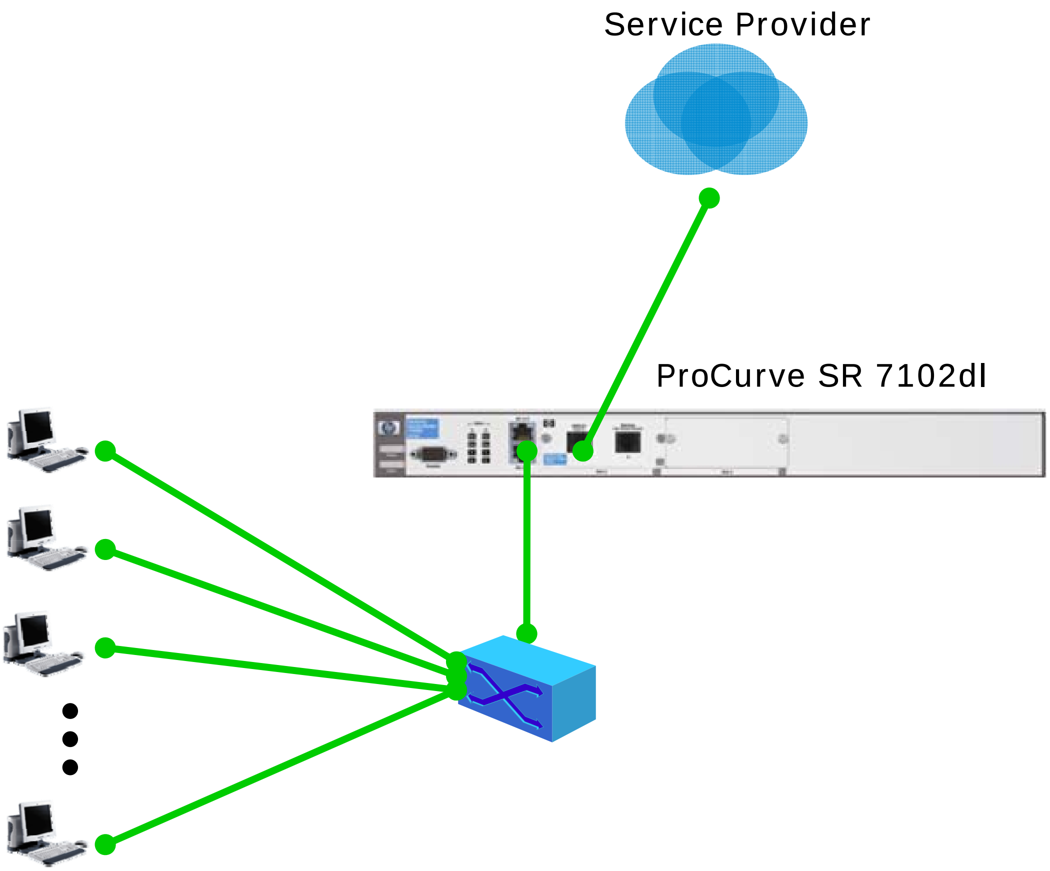


Figure 20: ADSL Solution Example with PPPoE

ProCurve Secure Router 7102dl

```
!
hostname "ADSL-Router"
!
ip routing
!
!
ip dhcp-server pool "pool-for-
lan"
  network 192.168.1.0
255.255.255.0
  domain-name "yourdomain.com"
  dns-server x.x.x.x y.y.y.y
  netbios-node-type h-node
  default-router 192.168.1.1
  lease 1
!
interface eth 0/1
  ip address  192.168.1.1
255.255.255.0
  no shutdown
!
!
interface eth 0/2
  no ip address
  shutdown
!
!
interface adsl 1/1
  training-mode multi-mode
  no shutdown
!
!
interface atm 1 point-to-point
  no shutdown
  bind 1 adsl 1/1 atm 1
!
!
interface atm 1.1 point-to-point
  no shutdown
  pvc 8/35
  no ip address
!
!
!
interface ppp 1
  ip address negotiated
  no fair-queue
  ppp chap hostname id-given-by-isp
  ppp chap password pw-given-by-isp
  no shutdown
  bind 2 atm 1.1 ppp 1 pppoe-client
!
!
!
ip access-list extended lan-acl
  permit ip any  any
!
!
ip policy-class FROM-LAN
  nat source list lan-acl interface ppp 1 overload
!
!
end
```

ADSL Solution Example with RFC 1483

The customer needs to bridge on the ATM/ADSL interface into the service provider. RFC 1483 support gives the customer the ability to bridge traffic over the ADSL/ATM interface and still forward that traffic to its Ethernet interface.

Note: Layer 1 (Physical) is ADSL (interface ADSL 1/1), Layer 2 (Link Layer) is ATM (interface ATM 1) and is bound to ADSL 1. Layer 2.1 is on top of ATM where there is an adaptation layer AAL5MUX or AAL5SNAP that we define for the ATM interface

Data in ATM is sent in a Permanent Virtual Circuit (PVC) defined with its VPI / VCI and is bound to the Point to point ATM interface named ATM 1.1

Layer 2.2 is the PPP Layer as defined in logical interface PPP 1 that used

```
!
hostname "Secure-Router"
!
ip routing
!
!
!
ip firewall
!
!
!
!
ip dhcp-server excluded-address 192.168.1.1
!
ip dhcp-server pool "pool-for-lan"
  network 192.168.1.0 255.255.255.0
  domain-name "yourprovider.com"
  dns-server x.x.x.x, y.y.y.y
  netbios-node-type h-node
  default-router 192.168.1.1
  lease 1
!
!
!
!
interface eth 0/1
  ip address  192.168.1.1  255.255.255.0
  access-policy FROM-LAN
  no shutdown
!
interface eth 0/2
  no ip address
  shutdown
!
interface adsl 1/1
  training-mode multi-mode
  no shutdown
!
interface atm 1 point-to-point
  no shutdown
  bind 1 adsl 1/1 atm 1
!
interface atm 1.1 point-to-point
  no shutdown
  pvc 8/36
  encapsulation aal5mux ip
ip address dhcp
  bandwidth 576
!
!
ip access-list standard manage-rtr
  permit 192.168.1.0 0.0.0.255
!
ip access-list extended lan-acl
  remark used for Nat
  permit ip any  any
!
ip policy-class FROM-LAN
  allow list manage-rtr self
```

```
 nat source list lan-acl interface atm 1.1 overload
!
!
end
```

Feature Set Consideration for ProCurve Secure Router 7000dl Series

- The ProCurve Secure Router 7000dl series routers are the 7102dl and the 7203dl as of this writing. Check http://www.procurve.com for further specifications.
- The ProCurve Secure Router 7000dl series supports the following physical interfaces as of this writing:
  - J8451A ProCurve SR dl 1xT1 module
  - J8452A ProCurve SR dl 1xT1 + DSX-1 module
  - J8453A ProCurve SR dl 2xT1 module
  - J8454A ProCurve SR dl 1xE1 module
  - J8455A ProCurve SR dl 1xE1 + G.703 module
  - J8456A ProCurve SR dl 2xE1 module
  - J8458A ProCurve SR dl 1-port Serial module
  - J8459A ProCurve SR dl 1xADSL2+ /A module
  - J8759A ProCurve SR dl 1xADSL2+ /B module
  - J8460A ProCurve SR dl 1-port ISDN BRI U backup module
  - J8461A ProCurve SR dl 1-port ISDN BRI S/T backup module
  - J8462A ProCurve SR dl Analog Modem backup
  - J8463A ProCurve SR dl Wide 8xT1/E1 module
  - J8755A ProCurve SR Serial Cable V.35 DTE
  - J8757A ProCurve SR Serial Cable X.21 DTE
- The ProCurve Secure Router 7000dl series supports the following Layer 2 WAN protocols as of this writing:
  - HDLC Cisco compatibility
  - PPP
  - Multilink PPP
  - Frame Relay (FRF.12)
  - Multilink Frame Relay (FRF.16)
  - ATM
  - PPPoE
  - PPPoA
- Early releases of the ProCurve Secure Router 7000dl series did not allow the HDLC link to initiate the backup module upon failure. Options for deployment include:
  - Using PPP or Frame Relay if there is requirement to monitor the data link layer.
  - Apply the backup to the physical interface.
- The current implementation of ATM only support AAL 5 or UBR which is acceptable for IP data traffic.
- Check http://www.procurve.com for the latest free software update, or for additions to the physical interfaces supported.

How to Use the ProCurve Secure Router 7000dl Series

- Use the 7102dl at the branch offices that primarily need access to their central site. If the branch needs to increase bandwidth out from the site, consider using a single 7203dl in a stacked configuration along with one or more of the suggestions below for increasing bandwidth.
- Use a single 7203dl at the central sites of networks not requiring greater throughput than 12 Mbps or do not require more connectivity than the equivalent of 12 E1 or T1 interfaces.

- Use multiple 7203dl at central sites requiring greater throughput or connectivity. Stacking 7203dl routers at the central site is possible. Properly designed this “stacked” solution can enhance overall network availability since a single device failure, instead of a stack, could take down the entire network. Multiple devices are sometime preferable for high availability.
- Backup for the 7102dl can be either through an optional “backup” module, or through use of the Internet as a backup route and the use of a “floating” static route.
  - See High Availability section of this paper for details.
- Increasing bandwidth for the primary routes may be accomplished with one or more of the following:
  - Use of serial interface over a single T1 or E1 that connects into a carrier supplied CSU/DSU that has greater bandwidth than a singe T1 or E1 can supply. Often these “special” devices are region and location specific and may not be available in all areas. Ask your carrier or service provider.
  - Multilink PPP or Multilink Frame Relay
  - Limit your Multilink implementation to a maximum of 8 physical links.

An Overview of IP, Static and Dynamic Routing Protocols

Executive Summary

For the interconnection of IP networks over a WAN the routers must have these basic elements:

- A routable protocol, in this case IP.
- A means to inform the routers of the proper path to forward the IP packet along, such as with static routes or dynamically with RIP or OSPF.
- The ability to bridge other routable protocols, such as DecNet or IPX.

Overview

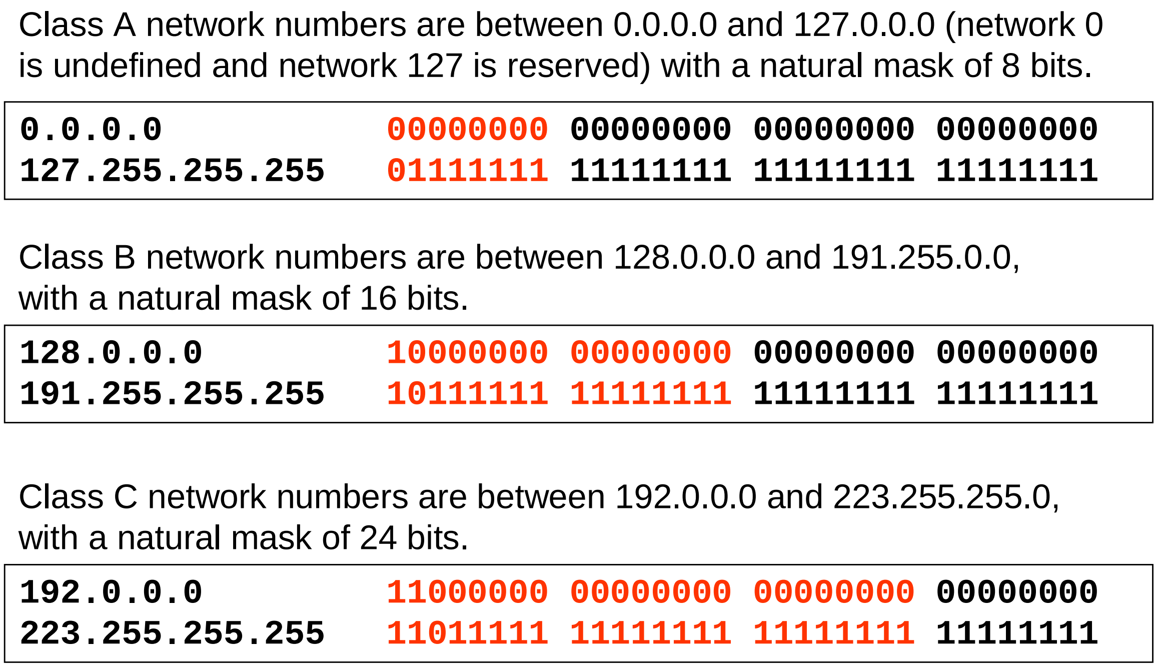
Routers perform many functions; mainly they connect multiple networks together. Routers can function as LAN or WAN devices, with the ability to interconnect both local area and wide area networks. When multiple logical networks must communicate or be interconnected, the network requires a router. One of the router’s most prominent functions is to forward Layer 3 packets based upon logical addresses. For the WAN router, another critical feature that is often overlooked is the complete replacement of Layer 2 header information and protocol when forwarding a packet from one network to another.

A router examines and learns the source layer 3 address of each packet. Its routing table is contained in memory and used for these learned addresses. Routers determine the best path of each packet through consulting the routing table and using routing metrics. The router can then forward packets from one network to another.

Routing metrics are based upon criteria such as speed of the link, number of points between final end points, or other such factors. Customers may choose to administrate this “routing decision” manually, as with static routes, or dynamically, as with dynamic routing protocols such as RIP and OSPF. Typically smaller installations, those less than approximately 5 sites, will choose to control the paths that forwarded IP packets take through the use of static routes. Another common usage for static routes is when there is a “star” topology where all the remote sites go directly back to the central site. These simple topologies or smaller installations can use static routing effectively. On the other hand static routing can be administratively burdensome with more than a handful of sites so dynamic routing protocols are chosen for lager installations. All routers should interoperate with each other using a standard routing protocol such as RIP or OSPF. There are other proprietary routing protocols such as IGRP or EIGRP, but installations today that need interoperability between protocols choose OSPF for speed and efficiency. If a router has a proprietary routing protocol it will also support a number of standards based protocols also. Customers can, and do, effectively use these together in their networks.

IP General

An IP network is a collection of IP hosts that share a common network number. The network portion of each host’s IP address is defined by a mask, which is often called the “subnet mask”. The concept of a “subnetwork”, “subnet”, or “subnet mask” is related to classful IP addressing. The 32-bit IP address space was originally carved up into several classes. Each class has a “natural” mask that initially determines what portion of the address represents the network and what portion represents the host. The picture below shows the class divisions and the resulting natural masks.



Class A network numbers are between 0.0.0.0 and 127.0.0.0 (network 0 is undefined and network 127 is reserved) with a natural mask of 8 bits.

0.0.0.0	00000000	00000000	00000000	00000000
127.255.255.255	01111111	11111111	11111111	11111111

Class B network numbers are between 128.0.0.0 and 191.255.0.0, with a natural mask of 16 bits.

128.0.0.0	10000000	00000000	00000000	00000000
191.255.255.255	10111111	11111111	11111111	11111111

Class C network numbers are between 192.0.0.0 and 223.255.255.0, with a natural mask of 24 bits.

192.0.0.0	11000000	00000000	00000000	00000000
223.255.255.255	11011111	11111111	11111111	11111111

Table 7: IP address classes and natural masks

The three IP address classes can be summarized as follows:

- When the first octet of an IP address is between 1 and 126, the address falls within the Class A range, with a natural mask of 8 bits. The 8-bit mask results in a range of over 16 million addresses for each of the 126 Class A network numbers.
- When the first octet of an IP address is between 128 and 191, the address falls within the Class B range, with a natural mask of 16 bits. The 16-bit mask results in a range of 65,536 addresses for each of the 16,384 Class B network numbers.
- When the first octet of an IP address is between 192 and 223, the address falls within the Class C range, with a natural mask of 24 bits. The 24-bit mask results in a range of 256 addresses for each of the 2,097,152 Class C network numbers.

IP networks and subnetworks

The rules of classful IP addressing dictate that the mask associated with each address can be made longer than the natural mask.

Classful addressing does not allow you to use a mask that is shorter than the natural mask. If you are using public addresses within an enterprise, this is a reasonable restriction, because the use of a shorter mask will overlap with the addresses assigned to other enterprises. However, particularly when using private addressing, there can be a valid use for masks that are shorter than the natural mask (sometimes called a "supernet mask").

If you are using RIP version 1 as route exchange protocol, you need to comply with the classful addressing restriction mentioned above.

Classful vs. classless IP addressing

When you are using an IP route exchange protocol that supports classless IP addressing, such as RIP version 2 or OSPF, every range is defined by a starting address and a mask. The mask may be expressed in dotted-decimal format or as a count of the number of consecutive "1" bits (often referred to as "CIDR" notation). Although you may see or hear references to a "subnet" mask, the term "subnet" is actually relevant only in a classful environment. Consider the following comparison:

In classful addressing, the two address ranges 10.1.1.0/24 and 10.1.2.0/24 have an inherent relationship as portions (sometimes called "children") of the same classful (sometimes called "parent") network 10.0.0.0.

With classless addressing, the mask defines the boundaries of each address range; the value in the first octet has no effect on determining the size of the address range.

IP routing

The primary role of an IP router is to interconnect networks and facilitate the forwarding of IP traffic between hosts. The destination of any particular packet may be a “unicast” address in the range 1.0.0.0 through 223.255.255.255, or a “multicast” address in the range 224.0.0.0 through 239.255.255.255.

A router uses a variety of methods to gather information about networks, which are groups or ranges of IP addresses. The router stores this information in a table and uses the entries to forward traffic toward its ultimate destination.

Remote networks

When some of the networks are reached through a different router, there must be a way to share information between routers and facilitate the movement of customer traffic between remote networks.

Each router records in its route table the existence of its directly connected networks. However, in order to dynamically acquire information about non-local networks each router needs to receive information from neighboring routers.

Route exchange protocols define rules for exchanging information. These rules may specify:

- The format of the information to be exchanged,
- conditions that trigger the transmission of information,
- procedures for adding new information to the routing table, and
- procedures for replacing or removing inaccurate information.

Routing Information Protocol (RIP)

The simplest route exchange protocol is the Routing Information Protocol. When RIP is applied to an IP interface, the router sends periodic updates (every 30 seconds) to neighboring routers.

RIP is a distance vector protocol, which means that its updates include the distance, measured in the number of hops, between a particular router and a network.

Static routes

Another way to administratively intervene on path selection is to create a static route that specifies a next hop that leads to the more desirable path. While cost is used for path selection when all choices come from the same source, such as RIP, cost alone is not used as tie-breaker when routing information comes from different sources. By default, statically defined routes are preferable over RIP-learned routes.

Administrative distance

Static routes rely upon information supplied by an administrator; they do not use RIP to dynamically gather information. Static routes thus constitute a different source of information. Most routers use administrative distance to make path selection choices when routing information comes from different sources. You can think of administrative distance as a "reliability" or "believability" factor, where the lower number is considered more reliable or closer.

All route exchange protocols and sources of routing information, including static routes, have a default administrative distance. RIP-learned routes have a default administrative distance of 120, which may be modified. Static routes have a default administrative distance of 1, which makes them preferable over RIP routes. The administrative distance for a static route may be specified when the route is defined.

When static routes are intended to replace dynamically learned routes, the administrative distance may be left at the default value of 1. However, another choice for administrative intervention would be to use a static route as a backup to a RIP-learned route.

Default static route

A commonly defined static route is the default static route 0.0.0.0 with a mask of 0.0.0.0. The default route is used to minimize the size of routing tables, thus maximizing router performance.

For example, in networks that are connected to the public Internet, it would be impractical for the routers to maintain routing table entries for every network available worldwide. Instead, the routers typically keep detailed information only about networks within their own domain or "autonomous system".

By using the default route, traffic destined for networks not listed in the routing table is forwarded toward a router with more specific information. Typically, there are several levels of default routes that ultimately lead to a "default-free zone," where detailed Internet routing information is available.

Default routes are also used in private enterprise networks to minimize route table size. Some remote areas may maintain detailed information only about their site, and use the default route to represent any destination not specifically listed in the route table.

The existence of the default route does not change the lookup process. However, since the default route specifies an address range that matches with EVERY destination address, some packets will have multiple matches. In this case, the MOST SPECIFIC MATCH is chosen. This is the match with the longest mask.

The primary value of the default route is that, since it matches with every packet, it provides a "next hop" for packets that are destined for unknown networks.

Open Shortest Path First (OSPF)

OSPF is a link state route exchange protocol that was standardized by the Internet Engineering Task Force to support scaleable, resilient networks. A primary goal of OSPF is to reduce the frequency of update traffic. Another goal is fast convergence. Meeting these two goals results in a tradeoff, that OSPF consumes more memory and CPU resources on the router than distance vector protocols.

RIP has a diameter limit due to the way that information is passed between routers. RIP routers pass on to neighbors their own view of the network every 30 seconds. The neighbor, in turn, interprets the information from its own perspective and passes it on again. One inevitable result is slow convergence. Another possible outcome is that this "rumor-based" information can be misinterpreted and disrupt connectivity.

Every OSPF router generates an advertisement that includes the identities of its active IP OSPF interfaces, including address, mask, and cost. The advertisements are immediately flooded, without being changed, by other OSPF routers and this results in very fast convergence. All OSPF routers within a defined domain (known as an “area”) receive exactly the same advertisements.

OSPF routers collect the advertisements in a database and each independently calculates the lowest cost (shortest) path to each network within the domain. It does this by examining each element in the database and building a tree, with itself as the root. The advertised networks are either branches or leaves of the tree, joined by the advertising routers.

From the shortest path tree, each router derives the "next hop" for each destination network, and places that information in its routing table. The maximum path cost is over 65,000.

If any OSPF router experiences a state change, i.e. an OSPF interface goes up or down, it generates a new advertisement. The advertisement is flooded throughout the domain. Each router replaces the obsolete advertisement with the latest information, and rebuilds the tree, based on the very latest information. The resulting routes replace the ones in the routing table.

It is important to recognize that, although advertisements are flooded by OSPF routers, this does not mean that IP customer traffic is flooded. The IP forwarding process used by OSPF routers is the same as that used by RIP routers. IP traffic is always forwarded one "hop" at a time.

OSPF hierarchy

An area is a collection of contiguous networks, identified by its area ID. The area ID may be expressed as a decimal number or a dotted-decimal number, depending on router vendor and customer preferences. The ProCurve Secure Router 7000dl Series supports both formats.

The definition of multiple areas introduces an additional level of hierarchy that makes it possible to simplify routing tables by hiding the topology of some portions of the network. The highest level of hierarchy is an Autonomous System (AS), which may be defined as “a group of networks under common administrative control.” An OSPF AS consists of one or more areas. Every OSPF router is uniquely identified by a router ID.

Each OSPF area is made up of two basic types of networks:

- Networks that have only one router are recognized as stub networks. A stub network is a destination address range, but is like a leaf on the tree because it does not serve as a path to any other network.
- Networks that have multiple connected routers are recognized as transit networks. Transit networks provide potential paths to other destinations, like the branches of a tree.

The flow of link state information

While routers using RIP send updates that contain the entire content of their route table to neighbors, OSPF routers send information about their directly connected links.

A link state advertisement (LSA) is a unit of information that is generated by an OSPF router and flooded through the OSPF domain. There are six types of LSAs; some are flooded throughout an area, while others cross the boundaries between areas and are flooded throughout the entire AS.

Each router collects LSAs in a link state database. Due to the flooding of LSAs, all routers in the same domain have an identical link state database. Routers in different areas will have different link state database entries.

Each router runs a link state algorithm, called the Dijkstra algorithm, using the information in the link state database as input. The output of the link state algorithm is a “shortest path first” tree that maps out a loop-free path to every known network and router.

Multiple OSPF areas

OSPF was designed to scale to very large networks. To keep the database at a manageable size, and to minimize the area that is affected by interface state changes, OSPF networks are often divided into multiple areas.

Because router LSAs and network LSAs flow freely within an area, each router in that area has detailed, consistent information in its link state database. Routers that have all of their interfaces in the same area are known as internal routers – their link state database entries all relate to the same area. Routers that connect to more than one area are known as area border routers (ABR).

An area border router maintains a link state database for each the areas it interconnects. The area border router transfers information between areas by generating a third type of LSA, the summary LSA, which reports the networks in one area into another area. Network and router information from one database is converted into summary LSAs and copied into the other database.

In addition to the reduction in the size of the link state database for internal OSPF routers, dividing the internetwork into multiple areas reduces the impact of link state changes. Since the scope of router LSAs and network LSAs is a single area, those advertisements are not flooded between areas. For example, if a link state change occurs in area 0.0.0.1, the routers in other areas do not need to run the link state algorithm and recalculate routes. This is because routers internal to an area represent networks from other areas as “leaf” objects in the SPF tree.

To minimize the number of advertisements that are sent between areas, administrators often configure network summaries. One can summarize four networks with 24-bit masks into a single advertisement with a 22-bit mask.

Summarization can help to minimize the number of summary LSAs that are sent between areas and, as a result, minimizes the number of entries in the routing table.

Autonomous System Boundary Router (ASBR)

While an OSPF autonomous system (AS) is often made up of multiple areas, information regarding non-OSPF networks is considered "external" to the OSPF AS. OSPF routers that have learned route information from sources other than OSPF are known as autonomous system boundary routers (ASBRs). RIP routes, static routes, and directly connected networks non-OSPF interface, are some examples of external information.

ASBRs are configured to redistribute non-OSPF routes into the OSPF domain using type 5 LSAs, known as external LSAs. To cause an ASBR to generate external LSAs to represent RIP and static routes, enter the following command within the OSPF configuration level:

The ASBR generates one external LSA for each non-OSPF network, floods the LSAs to its neighbors, who flood the LSAs, unchanged, to their neighbors. As a result, all of the routers in the area know about the external networks.

To minimize the number of LSAs, the external address space may be summarized using the summary-address command within the OSPF configuration level. More on “route summarization” at the end of this section.

External LSAs flow over area boundaries. When an area border router receives type 5 LSAs over an adjacency with a router in a non-backbone area, it copies them into the backbone area link state database and floods them over adjacencies with routers in the backbone. External LSAs that it receives over adjacencies with other backbone routers will be flooded into non-backbone areas only if they are “normal” areas.

Normal areas and stub areas

While type 5 LSAs flow freely between “normal” areas, they are not copied into "stub" areas. Instead, the area border routers inject the default route to represent external (non-OSPF) networks. The practical effect of defining a stub area is to reduce the number of entries in the link state database of the internal routers in the stub area, resulting in lower memory consumption and a shorter time to run the link state algorithm.

The route table within a stub area will have an entry for each network in the area, a summary of the address space in each of the other areas, and a default route that represents external (non-OSPF) networks. The backbone cannot be configured as a stub area.

Not-so-stubby areas (NSSA)

Stub areas are an important tool in minimizing the size of the link state database and the route table within non-backbone areas. However, a stub area cannot contain any ASBRs; type 5 LSAs cannot exist within the link state database of routers in a stub area.

The not-so-stubby area (NSSA) allows ASBRs to exist within an area that uses the default route to reach non-OSPF networks in other areas.

The NSSA combines the benefits of the stub area with some of the flexibility of a normal area. The ASBR within the NSSA advertises the external networks as type 7 LSAs, which is a legal LSA type within the NSSA. The ABR connected to the NSSA converts the type 7 LSAs to type 5 LSAs and floods them into the backbone area, where they are handled like any other type 5 LSA. ABRs that connect stub areas to the backbone will block the external information and inject the default route to spare the internal routers from tracking the details about non-OSPF destinations.

Border Gateway Protocol

When one looks at the Internet from the perspective of a customer, it appears as a collection of resources that you can access through an ISP. The underlying topology of the Internet, as well as the processes that enable communication between distinct entities all over the world, are irrelevant from the customer perspective. However, in order to understand the operation of Border Gateway Protocol (BGP) it is useful to understand a few things about Internet topology and communication between different enterprises.

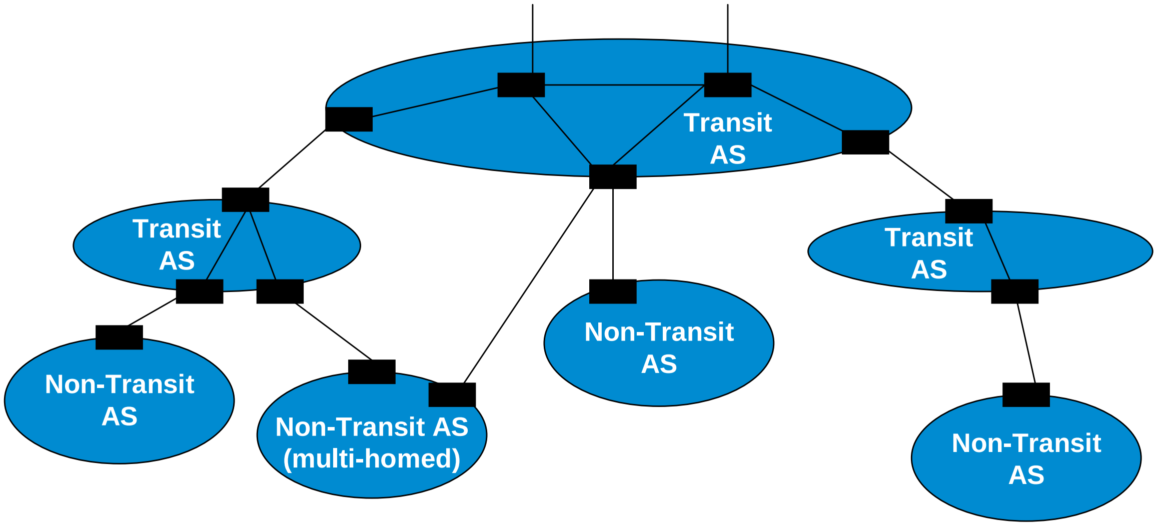


Figure 21: Types of Autonomous Systems in the Internet

In its current form, the Internet is an arbitrary collection of autonomous systems. Exterior gateway protocols are used for communication between autonomous systems, and their use obscures the interior topology of an AS in such a way as to make it irrelevant what route exchange protocols are used within.

An enterprise that uses Border Gateway Protocol (BGP) to exchange "internal" address space information with an ISP must have its own AS number. The connection between a router in one autonomous system and another router in a different autonomous system is called an "external BGP" connection.

BGP operates over the connection-oriented transport layer protocol TCP. The BGP routers are each configured with a "peer" session that specifies the IP address and AS number of the other, and they form a connection that remains up indefinitely.

Routers that are configured to support BGP are called "BGP speakers". Two BGP speakers communicate over a "peer" session. The BGP router on the other side of a peer session is called a BGP "neighbor".

External BGP operation

Once the connection has been established over the external BGP peer session, BGP routers send incremental updates that include summarized address ranges and AS numbers. They also send "keepalives" to maintain the session. All BGP messages are sent to TCP port 179.

Network Layer Reachability Information

A "route" is not a network or subnet as in the previous route exchange protocols, but is a unit of information that pairs a **destination** with **path attributes**.

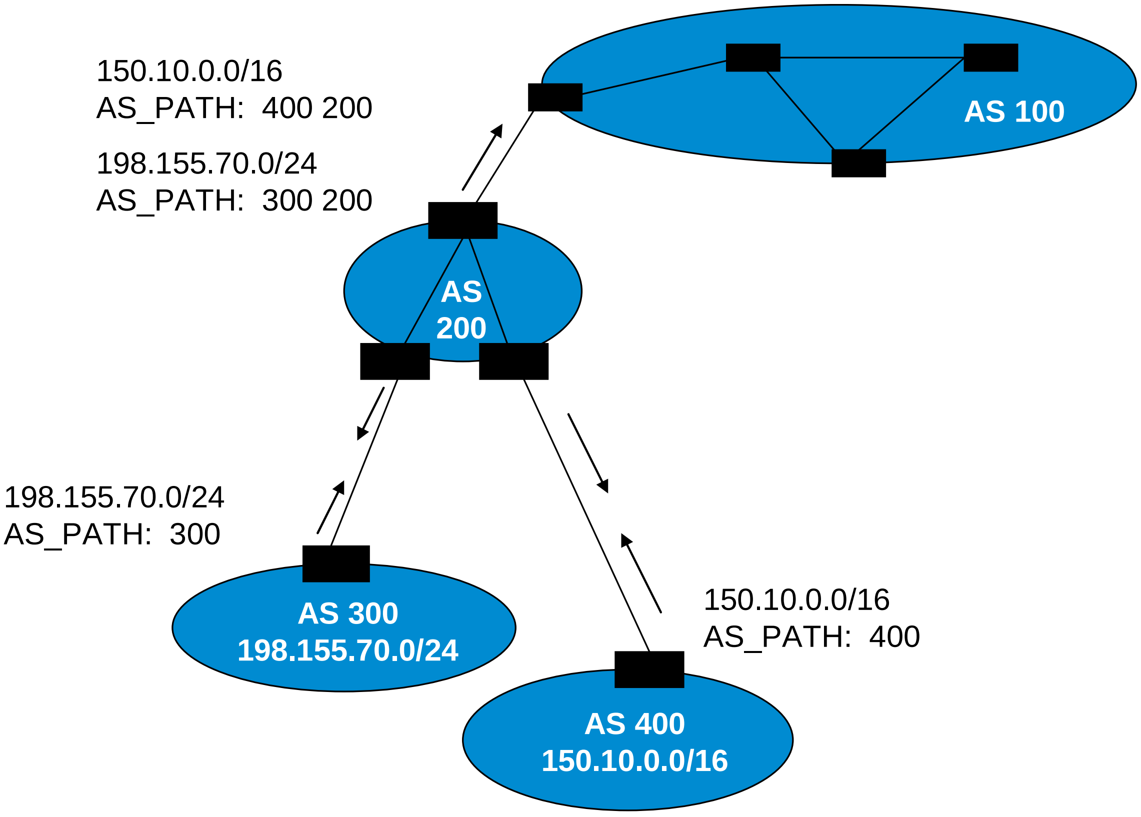


Figure 22: Network Layer Reachability Information

A "destination" is a range of IP addresses that are reported using prefix/length notation, where the "prefix" is the starting address of the range and "length" defines the size or boundaries of the range. For example, the destination 150.10.0.0/16 is a range consisting of the 65,536 (216) IP addresses between 150.10.0.0 and 150.10.255.255.

Path attributes, known in the BGP specification as AS_PATH, is a list of the autonomous systems through which a route passes. BGP4 routers can use this list of traversed autonomous systems to detect and eliminate routing loops.

Internal BGP

The ProCurve Secure Router 7000dl series supports both Internal iBGP and External eBGP. While there are many similarities between external and internal BGP, the most important difference is that the BGP speakers in an Internal BGP peer session are in the same AS. Internal BGP is used within a transit AS, as is shown in the diagram below. Please check http://www.procurve.com for free software updates due soon that will include further enhancements to BGP.

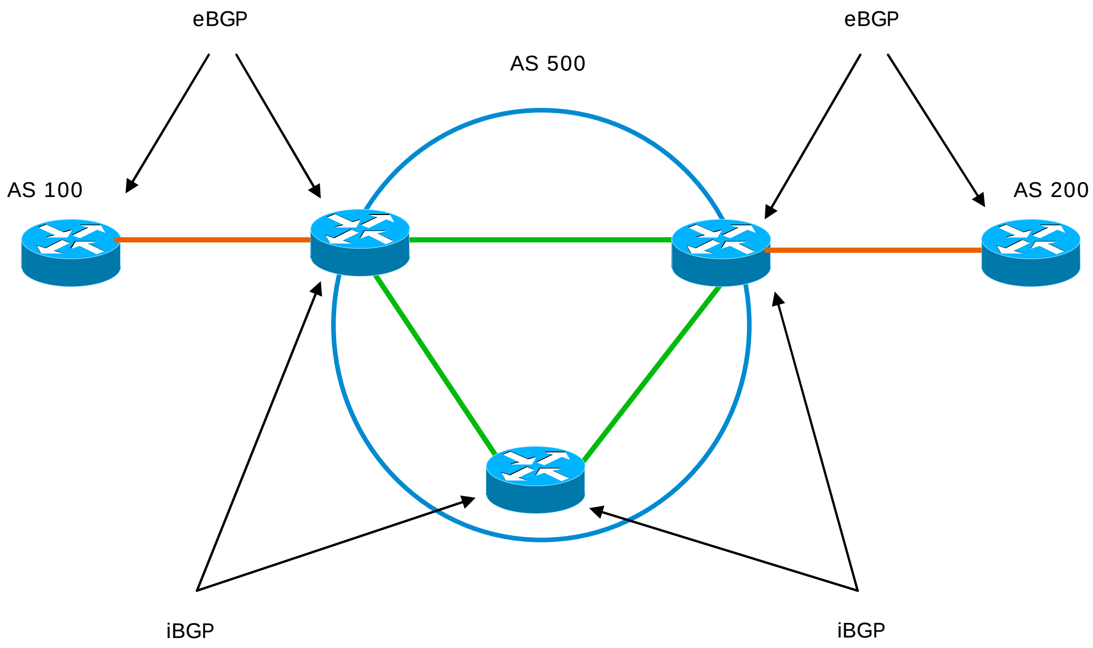


Figure 23: Internal BGP

If an AS has multiple BGP speakers, it could be used as a transit service for other ASs. As you can see in the iBGP diagram, AS 500 is a transit AS for AS 100 and AS 200.

It is necessary to ensure reachability within an AS before sending the information to an external AS. This is done by a combination of internal BGP peering between router inside an AS and by redistributing BGP information to Internal Gateway Protocols (IGPs) running in the AS.

When BGP is running between routers belonging to the same AS, it is call iBGP. When BGP is running between routers that are in different ASs, it is called eBGP.

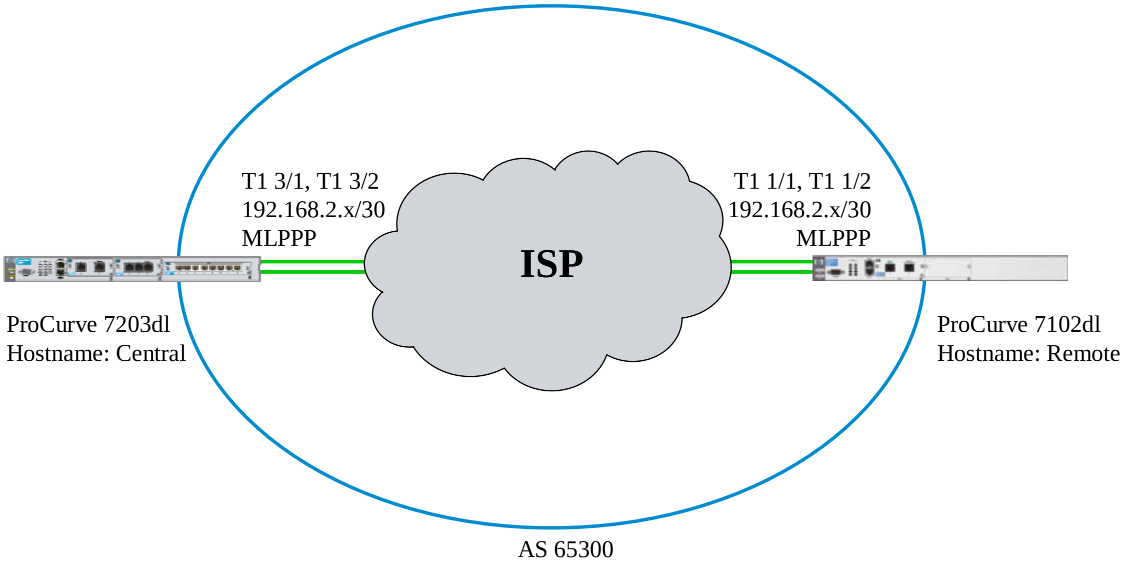


Figure 24: BGP Example

ProCurve Secure Router 7203dl

```
!
hostname "Central"
no enable password
```

```
!
ip subnet-zero
ip classless
ip routing
!
event-history on
no logging forwarding
no logging email
logging email priority-level info
!
!
!
interface eth 0/1
  ip address  192.168.3.254  255.255.255.0
  no shutdown
!
interface eth 0/2
  no ip address
  shutdown
!
!
!
interface t1 3/1
  tdm-group 1 timeslots 1-24 speed 64
  no shutdown
!
interface t1 3/2
  tdm-group 2 timeslots 1-24 speed 64
  no shutdown
!
interface t1 3/3
  shutdown
!
interface t1 3/4
  shutdown
!
interface t1 3/5
  shutdown
!
interface t1 3/6
  shutdown
!
interface t1 3/7
  shutdown
!
interface t1 3/8
  shutdown
!
interface ppp 1
  ip address  192.168.2.2  255.255.255.252
  ppp multilink
  no shutdown
  bind 1 t1 3/1 1 ppp 1
  bind 2 t1 3/2 2 ppp 1
!
!
router BGP 65300
no auto-summary
no synchronization
network 192.168.2.0 mask
255.255.255.252
neighbor 192.168.2.1
default-originate
soft-reconfiguration inbound
remote-as 65300
!
!
!
!
no ip tftp server
no ip http server
no ip http secure-server
no ip snmp agent
no ip ftp agent
!
!
!
!
!
!
!
line con 0
  no login
!
line telnet 0 4
  login
!
End
```

ProCurve Secure Router 7102dl

```
Remote#sh run
Building configuration...
!
!
hostname "Remote"
no enable password
!
ip subnet-zero
ip classless
ip routing
!
```

```
event-history on
no logging forwarding
no logging email
logging email priority-level info
!
!
!
!
!
interface eth 0/1
  ip address  192.168.1.254  255.255.255.0
  no shutdown
!
interface eth 0/2
  no ip address
  shutdown
!
!
!
interface t1 1/1
  clock source internal
  tdm-group 1 timeslots 1-24 speed 64
  no shutdown
!
interface t1 1/2
  clock source internal
  tdm-group 2 timeslots 1-24 speed 64
  no shutdown
!
interface adsl 2/1
  training-mode multi-mode
  shutdown
!
interface ppp 1
  ip address  192.168.2.1  255.255.255.252
  ppp multilink
  no shutdown
  bind 1 t1 1/1 1 ppp 1
  bind 2 t1 1/2 2 ppp 1
!
!
router BGP 65300
no auto-summary
no synchronization
network 192.168.2.0 mask
255.255.255.252
neighbor 192.168.2.2
     no default-originate
   soft-reconfiguration inbound
   remote-as 65300
!
!
!
!
no ip tftp server
no ip http server
no ip http secure-server
no ip snmp agent
no ip ftp agent
!
!
!
!
!
!
!
line con 0
  no login
!
line telnet 0 4
  login
!
end
```

Classless InterDomain Routing (CIDR)

It is within the BGP environment that the benefits of Classless InterDomain Routing (CIDR) become apparent. CIDR was suggested in the late 1980s and then later mandated by the Internet Engineering Task Force in the early 1990s when the number of networks attached to the Internet started to increase rapidly.

The diagram below illustrates the addressing relationship between an ISP, its subscribers, and other ISPs. Recall that in classless addressing, a starting address followed by a mask defines a range address whose size is some power of 2, regardless of the value in the first octet of the address.

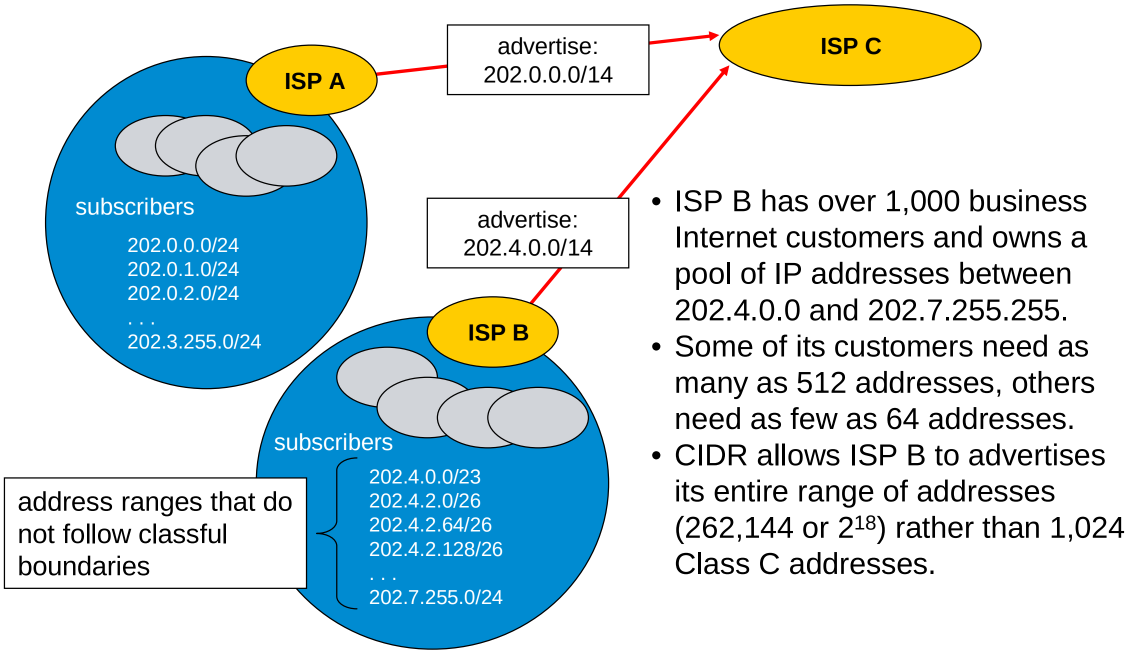
In the example, ISP A owns the range of addresses 202.0.0.0/14, provides Internet service to 1,024 businesses. This means that 262,144 (218) IP addresses between 202.0.0.0 and 202.3.255.255 are all reachable through ISP A. This ISP allocates a range of 256 addresses to each of its subscribers. Each of these address ranges is equivalent to a Class C network.

When ISP A advertises its address range to another service provider, ISP C, Classless InterDomain Routing allows the service provider to summarize the address range using a mask that breaks the rules of classful addressing because it is shorter than the natural mask.

If classless addressing were not allowed, this service provider would have to individually advertise 1,024 Class C network numbers (each with a classful 24-bit mask), beginning with 202.0.0.0, 202.0.1.0, 202.0.2.0, and continuing on through 202.3.255.0.

Given the fact that the total 32-bit IP address space allows over 2 million individual IP addresses, the ability to aggregate address space beyond classful boundaries minimizes the number of IP address ranges in the “core” of the Internet.

In the diagram below, ISP B advertises another address range –- 202.4.0.0/14.



- ISP B has over 1,000 business Internet customers and owns a pool of IP addresses between 202.4.0.0 and 202.7.255.255.
- Some of its customers need as many as 512 addresses, others need as few as 64 addresses.
- CIDR allows ISP B to advertises its entire range of addresses (262,144 or 2^{18}) rather than 1,024 Class C addresses.

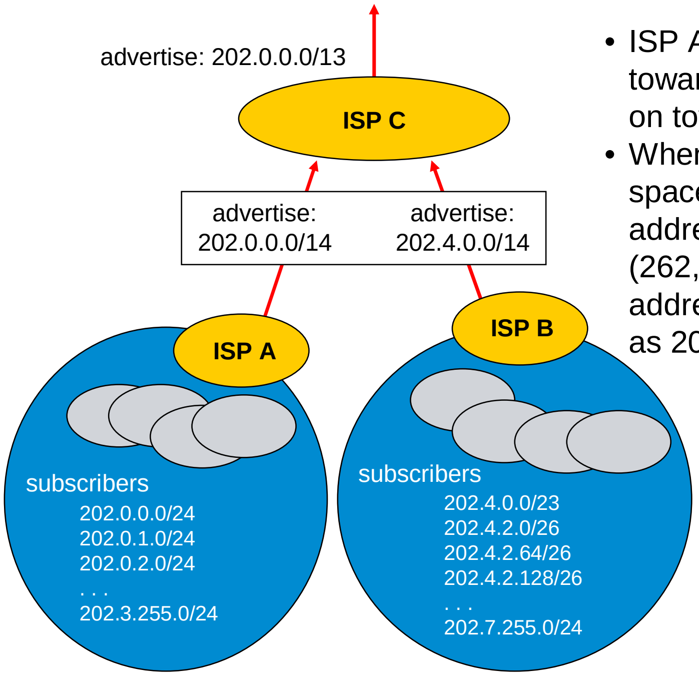
Figure 25: Classless InterDomain Routing – ISP B

As was true with ISP A, a range of 262,144 (218) IP addresses between 202.4.0.0 and 202.7.255.255 are reachable through ISP B. If constrained to classful addressing, this service provider would also have to individually advertise 1,024 Class C network numbers, beginning with 202.4.0.0, 202.4.1.0, 202.4.2.0, and continuing on through 202.7.255.0.

Notice that ISP B’s business customers have different size networks and thus require different address range sizes. In the diagram, some of the subscribers have an address range that uses a 26-bit mask and other subscribers use a 23-bit mask. Customers that have address ranges with a mask shorter than the 24-bit mask allowed by classful IP addressing may need to use classless internal route exchange protocols as well. RIP version 1 follows classful addressing rules, which means that an IP address in the range between 192.0.0.0 and 223.255.255.255 cannot have a mask shorter than 24 bits.

Classless addressing defines address ranges by specifying a starting address and a mask whose length is not restricted by the value in the first octet. An address range that has a 23-bit mask contains 512 addresses, and any address range that has a 26-bit mask contains 64 addresses.

When ISP C advertises this range of addresses to other providers, it can aggregate the address space into a single statement, which is shown below. The address range 202.0.0.0/13, defines a range of 524,288 addresses (219) between 202.0.0.0 and 202.7.255.255. If we were referring to this block of addresses in classful terms, there would be 2,048 Class C networks (211) between 202.0.0.0 and 202.7.255.0. CIDR minimizes the number of advertisements that are required to advertise this address space.



- ISP A and ISP B forward their traffic toward ISP C, who in turn forwards it on toward the Internet core.
- When ISP C reports the address spaces owned by ISP A (262,144 addresses or 2^{18}) and ISP B (262,144 or 2^{18}), it aggregates the address ranges in a single statement as 202.0.0.0/13 (524,288 or 2^{19}).

Figure 26: Classless InterDomain Routing – ISP C

The true benefit of CIDR is found in the "default-free zone" of the Internet. This is the top level of the hierarchy, a place that is sometimes called the "core". In every other part of the Internet, as well as in private enterprises, routers often make use of a "default route" that is used for forwarding traffic toward destinations whose addresses are not specifically known. However, every address range is represented in the default-free zone of the Internet; there are no default routes.

The developers of the CIDR concept saw it as a way to limit the complexity of route selection within the default free zone by limiting number of "routes" or address ranges. Without the classless address space aggregation that CIDR allows, there would be potentially over 2 million Class C addresses, 16,384 Class B addresses, and 126 Class A addresses, rather than the approximately 60,000 routes there are today.

Bridging and Routing at the same time. Caveats. The issue is when you have multiple layer 3 protocols and IP on the same remote network. Do I discuss or mention we will have it in future releases.

Overlapping address spaces and the longest mask rule

Though it is possible to encounter overlapping address spaces when using a single IP route exchange protocol, the use of multiple route exchange protocols increases the likelihood.

When the lookup process encounters multiple matches, it places the “next hop” for the MOST SPECIFIC match into the address cache. This is easiest to understand if you think of routing table entries as address ranges, rather than networks or subnets.

The “most specific match” rule is also known as the “longest mask” rule. If there is any match other than the default route (starting address 0.0.0.0 with a 0-bit mask), it will be the one used to route the traffic in question.

We will consider a few path selection examples. The following address spaces exist in the routing table:

- 10.10.15.0/24
- 10.10.0.0/16
- 10.0.0.0/8
- 0.0.0.0/0

In path selection example 1 a packet comes through with the destination address 10.10.15.12. This packet matches with all 4 address ranges, but the most specific match for that destination address is 10.10.15.0/24, which is a range of 256 addresses.

In path selection example 2 a packet comes through with the destination address 10.15.125.33. This packet matches with the last two address ranges. The most specific match is 10.0.0.0/8, which is a range of over 16 million addresses.

In path selection example 3 a packet comes through with the destination address 129.130.15.3. The most specific (and only) match is the default route (0.0.0.0).

Summary of Major Points

- IP version 4 overview of IP networks and subnetworks as it is still the primary addressing scheme used for by most companies world wide.
- There are both classful and classless IP addressing schemes.
- Route tables are used by routers to forward IP data from network to network
- Routers make decisions about forwarding IP through configuration of static routes or dynamic routing protocols.
- Static routes can be used to manually administer routing
- Dynamic routing protocols include, Routing Information Protocol (RIP), a distance vector protocol, and OSPF, a link state protocol.
- RIP is an early distance vector dynamic routing protocol, version 2 allows for CIDR
- OSPF version 2 is a link state dynamic routing protocol.
- Route summarization is a technique to help control the size of routing tables in routers and also control the amount of routing protocol traffic across WAN links.
- BGP is an external gateway protocol for interconnecting private autonomous systems.

How These Technologies are Used

- Use static routes for simpler topologies and smaller networks.
- Dynamic for multiple routing choices to make from point “A” to point “B”.
- Some dynamic routing protocols require multicasts, OSPF and RIP version 2. In order for these protocols to be used across the Internet, while IPSec VPNs are used, GRE will also need to be implemented. (IPSec VPN and GRE are discussed later in this paper).
- All of these protocols are used for the maintaining routing information for forwarding of IP data.

One of the most common techniques for controlling routing updates is the use of route summarization. It is used to both minimize the processing of routing data and to control traffic on a WAN. This paper summarizes the technique in a separate appendix at the end of this paper.

Advantages

The primary advantage of the dynamic over static routing protocols is that they update routing information based upon current route states.

The primary advantage of OSPF over RIP is that OSPF is more responsive than RIP. OSPF also allows for a greater diameter network and have greater flexibility for integration.

OSPF can be used effectively in both small and large networks. One key to remember is that for small networks you do not need to have “multiple areas”. Everything will work quite well on the backbone area.

Disadvantages

RIP is slower to converge. This means that if the network has become temporarily unstable, due to link outages or other reasons, network users will gain access to resources as quickly as with OSPF or Static routes.

OSPF is CPU and memory intensive in very large networks but this can be adjusted for with proper use of route summarization. Much of this also depends on the complexity and scale of the network.

What to Determine During Planning or for Implementation

- Addressing Schemes
- Ways to take advantage of summarization

Solution Examples for Layer 3

OSPF Solution Example 1

The customer has many customers that access their core network at Area 0. The customers need a reliable way to assure access to Area 0. Redundant routers with multiple links into Area 0 provide this reliability.

Note: Please note that these examples, and those in further sections, are given for your study and consideration only. They are to help you reach a better understanding of the fundamental concepts before configuring your own application. It will be necessary for you to modify these examples to match your own network design.

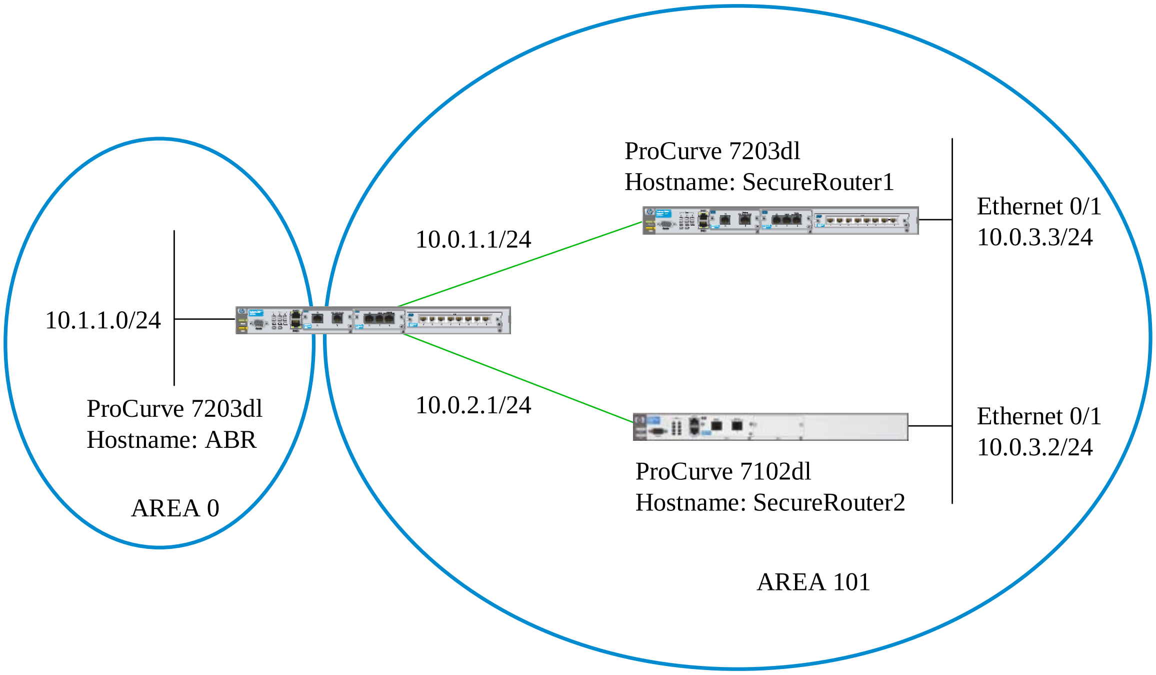


Figure 27: OSPF Solution Example 1

ABR (Area 0)

```
!
!
hostname "abr"
enable password pnb
!
ip subnet-zero
ip classless
ip routing
!
event-history on
no logging forwarding
no logging email
logging email priority-level info
!
!
!
interface eth 0/1
  ip address dhcp
  no shutdown
!
interface eth 0/2
  no ip address
  shutdown
!
!
!
interface t1 3/1
  tdm-group 1 timeslots 1-24 speed 64
  no shutdown
!
interface t1 3/2
  tdm-group 2 timeslots 1-24 speed 64
  no shutdown
!
interface t1 3/3
shutdown
!
interface t1 3/4
  shutdown
!
interface t1 3/5
  shutdown
!
interface t1 3/6
  shutdown
!
interface t1 3/7
  shutdown
!
interface t1 3/8
  shutdown
!
interface ppp 1
  ip address  10.0.1.1 255.255.255.252
  ip ospf network point-to-point
  no shutdown
  bind 1 t1 3/1 1 ppp 1
!
interface ppp 2
  ip address  10.0.2.1 255.255.255.252
  no shutdown
  bind 2 t1 3/2 2 ppp 2
!
!
router ospf
  network 10.1.1.0 0.0.0.255 area 0
  network 10.0.1.1 0.0.0.255 area 101
  network 10.0.2.1 0.0.0.255 area 101
  area 0 default-cost 1
!
!
!
no ip tftp server
no ip http server
no ip http secure-server
no ip snmp agent
no ip ftp agent
!
!
!
!
!
!
!
line con 0
  no login
!
line telnet 0 4
  login
  password pnb
!
end
```

Secure Router 1

```
!
!
hostname "SecureRouter1"
no enable password
!
ip subnet-zero
ip classless
ip routing
!
event-history on
no logging forwarding
no logging email
logging email priority-level info
!
```

```
!
!
!
!
!
!
!
!
!
!
!
!
interface eth 0/1
  ip address  10.0.3.3
255.255.255.0
  no shutdown
!
interface eth 0/2
  ip address dhcp hostname
"ProCurveSR7102dl"
  shutdown
!
!
!
interface t1 1/1
  tdm-group 1 timeslots 1-24
speed 64
  no shutdown
!
interface t1 1/2
  line-length 0
  shutdown
!
interface bri 1/3
 shutdown
!
```

```
interface ppp 1
  ip address  10.0.1.2
255.255.255.252
  ip ospf network point-to-point
  no shutdown
  bind 1 t1 1/1 1 ppp 1
!
!
router ospf
  network 10.0.3.1 0.0.0.255 area
101
  network 10.0.1.2 0.0.0.255 area
101
  area 101 default-cost 1
!
!
!
no ip tftp server
no ip http server
no ip http secure-server
no ip snmp agent
no ip ftp agent
!
!
!
!
!
!
!
line con 0
  no login
!
line telnet 0 4
  login
!
end
```

Secure Router 2

```
!
!
hostname "SecureRouter2"
no enable password
!
ip subnet-zero
ip classless
ip routing
!
event-history on
no logging forwarding
no logging email
```

```
logging email priority-level info
!
!
!
interface eth 0/1
  ip address  10.0.3.2
255.255.255.0
  no shutdown
!
interface eth 0/2
  no ip address
  shutdown
```

```
!
!
!
interface t1 3/1
  tdm-group 1 timeslots 1-24 speed 64
  no shutdown
!
interface t1 3/2
  shutdown
!
interface t1 3/3
  shutdown
!
interface t1 3/4
  shutdown
!
interface t1 3/5
  shutdown
!
interface t1 3/6
  shutdown
!
interface t1 3/7
  shutdown
!
interface t1 3/8
  shutdown
!
interface ppp 1
  ip address  10.0.2.2 255.255.255.252
  no shutdown
  bind 1 t1 3/1 1 ppp 1
!
!
router ospf
  network 10.0.3.1 0.0.0.255 area 101
  network 10.0.2.1 0.0.0.255 area 101
!
!
!
no ip tftp server
no ip http server
no ip http secure-server
no ip snmp agent
no ip ftp agent
!
!
!
!
!
!
!
line con 0
  no login
!
line telnet 0 4
  login
!
end
```

OSPF Solution Example 2

The customer has grown their business. Some new sectors were purchased, other sectors of their business have grown internally. They would like each entity to administer their own networks at each location as a separate entity or “area”. Some locations have RIP in their AS so that must be integrated also.

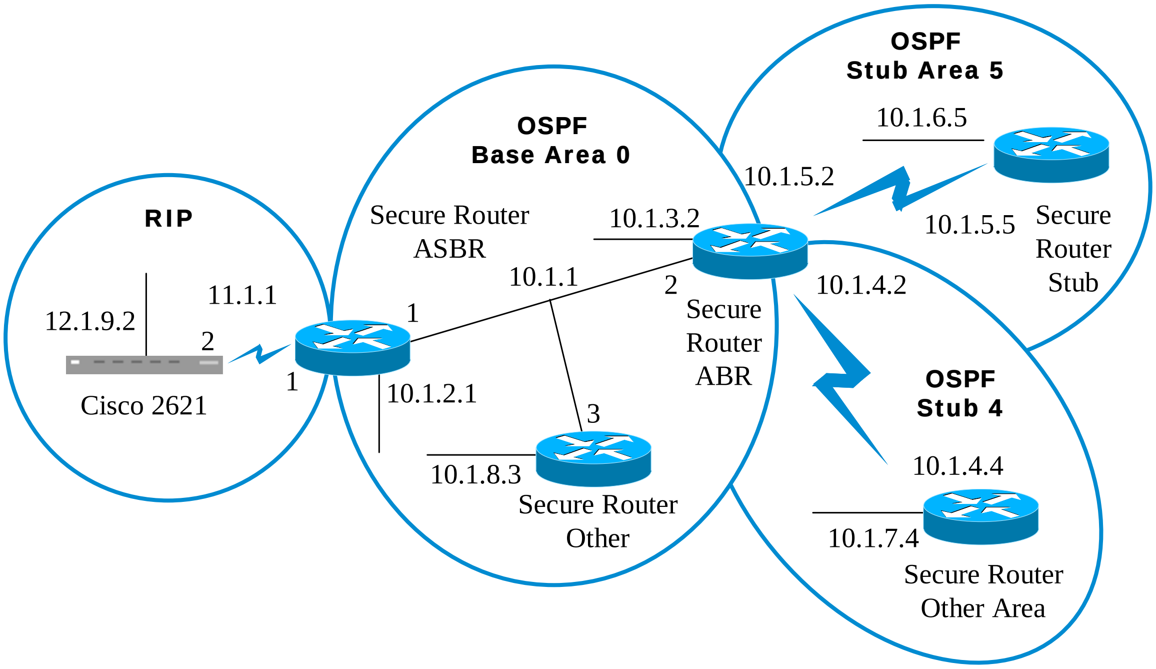


Figure 28: OSPF Solution Example 2

Base-Area.cfg

```
!
!
hostname "Other Area"
enable password pnb
!
ip subnet-zero
ip classless
ip routing
!
event-history on
no logging forwarding
no logging email
logging email priority-level info
!
username "pnb" password "pnb"
!
!
!
interface eth 0/1
  ip address  10.1.7.4
255.255.255.0
  no shutdown
  no lldp send system-description
  lldp send management-address
!
interface eth 0/2
  no ip address
  shutdown
```

```
  no lldp send system-description
  lldp send management-address
!
!
!
interface t1 1/1
  tdm-group 1 timeslots 1-24
speed 64
  no shutdown
!
interface ppp 1
  ip address  10.1.4.4
255.255.255.0
  no lldp send system-description
  lldp send management-address
  no shutdown
  bind 1 t1 1/1 1 ppp 1
!
!
router ospf
  network 10.1.4.0 0.0.0.255 area
4
  redistribute connected
!
!
!
no ip tftp server
no ip http server
no ip http secure-server
no ip snmp agent
no ip ftp agent
!
!
!
line con 0
  no login
!
line telnet 0 4
  login
!
end
```

Other-Base-Area.cfg

```
!
!
hostname "Other Base Area"
enable password pnb
!
ip subnet-zero
ip classless
ip routing
!
event-history on
no logging forwarding
no logging email
logging email priority-level info
!
username "pnb" password "pnb"
!
!
!
interface eth 0/1
  ip address  10.1.1.3
255.255.255.0
  no shutdown
  no lldp send system-description
  lldp send management-address
!
interface eth 0/2
  ip address  10.1.8.3
255.255.255.0
  no shutdown
  no lldp send system-description
  lldp send management-address
!
!
!
interface e1 1/1
  no shutdown
!
interface e1 1/2
  no shutdown
!
!
router ospf
  network 10.1.1.0 0.0.0.255 area
0
  redistribute connected
!
!
!
no ip tftp server
no ip http server
no ip http secure-server
no ip snmp agent
no ip ftp agent
!
!
!
line con 0
  no login
!
line telnet 0 4
  login
  password pnb
!
end
```

ABR.cfg

```
!
hostname "ABR"
enable password pnb
!
ip subnet-zero
ip classless
ip routing
!
event-history on
no logging forwarding
no logging email
logging email priority-level info
!
username "pnb" password "pnb"
```

```
!
!
!
interface eth 0/1
  ip address  10.1.1.2
255.255.255.0
  no shutdown
  no lldp send system-description
  lldp send management-address
!
interface eth 0/2
  ip address  10.1.3.2
255.255.255.0
  no shutdown
  no lldp send system-description
  lldp send management-address
!
!
!
interface t1 1/1
  tdm-group 1 timeslots 1-24
speed 64
  no shutdown
!
interface t1 1/2
  clock source through
  tdm-group 2 timeslots 1-24
speed 64
  no shutdown
!
interface ppp 1
  ip address  10.1.4.2
255.255.255.0
  no lldp send system-description
  no lldp send system-
capabilities
  lldp send management-address
  no shutdown
  bind 1 t1 1/1 1 ppp 1
!
interface ppp 2
  ip address  10.1.5.2
255.255.255.0
  no lldp send system-description
  lldp send system-capabilities
  no shutdown
  bind 2 t1 1/2 2 ppp 2
!
!
router ospf
  network 10.1.1.0 0.0.0.255 area
0
  network 10.1.4.0 0.0.0.255 area
4
  network 10.1.5.0 0.0.0.255 area
5
  area 5 stub no-summary
!
!
!
no ip tftp server
no ip http server
no ip http secure-server
no ip snmp agent
no ip ftp agent
!
!
!
line con 0
  no login
!
line telnet 0 4
  login
  password pnb
!
end
```

ASBR.cfg

```
!
!
hostname "ASBR"
enable password pnb
!
ip subnet-zero
ip classless
ip routing
!
event-history on
no logging forwarding
no logging email
logging email priority-level info
!
username "pnb" password "pnb"
!
!
!
```

```
!
!
!
interface eth 0/1
  ip address  10.1.1.1  255.255.255.0
  no shutdown
  no lldp send system-description
  lldp send management-address
!
interface eth 0/2
  ip address  10.1.2.1  255.255.255.0
  no shutdown
  no lldp send system-description
  lldp send management-address
!
!
!
interface t1 1/1
  tdm-group 1 timeslots 1-24 speed 64
  no shutdown
!
interface t1 1/2
  clock source through
  shutdown
!
interface t1 3/1
  shutdown
!
interface t1 3/2
  shutdown
!
interface t1 3/3
  shutdown
!
interface t1 3/4
  shutdown
!
interface t1 3/5
  shutdown
!
interface t1 3/6
  shutdown
!
interface t1 3/7
  shutdown
!
interface t1 3/8
  shutdown
!
interface modem 1/3
  shutdown
!
interface ppp 1
  ip address  11.1.1.1  255.255.255.0
  no lldp send system-description
  no lldp send system-capabilities
  lldp send management-address
  no shutdown
  bind 1 t1 1/1 1 ppp 1
!
!
router rip
  redistribute ospf
  redistribute connected
  network 11.1.1.0 255.255.255.0
!
!
router ospf
  network 10.1.1.0 0.0.0.255 area 0
  redistribute rip
  redistribute connected
!
!
!
no ip tftp server
no ip http server
no ip http secure-server
no ip snmp agent
no ip ftp agent
!
!
!
!
!
!
!
line con 0
  no login
!
line telnet 0 4
  login
  password pnb
!
end
```

Stub.cfg

```
!
!
hostname "Stub"
enable password pnb
!
ip subnet-zero
ip classless
ip routing
!
event-history on
no logging forwarding
no logging email
logging email priority-level info
!
username "pnb" password "pnb"
!
!
!
!
!
!
!
!
!
!
!
!
!
interface eth 0/1
  ip address  10.1.6.5
255.255.255.0
  no shutdown
  no lldp send system-description
  lldp send management-address
!
interface eth 0/2
  no ip address
  shutdown
  no lldp send system-description
  lldp send management-address
!
!
!
interface t1 1/1
  tdm-group 1 timeslots 1-24
speed 64
  no shutdown
!
interface t1 1/2
  line-length 0
  shutdown
!
interface ppp 1
  ip address  10.1.5.5
255.255.255.0
  no lldp send system-description
  lldp send management-address
  no shutdown
  bind 1 t1 1/1 1 ppp 1
!
!
router ospf
  network 10.1.5.0 0.0.0.255 area
5
  redistribute connected
  area 5 stub
!
!
!
no ip tftp server
no ip http server
no ip http secure-server
no ip snmp agent
no ip ftp agent
!
!
!
!
!
!
!
line con 0
  no login
!
line telnet 0 4
  login
!
end
```

Cisco 2621xm.cfg

```
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 2621_left
!
boot-start-marker
boot-end-marker
!
!
no network-clock-participate slot 1
no network-clock-participate wic 0
no aaa new-model
ip subnet-zero
ip cef
!
!
!
!
ip audit po max-events 100
no ftp-server write-enable
!
!
!
!
!
no crypto isakmp enable
!
!
!
interface FastEthernet0/0
 ip address 192.168.1.253 255.255.255.0
 ip rip send version 1
 ip rip receive version 1
 duplex auto
 speed auto
!
interface Serial0/0
 ip address 11.1.1.2 255.255.255.0
 ip rip send version 1
 ip rip receive version 1
 encapsulation ppp
 backup delay 30 60
 backup interface Dialer1
!
interface BRI0/0
 ip address 10.10.2.241 255.255.255.0
 shutdown
 dialer string 7850254
 dialer-group 1
!
interface FastEthernet0/1
 ip address 12.1.9.2 255.255.255.0
 duplex auto
 speed auto
!
interface Dialer1
 no ip address
!
router rip
 redistribute connected
 network 11.0.0.0
!
ip classless
ip http server
no ip http secure-server
!
!
dialer-list 1 protocol ip permit
!
!
control-plane
!
!
!
line con 0
line aux 0
line vty 0 4
 password password
 login
!
!
!
end
```

BGP Solution Example 1

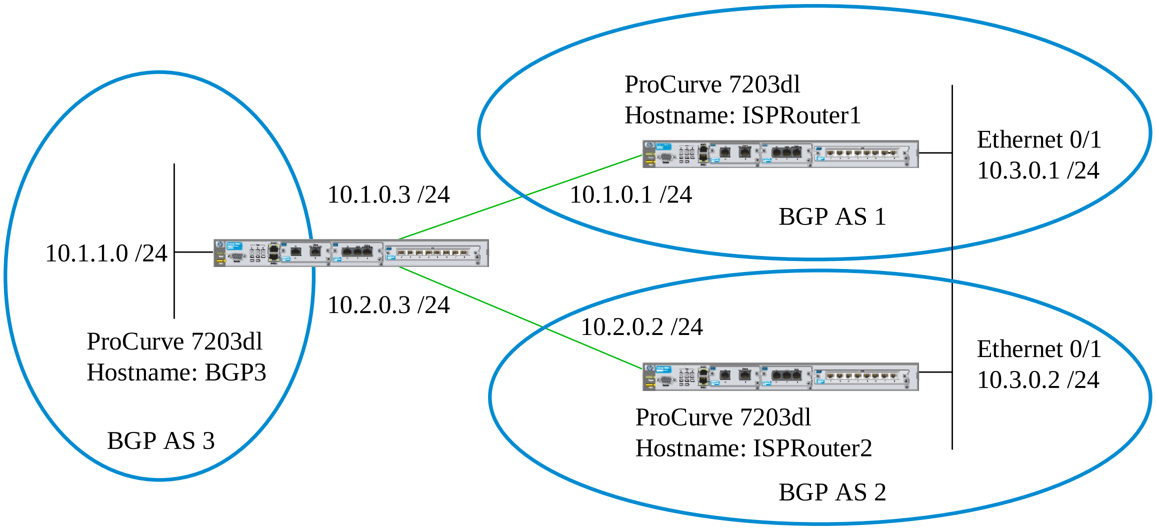


Figure 29: BGP Solution Example 1

BGP3

```
!
!
hostname "bgp3"
enable password pnb
!
ip subnet-zero
ip classless
ip routing
!
event-history on
no logging forwarding
no logging email
logging email priority-level info
!
!
!
interface eth 0/1
  ip address 10.1.1.0 /24
  no shutdown
!
interface eth 0/2
  no ip address
  shutdown
!
!
!
interface t1 3/1
  tdm-group 1 timeslots 1-24
speed 64
  no shutdown
!
interface t1 3/2
  tdm-group 2 timeslots 1-24
speed 64
  no shutdown
!
interface t1 3/3
  shutdown
!
interface t1 3/4
  shutdown
!
interface t1 3/5
  shutdown
!
interface t1 3/6
  shutdown
!
interface t1 3/7
  shutdown
!
interface t1 3/8
  shutdown
!
interface ppp 1
  ip address  10.1.0.3
255.255.255.0
  no shutdown
  bind 1 t1 3/1 1 ppp 1
!
interface ppp 2
  ip address  10.2.0.3
255.255.255.0
  no shutdown
  bind 2 t1 3/2 2 ppp 2
!
!
router ospf
  network 10.1.1.0 0.0.0.255 area
0
!
router bgp 3
  no auto-summary
  no synchronization
  bgp router-id 10.1.0.3
  neighbor 10.1.0.1
    no default-originate
    soft-reconfiguration inbound
    remote-as 1
  neighbor 10.2.0.2
    no default-originate
    soft-reconfiguration inbound
    remote-as 2
!
!
no ip tftp server
no ip http server
no ip http secure-server
no ip snmp agent
no ip ftp agent
!
!
!
!
!
!
!
line con 0
  no login
!
line telnet 0 4
  login
  password pnb
!
end
```

ISP Router 1

```
!
!
hostname "ISProuter1"
no enable password
!
ip subnet-zero
ip classless
ip routing
!
event-history on
no logging forwarding
no logging email
logging email priority-level info
!
!
!
interface eth 0/1
  ip address  10.3.0.1
255.255.255.0
  no shutdown
!
interface eth 0/2
  ip address dhcp hostname
"ProCurveSR7102dl"
  shutdown
!
!
!
interface t1 1/1
  tdm-group 1 timeslots 1-24
speed 64
  no shutdown
!
interface t1 1/2
  line-length 0
  shutdown
!
interface t1 2/1
  tdm-group 2 timeslots 1-24
speed 64
  no shutdown
!
interface t1 2/2
  clock source through
  shutdown
!
interface bri 1/3
  shutdown
!
interface modem 2/3
  shutdown
!
interface ppp 1
  ip address  10.1.0.1
255.255.255.0
  no shutdown
  bind 1 t1 1/1 1 ppp 1
!
interface ppp 2
  ip address  10.4.0.1
255.255.255.0
  no shutdown
  bind 2 t1 2/1 2 ppp 2
!
!
!
router bgp 1
  no auto-summary
  no synchronization
  network 10.1.0.0 mask
255.255.255.0
  network 10.3.0.0 mask
255.255.255.0
  network 10.4.0.0 mask
255.255.255.0
  neighbor 10.1.0.3
    no default-originate
    soft-reconfiguration inbound
    remote-as 3
  neighbor 10.3.0.2
    no default-originate
```

```
    soft-reconfiguration inbound
    remote-as 2
!
!
no ip tftp server
no ip http server
no ip http secure-server
no ip snmp agent
no ip ftp agent
!
!
!
!
!
!
!
line con 0
  no login
!
line telnet 0 4
  login
!
end
```

ISP Router 2

```
!
!
hostname "ISProuter2"
no enable password
!
ip subnet-zero
ip classless
ip routing
!
event-history on
no logging forwarding
no logging email
logging email priority-level info
!
!
!
interface eth 0/1
  ip address  10.3.0.2
255.255.255.0
  no shutdown
!
interface eth 0/2
  no ip address
  shutdown
```

```
!
!
!
interface t1 3/1
  tdm-group 1 timeslots 1-24
speed 64
  no shutdown
!
interface t1 3/2
  shutdown
!
interface t1 3/3
  shutdown
!
interface t1 3/4
  shutdown
!
interface t1 3/5
  shutdown
!
interface t1 3/6
  shutdown
!
interface t1 3/7
```

```
  shutdown
!
interface t1 3/8
  shutdown
!
interface ppp 1
  ip address  10.2.0.2
255.255.255.0
  no shutdown
  bind 1 t1 3/1 1 ppp 1
!
!
!
router bgp 2
  no auto-summary
  no synchronization
  network 10.2.0.0 mask
255.255.255.0
  network 10.3.0.0 mask
255.255.255.0
  neighbor 10.2.0.3
    no default-originate
    soft-reconfiguration inbound
    remote-as 3
  neighbor 10.3.0.1
    no default-originate
    soft-reconfiguration inbound
    remote-as 1
!
!
no ip tftp server
no ip http server
no ip http secure-server
no ip snmp agent
no ip ftp agent
!
!
!
line con 0
  no login
!
line telnet 0 4
  login
!
end
```

Customer Site 2

```
!
!
hostname "Customer2"
enable password pnb
!
ip subnet-zero
ip classless
ip routing
!
event-history on
no logging forwarding
no logging email
logging email priority-level info
!
!
!
!
interface eth 0/1
  no ip address
  shutdown
!
interface eth 0/2
  no ip address
  shutdown
!
!
!
interface t1 3/1
  tdm-group 1 timeslots 1-24
speed 64
  no shutdown
!
interface t1 3/2
  shutdown
!
interface t1 3/3
  shutdown
!
interface t1 3/4
  shutdown
!
interface t1 3/5
  shutdown
!
interface t1 3/6
  shutdown
!
interface t1 3/7
  shutdown
!
interface t1 3/8
  shutdown
```

```
!
interface adsl 2/1
  training-mode multi-mode
  shutdown
!
interface ppp 1
  ip address  10.4.0.2
255.255.255.252
  no shutdown
  bind 1 t1 3/1 1 ppp 1
!
!
!
ip route 0.0.0.0 0.0.0.0 10.4.0.1
!
no ip tftp server
no ip http server
no ip http secure-server
no ip snmp agent
no ip ftp agent
!
!
!
line con 0
  no login
!
line telnet 0 4
  login
  password pnb
!
end
```

Feature Set Consideration for ProCurve Secure Router 7000dl Series

- The ProCurve Secure Router 7000dl series supports the following Layer 3 protocols as of this writing:
    - o Static Routing
    - o RIP version 1 and 2
    - o OSPF
    - o BGP 4
- RIP versions must be set to only version 1 or version 2. There is currently no “compatibility” mode.
- Check http://procurve.com for the latest free software update, or for additions to the physical interfaces supported.

How to Use the ProCurve Secure Router 7000dl Series

- Both the 7102dl and 7203dl work effectively with all protocols. The 7203dl has the edge in memory; 7102dl at 128Mbytes and the 7203dl at 256Mbytes.

Additional Topics

The following topics are beyond the scope of this paper. Never the less they are covered here as overview information so the designer can make better decisions regarding these topics and be reminded that these are aspect they should consider after the basic design is met.

High Availability and Redundancy

The designer needs to keep in mind aspects of the customer need for resiliency in their network. Redundancy needs to be considered at all layers of the OSI model.

Redundancy can be built into the customer network at Layer 1 and 2 through optional backup modules, MLFR, MLPPP. Remember that ISDN will operate at up to 128K bps but is far short of the full speed of a T1 or E1.

Layer 3 redundancy methods include designs that use multiple routes between sites. An example of an OSPF configuration is included in this guide for consideration. For the client to router redundancy, the use of VRRP on the routing switches at the distribution layer are recommend so that if the primary router goes down, the clients still have connectivity through one of the switches.

Often the customer would like to use a different carrier for redundant paths. The Internet can provide such an option. The primary link can be through a private carrier and utilize PPP or

Frame Relay. The backup link would be to the ISP. Any interface can be used to gain access to the Internet and route selection can be controlled through the use of administrative distance parameters.

See the ProCurve Secure Router 7000dl Series documentation set for further information.

IP Multicast

From a branch office perspective there is little requirement for extensive routing of multicasts. There is a requirement for many to forward multicasts through the router to the central site. The ProCurve Secure Router 7000dl series use a multicast route helper to allow for this.

Use the “ip mcast-stub helper-address” command to specify an IP address toward which IGMP host reports and leave messages are forwarded. This command is used in IP multicast stub applications in conjunction with the ip mcast-stub downstream and ip mcast-stub upstream commands. Use the no form of this command to return to default. If there are multiple hops from the WAN edge (central office) to the remote site, GRE-tunneling can be used to from a virtual path between the central site and the remote site. This tunnel can be used as the foundation for multicast stub routing.

The helper-address is configured globally and applies to all multicast-stub downstream interfaces. The address specified may be the next upstream hop or any upstream address on the distribution tree for the multicast source, up to and including the multicast source. The router selects, from the list of multicast-stub upstream interfaces, the interface on the shortest path to the specified address. The router then proxies, on the selected upstream interface (using an IGMP host function), any host joins/leaves received on the downstream interface(s). The router retransmits these reports with addresses set as if the report originated from the selected upstream interface.

For example, if the router receives multiple joins for a group, it will not send any extra joins out the upstream interface. Also, if it receives a leave, it will not send a leave until it is certain that there are no more subscribers on any downstream interface.

See the “SROS Command Line Interface Reference Guide” for further information.

Security, Access Control Lists, and Virtual Private Networks

Security, which include many more facets than simply firewalls and access policies, should be considered during the design phase. This is especially critical if the routers will connect to a public network such as the Internet.

See the “SROS Command Line Interface Reference Guide” and the “Virtual Private Network (VPN) Configuration Guide” in the ProCurve Secure Router 7000dl Series documentation set for further information.

Quality of Service

Quality of Service should be considered apart from the WAN alone. How the customer uses the network will play heavily in these decisions. When building the “converged” network utilize the solution design guides at the http://www.procurve.com web site.

See the “Low-latency Queuing Configuration Guide”, and the “SROS Command Line Interface Reference Guide” in the ProCurve Secure Router 7000dl Series documentation set for further information.

Appendix A – Route summarization

Routing among locations

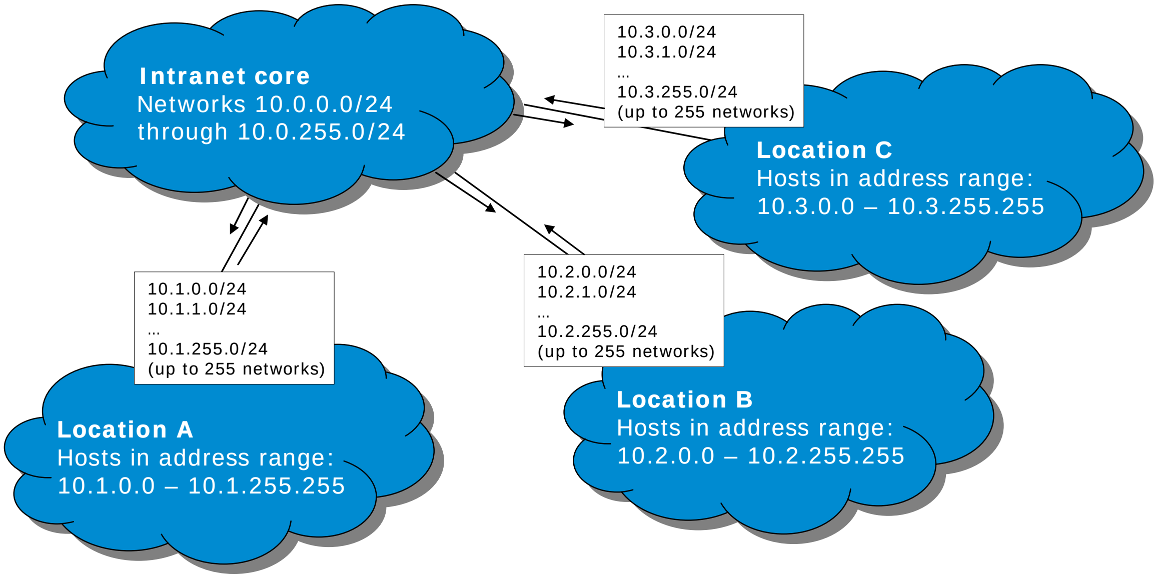


Figure 30: Routing among Locations

In this example, the routing infrastructure supports more than 750 user networks distributed across three physical locations. While the technologies in place are similar to earlier examples, which showed only eight user networks, the complexity of this topology presents a few new challenges.

For instance, because there are so many networks at each location, it is inefficient—and possibly impossible—to connect every router to the intranet core. Instead, the topology features redundant links among routers at each location. Another layer of aggregates the traffic from the hosts at each location and connects that router to the core. This multi-layered hierarchical approach can be scaled to support a network with hundreds of locations, if necessary.

Dynamic route exchange

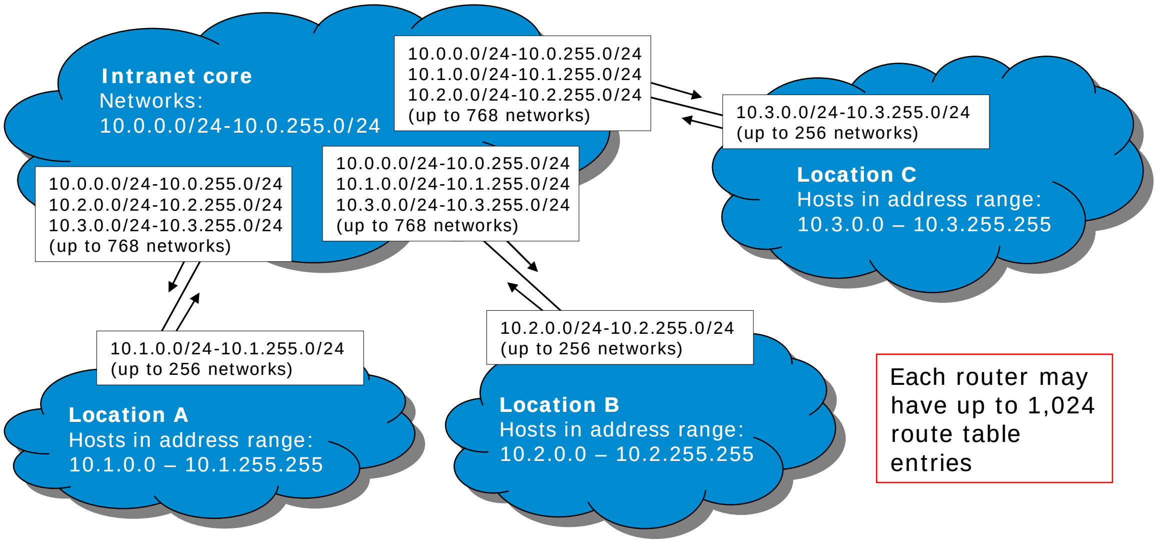


Figure 31: Dynamic Route Exchange

A topology such as the one shown can result in very inefficient route tables. In the example, each location includes 255 networks. Consequently, if every router advertises every route table entry to all of its neighbors, every router in the entire intranet will have over 750 entries in its route table. This is highly inefficient because it is not necessary for every router to know every network. The number of connections between each location and the intranet core is limited to one or two. Consequently, for each location all traffic destined for networks at other locations will travel on one link or, if the routers support ECMP, will be shared by both links.

To avoid this inefficiency, IP network designers usually assign contiguous address space to physically separated locations, regardless of whether they are buildings within the same campus separated by a short distance or campuses within a larger enterprise that are separated by a greater distance. This makes it possible to summarize the address space, enabling a larger number of physical networks to be represented by a single route table entry.

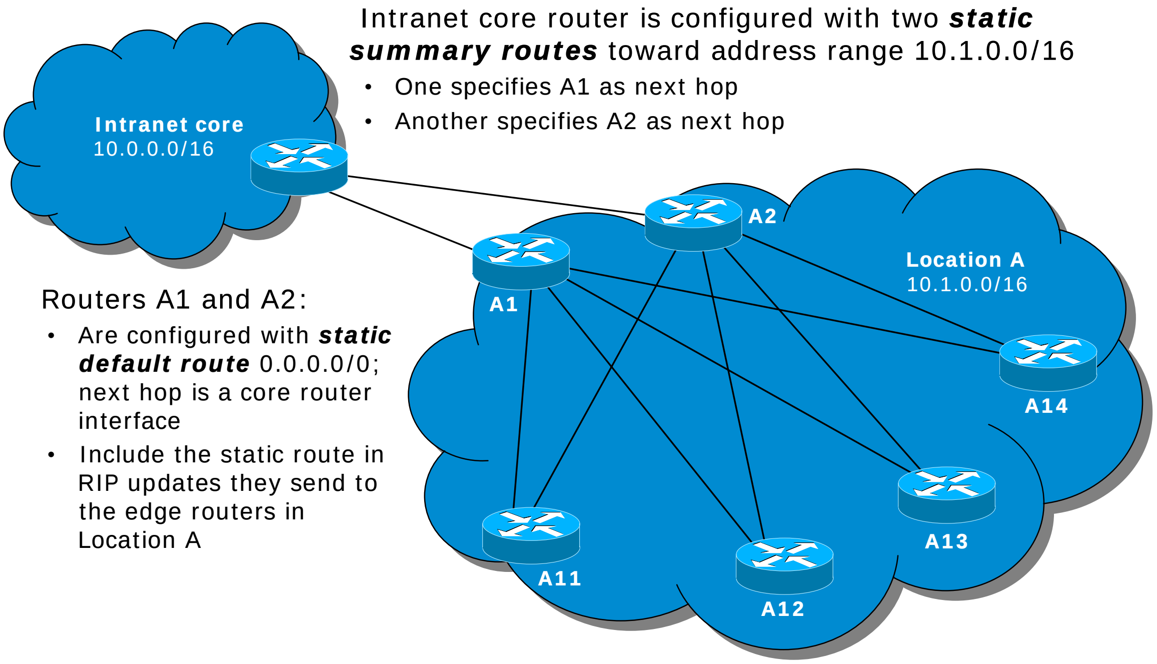
Network summarization

Often, routers at a location have a limited number of paths to the networks within a given address range. In these cases, you can increase routing efficiency by replacing many individual, specific network advertisements with a single statement that specifies a larger range of addresses using a shorter mask. In all cases, a shorter mask specifies a larger address range and a longer mask specifies a shorter range. Any starting address with a 24-bit mask specifies a range with 256 addresses. A starting address with a 16-bit mask specifies a range of 65,536 addresses.

This process is known as “network summarization.” In most vendor implementations, neither RIP nor OSPF performs this summarization automatically; both require that you perform some additional configuration steps to enable network summarization.

For example, in a hierarchical network, all traffic from Location A that is destined for other locations must go through one of the routers connected to the core.

Summarization of address space using static routes



Intranet core router is configured with two ***static summary routes*** toward address range 10.1.0.0/16

- One specifies A1 as next hop
- Another specifies A2 as next hop

Routers A1 and A2:

- Are configured with ***static default route*** 0.0.0.0/0; next hop is a core router interface
- Include the static route in RIP updates they send to the edge routers in Location A

Figure 32: Summarization of address space using static routes

In networks that implement RIP, static routes usually provide the mechanism for network summarization.

In this example, network summarization will prevent routers in Location A from obtaining detailed, specific advertisements for every network in the intranet. This process requires two steps:

1. Disable the operation of RIP on both sides of the links that connect Routers A1 and A2 to the intranet core. This, of course, prevents the routers in Location A from processing RIP advertisements sent from the core.
2. Define static routes for the path to networks or address ranges that do not appear as more specific routes in the route able.

In the example, the goal is to provide a path for hosts at Location A to reach all destinations that cannot be found at Location A, including addresses on the public Internet. To accomplish this, you would specify the default route (0.0.0.0/0) that uses an intranet core interface as the next hop.

While the core router may use a default static route to reach addresses in the pubic Internet, it can't use the default route to reach hosts at different locations. Instead, the intranet core might have a summarized route to each location. Because the addressing scheme is hierarchical, and all hosts between 10.1.0.0 and 10.1.255.255 are at Location A, you can define a static summary route for the path the core router has to Location A with the starting address 10.1.0.0 and a 16-bit mask (10.1.0.0/16). The 16-bit mask defines a range of over 65,536 addresses, although some number of the addresses in this range would be inappropriate for host addressing purposes.

Because the mask is 16 bits long, the first two octets of a destination address must match with the starting address (10.1.0.0). The values in the remaining 16 bits are irrelevant for the purposes of determining whether a given address is within the range. Any combination of zeros and ones in the last 16 bits constitutes an unconditional match.

This means that every address that starts with a “10” in the first octet, has a “1” in the second octet, and has any binary combination between 00000000 00000000 (0.0.) and 11111111 11111111 (255.255) is a member of the range specified by the starting address ‘10.1.0.0’ and the mask of “/16.” This includes all addresses between 10.1.0.0 and 10.1.255.255.

Although the diagram shows detailed operation only for Location A, the same procedures would be used for other locations. The intranet core router(s) would need to have static routes specifying each of the locations’ address ranges. It would forward traffic destined for a given address range in the direction of the appropriate location. The routers that connect each location to the intranet core will use the default route to forward all traffic for which it does not have a more specific route in its route table.

Many routers treat the default static route as a special case of static route. That is, without special configuration, some routers will not place the default route into its route table, even if it advertised within a RIP update. Typically, if a router does not automatically listen for or accept the default route, it is usually possible to selectively enable default route listening or to enable it for all RIP interfaces on the router.

Summarizing remote address space

Without network summarization, a large enterprise with many locations connected through a limited number of links to a centralized core may create an unnecessary burden on routers. Memory and route table space are used inefficiently when the route table on a router describes specific routes to every remote network and all of them have the same next hop.

RIP networks offer several options for summarizing address space. In one approach, you can define each location with a separate classful network address range and have the routers summarize all of the specific routes into the classful network.

For example, if you have 16 or fewer locations, you could assign Class B public addresses to each location and configure the routers that connect the location to the core to summarize all of the specific routes into the classful network. The Class B public address range is 172.16.0.0/12, which means that there are 16 individual Class B networks: 172.16.0.0/16, 172.17.0.0/16, 172.18.0.0/16, up to 172.31.0.0/16. Each location could support 65,536 addresses, which might be divided into 256 subnets, each of which has a 24-bit mask. Networks at Location 1, for example, might be 172.16.0.0/24, 172.16.1.0/24, 172.16.2.0/24, 172.16.3.0/24 and so on. Other locations would be configured similarly.

The routers that connect the location to the core would be configured to automatically summarize all of the specific networks into the Class C “parent” network such as 172.16.0.0/16.

Summarizing at classful network boundaries

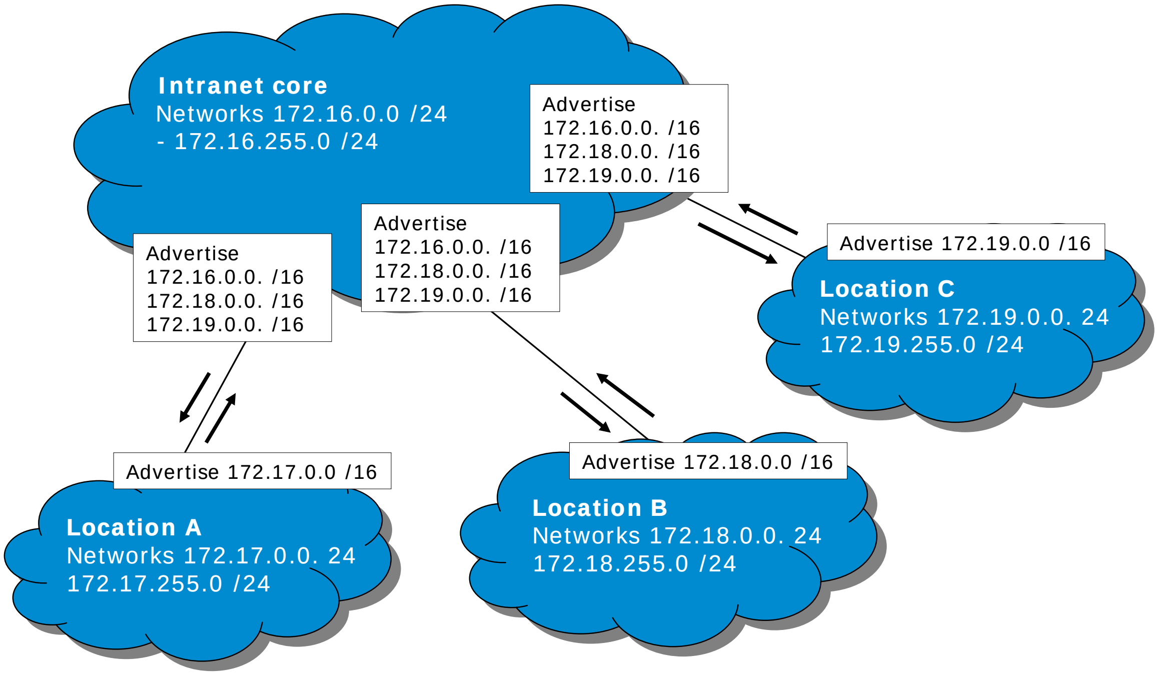


Figure 33: Example of Classful Network Summarization

In this example, the administrator of an intranet using Class B private addresses for the enterprise has allocated network numbers along classful boundaries. All of the networks at a given location are within the same Class B network.

If each location is connected to the core by 5300xl/3400cl routing switches, the switches will automatically summarize the subnets at classful boundaries. All such networks will be summarized if they do not extend into the network that connects the location to the core.

For example, the link that connects Location A to the core must not be within the address range 172.17.0.0/16. An appropriate address for this network (to enable auto-summarization) would be within the 172.16.0.0/16 range, the range assigned to the core. You could assign to this network a Class C private address such as 192.168.10.0/24. Basically, any address that is not within 172.17.0.0/16 would allow auto-summarization to work.

However, if you assigned individual class C private networks to each of the location-to-core links, each of these networks would appear in every router's route table at all locations. These network addresses could not be automatically summarized. They are not subnets of a larger parent network, but, from a classful perspective, each network in the range 192.168.0.0/24-192.168.255.0/24 is a separate network.

It would be more efficient to make the location-to-core links a part of the range assigned to the core. That way they would be part of the larger summary network and not represented individually in each route table (across the entire intranet).

Summarizing a larger address space

Static routes are completely flexible. As long as an address range can be summarized using a starting address and mask, you can create a static route for it. In the example above, an administrator has used a single statement to define a range that includes all 16 private Class B networks. Consequently, each route table requires one static route instead of three.

Note that the specific networks 172.17.10.0/24 and 172.17.30.0/24 are contained within the summarized address range 172.16.0.0/12. Actually, that range contains 1,048,576 (65,536 * 16) addresses.

When the router receives packets to be forwarded, it runs a matching operation against route table entries and forwards the traffic to the next hop (gateway) associated with the most specific match.

In the example, a packet with the destination address 172.17.10.10 matches the first and second entries. The second entry, 172.17.10.0/24, is more specific because it has a longer mask. The router will forward the packet accordingly.

The summarization rules provide a useful guideline for address range assignment. Suppose, for instance, that you were developing the IP addressing scheme for the Northwest campus of ProCurve University, which uses 10.2 for the first octets. The lowest numbered range of four networks would have starting addresses of 10.2.0.0 and mask of 255.255.252.0 or 22 bits.

The four networks in the range are:

- 10.2.0.0/24
- 10.2.1.0/24
- 10.2.2.0/24
- 0.2.3.0/24

Other ranges of four networks are expressed as 10.2.4.0/22, 10.2.8.0/22, 10.2.12.0/22, 10.2.16.0/24 etc. all the way up to 10.2.240.0/22, 10.2.244.0/24, 10.2.248.0/24, and 10.2.252.0/24.

The complete set of starting addresses for a range of eight networks that each have a 24-bit mask are 10.2.0.0/21, 10.2.8.0/21, 10.2.16.0/24, 10.2.24/0/24, all the way up to 10.2.224.0/24, 10.2.232.0/21, 10.2.240.0/21, and 10.2.248.0/21. Since all of the addresses in the address scheme that have a 2 in the second octet are reserved for the Northwest campus, the entire third octet can be distributed among the networks at this location.

Appendix B – Glossary

The following glossary is included for convenience and is not exhaustive. This paper focuses on WAN design and so this glossary. For further information the designer should consult the many references listed on the Internet along with the references noted at the end of this paper.

2B1Q

Short for 2 Binary, 1 Quaternary. 2B1Q is a full-duplex digital signaling technique used by many digital communications technologies (like ISDN) to send data over a single pair of wires. It uses a system of three different voltages: one for each of the two binary states (the 2B part of "2B1Q") and a third, quaternary voltage that indicates both ends of the data connection are sending the same binary value.

AAL

ATM Adaptation Layer– The standards layer that allows multiple applications to have data converted to and from the ATM cell. A protocol used that translates higher layer services into the size and format of an ATM cell.

ADPCM

Adaptive Differential Pulse Code Modulation– A technique for converting sound or analog information to binary information (a string of 0’s and 1’s) by taking frequent samples of the sound and expressing the value of the sampled sound modulation in binary terms.

ADSL

Asymmetric Digital Subscriber Line– Supports two way asymmetrical transmission of data over voice lines, downstream data bandwidth differs from upstream data bandwidth. Check current implementation for data rates.

AMI

Alternate Mark Inversion– Line-coding used with a T1 circuit where zeros are transmitted as zeros and ones are transmitted as pulses with alternating polarity.

Analog

Continuously varying electrical signal in the shape of a wave used for voice or data transmission.

ANI

Automatic Number Identification– A service that provides the receiver of a telephone call with the number of the calling phone.

ANSI

American National Standards Institute– The primary organization for fostering the development of technology standards in the United States.

AO/DI

Always On/Dynamic ISDN– Allows the BRI “D” channel to be used for low-speed data connection.

ASCII

American Standard Code for Information Interexchange– ASCII is the most common format for text files in computers and on the Internet. In an ASCII file, each alphabetic, numeric, or special character is represented with a 7-digit binary number (a string of seven 0s or 1s). 128 possible characters are defined.

ASIC

Application-Specific Integrated Circuit– A silicon chip designed for a special application, such as a particular kind of transmission protocol or hand-held computer.

Asymmetric Connection

A connection where data can flow in one direction at a much higher speed than in the other. Some examples of asymmetric connections are ADSL, 56K Modems, and satellite downlinks.

Asynchronous

A method of data transmission which allows characters to be sent at non-predetermined intervals by preceding each character with a start bit and ending each character with a stop bit.

ATM

Asynchronous Transfer Mode– A dedicated, packet switched technology that allows high-speed transmission of data through the use of small, fixed-length packets (cells). These cells are of 53 bytes, with 48 bytes being payload and the remaining 5 bytes for header information. The transfer mode in which the information is organized into cells. It is asynchronous in the sense that the recurrence of cells containing information from an individual user is not necessarily periodic.

Authentication

The process of establishing an information source or users identity for secure transactions like virtual private networking.

B8ZS

Bipolar 8 Zero Substitution– The coding used to maintain ones density on a T1 circuit. This is done by the insertion of two deliberate bipolar violations (two consecutive ones having the same voltage) which replace the customers consecutive zero bits.

BECN

Backward Explicit Congestion Notification– A bit set by a Frame Relay network to notify an interface device (DTE) that congestion avoidance procedures should be initiated by the sending device.

BER

Bit Error Rate– The percentage of bits that have errors relative to the total number of bits received in a transmission usually expressed as ten to a negative power. For example, a transmission might have a BER of 10 to the minus six, meaning that out of 1,000,000 bits transmitted, one bit was in error.

BERT

Bit Error Rate Test– A procedure or device that measures the BER for a given transmission.

BISDN

Broadband Integrated Services Digital Network– Any circuit capable of transmitting more than one Basic Rate ISDN.

BGP

Border Gateway Protocol– A protocol for exchanging routing information between gateway hosts (each with its own router) in a network of an autonomous system. BGP is often the protocol used between gateway hosts on the Internet.

BOC

Bell Operating Company– A term for any of the 22 original companies (or their successors) that were created when AT&T was broken up in 1983 and given the right to provide local telephone service in a given geographic area.

BONDING

Bandwidth ON Demand INteroperability Group– This group develops the standard that provides for the aggregation of data from multiple ISDN calls into a coherent data stream.

bps

Bits per second– In data communications, a common measure of data speed for computer modem and transmission carriers. As the term implies, the speed in Bps is equal to the number of bits transmitted or received each second.

BRI

Basic Rate Interface ISDN– A user to network interface consisting of two 64KBIT/s bearer (B) channels and one 16KBIT/s signaling (D) channel. The “B” channels carry data, voice or video traffic. The “D” channel is used to set up calls on the B channels and carry packet data.

Bursty/Burstiness

Sporadic use of bandwidth that does not use the total bandwidth of a circuit 100 percent of the time.

Caller ID

Caller ID is a telephone company feature that notifies a telephone being called of who is (or at least what phone number is) originating the call. On analog POTS phone systems, Caller ID information is transmitted to the telephone set between the first and second ring of the phone. On ISDN sets, Caller ID data is sent as part of the Q9.31 "call setup" information sent of the ISDN D channel. Some states, like California, regulate the implementation of Caller ID very strictly, requiring that phone companies offer their customers the option of keeping their numbers private when placing a call.

Carrier

(1) Telecommunications term for the PTT, LEC, or RBOC that provides the physical medium and the transmission technology for connecting customers to the resources allowing Wide Area Networking. (2) An alternating-current wave of constant frequency, phase and amplitude. By varying (modulating) the frequency, phase or amplitude of a carrier wave, information is transmitted.

C-Bit Parity

Framing format for a DS-3 signal. This provides possibilities for in-service, end-to-end path performance monitoring of the DS-3 signal, and in-band data links.

CCITT

Consultative Committee on International Telegraphy and Telephony– The CCITT, now known as the ITU-T (International Telecommunications Union– Telecommunications Services Sector), is the primary international body for fostering cooperative standards for telecommunications equipment and systems.

CDMA

Code Division Multiple Access– One of the three wireless telephone transmission technologies. After digitizing the data, it spreads it out over the entire bandwidth it has available. Multiple calls are overlaid over each other on the channel, with each assigned a unique sequence code.

CDR (Call Detail Record)

A data record typically used in a telephony system to record usage information on a per-call basis. Typical fields in the record include originating number, terminating number, start-time, duration, etc.

Content Delivery Network or Content Distribution Network

Intelligent or “content-aware” networks that enable dependable and responsible delivery of content to the edge of the Internet or the eventual end user.

CDSL

Consumer Digital Subscriber Line– A trademarked version of DSL that is somewhat slower than ADSL (1 Mbps downstream, probably less upstream) but has the advantage that a “splitter” does not need to be installed at the user’s end.

Channelized

A circuit that is created by the multiplexing-demultiplexing voice and/or data bandwidth using analog or digital techniques.

CIR

Committed Information Rate– The committed rate (usually less than the access rate) which the carrier guarantees to be available to transfer information to its destination under normal circumstances for a particular PVC.

CLEC

Competitive Local Exchange Carrier– In the United States, a CLEC is a company that competes with the already established local telephone business by providing its own network and switching. The term distinguishes new or potential competitors from established local exchange carriers and arises from the Telecommunications Act of 1996 which was intended to promote competition among both long-distance and local phone service providers.

CMIP

Common Management Information Protocol– A network management protocol built on the Open Systems Interconnection (OSI) communication model. The related Common Management Information Services (CMIS) defines services for accessing information about the network objects or devices, controlling them, and receiving status reports from them.

CO

Central Office– In the United States, an office in a locality to which subscriber home and business lines are connected on a local loop. It has equipment that can switch calls locally or to long-distance carrier phone offices.

CoS

Class of Service– A way of managing traffic in a network by grouping similar types of traffic together and treating each type as a class with its own level of service priority.

CPE

Customer Premises (Provided) Equipment– Equipment that is on the end user's side of the network interface and is not usually owned by the Local Exchange Carrier. Some examples of this equipment are CSU/DSUs, modems and telephones.

CRC

Cyclic Redundancy Check– A method of checking for errors in data that has been transmitted on a communications link. A sending device applies a 16- or 32-bit polynomial to a block of data that is to be transmitted and appends the resulting cyclic redundancy code to the block.

CRM

Customer Relationship Management– An information industry term for methodologies, software, and usually Internet capabilities that help an enterprise manage customer relationships in an organized way.

CSP

Competitive Service Provider– All companies in competition to deliver telecommunications services to both businesses and individuals.

CSU

Channel Service Unit– A device that provides an accessing arrangement at a user location to either switched or pointto- point, data-conditioned circuits at a specifically established data signaling rate. Note: A CSU provides local loop equalization, transient protection, isolation, and Central Office loop-back testing capability.

CTI

Computer Telephony Integration– The use of computers to manage telephone calls.

D4 (SF)

A T1 transmission Superframe format consisting of 12 frames of 192 bits each plus an additional 193rd bit used for link control and error checking.

DACS

Digital Access & Cross-connect System– Allows T1 carrier facilities (or any other subchannels) to be switched or cross-connected to another T1 carrier.

DBU

Dial Back-Up– A means of providing disaster recovery for a circuit that has failed.

DCE

Data Communications Equipment– A device which provides all the functions required for connection to local exchange carrier's lines and for converting signals between telephone lines and DTE.

DDS

Dataphone Digital Service or Digital Data System– A non-switched (dedicated) digital service network for data rates of up to 56,000 bits per second typically only seen in North America.

DE

Discard Eligible– A user-set mark indicating that a frame may be discarded in preference to other frames if congestion occurs, to maintain the committed quality of service within the network.

DES

Data Encryption Standard– DES is a published encryption algorithm which uses a 56-bit symmetric key to encrypt data in 64-bit blocks.

DHCP

Dynamic Host Configuration Protocol– A protocol that lets network administrators manage centrally and automate the assignment of Internet Protocol (IP) addresses within an organization’s network.

Digital Certificates

A digital certificate is an electronic means to establish a users identity when establishing a virtual private network connection. It is issued by a certification authority (CA) and contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting and decrypting messages).

DLC

Digital Loop Carrier– Equipment that bundles a number of individual phone line signals into a single-multiplexing digital signal for local traffic between a telephone company central office and a business complex or other outlying service area.

DLCI

Data Link Connection Identifier– A 10-bit field within the address field which identifies the data link and its service parameters.

DNIS

Dialed Number Identification Service– A telephone service that provides for the receiver of a call the number the caller dialed. It is a common feature of 800 and 900 lines. If there are multiple 800 or 900 lines to the same destination, DNIS tells which number was called.

DNS

Domain Name Server– Computers that convert domain names to IP addresses.

DOCSIS

Data Over Cable Service Interface Specification– A project for the North American cable industry aimed at developing specifications for cable modems and associated equipment.

DS-0

Digital Signal at the Zero Level– A bipolar signal transmitted at 64Kbps. Often referred to as an individual channel on a T1 which consists of a total of 24 DS-0s or channels.

DS-1

Digital Signal at the First Level– The combination of 24 DS-0s creating a bipolar signal that is transmitted at 1.544 Mbps. Also called T1.

DS-3

Digital Signal at the Third Level– Circuit that can carry 672 DS-0 channels and has a bipolar signal transmitted at 44.736 Mbps.

DSL

Digital Subscriber Line– A family of digital lines provided by CLECS and telephone companies to local customers.

DSLAM

Digital Subscriber Line Access Multiplexer– a network device, usually at a telephone company Central Office, that receives signals from multiple customer DSL connections and puts the signals on a high-speed backbone line using multiplexing techniques.

DSP

Digital Signal Processor– A specialized computer chip that performs a variety of complex operations on digitized signals. DSP works by clarifying or standardizing, the levels or states of a digital signal. A DSP circuit is able to differentiate between human-made signals, which are orderly, and noise which is inherently chaotic.

DSU

Data Service Unit– A device used for interfacing Data Terminal Equipment (DTE) to the public telephone network. (2) A type of short-haul, synchronous-data line driver, usually installed at a user location that connects user synchronous equipment over a 4-wire circuit at a preset transmission rate to a servicing Central Office. Note: This service can be for a point-to-point or multipoint operation in a digital data network.

DSX-1

Digital Cross-Connect– Often used for connecting devices at 1.544 megabits. Also known as a short-haul DS-1 (655 feet). Often used with a PBX.

DTE

Data Terminal Equipment– Equipment that sends and receives information. An example of a DTE is a user's PC.

DWDM

Dense Wavelength Division Multiplexing– A technology

that puts data from different sources together on an optical fiber with each signal carried on its own separate light wavelength. Using DWDM, up to 80 (and theoretically more) separate wavelengths or channel of data can be multiplexing into a lightstream transmitted on a single optical fiber. In a system with each channel carrying 2.5 Gps, up to 200 billion bits can be delivered a second by the optical fiber. DWDM is also sometimes called Wave Division Multiplexing (WDM).

E1

Similar to T1, see T1, yet with 32 DS0 channels running at a 2.048Mbps rate. Other differences from T1 include framing type and encoding. HDB3 is the most common encoding scheme and is similar to AMI.

Echo Cancellation

A device that support this technique provides filtering of unwanted signals that are called “echoes” This technique is typically used for voice applications over packet-based networks.

Encryption

Scrambling data in such a way that it can only be unscrambled through the application using a special key.

Error Rate

A measure of the performance of a digital transmission system. It can be specified as a bit error rate (the probability of error per bit transmitted), as a block error rate (the probability of one or more errors in a specified-length block of bits), or in other forms such as percent error-free seconds.

Errored Second

Any 1-sec interval containing at least one bit error.

ESF

Extended Superframe Format– A T1 format consisting of 24 consecutive frames that use the framing bit to provide maintenance and diagnostic functions.

ESP

Encapsulated Security Payload– The ESP provides confidentiality for packets, which are the message units that the Internet Protocol deals with and that the Internet transports, by encrypting the payload data to be protected.

European Telecommunications Standards Institute (ETSI)

The European equivalent of ANSI (American National Standards Institute).

FDL

Facilities Data Link– An out-of-band, 4 kbit management path, available on ESF T-1s.

FDM

Frequency Division Multiplexing– A technique in which numerous signals are combined for transmission on a single communications line or channel. Each signal is assigned a different frequency (subchannel) within the main channel.

FECN

Forward Explicit Congestion Notification– A bit set sent by a Frame Relay network to notify an interface device (DTE) that congestion avoidance procedures should be initiated by the receiving device.

Fiber Optics

An optical transmission medium that consists of thin, plastic (or glass) strands which reflect light pulses within their interior along their length as a means to transmit large amounts of data.

Firewall

A security device that establishes a barrier to contain designed network traffic within a specified area by allowing or denying access.

FRAD

Frame Relay Access Device– A generic name for a device that multiplexes and formats traffic for entering a Frame Relay network.

Frame Relay

A Layer 2, Packet-Based, carrier-switching technology. It provides features and benefits of a dedicated DDS or T1 network, but without the expense of multiple dedicated circuits. Frame Relay is deployed over the same services used to deploy DDS and T1. In a Frame Relay network, circuits are connected to a packet switch within the network that ensures packets are routed to the correct location.

FT1 or FrT1

Fractional T-1– A portion of a T-1 circuit. A full T-1 circuit has a capacity of 1.544 Mbps composed of twenty-four (24) 64 kbps channels. A customer may lease a portion of the full circuit to effect cost-savings. A fractional T-1 can only be configured in increments of 64 kbps or a certain number of channels.

FTTC

Fiber To The Curb– Refers to the installation and use of fiber optic cable directly to the curbs near homes or any

business environment as replacement for “plain” old telephone service.

FX

Foreign Exchange– A telephone service that allows a user to have a number with an exchange that is not the normal exchange for their geographic area. The service is provided by linking the user's normal Central Office with the foreign central office by a leased line.

FXO

Foreign Exchange Office– Office side of a Foreign Exchange.

FXS

Foreign Exchange Station– Station side of a Foreign Exchange.

GUI

Graphical User Interface– A user interface that substitutes graphics for characters.

HDLC

High level Data Link Control– A group of protocols or rules for transmitting data between network points (sometimes called nodes). In HDLC, data is organized into a unit (called a frame) and sent across a network to a destination that verifies its successful arrival.

HFC

Hybrid Fiber Coax– A telecommunication technology in which fiber optic cable and coaxial cable are used in different portions of a network to carry broadband content (such as video, data, and voice). Using HFC, a local cable TV company installs fiber optic cable from the cable head-end (distribution center) to serving nodes located close to business and residential users and from these nodes uses coaxial cable to individual businesses and homes.

HDSL

High-bit-rate Digital Subscriber Line– This employs a 2B1Q modulation technique across the same type pairs traditionally encountered with metallic T1 delivery systems. This satisfies Telco distance requirements without the use of repeaters. (Usually used in a campus environment.)

HDSL2

High-bit-rate Digital Subscriber Line version 2– (also known as g.SHDSL or SHDSL) Allows service providers to deliver full T-1 and possibly E-1 over a single twisted pair.

HIPPI

High Performance Parallel Interface– A method of delivering high-speed point-to-point data between supercomputers or high-end workstations and peripherals.

HSSI

High Speed Serial Interface– A serial interface operating up to 52 Mbps and up to 50 ft.

IAD

Integrated Access Device– A device which supports voice, data and video streams over a single high-speed connection.

IDF

Intermediate Distribution Frame– A freestanding or wallmounted rack for managing and interconnecting the telecommunications cable between end-user devices and a Main Distribution Frame (MDF).

IDSL

ISDN Digital Subscriber Line– (2B1Q ISDN without the dial-up capabilities). A symmetric DSL service that can transmit and receive data up to 144 Kbps.

IKE

Internet Key Exchange— A protocol whose purpose is to negotiate and provide authenticated keys for security associations in a protected manner. Processes which implement this protocol can be used for negotiating virtual private networks (VPNs) to a secure host or network.

IEC

Interexchange Carrier– A long distance carrier.

ILEC

Incumbent Local Exchange Carrier– A telephone company in the United States that was providing local service in a specific geographic area when the Telecommunications Act of 1996 was enacted. ILECs include the former Bell operating companies which were grouped into holding companies known collectively as the Regional Bell Operating Companies (RBOC) when the Bell System was broken up by a 1983 consent decree.

IP

Internet Protocol– The method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from other computers on the Internet.

IPSec

A developing standard for security at the network or packet processing layer of network communication. Earlier security approaches have inserted security at the application layer of the communications model. IPSec will be especially useful for implementing virtual private networks and for remote user access through public connection to private networks.

ISDF

Integrated Service Development Framework– A set of CCITT/ITU standards for digital transmission over ordinary telephone copper wire as well as over other media. Home and business users who install an ISDN adapter (in place of a modem) can see highly-graphic web pages arriving very quickly (up to 128 Kbps).

ISDN

Integrated Services Digital Network– An extension of the digital transmission and common channel signaling concepts of the public telephone network to the CPE. This includes BRI and PRI.

ISO

International Standards Organization– Group responsible for the creation of a set of CCITT/ITU standards for digital transmission over ordinary telephone copper wire as well as over other media.

ISP

Internet Service Provider– A company that provides individuals and/or businesses access to the Internet and other related services such as web site building and virtual hosting. An ISP has the equipment and the telecommunication line access required to have POP on the Internet for the geographic area served.

ITU (International Telecommunications Union)

A United Nations organization that establishes standards for telecommunications devices, like ISDN hardware, modems, and Fax machines. ITU standards include J.112, J.122, H.323, V.90, X.25, and X.500.

IXC

IntereXchange Carrier– A telephone company that provides connections between local exchanges in different geographic areas. IXCs provide interlocal access and transport area service as described in the Telecommunications Act of 1996.

Kbps

Kilobits per second– (one thousand bits per second)- A measure of bandwidth (the amount of data that can flow in a given time) on a data transmission medium. Higher bandwidths are more conveniently expressed in Megabit per second (Mbps or millions of bits per second) and in Gigabits per second (Gbps, or billions of bits per second).

Key

In cryptography, a key is a unique value that is applied to encrypt and/or decrypted data. The length of a key generally determines how difficult it will be to decrypt the data. Both Public and Private keys are available and can be used together known as asymmetric encryption. A system for using just public keys is called a public key infrastructure (PKI).

L2TP

Layer 2 Tunneling Protocol– An extension of the Pointto- Point Tunneling Protocol (PPTP) used by an Internet Service Provider (ISP) to enable the operation of a Virtual Private Network (VPN) over the Internet.

LAN

Local Area Network– A group of computers and associated devices that share a common communications line and typically share the resources of a single processor or server within a small geographic area.

LATA

Local Access and Transport Area– A term in the United States for a geographic area covered by one or more local telephone companies, which are legally referred to as local exchange.

LDN

Listed Directory Number– Your seven digit phone number hence, the number that would be listed in the phone directory.

LEC

Local Exchange Carrier– The term for a public telephone company in the U.S. that provides local service. These can be either one of the Bell operating companies or an independent.

LS

Loop Start– A method of signaling to a switch to start a call, under which an off-hook condition closes a circuit and causes current to flow, informing the switch to provide dial tone. (Compare to ground start).

Local Loop

This portion of the telecommunications network physically connects end users to the central office network facilities and generally is dedicated to that particular user. Twisted pairs of copper wire form the traditional medium of the telephone network local loop, although other connections now are used in some cases.

MAN

Metropolitan Area Network– A network that interconnects users with computer resources in a geographic area or region larger than that covered by a large local area network, but smaller than the area covered by a wide area network. It typically extends as far as 50-kilometers and operates at speeds between 1 Mbps to 200Mbps.

Mbps

Million (Mega) bits per second– The measure of bandwidth (the total information flow over a given time) on a data transmission medium such as twisted-pair copper cable, coaxial cable, or optical fiber line.

MIPS

Millions of Instructions Per Second– A general measure of computing performance and, by implication, the amount of work a larger computer can do. Generally, this refers to the number of instructions that can be processed by the CPU in a given second.

MTBF

Mean Time Between Failure– A measure of how reliable a hardware product or component is. For most components, the measure is typically in thousands or even tens of thousands of hours between failures.

MTU

Maximum Transmission Unit– the largest unit of data that can be sent across a given medium.

Multiplexing

Transmission of multiple signals over a single channel.

NAT

Network Address Translation– The translation of an IP address used with one network to a different IP address that is known within another network. One network is designated as the inside network and the other is the outside.

NEBS

Network Equipment Building Standards– NEBS testing is required for vendors who wish to sell equipment to the Regional Bell Operating Companies (RBOCs) and the Competitive Local Exchange Carriers (CLECs). Level 3 testing is the most stringent level of testing.

Network

A generic term describing the tying of like things together. In telecommunications, it usually refers to infrastructure that provides for user voice and data transmission.

NEXT

Near End Crosstalk– An error condition that can occur when connectors are attached to twisted pair cabling. NEXT is usually caused by crossed or crushed wire pairs. The error condition does not require that the wires be crushed so much that the conductors inside become exposed. Two conductors only need to be close enough so that the radiating signal from one of the wires can interfere with the signal traveling on the other.

NOC

Network Operations Center– A place from which a telecommunications network is supervised, monitored, and maintained. Enterprises with large networks and large network service providers such as GTE Internetworking typically have a network operations center.

NNI

Network to Network Interface– The connection between two public service network providers.

NT-1

Network Termination type 1– A Basic Rate ISDN-only device that converts a service provider's U-Interface to a customers S/T interface. It can be stand-alone or integrated into a terminal adapter.

OC-N

Optical Carrier Level N– These are fundamental transmission rates for SONET with N=1, 3, 9, 12, 18, 24, 36, or 48.

OCUDP

Office Channel Unit Data Port– Provides signal conversion from any rate of a customer's access line (i.e. T1) to a 56 or 64Kbps single DDS line. This is often used with a DDS or a SW56 DSU/CSU.

OPX

Off Premise Extension– The ability to have local access to a remote site (dial an extension) across a Wide Area Network link.

OSPF

Open Shortest Path First– A router protocol used within larger autonomous system networks in preference to the Routing Information Protocol, an older routing protocol that is installed in many of today’s corporate networks.

PBX

Private Branch eXchange– A customer premises switch that connects the customer location with the public telephone network.

PCM

Pulse Code Modulation– A digital scheme for transmitting analog data. The signals in PCM are binary; that is, there are only two possible states represented by logic 1 (high) and logic 0 (low).

PCS

Personal Communications Service– A wireless phone service somewhat similar to cellular telephone service, but emphasizing personal service and extended mobility. It is sometimes referred to as digital cellular (although cellular systems can also be digital). Like cellular, PCS is for mobile users and requires a number of antennas to blanket an area of coverage.

PKI

Public Key Infrastructure– PKI enables users to privately exchange data through a public infrastructure like the Internet, through the use of a public and a private key pair that is obtained and shared through a trusted authority.

PON

Passive Optical Network– A system that brings optical fiber cabling and signals all or most of the way to the end user. Depending on where the PON terminates, the system can be described as Fiber-To-The-Curb (FTTC), Fiber-To-The-Building (FTTB), or Fiber-To-The-Home (FTTH).

PoP (POP)

Point of Presence– A physical layer within a LATA at which an inter-LATA carrier establishes itself for the purpose of obtaining LATA access and to which the local exchange carrier provides access services.

PoP3 (POP3)

The current version of the most common protocol for receiving e-mail on a TCP/IP network.

PORT

The physical connection between a device and a circuit. It's capacity determines the greatest amount of data that can be transmitted at any given time.

P**OTS**

Plain Old Telephone Service– Analog, voice-only telephone service.

PPP

Point-to-Point Protocol– A protocol for communication between two computers using a serial interface, typically a personal computer connected by phone line to a server. This protocol is typically used for Internet connections originating from a dial-up line and a high-speed modem.

PPTP

Point-to-Point Tunneling Protocol– A protocol that allows corporations to extend their own corporate network through private "tunnels" over the public Internet.

PRI

Primary Rate Interface-ISDN– A user to network interface consisting of 23 64Kbps bearer (B) channels and one 64Kbps signaling (D) channel earned over a 1.544Mb/s DS-1 circuit. The "B" channels carry data, voice or video traffic. The "D" channel is used to set up calls on the B channels and carry packet data.

PSTN

Public Switched Telephone Network– The public network that provides switched digital/analog services to a customer/end user.

PTT

A term describing one of the telephone companies for most of the world outside of North America.

PVC

Permanent Virtual Circuit– The logical connection between two nodes. Each PVC is assigned a CIR. A PVC can burst up to the port speed. See also SVC.

QoS

Quality of Service– The "quality" of the telephone service provided to any given individual or business.

RAS

Remote Access Server– A computer and associated software that allows users to dial in or gain access to a network remotely.

RBOC

Regional Bell Operating Company– A term describing one of the U.S. Regional telephone companies (or their successors) that were created as a result of the breakup of American Telephone and Telegraph Company (AT&T, known also as the Bell System) by a U.S. Federal Court consent decree on December 31, 1983. The seven original regional Bell operating companies were Ameritech, Bell Atlantic, BellSouth, NYNEX, Pacific Bell. Southwestern Bell, and US WEST. Each of these companies owned at least two Bell operating companies. The BOCs were given the right to provide local phone service while AT&T was allowed to retain its long distance service. The RBOCs and their constituent BOCs are part of the class of local exchange carriers.

RBS

Robbed-Bit Signaling– The process where the least significant bit in the 6th and 12th frame (of a SF T1) and the 18 & 24th frame (of an ESF T1) is “robbed” for voice A, B, C, and D signaling bits. These signaling bits indicate on/off hook conditions etc.

REN

Ringer Equivalency Number– FCC Certification number approving a terminal telephone product for direct sale to an end user as to not harm the network. The total number of RENs on one telephone line must not exceed is 5.

RFC

Request For Comment– The core method of specification for the Internet. (Some RFCs are standards for the Internet.)

RIP

Routing Information Protocol– A widely-used protocol for managing router information within a self-contained network such as a LAN or an interconnected group of such LANs.

RJ45

A modular 8-wire jack/connector used with copper cable having four twisted pairs.

Router

Communications equipment which forwards information on a connectionless basis. More specifically, a computer that connects different networks (LANs and WANs) at the Layer 3 of the OSI Reference Model level often using IP addresses.

RSVP

Resource Reservation Protocol– A protocol that allows channels or paths on the Internet to be reserved for the multicast (one source to many receivers) transmission of video and other high-bandwidth messages. RSVP is part of the Internet Integrated Service model, which ensures best-effort service, real-time service, and controlled link sharing.

S/T Interface

A common way of referring to either an S or T Interface. This can be used to connect directly to an ISDN 2B+D NT1 or an NT2 device with a terminal adapter.

SDH

Synchronous Digital Hierarchy– A standard technology for synchronous data transmission on optical media. It is the international equivalent of Synchronous Optical Network. Both technologies provide faster and less expensive network interconnection than traditional Plesiochronous Digital Hierarchy equipment.

SDLC

Synchronous Data Link Control– The exclusive transport for a SNA network.

SDSL

Symmetric Digital Subscriber Line– A DSL based on ISDN with 2B1Q, but is symmetric in nature where both downstream and upstream traffic bandwidth may be up to 2.3 Mbps.

SHDSL

Symmetric High Bit Rate Digital Subscriber Loop– SHDSL is defined by the new ITU Global Standard G991.2 from February 2001 and provides high symmetric data rates with guaranteed bandwidth and low interference with other telecommunications services.

SLA

Service Level Agreement– A contract set up between an end-user and a service provider outlining the guarantees of what will be provided for that digital service.

SONET

Synchronous Optical NETwork– The U.S. (American National Standards Institute) standard for synchronous data transmission on optical media. The international equivalent of SONET is synchronous digital hierarchy (SDH). Together, they ensure standards so that digital networks can interconnect internationally and that existing conventional transmission systems can take advantage of optical media through tributary attachments.

SPID

Used only in North America, a Service Profile Identifier is a unique identifier that is used to represent the service and feature identifiers of a particular Basic Rate ISDN line or service provider. (This number generally is 10+ digits long and includes the LDN.) The telephone company should give you your SPIDs at the time they assign you your ISDN directory numbers.

SSL

Secure Sockets Layer– A commonly used protocol for managing the security of message transmission on the Internet. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers.

Stateful Inspection

Stateful Inspection is an advanced packet-filtering technology within firewalls that checks and verifies each network packet in order to detect suspicious activity. Many network security experts recommend the Stateful Inspection as the most trusted firewall technology.

STP

Shielded Twisted Pair– A special kind of copper telephone wiring used in some business installations. An outer covering or shield is added to the ordinary twisted pair telephone wires and functions as a ground.

SVC

A and SVC, Switched Virtual Circuit, allows an end-user to establish on-demand data connections between two end points through an ATM, Frame Relay, or X.25 network. See also PVC.

Synchronous Transmission

A method of data transmission which allows characters to be sent in a continuous stream; the beginning of one character contiguous with the end of the preceding one. Separation of characters requires the receiver to maintain synchronization to a master timing source. It does not use start and stop bits at the beginning and end of each byte to synchronize the data time clocks at each end of a connection. Instead it sets its timing signal at the beginning and end of each connection, and corrects discrepancies that arise over time by using the changing values each device on the connection sends and receives to keep their clocks "in sync." Eliminating the start and stop bits reduces the "overhead" required to transmit each byte, and allows for increased throughput.

T1

A digital carrier signal designed to carry speech or data at the DS-1 rate. (See DS-1.)

T3

A digital carrier signal designed to carry speech or data at the DS-3 rate. (See DS-3.)

TMN

Telecommunications Management Network– A network management model originated formally in 1988 under the auspices of the International Telecommunication Union (ITU-TS) This was done as a strategic goal to create or identify standard interfaces that would allow a network to be managed consistently across all network element suppliers.

TDM

Time Division Multiplex– Once digitized, voice/data signals from many sources may be combined or multiplexed and transmitted over a single digital link.

TE1

Terminal Equipment type 1– Equipment that can directly connect to the ISDN line (often using an S/ T Interface). Examples are ISDN phones, ISDN routers, ISDN computers etc.

TE2

Terminal Equipment type 2– Equipment that is non- ISDN equipment. Needs an external terminal adapter. Examples are PCs with EIA 232 interfaces and analog telephone sets.

Telco

American slang for Telephone Company– The local telephone company.

Telnet

TCP/IP application that provides a terminal interface

between computers attached to a TCP/IP network. This allows a user at one site to interact with a terminal at another site as if by a local terminal.

Trunk

An analog or digital connection from a circuit switch which carries user media content and may carry telephony signaling (MF, R2, etc.). Digital trunks may be transported and may appear at the Media Gateway as channels within a framed bit stream. Trunks are typically provisioned in groups, each member of which provides equivalent routing and service.

Trunking

Transporting signals from one point (an antenna site for instance) to another point (such as a headend), usually without serving customers directly. Trunking can be accomplished using coaxial cable, fiber optics or microwave radio.

Tunnel

An established network connection in which data is encrypted and encapsulated for transmission across a public or untrusted network, for eventual de-encapsulation and decryption.

U loop (or) U-Interface

An ISDN 2-wire digital circuit between the customer's network termination and the Local Exchange Carrier's termination in the Central Office.

UNI

User to Network Interface– Describes the connection between the user and the public network service provider.

V.35

High Speed Digital Interface used for synchronous data rates up to approximately full Mbps speed.

VAD

Voice Activation Detection– A software application that allows a data network carrying voice traffic over the Internet to detect the absence of audio and conserve bandwidth by preventing the transmission of “silent packets” over the network. Most conversations include about 50 percent silence. VAD (also called “silence suppression”) can be enabled to monitor signals for voice activity so that when silence is detected for a specified amount of time, the application informs the Packet Voice Protocol and prevents the encoder output from being transported across the network.

VC

Virtual Circuit– A circuit or path between points in a

network that appears to be a discrete, physical path but is actually a managed pool of circuit resources from which specific circuits are allocated as needed to meet traffic requirements.

Video Codec

A device that converts an analog signal into digital for transport and converts a digital signal into analog for display.

VoATM

Voice over ATM– A generic term for describing the delivery of voice services using Asynchronous Transfer Mode.

VoDSL

Voice over Digital Subscriber Line– A term used to describe the delivery of voice services using Asynchronous Transfer Mode and DSL. The typical voice over DSL model includes an IAD for delivering voice and data services to the end customer, a DSLAM for aggregating multiple DSL lines into a single ATM cell stream and a voice gateway for interfacing back into the existing public switched telephone network.

VoIP

Voice over IP– A term used in IP telephony for a set of facilities for managing the delivery of voice information using the Internet Protocol (IP). In general, this means sending voice information in digital form in discrete packet rather than in the traditional circuit-committed protocols of the public switched telephone. A major advantage of VoIP and Internet telephony is that it avoids the tolls charged by ordinary telephone service.

VPN

Virtual Private Network– A private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of tunneling protocol and security procedures. A virtual private network can be contrasted with a system of owned or leased lines that can only be used by one company.

WAN

Wide Area Network– A high-speed network within a wide geographical area (usually larger than a city or a metropolitan area) that shares data, programs, or equipment.

WDM

Wavelength Division Multiplexing– A technology that puts data from different sources together on an optical fiber, with each signal carried on its own separate light wave. Using WDM, up to 80 (and theoretically more) separate wavelengths or channel of data can be multiplexing into a lightstream transmitted on a single optical fiber. In a system with each channel carrying 2.5 Gbps (One thousand million bits per second). Up to 200 billion bits can be delivered a second by the optical fiber.

X.21

X.21 is a physical and electrical interface that uses two types of circuits: balanced (X.27N.1 1) and unbalanced (X.26N.10). CCITT X.21 calls out the DB-15 connector. The physical interface between the DTE and the local PTT-supplied DCE is defined in ITU-T recommendation X.21. The DCE provides a full-duplex, bit-serial, synchronous transmission path between the DTE and the local PSE. It can operate at data rates from 600bps to 64Kbps.

Appendix C – Differences with Cisco Routers

Often entities that have been around the longest have made early decisions that subsequent decisions, out of necessity, have been built upon. This is no different for any country, company, or system. For example: carrier systems in North America have been in place for many decades but have also decided to constrain newer technologies and demands for bandwidth within those older systems; this is not news to anyone. Parts of the world where there was not the same infrastructure have benefited by the ability to build new without working on top of the old. The same goes with routers and their methods of configuration and philosophies for structuring their architecture. The bottom line is that all systems will have some differences due to these factors, and these factors alone should never reflect poorly on any previous system or philosophy regarding the architecture decisions engineers and scientists have had to make during a previous time.

Cisco routers have been available for building WAN networks for many years. Historical decisions and their usage, it seems, have influenced subsequent features and their associated commands. It is acknowledged that they have made the best engineering decisions they could at that time, that required they accommodate their historical usage and the customer requirements. As technology progressed so have these routers, yet many of the required decisions for configuration appear to have historical usage influencing newer features and their associated commands. This is not a poor reflection upon their decisions because this occurs for any country, company, or system.

To help the designer and implementation engineer, this paper includes a table of major known differences either with the command line interface configuration, or regarding a particular philosophy for usage. It is not intended to show a “best method” but only allow the designer and installer to readily discern the differences, and study the appropriate text to understand more. The reader can also use the configuration examples in this guide to see some of these differences.

This paper acknowledges that their will be future revisions to both router operating systems and at some point the information contained below may not be completely accurate. The information below is subject to change without notice.

ProCurve Feature or Command	Cisco Feature or Command
WAN interfaces named for their technology; E1, T1, BRI (ISDN), ADSL, etc…	WAN interfaces contained under a “serial” interface.
Layer 2 interfaces named for their technology; PPP, Frame Relay, ATM, etc…	Layer 2 as part of interface definition.
Interface configuration (use “bind” command)	Interface and encapsulation contained inside the interface configuration.
ACL and ACP used together. ACLs may still also be used alone. ACL and ACP combinations are “ingress” only. ACL usage with “ip access-group” command can be “ingress” and “egress”.	Traditional ACL usage.
Routed networks use mask to define them.	Routed networks do not require mask.

Appendix D – References

These are ranked in order of this paper’s preference regarding WAN design:

1. Designing Wide Area Networks and Internetworks: A Practical Guide by Marcus, J. Scott: ISBN: 0201695847
    a. Great text for considering all aspects of a WAN design.
2. T-1 Networking: How to Buy, Install and Use T-1 From Desktop to DS-3 by Flanagan, William: ISBN: 1578200210
    a. Another classic text and does include some information on E-1.
3. ADSL & DSL Technologies (second edition) by Walter J. Goralski: ISBN: 0072132043
    a. This text also has good all around networking discussions.
4. VPNs (A Beginner’s Guide) by John Mairs: ISBN: 0072191813
    a. This text also has good all around networking discussions.
5. Practical BGP by White, Russ / McPherson, Danny / Sangli, Srihari: ISBN: 0321127005
    a. Great book for BGP. Easy to read and understand.
6. Wide Area Network Design: Concepts and Tools for Optimization by Robert S.Cahn: ISBN: 1558604588
    a. The depth of this text may not be completely for the intended audience of this paper so it is prioritized here in this list. This text seems good but was not critically analyzed to form a more informed opinion.
7. Emerging Communications Technologies, 2nd Edition by Uyless Black: ISBN: 0137428340
    a. A classic reference text.
8. Guide to Designing and Implementing Local and Wide Area Networks, 2nd Edition by Michael Palmer and Robert Bruce Sinclair: ISBN: 061912122X
    a. Intended to be a course in LAN and WAN Design and Implementation, it spends 10 of its 11 chapters on foundational LAN and WAN material, which is useful, and 1 chapter on design and although much must be considered from earlier information given in the text, only 3 pages dedicated to WAN design. I still recommend the book if one needs a good discussion of both LAN and WAN technologies and design.
9. Telecommunications Technologies Reference by Bradley Dunsmore and Toby Skandier: ISBN: 1587050366
    a. A very nice text on telecommunications technologies.
10. The Telecommunications Illustrated Dictionary, 2nd Edition by Julie K. Petersen: ISBN: 084931173X

11. Newton's Telecom Dictionary, 21st Updated and Expanded Edition by Harry Newton: ISBN: 157820315

[i] J-carrier WAN connections are a closely related variant of T-carrier WAN connections. Like T1 WAN connections, J1 WAN connections provide a transmission speed of 1.544 Mbps and 24 channels. J1 WAN connections also perform all signaling and control functions in-band.

However, J1 WAN connections use a slightly different framing format for signal transport than T1 WAN connections use. J1 WAN connections use the J1 signaling format, rather than DS1.

Although the J1 standard is defined, most PTTs in Japan don’t appear to be using this standard for leased lines. For example, Nippon Telegraph and Telephone (NTT), the largest PTT in Japan, offers a DS3 connection with a transmission speed of 44.736 Mbps.

PTTs in Japan are using the T1 standard because they are delivering WAN connections over fiber optic networks that support the Synchronous Optical Network (SONET) standard. SONET is the standard adopted by the United States and Canada for fiber optic networks. Not surprisingly, SONET provides backward compatibility for T-carrier lines.

To find out more about
ProCurve Networking
products and solutions,
visit our web site at

www.procurve.com

ProCurve Networking
HP Innovation

4AA0-0717ENW, 8/2005