INTERNATIONAL CIVIL AVIATION ORGANIZATION

PROJECT RLA/06/901

GUIDANCE FOR THE IMPLEMENTATION OF NATIONAL DIGITAL NETWORKS THAT USE THE IP PROTOCOL, TO SUPPORT CURRENT AND FUTURE AERONAUTICAL APPLICATIONS

The designations employed and the presentation of material in this publication do not imply the expression of any opinion whatsoever on the part of ICAO concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimination of its frontiers or boundaries.

TABLE OF CONTENTS

1. Background

1.1 When the SICAS Panel was first entrusted with the development of SARPs for the Aeronautical Telecommunications Network (ATN), it was requested to use open protocols considered to be the "industry standard" as the basis for the ATN. This lead to the selection of the OSI protocols Open Systems Interconnection.

1.2 At that time, the use of this protocol was mandated by many ICAO Contracting States. Prior to 1997, the Panel and its successor, the ATNP, had worked successfully, and the ATN SARPs were validated. Since then, air traffic services (ATS) based on these SARPs have moved to the deployment stage and are now operating in some areas.

1.3 However, although ISO protocols were strongly supported by Contracting States outside of aeronautical communication services, industry protocols were converted using an older system of standards collectively known as "TCP/IP" (more appropriately called the Internet Protocol Suite (IPS)). Now these are the *de facto* standards for open communications, and IPS-based products are extensively available at a low cost.

1.4 In the ground environment, considerable cost savings can be achieved with the introduction of IPS-based products, such as the ATS message handling service (ATSMHS), and others, in support of air-ground communications. ICAO Contracting States have started to deploy IPS in these areas.

1.5 In the air-ground setting, there is interest in the use of IPS. However, this setting is very different from the ground environment. There are specific tasks to perform concerning mobility and security that must be carefully considered. While there is a desire to apply the industry standards in the air-ground environment, it is recognized that it is more complex and thus their implementation will take longer compared to the ground environment.

1.6 In view of the above, the Air Navigation Council charged Working Group I of the ACP (Aeronautical Communications Panel) with analyzing the use of TCP/IP for the establishment of an aeronautical network and making recommendations for future work in this area.

1.7 Working Group I of the ACP conducted the task using the following methodology:

1.7.1 An analysis was made of States members to determine to what extent the IPS was being used for aeronautical communications in each State, and within what context.

1.7.2 Consideration was given to aeronautical communication requirements in areas such as operations, security, mobility, etc.

1.7.3 Consideration was also given to ground-ground and air-ground environments, as well as to the capacity of existing IPS products to meet these requirements.

1.7.4 It was concluded that the IPS was appropriate for meeting aeronautical communication requirements, and a draft future work program was formulated to expedite the use of IPS in the selected area of aeronautical communications.

1.8 *The conclusion of the ACP report was that the use of IPS to support aeronautical communications in the ground environment was entirely justified.*

1.9

2. General Decision-Making Considerations

2.1 Business

2.1.1 The decision to implement the IPS must be both a cost-effective and a technical decision. It should be noted that while the existing IPS protocols have no patent restrictions and are available at no charge, this might not be true for future protocols.

2.1.2 There are many vendors and service providers for the equipment and the establishment of an IPS network. This has created a competitive environment that should offer ICAO Contracting States favourable prices when buying equipment and network services.

2.2 Industrial Support

2.2.1 There are many companies that provide network equipment and IPS-based services, while the establishment of an OSI network gradually reduces their capacity to provide support. Furthermore, IPS standards are maintained by the Internet Engineering Task Force (IETF) with the active assistance of the industry.

2.2.2 The number of nodes displayed by the IPS is about ten million, while OSI-based WAN networks are not displayed in that same scale, and those that have been displayed are being replaced by IPS.

2.3 Security Policies to Consider

2.3.1 The establishment of an IPS network increases the need for effective security, due to its openness. The obscurity of ISO/OSI protocols as a result of not being extensively displayed in networks provides a certain amount of protection.

2.3.2 Attacks against IPS networks are widely published, and hackers spend a lot of energy trying to devise new forms. The cost of a system capable of inflicting significant damage to a network could be just that of a cheap computer that supports IPS.

2.3.3 This means that ATS systems that use IPS without any effective security mechanisms would be vulnerable to the various forms of security breach. Therefore, it is recommended that the security systems that underlie ATN vulnerability analyses be updated to reflect the use of IPS.

2.3.4 There are many security mechanisms that can be used in an IPS network. Current systems can use the IP security protocol (IPSec) to ensure the security of the network layer, and/or the SSL/TLS protocol to ensure the security of the IPS transport layer. IPSec can provide encryption and/or authentication services.

2.3.5 On the other hand, the Aeronautical Administration of each State shall comply with the internal Information Security Policies established by its own government.

2.3.6 Reading of the "Information Technologies – Security techniques – Codes of practice for information security management ISO-IEC 17799" standard published in 2005 by ISO (International Standardization Organization) and IEC (International Electrotechnical Commission) is recommended. The latest version, BS ISO IEC 17799: 2005 supersedes older versions of standards BS 7799 and ISO 17799. It is based on British Standard 7799. Although standard ISO 17799 is not mandatory, *it provides a sound basis for an information security programme*.

2.3.7 The provisions contained in ICAO *Manual of Technical Provisions for the Aeronautical Telecommunications Network (ATN)* (Doc 9705), and the security audit Checklist (Information Security Management BS 7799.2:2005 Audit Check List for SANS) should also be observed.

2.4. Implementation

2.4.1 Since IPS is the global *de facto* standard for the establishment of a network, supported by many years of implementation, there are many engineers with experience in the establishment of networks who are available to support implementation. This knowledge base can support the deployment of an IPS-based ATN.

2.5 Training

2.5.1 Notwithstanding the above, it is absolutely necessary to quickly start a training and/or certification program in IPS networks that will provide the State with a minimum number of individuals for the satisfactory installation, implementation, management, and maintenance of the IPS network.

3. Specific Design and Deployment Considerations

3.1 Basic Decisions for the Preliminary Design of the National Network

3.1.1 The basic recommendation that should be followed by each State is that the IPS network *must be exclusively private*.

3.1.2 Each State may select the *provider* of the *IPS elements* that it deems advisable; however, this selection must be practically definitive, since it is not advisable to have equipment of various brands being used for the same purpose, since that would represent an unnecessary *multiplication* of:

3.1.2.1 Training.

3.1.2.2 Spare parts.

3.1.2.3 Human resources.

3.1.2.4 Remote management.

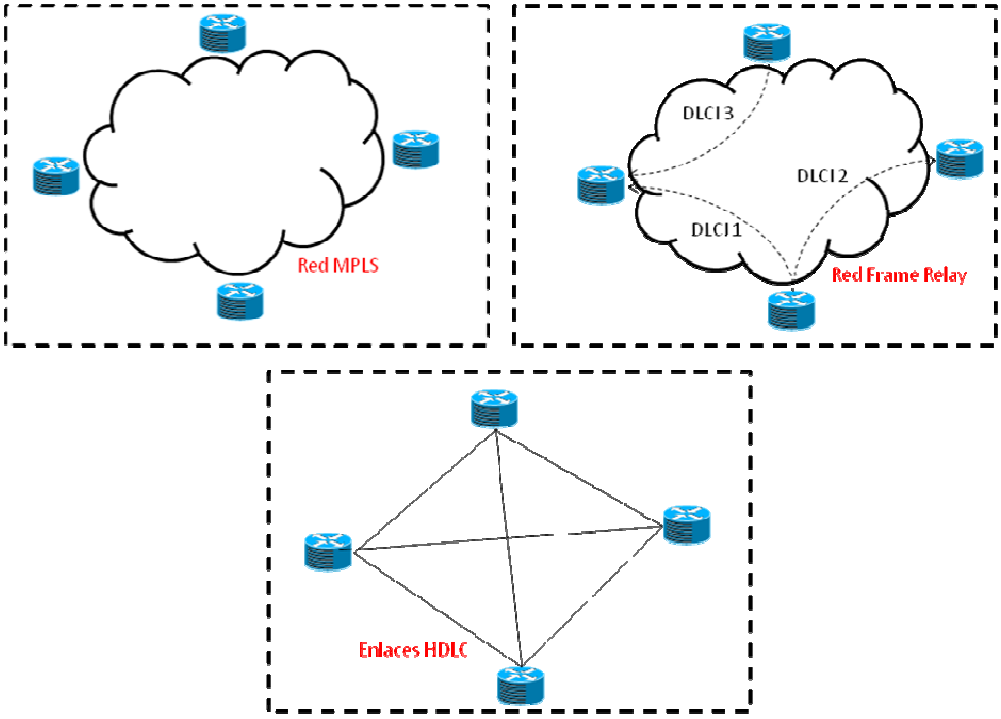
3.1.3 Likewise, each State (based on its technical and economic policies) shall decide if the IPS network will be:

3.1.3.1 Supported by *ground or satellite networks* (or a combination of both).

3.1.3.2 Based on a network of *self-owned or leased* links to the PTTs (*).

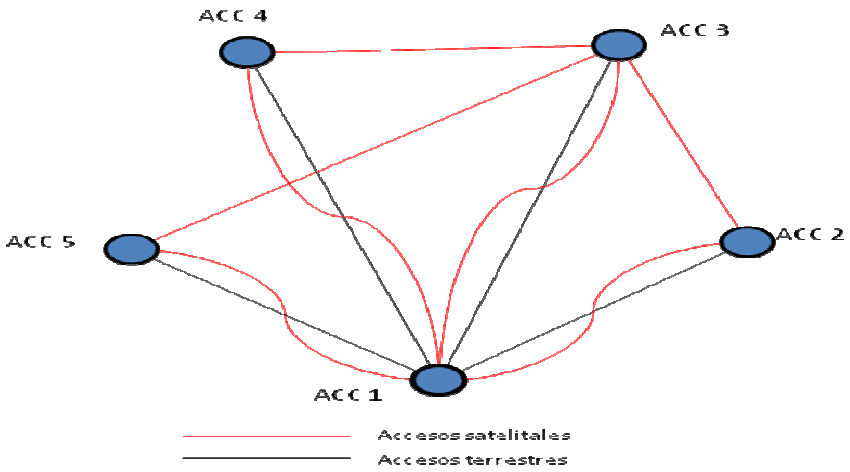
3.1.3.3 Carried on dedicated lines or switched connections. Switched connections, in turn, may consist of switched circuits or switched packages/cells (*).

FIGURA 1: MPLS, Frame Relayy HDLC



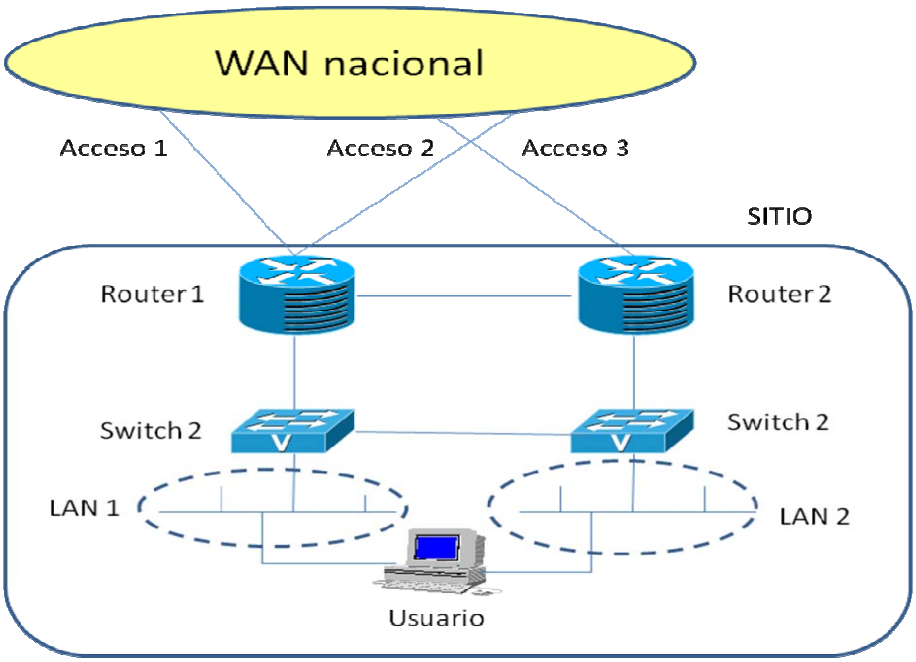
3.1.3.4 If use is made of point-to-point and of *simple or duplicated accesses* to the WAN (wide area network) at each end point, *see Figure 2 (*).

FIGURA 2: EJEMPLO DE RED IP, HDLC, ACCESOS REDUNDANTES



3.1.3.5 With *simple or duplicated* networking *elements (see Figure 3)*.

Figura 3: Elementos de networking redundados



(*): These matters are extensively discussed in Appendix 1.

Appendix 1 "Networking Concepts" describes in detail the various aspects of network design and configuration, as well as everything related to data segmentation elements (*routers and switches*).

Appendix 2 "Description of a Router", gives details of all the constructive, functional, and technical aspects of a router.

Appendix 3 "Routing Protocols" describes routing aspects.

NOTE: All appendices make ample reference to Cisco elements, without pretending to influence the selection of the elements to be installed by each State.

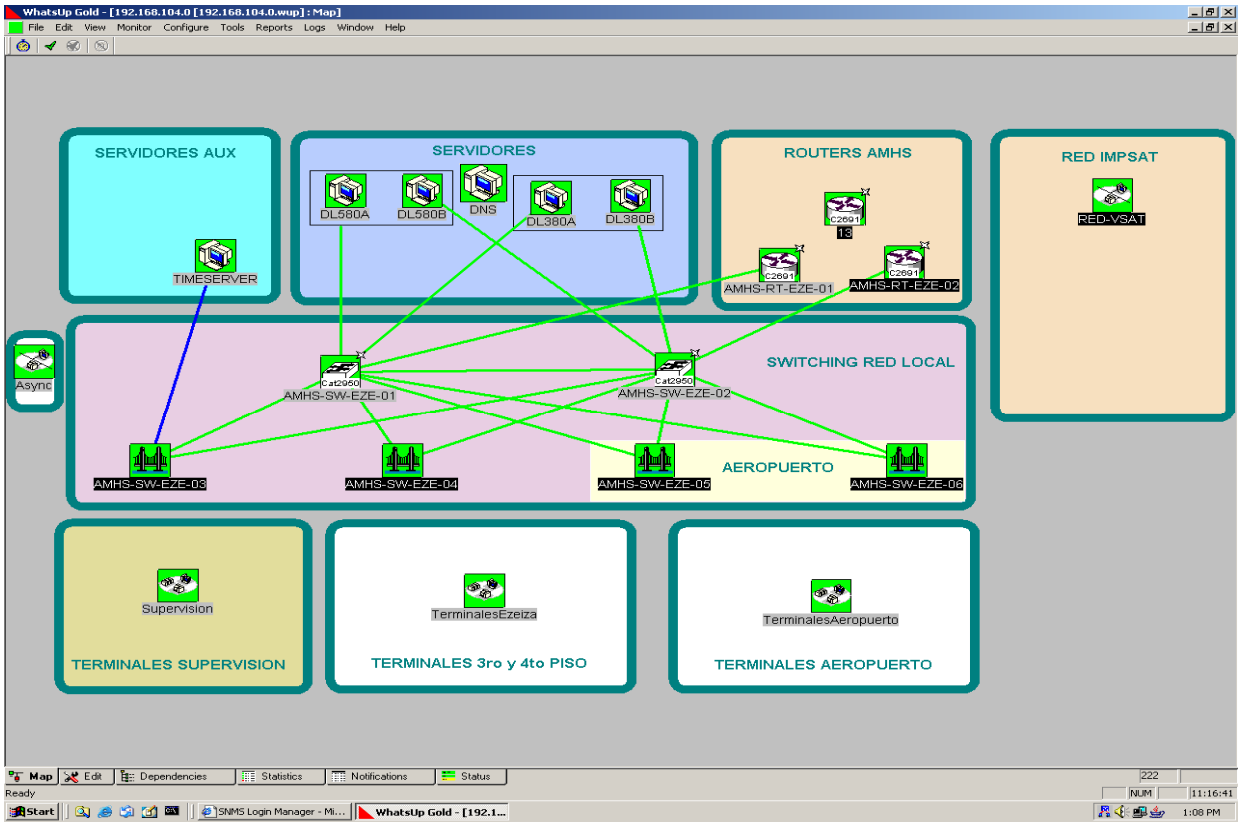
3.2 Remote Network Management

3.2.1 The network shall be installed in such a way to permit the display and remote management of *all and each one of its components.*

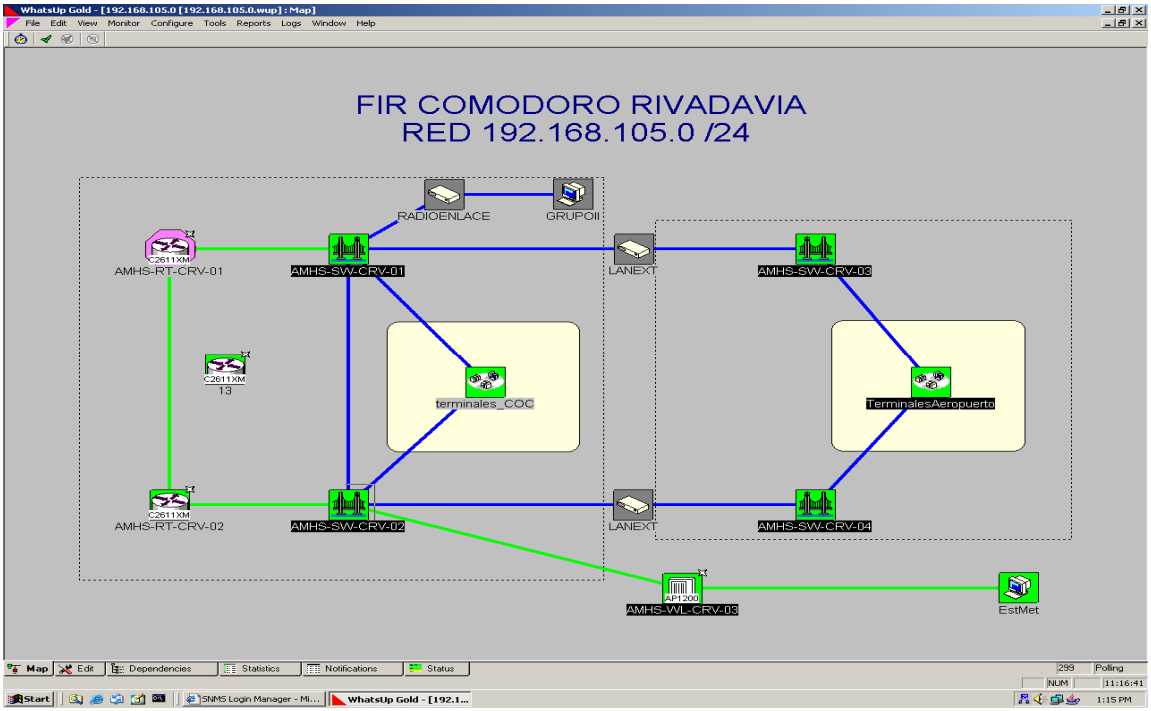
Appendix 4 "Device Management Package" describes the management elements that are available and their role in the operation of the IPS network.

3.2.2 The following figures contain display examples of network elements corresponding to:

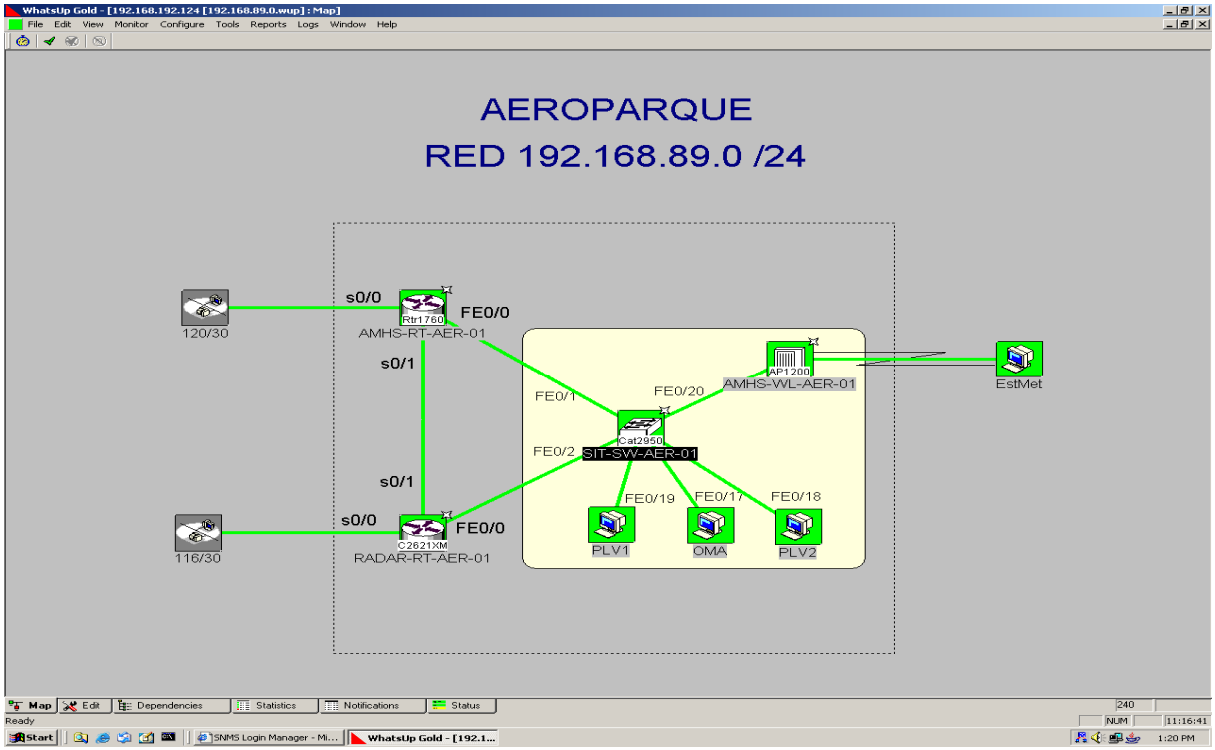
3.2.2.1 The headquaters of an AMHS service



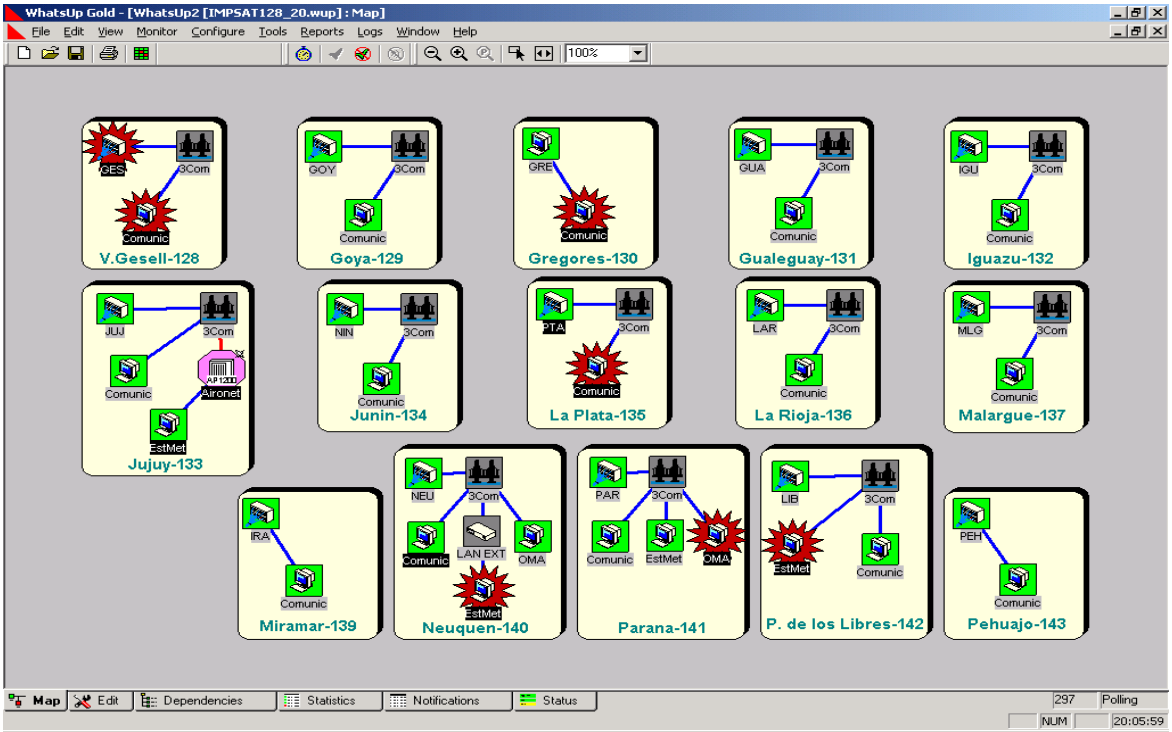
3.2.2.2 An ACC, under the concept “non existance of a common failure point”.



3.2.2.3 A very busy airport



3.2.2.4 A group of small airports



3.3. Addressing Plan

3.3.1 Each State may use the addresses and the addressing scheme it prefers, but it is recommended that:

3.3.1.1 Network addresses be assigned in continuous blocks.

3.3.1.2 Address blocks be distributed in hierarchical order to allow for routing scalability.

3.3.1.3 Subnetwork configuration be allowed in order to maximise the use of each assigned network.

3.3.2 The only addresses assigned and known to the other States will be those of communication equipment interfaces used in the interconnection boundaries between internal and external networks in each State.

3.3.3 Thus, each State must guarantee the routing through its network to the internal address(es) of the application servers used in other States.

3.3.4 The Regional Office will determine which *regional routing* option will be finally selected, and will also coordinate and assign the addresses and modality to be established based on the corresponding institutional arrangements (ATN Task Forces, CNS Committee, GREPECAS, ACP, etc.).

3.4 Service Transfer

3.4.1 So as not to disturb the normal development of air operations, it is recommended that services be transferred to the IPS network gradually, one at a time. As already established, *AMHS* **must** be the first service to be mounted on the IPS-based ATN.

3.4.2 Once the deployment of this particular service has been completed, each State may choose:

3.4.2.1 To continue with other data services (radar signals, AIS and/or MET applications, AIDC, OLDI, etc.); or

3.4.2.2. To begin the transfer of operational voice services (direct or switched ATS communications); or

3.4.2.3 A combination of both.

3.4.3 *Radar signals*: If these are generated in a native IP form, they will be mounted directly according to the corresponding addressing. If they are generated in a synchronous serial form, be it V.35 or V.24, they must be entered in the network in a “multicast” so that they can be received at their destination.

3.4.4 *AIDC*: This application shall be “mounted” over the AMHS application; thus, its transport over the IP network is immediate.

3.4.5 *OLDI*: The States that have OLDI X.25 instead of AIDC service should make the necessary software arrangements for its transport over IP instead of X.25.

3.4.6 *ATS speech communications (ACC – TWR or between ACCs of the same State):* Pre-operational tests should be started by duplicating conventional circuits with high traffic density airports in order to detect/correct problems that might emerge. Once this stage has been completed, use shall be extended to the rest of the network.

3.4.7 *ATS speech communications (between ACCs of different States): via* REDDIG, once the necessary bilateral or multilateral arrangements have been made.

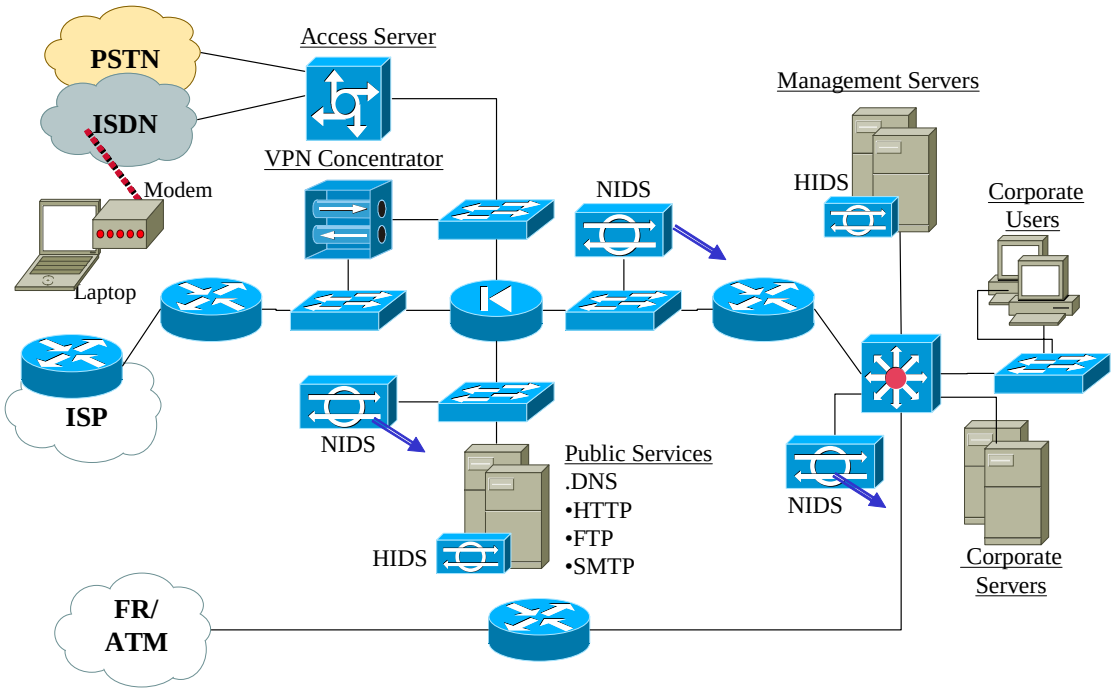
3.4.8 *ADS –B*: When this service becomes available.

Appendix 1. – Networking Concepts

TABLE OF CONTENTS

1. NETWORKING

1.1 The term networking (or internetworking) is applied to the industry, products and activities related to the interconnection, design and administration of individual networks so that they operate and behave like a single large network.



1.2 The above figure illustrates a medium-sized corporate network, showing frequently used network devices. Network design objectives are generally:

1.2.1 Functionality

1.2.2 Performance

1.2.3 Security

1.2.4 Management

1.2.5 Scalability

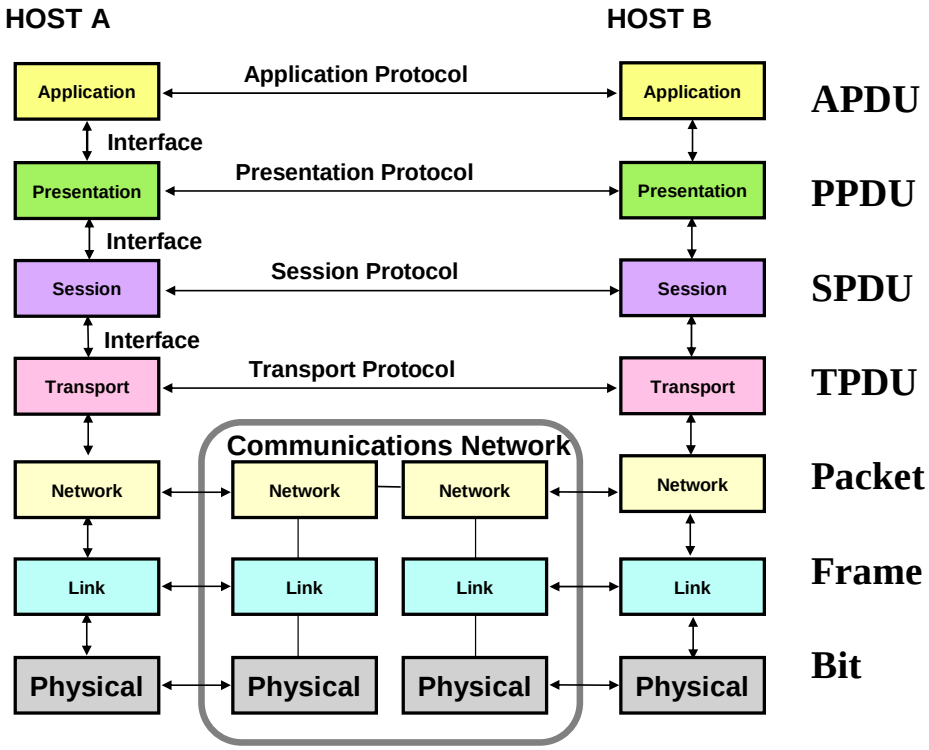
1.2.6 Compatibility

Reference models

1.3 The advantage of reference models is that they break down network operation complexity into a manageable series of levels or layers. Reference model-based protocol design allows changes to be made in one layer without affecting others. It is an effective instrument for analyzing networks of all kinds.

OSI Reference Model

1.4 Developed by ISO, the OSI reference model is a framework for promoting standardization of protocols used to interconnect heterogeneous (open) systems.



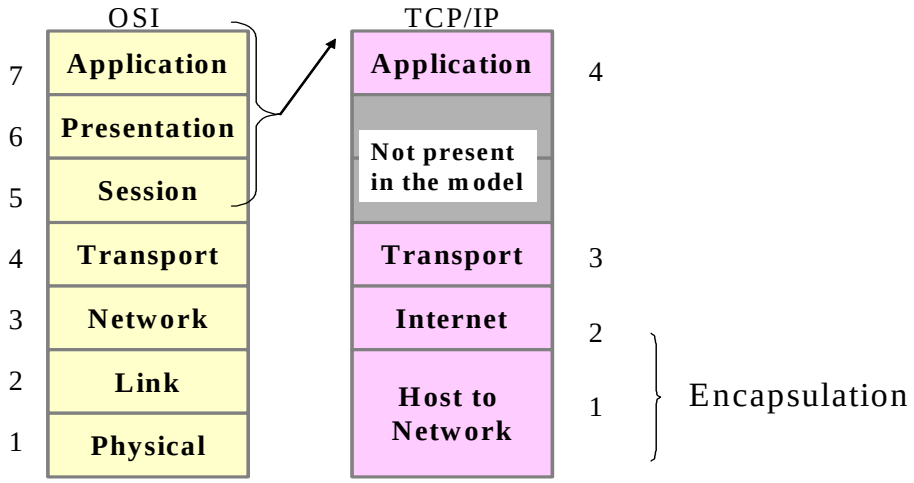
OSI LAYER	FUNCTIONAL DESCRIPTION	EXAMPLES
7.- APPLICATION	Semantics. Interface with applications/users.	Telnet, HTTP, FTP, www, NFS, SMTP, SNMP, X.400
6.- PRESENTATION	Data format. Syntax. Special processing (encryption).	JPEG, ASCII, EBCDIC, TIFF, GIF, PICT, encryption, MPEG, MIDI
5.- SESSION	Orderly data flow among participating parties (transactions).	RPC, SQL, NFS, NetBIOS names, AppleTalk ASP, DECnet SCP
4.- TRANSPORT	Service quality. Division between network and upper layers. Mux.	TCP, UDP, SPX
3.- NETWORK	Logical addressing. Routing.	IP, IPX, APPLETALK, ICMP
2.- DATA LINK	Medium access. Link between neighbouring stations. Error management.	IEEE 802.3/802.2, HDLC, Frame Relay, PPP, FDDI, ATM, IEEE 802.5/802.2
1.- PHYSICAL	Physical signals. Connectors. Timing.	EIA/TIA-232, V.35, EIA/TIA-449, V.24, RJ-45, Ethernet, 802.3, 802.5, FDDI, NRZI,NRZ, B8ZS[1]

[1] Note: these specifications are often complementary (i.e.: RJ-45 is only the connector).

TCP/IP Reference Model

1.5 There are no presentation and session layers in the TCP/IP model. The application layer containing all of the high-level protocols rests directly over the transport layer.

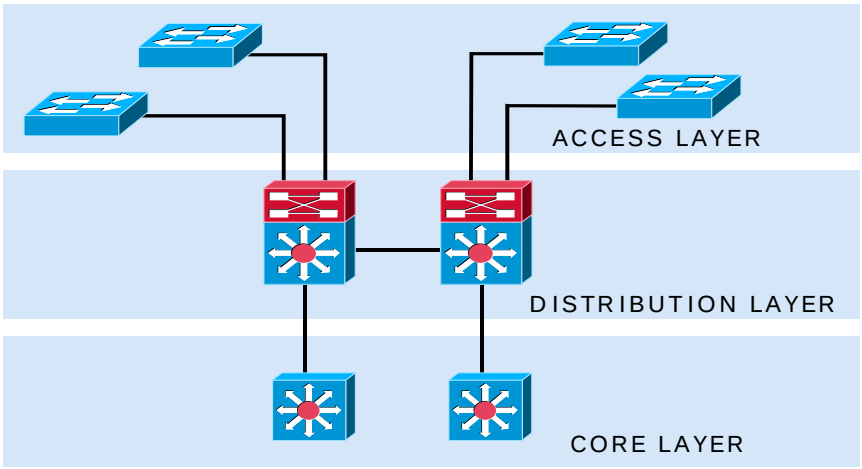
1.6 There is a large gap (and for that reason a great deal of flexibility) below the internet layer because no protocol is defined in the TCP/IP model (it only mentions that a protocol must be used to connect the host to the network in order to send packets).



1.7 Whenever mention is made of the layer model, the OSI reference model will be used (unless otherwise indicated). Thus, everyone knows that IP is a Layer 3 protocol (note that in the TCP/IP model, it corresponds to Layer 2).

CISCO hierarchical model

1.8 CISCO, while enjoying the same layer modelling advantages as OSI, together with others oriented toward the practical implementation of Campus networks, has its own hierarchical design--easy operation and management, better understanding, scalability, policy implementation, addressing efficiency and problem resolution.



1.9 The table below summarizes the characteristics of each layer of the hierarchical model:

CISCO LAYER	DESCRIPTION
CORE	High-speed transport with high reliability, redundancy and low latency. Site interconnections. High-speed switches. No compression, filtering, encryption or other processing loads.
DISTRIBUTION	Access lists, distribution lists, route summarization, VLAN routing, security policies, filters, aggregation, encryption, compression and service quality. High-speed routers and Level 3 switches.
ACCESS	Remote access services, shared and switched local access, MAC address filtering, and segmentation. VPN aggregation. Access switches.

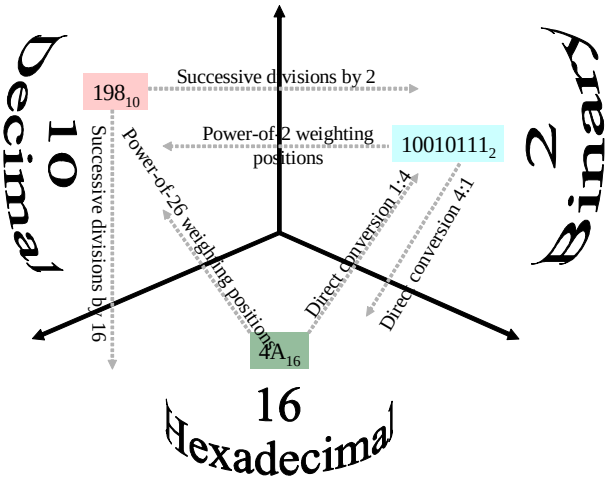
Numerical Bases

1.10 The study of physical and logical addresses requires a review of numerical bases and conversions. The diagram below demonstrates the principle of number formation using different bases.

b^n	b^7	b^6	b^5	b^4	b^3	b^2	b^1	b^0	base
• • •	10^7	10^6	10^5	10000	1000	100	10	1	b=10
• • •	128	64	32	16	8	4	2	1	b=2
• • •	8^7	8^6	32768	4096	512	64	8	1	b=8
• • •	16^7	16^6	16^5	65536	4096	256	16	1	b=16

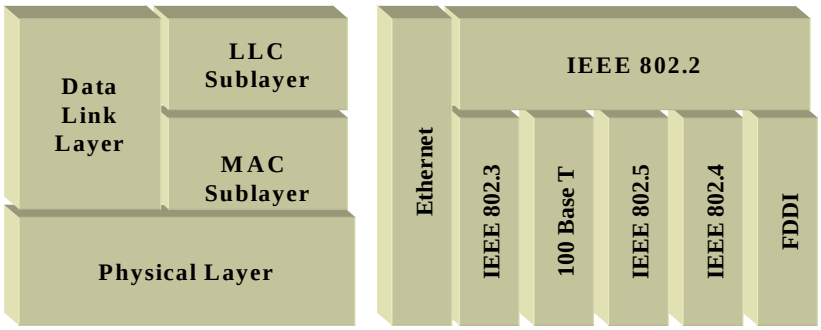
Decimal base : 0 1 2 3 4 5 6 7 8 9
Binary base : 0 1
Octal base : 0 1 2 3 4 5 6 7
10 11 12 13 14 15
Hexadecimal base : 0 1 2 3 4 5 6 7 8 9 A B C D E F

1.11 The keys to conversions between the different bases are represented by:



2. LAN PROTOCOLS

2.1 LAN protocols operate in the two lowest layers of the OSI reference model.



2.2 The IEEE (Institute of Electrical and Electronic Engineers) divides the data link layer into two sublayers: MAC (Media Access Control) and LLC (Logical Link Control). The MAC sublayer permits and implements medium access, such as through the contention method or token-passing, while the LLC sublayer is responsible for MAC sublayer framing, flow control, error control and addressing.

Medium access methods

2.3 LAN protocols normally use one of two methods for physical access to the network: CSMA/CD (Carrier Sense Multiple Access/Collision Detect) and Token-passing. Network devices in the CSMA/CD scheme compete for use of the physical means and for that reason it is called access by contention. Ethernet/IEEE 802.3, including 100BaseT, are the most characteristic examples of LAN networks using CSMA/CD.

2.4 The network devices in the Token-Passing medium access system accede to the physical medium based on the possession of a token. The most typical examples are Token Ring/IEEE 802.5 and FDDI (Fiber Distributed Data Interface).

Name	MAC Sublayer	LLC Sublayer	Comments
Ethernet_II (DIX)	Ethernet	There is no differentiation	Digital, Intel and Xerox proprietary specification.
IEEE Ethernet	IEEE 802.3	IEEE 802.2	Known as Ethernet 802.3
Token-Ring	IEEE 802.5	IEEE 802.2	Originated at IBM
FDDI	ANSI X3T9.5	IEEE 802.2	No comment

Transmission Methods

2.5 LAN transmissions are classified into three types*: unicast*, *multicast* and *broadcast*, in which a frame is sent to one or more nodes.

2.5.1 In the *unicast* transmission, a single packet is sent from a source to a destination.

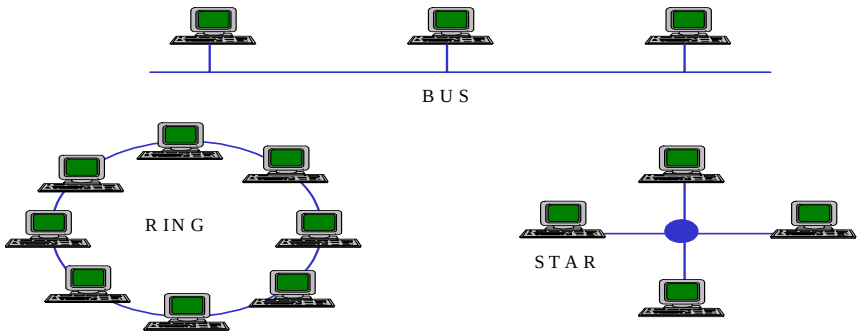
2.5.2 In the *multicast* transmission, a single packet generated by a source node is copied and sent to a specified subset of network nodes.

2.5.3 In the *broadcast* transmission, a single packet is copied and sent to all network nodes. The source node generates a single packet using the broadcast address.

LAN Topologies

2.6 LAN topologies define how the devices are organized within the network.

2.7 There are three common topologies: **bus, ring and star.**



2.8 Although these topologies are logical architectures, the real devices do not need to be physically organized according to these configurations. Logical bus and ring topologies, for example, tend to be physically organized in the shape of a star (through a hub).

2.9 Most frequently used Ethernet implementations (including Fast Ethernet, Giga Ethernet and 10 GE) use a *bus topology*, although the physical topology that is implemented through hubs and switches may have the appearance of a star.

3. ETHERNET TECHNOLOGIES

3.1 Ethernet has survived its initial battle as an essential physical medium technology because it is extremely flexible and relatively easy to implement and understand. Today it is without a doubt the dominant LAN network technology.

3.2 The term Ethernet is applied to a family of LAN implementations that include:

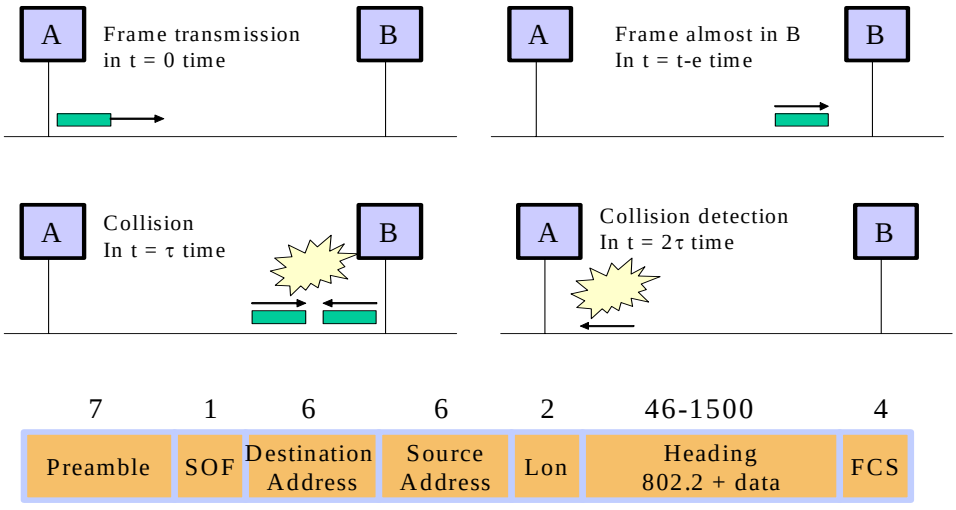
Standard	MAC Sublayer	Max Segment (meters)	Type of Cable	#Pairs
10Base5	802.3	500	50 ohm thick	-
10Base2	802.3	185	50 ohm thin	-
10BaseT	802.3	100	UTP 3-4-5	2
10BaseFL	802.3	2000	FO	1

Standard	MAC Sublayer	Max Segment (meters)	Type of Cable	#Pairs
100BaseFL	802.3u	100	UTP 5	2
100BaseFL	802.3u	100	UTP 3	4
100BaseFL	802.3u	100	UTP 3-4-5	2
100BaseFL	802.3u	400/2000	Multimode FO	1
100BaseFL	802.3u	10000	Monomode FO	1
1000BaseSx	802.3z	220-550	Multimode FO	1
1000BaseLx	802.3z	3000	FO	1
1000BaseCx	802.3z	25	STP	2
1000BaseT	802.3ab	100	UTP 5	2
10GBaseE[2]	802.3ae	40000	Monomode FO	1

Ethernet and IEEE 802.3

3.3 Ethernet is a baseband LAN specification invented by Xerox Corp. to operate at 10 Mbps, using CSMA/CD, over coaxial cable. The design was created to serve in networks with sporadic high traffic requirements. The IEEE 802.3 specification was developed on the basis of Ethernet. IEEE 802.3 offers a large variety of cabling options (for example 10Base5, in which 10 is the Mbps. speed, Base is the baseband signalling method, and 5 is the coaxial physical medium).

3.4 In the Ethernet broadcast environment, all stations "see" the frames transmitted over the network. Each station must examine the frames to determine whether it is the addressee, in which case those frames are passed to the upper layer.



[2] There are other monomode and multimode FO standards.

3.5 Any station on a CSMA/CD LAN can accede to the physical medium at any time, but, before transmitting data, stations check ("listen") to see whether there are any transmissions in the medium. If it is inactive, they can start their data transmission.

3.6 If two or more stations start transmitting at the same time, there will be a collision, in which case both transmissions are damaged. It will then be necessary to retransmit after a certain back-off period has passed, as imposed by an algorithm executed by the stations.

3.7 The IEEE 802.3 frame fields are:

3.7.1 *Preamble*: Alternating pattern of ones and zeros to indicate the presence of a frame to the stations.

3.7.2 *SOF* (Start of frame): delimitation byte to synchronize frame reception.

3.7.3 *Destination and Origin Addresses*: The first three bytes of the address are specified by the IEEE to identify the manufacturer and the last three are configured by the manufacturer. The origin address is always unicast (one node), but the destination address can be unicast, multicast (group) or broadcast (all nodes).

3.7.4 *Length*: Number of data bytes following this field.

3.7.5 *Data*: If the data in the frame are insufficient to fill the field to its minimum 64-byte value, padding bytes are added to ensure a length of at least 64 bytes.

3.7.6 *FCS* (Frame Check Sequence): A 4 byte CRC value to implement error control.

100-Mbps Ethernet (IEEE 802.3u)

3.8 This high-speed LAN technology offers important updating in the available bandwidth. 100BaseT is the 100 Mbps Ethernet implementation specification on UTP and STP.

3.9 The MAC sublayer is compatible with IEEE 802.3, so that format, size and error detection mechanisms are kept, while it also supports all 802.3 network applications and software.

3.10 100BaseT supports both 10 and 100 Mbps speeds, but the maximum network diameter is reduced by approximately 10 times as compared with 10BaseT (from 2000 to 205 meters), because of the need to detect collisions within the necessary timeframe for transmitting a minimum 64-byte length frame, even if the stations are located at the ends of the network.

1 Gigabit Ethernet

3.11 1 GE is an extension of the IEEE 802.3 standard that offers a 1 Gbit/s bandwidth, while remaining compatible with Ethernet and Fast Ethernet network devices.

3.12 1 GE provides a new full-duplex operating mode for switch-to-switch and switch-to-station connections. Even so, it uses the same frame format and size and management objectives as the IEEE 802.3 networks.

3.13 This network has been designed to operate on fibre optics, but can be implemented on UTP 5 and coaxial cable. The IEEE 802.3 Working Group established the 802.3z Gigabit Ethernet Task Force to develop the standards. The aim was to permit full and half-duplex operations at 1 Gbps., in keeping with the traditional frame format and the CSMA/CD medium access method. Retroactive compatibility with 10BaseT and 100BaseT is also foreseen.

3.14 The standard also specifies 500-meter maximum length monomode fiber link support, up to 2 km. of monomode fiber links, and a minimum of 25 meters of copper links.

10 Gigabit Ethernet

3.15 The 10 Gigabit (10GE) Ethernet specification is significantly different from the first Ethernet standards in several aspects, the most important of which are that it only supports fibre optics and operates in full-duplex mode. This means that collision detection protocols are not needed.

3.16 Despite reaching a speed of 10 gigabits per second, Ethernet maintains its frame format and current capacities, with the result that network infrastructure investments do not become obsolete. 10GE is interoperable with other networking technologies like SDH, making possible Ethernet frame transit over SDH paths highly efficient.

3.17 Ethernet expansion for use in metropolitan networks spurs technological advances beyond those achieved with 1 Gbps. networks, making Ethernet end-to-end connections possible. 1-Gigabit Ethernet has already been developed as backbone technology for metropolitan dark fibre networks. Service providers can now build links reaching 40 km. and more using 10GE interfaces, optical transceivers and monomode fibre.

4. LAN DEVICES

4.1 The most used network devices are:

Repeaters

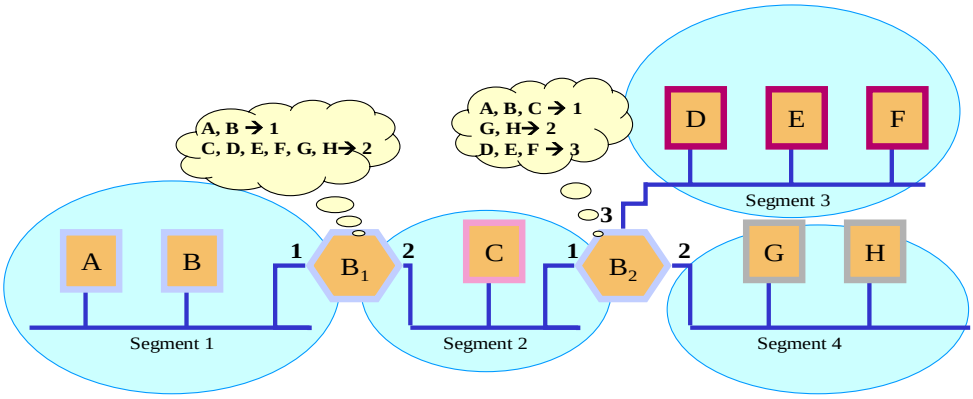
4.2 A repeater is a physical layer device used to interconnect the segments of an extended network. Essentially, it allows several cable segments to be treated as a single unit. It receives signals from a network segment, amplifies them, then retimes and relays them to the other segments. This prevents signal deterioration created by the length of the cable and the number of devices connected to it.

Hubs

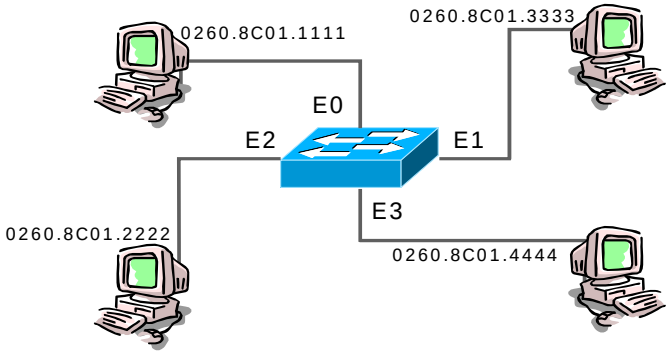
4.3 A hub is a physical layer device that interconnects multiple user stations through a dedicated cable. Electrical connections are established inside the hub. Hubs create a star physical network, while maintaining the LAN logical bus or ring configuration. The hub could be said to function as a multiport repeater.

Bridges and Switches

4.4 Bridges and switches[3] are devices that operate mainly in layer 2 of the OSI Reference Model (data link layer devices). Several types of bridging operations have taken place in internetworking scenarios. Transparent bridges have been applied mainly in Ethernet environments, while source-route bridges were used in token ring networks. MAC layer bridges are designed to operate between homogeneous networks, while others are able to translate different data link layer protocols (IEEE 802.3 and IEEE 802.5, for example).



4.5 Switching technology has emerged as the successor in the evolution of network solutions. Superior performance, throughput, greater port density, lower per-port cost and more flexibility are the characteristics responsible for the success of switches in replacing bridges and complementing routers.



4.6 Switches are considerably faster than bridges because the switching takes place in the hardware (there are store & forward, cut-through and fragment-free switches). They are able to interconnect Ethernet networks at a rate of 10, 100 and 1000 Mbps.

Full-duplex

4.7 Half-duplex behaviour is needed when stations use an Ethernet 10BaseT hub, which recreates an electrical equivalent of the bus, and CSMA/CD rules remain in effect. If the topology permits collisions, CSMA/CD can be used to react to them.

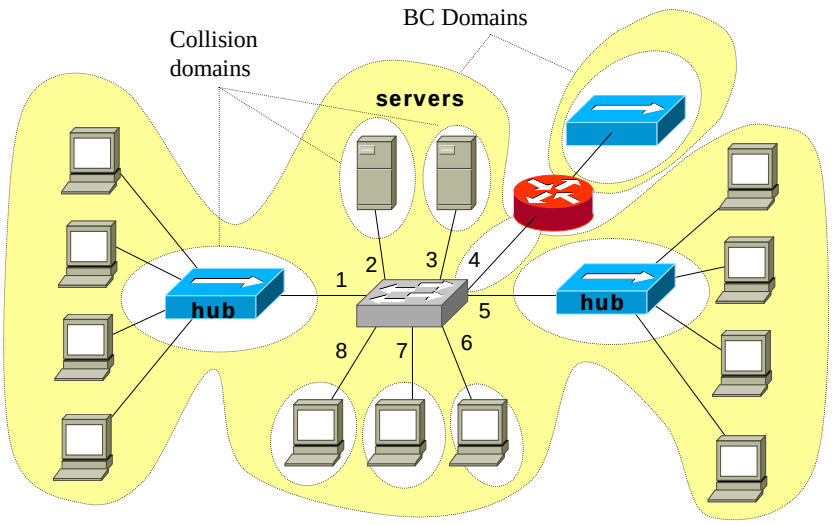
[3] Note: there are ATM switches, LAN switches, and several types of WAN switches.

4.8 Full-duplex operation is impossible with a shared 10BaseT hub, but it can be done if the possibility of collision is removed (as with a switch). This gives rise to switched networks.

Collisions and Broadcasts

4.9 Different devices delimit collision and broadcast domains.

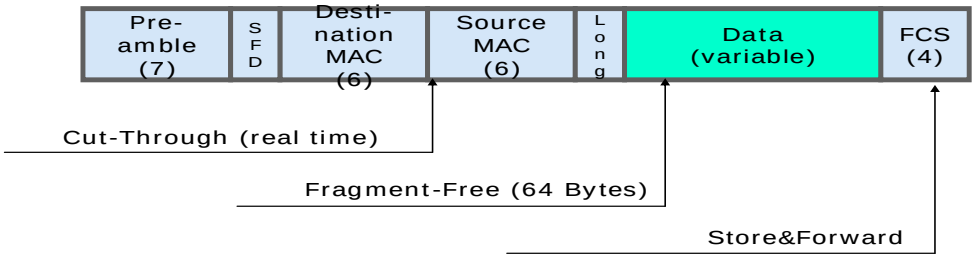
4.10 The **collision domain** encompasses all network plates that receive a transmission originating in this domain (in a hub, they are all the interfaces connected to its ports). This means that so long as signals are present in the transmission medium, all other stations will have to wait for a chance to transmit.



4.11 The **broadcast domain** consists of all network interfaces that receive a broadcast (bc) or multicast (mc) transmission originating in the domain (a bc transcends hubs, bridges and switches, but not a router). The diagram shows the collision and broadcast domains in a multi-device network.

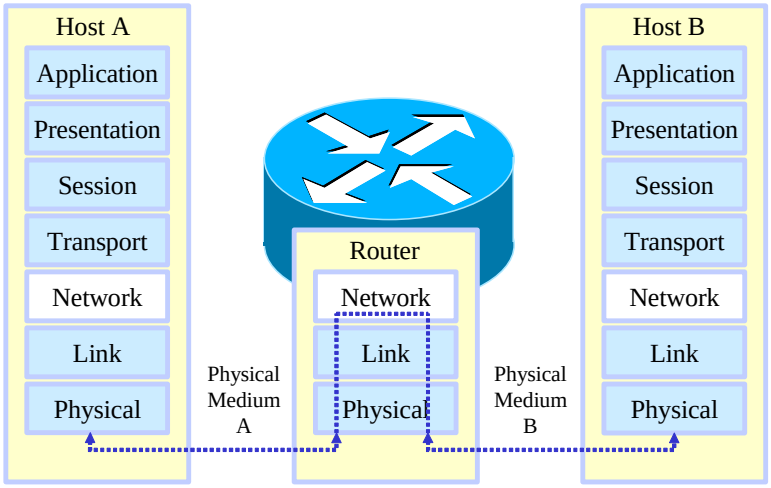
Types of operation

4.12 Among the advantages of switches are their capacity to operate in different modes with regard to the moment of transmission of the frames received. **Store & Forward** is the slowest traditional mode, in which the switch awaits reception of the complete frame in order to check that all form requirements are correctly met before its retransmission. The **Cut-Through** mode is the quickest, for once the destination address has been determined, the frame is immediately transmitted through the output port, although without the possibility of checking whether the unit meets the criteria for length, error detection, etc. Lastly, the Fragment-Free mode is an intermediate one in which the switch waits to receive the minimum number of bits in order to ensure that it is not a runt (abnormally short frame produced by a collision or a transmission error).



Routers

4.13 One of the most usual forms of interconnecting LANs and subnets today is by routers. Routers are installed at the boundaries between two physical and/or logical networks. For internetworking, routing is a more sophisticated method than bridging. In theory, a router (or a network layer switch) can act as a translator between a subnet with a P1 physical layer protocol, a DL1 data link layer protocol, and an N1 network layer protocol, and another subnetwork with a P2 physical layer protocol, a DL2 data link layer protocol, and an N2 network layer protocol. Routers are generally used to interconnect networks using the same network layer, but different link layer protocols.



4.14 Routers allow for the interconnection of LANs through WANs, using traditional services (point-to-point, Frame Relay and ATM lines), and new IP/MPLS network services. Some routers operate directly on SDH and can also interconnect different LANs like Token Ring and Ethernet.

4.15 The use of routers makes its possible to establish different networks both physically and logically, each with its own address space. Routing methods become increasingly sophisticated as topology size and complexity increase. IP, IPX, and AppleTalk are the most common network layer protocols, although the general trend is toward IP use.

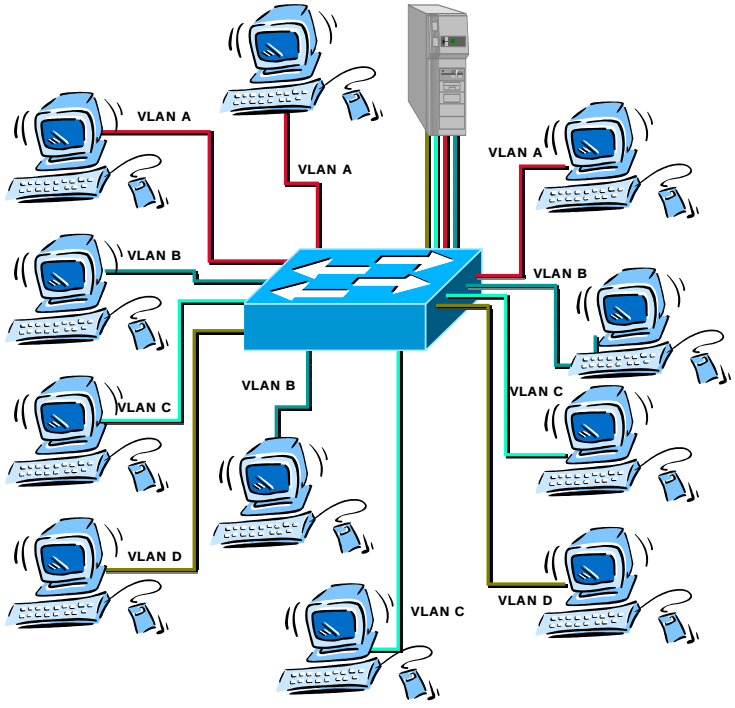
5. VLANs

5.1 Switches segment the collision domain to the maximum (only one device is connected to each port, making it possible to disable collision control and full-duplex transmission). Full network performance, however, is vulnerable to an excess of a certain kind of traffic because the switches propagate the bc's and mc's to all ports.

5.2 One way to limit mc and bc traffic is by configuring VLANs (virtual LAN networks). VLAN support makes it possible to isolate networks within a single (or several) switches, impeding communication between devices connected to different VLAN ports (unless integrated by a router). VLAN design is based on security, performance, management and other considerations.

5.3 The diagram shows a VLAN-supported switch in which 4 VLANs have been configured: A, B, C and D.

5.4 In this example, each switch port constitutes a collision domain (actually, there will be no collisions and their detection can be deactivated in both the devices and the switch ports). The basic difference between this example and that of a switch without VLANs is that now each VLAN constitutes a broadcast domain (that is, a bc or mc transmitted in VLAN 2, for example, will not be transferred to the three other VLANs.)



5.5 All terminals connected to ports belonging to a single VLAN can communicate with each other, but cannot with those connected to other VLANs.

5.6 There are two ways for all terminals to accede to the server:

5.6.1 Use four of the switch ports, each belonging to a VLAN, and connect them to 4 Ethernet interfaces installed in the server.

5.6.2 Use a single interface with a trunking protocol (also supported by the switch) to connect it to the switch port transporting the traffic of all VLANs.

5.7 In both cases, if the server routing function is activated, it will also be possible for the terminals in the different VLANsto communicate with each other.

6. WAN NETWORKS AND DEVICES

WAN CHARACTERISTICS

6.1 The main WAN characteristics are:

6.1.1 Extended geographic area: the network operates beyond the local geographic field of a LAN and generally uses the services of a carrier to interconnect devices over global areas.

6.12 WANs use serial connections (interfaces) of different types and speeds to accede to the bandwidth.

6.1.3 They provide full-time and part-time connectivity.

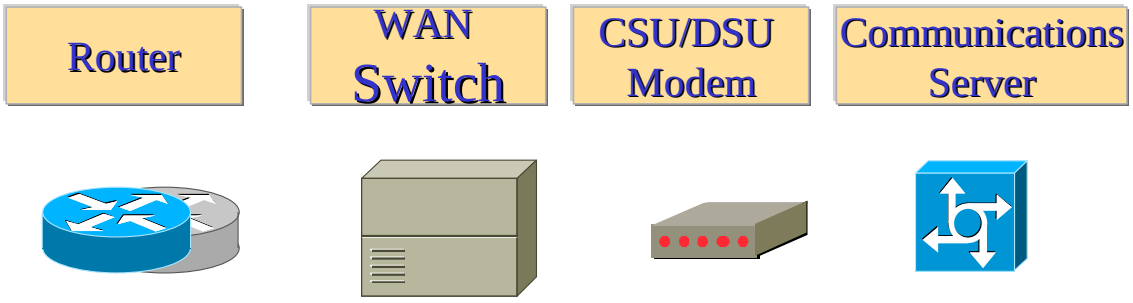
6.1.4 By definition, a WAN connects separate devices over wide areas. WAN devices include:

6.1.4.1 *Routers* that offer multiple services including internetworking and WAN interface ports.

6.1.4.2 *Switches* for voice, data and video communication that interconnect with the WAN bandwidth.

6.1.4.3 *Modems* that serve as an interface to voice grade services. They include channel service units/data service units (CSU/DSU) that serve as an interface for T1/E1 services, and terminal adaptors/network termination (TA/NT) that serve as an interface for integrated service digital network (ISDN) services.

6.1.4.4 *Communication servers* that concentrate communications by telephone for user access.



6.2 WAN networks use the OSI layer division method for encapsulation, as in LAN networks.

WAN TECHNOLOGIES

6.3 *WAN* protocol physical layer specifications describe how to provide electrical, mechanical, operational and functional connections for wide area networking services. These services are generally obtained from WAN service providers (carriers).

6.4 WAN protocol *data link* specifications describe how frames are transported over a single data route established between communicating systems. They include protocols designed for operation through dedicated *point-to-point, multipoint* and multi-access switched services like *Frame Relay*.

6.5 A number of recognized authorities, including the following organizations, define and administer WAN standards:

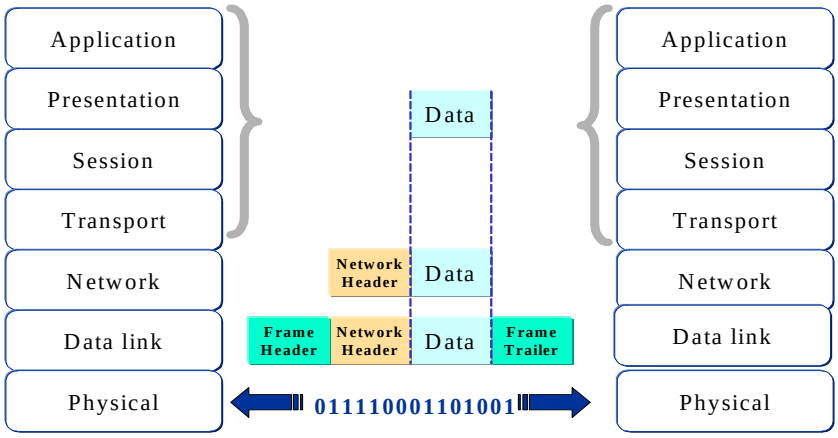
6.5.1 International Telecommunication Union - Telecommunication Standardization Sector (ITU-T), the former International Telegraph and Telephone Consultative Committee (CCITT)

6.5.2 International Organization for Standardization (ISO)

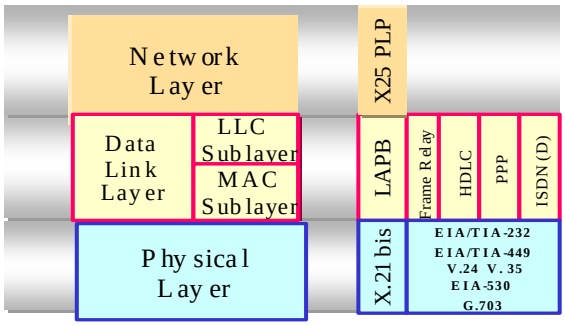
6.5.3 Internet Engineering Task Force (IETF)

6.5.4 Electronic Industries Alliance (EIA)

6.6 WAN standards and specifications describe both physical layer delivery methods and data link layer requirements, including data flow addressing and encapsulation. The diagram shows lower layer protocol generic data units.

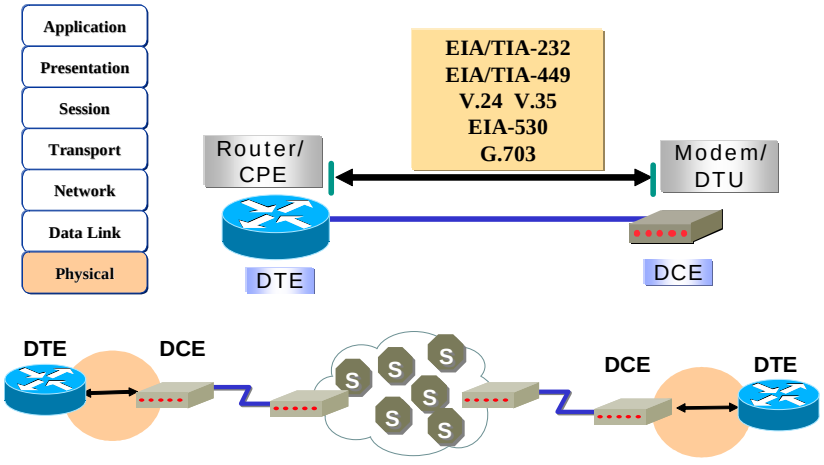


6.7 The following diagram shows the stack of protocols used by WAN networks.



Physical layer

6.8 The WAN physical layer describes the interface between the data terminal equipment (DTE) and the data communications equipment (DCE). The DCE is usually the service provider and the DTE, the connected device. Under this model, services are offered to the DTE through a modem or channel service unit/data service unit (CSU/DSU).



6.9 The following physical layer standards specify these interfaces:

6.9.1 EIA/TIA-232

6.9.2 EIA/TIA-449

6.9.3 V.24

6.9.4 V.35

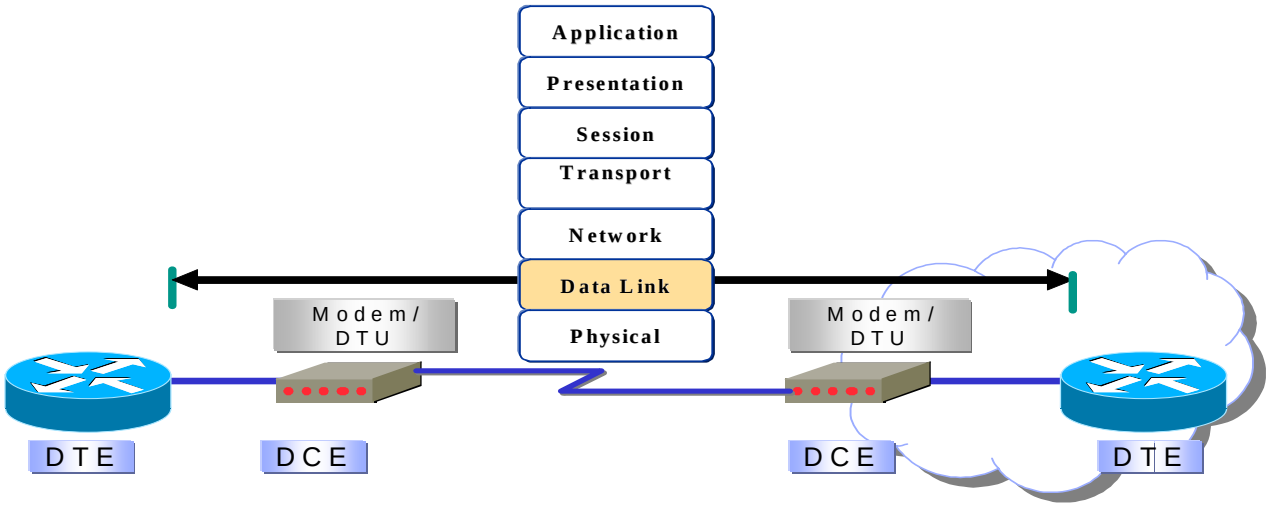
6.9.5 X.21

6.9.6 G.703

6.9.7 EIA-530

Data link layer

6.10 The most common data link encapsulation protocols associated with serial synchronous lines are cited below.



6.10.1 **High-level data link control (HDLC)** - An ISO standard. HDLC may not be compatible among different manufacturers because of the way each manufacturer decides to implement it. HDLC supports both point-to-point and multipoint configurations.

6.10.2 **Frame Relay** – Using a simplified frame without error control mechanisms through high-quality digital facilities, Frame Relay can transmit data very rapidly compared with these other WAN protocols.

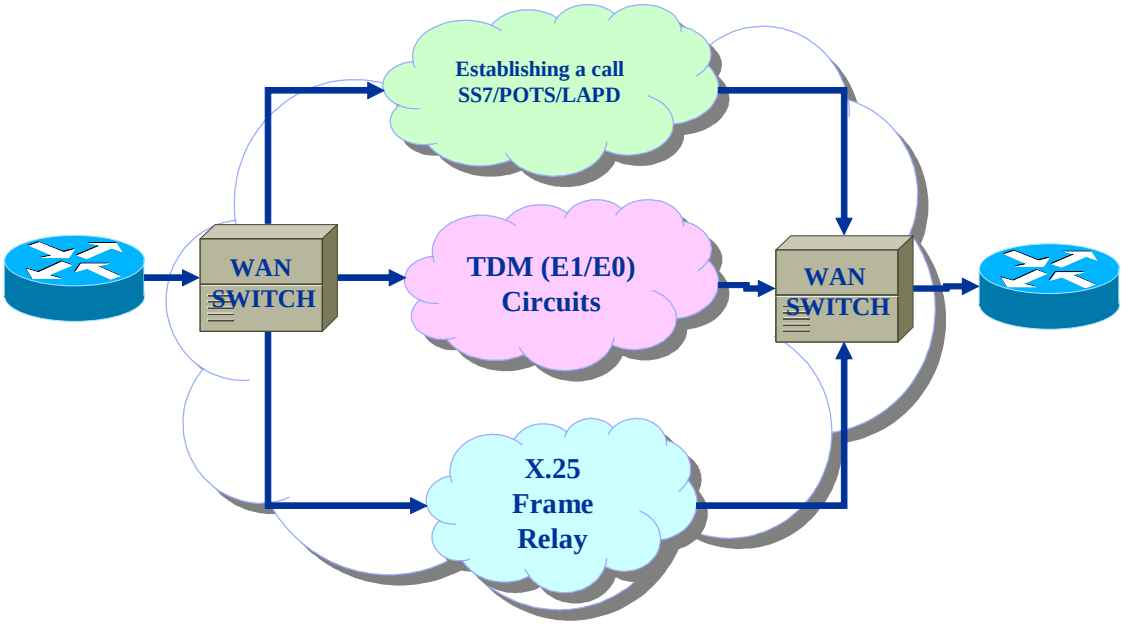
6.10.3 **Point-to-point protocol (PPP) –**Two standards developed by IETF, as described inRFC 1661. PPP contains a protocol field to identify the network layer protocol.

6.10.4 **Integrated services digital network (ISDN)** – A set of digital services that transmit voice and data over existing telephone lines.

7. WAN SERVICES

CLASSIFICATION OF SERVICES

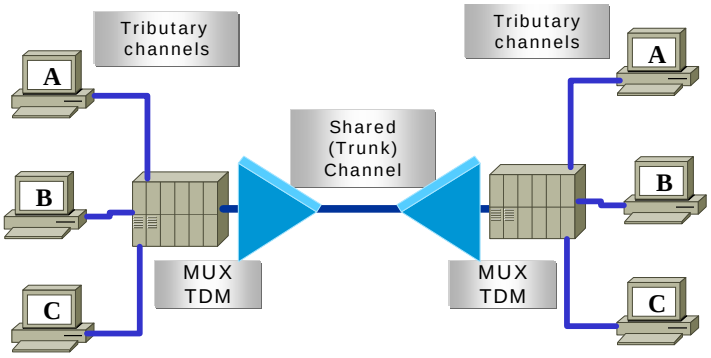
7.1 As already stated, one of the important differences between WANs and LANs is that in the former case a provider (carrier) must be hired in order to use the network transport resources.



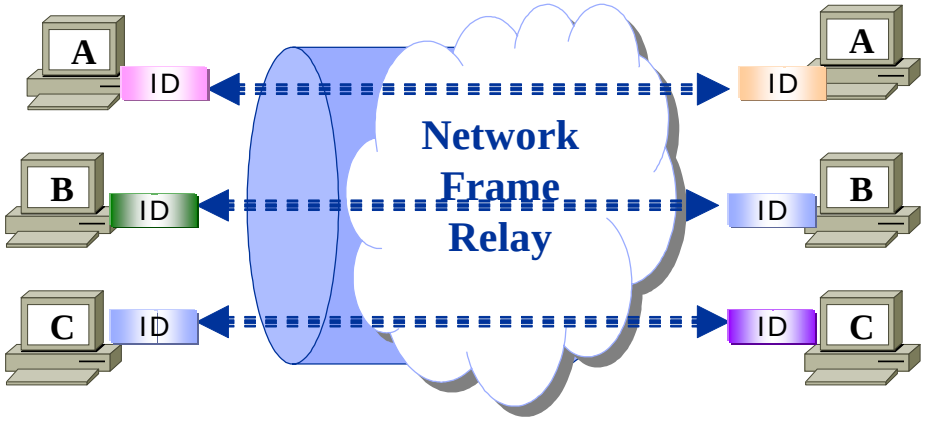
7.2 The most commonly used WAN service is basic telephone service. Both telephone and data services are connected from the point of presence (POP) of the building to the WAN provider central office (CO). A preliminary classification can be made of the "WAN cloud", which organizes the WAN provider services into three main types:

7.2.1 **Call establishment service** – Establishes and releases calls between telephone users. Signalling through common channel number 7 (SS7) is the most commonly used call establishment. It uses telephone control signals and messages between transfer points along the route to the dialled destination.

7.2.2 **Time division multiplexing (TDM) –** Information from multiple sources has a wideband location in a single medium. Circuit switching uses signalling to determine the call route, a dedicated route between the sender and the receiver. Time division multiplexing (TDM) avoids congested facilities and variable delays. Basic telephone service and the integrated services digital network (ISDN) use TDM circuits.

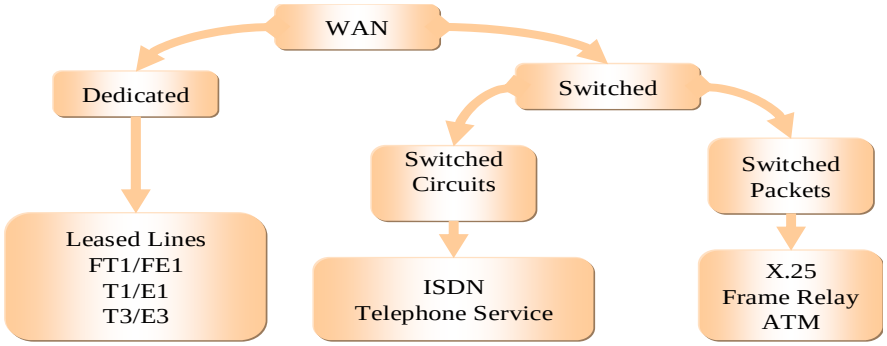


7.2.3 **Packet switching services** (like X.25 or Frame Relay). Information in packets or frames shares a non-dedicated bandwidth with other WAN frames of the subscriber. X.25 packet switching uses layer 3 routing with the sender and receiver addressing contained in the packet. X.25 can use switched virtual circuits (SVCs), with some initial delay for the call establishment, or permanent virtual circuits (PVCs), which avoid delays in call establishment. Frame Relay uses layer 2 identifiers and permanent virtual circuits (PVCs).



TECHNOLOGIES

7.3 There are two types of general options for wide area networking: dedicated lines or switched connections. The latter, in turn, can be either switched circuits or switched packets/cells .



7.4 The WAN provider can receive orders for wide area network links at different speeds stated in bits per second (bps) capacity. This bps capacity determines how rapidly data can be transmitted over the link.

7.5 The WAN bandwidth is provided in our setting, Europe and Japan based on PDH and SDH digital hierarchies. E1 is the first multiplexing level in PDH hierarchy and refers to a 2,048 Mbps signal.

7.6 A similar hierarchy has been developed in the United States, where each format is called a digital signal (DS). The term T1 tends to be used colloquially to refer to the DS1 signal and the term T3 to refer to the DS3 signal.

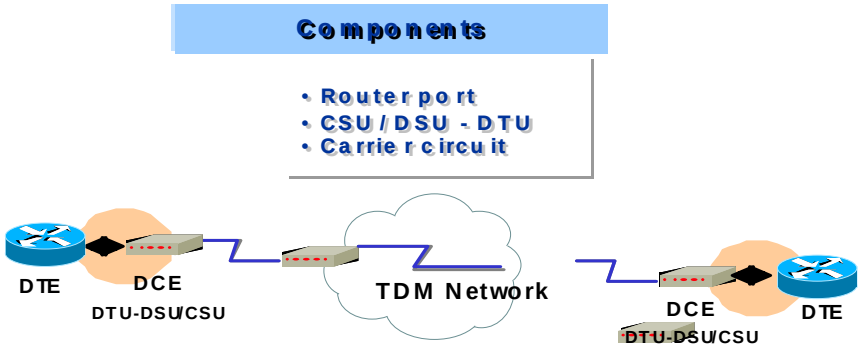
Dedicated line service

7.7 Dedicated—or leased--lines provide full-time service. Transmission speeds can reach up to E3 (34,364 Mbps), or higher, but are usually E1 (2,048 Mbps) or fractional E1 (in 64 kbps or n64Kbps increments).

7.8 Dedicated lines are generally used to transport data, voice and video. In data network design, leased lines usually provide the main connectivity among important sites or campuses and LAN-to-LAN connectivity.

7.9 When leased lines are connected, a router port will be needed for each connection, in addition to a CSU/DSU and the existing circuit of the service provider.

7.10 The cost of dedicated line solutions can become very high when used to connect many sites, especially if a complete gridded network is used. Serial point-to-point links provide full-time dedicated connectivity.



7.11 Connections are made using the router synchronous serial ports with typical bandwidth utilization of up to 2 Mbps (E1) available through a channel service unit/data service unit (CSU/DSU). Use of different encapsulation methods in the data link layer gives user traffic **flexibility and reliability**.

7.12 Leased lines of this kind are ideal for high-volume environments with a constant-speed traffic pattern. *Use of the available bandwidth is a matter of concern because the cost of the line is paid even when the connection is inactive.*

Switched circuit service

7.13 Switched circuit connections from one location to another are established on demand, only when a communication is needed, and are generally low bandwidth. Basic telephone service connections are usually limited to 33.6 Kbps. without compression and ISDN at 64 or 128 Kbps.

7.14 Switched circuit connections are used primarily to connect remote and mobile users to corporate LANs. They also serve as support lines for higher speed primary circuits, such as Frame Relay and dedicated lines.

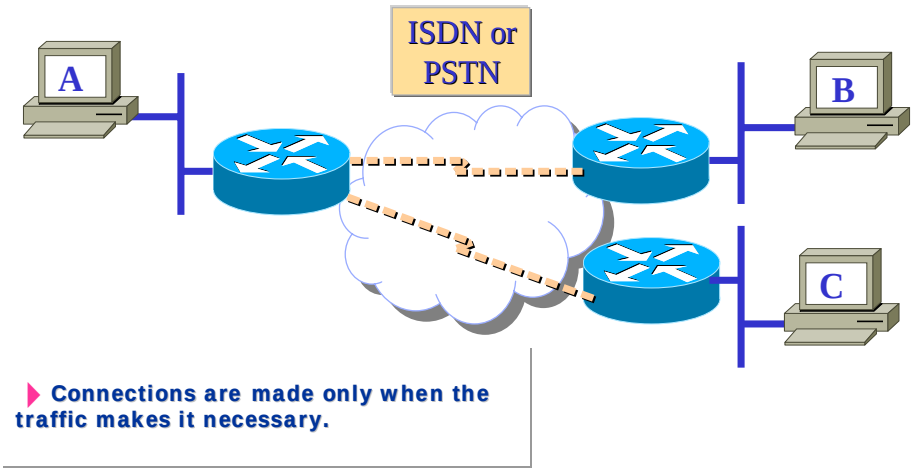
Dial-on-demand routing

7.15 Dial-on-demand routing (DDR) means the connection is made only when a specific type of traffic initiates the call or when a backup link is needed. These switched circuit calls are usually made over ISDN networks.

7.16 DDR is an ideal substitute for leased lines when full-time availability of the circuit is not needed, as in the following cases:

7.16.1 When traffic patterns are low volume or periodic. The calls are made and connections established only when the router detects traffic that is marked as "interesting." Care should be taken to keep periodic broadcasts, like routing protocol updates, from triggering calls.

7.16.2 When a backup connection is needed for redundancy or shared load. The DDR can be used to provide shared load and/or a backup interface. For example, there may be several serial lines, but the desire is to use the secondary line only when the primary one is very occupied, in order to share the load. When WAN lines are used for critical applications, secondary DDR lines--automatically enabled--can be configured as backup when the main lines are out of service.



ISDN

7.17 ISDN was developed by telephone companies intending to create a fully digital network.

General

7.18 ISDN includes the following devices:

7.18.1 **Terminal Equipment 1 (TE1) —** Denotes a device that is compatible with the ISDN network. A TE1 is connected to a type 1 or 2 (NT1/NT2) network termination.

7.18.2 **Terminal equipment 2 (TE2) —** Denotes a device that is not compatible with ISDN and requires a terminal adaptor (TA).

7.18.3 **Terminal adaptor (TA) —** Converts standard electrical signals to the form used by ISDN so that non-ISDN devices can connect to the ISDN network.

7.18.4 **Type 1 network termination (NT1) —** Connects 4-wire cabling of the ISDN subscriber to the conventional 2-wire local loop facility.

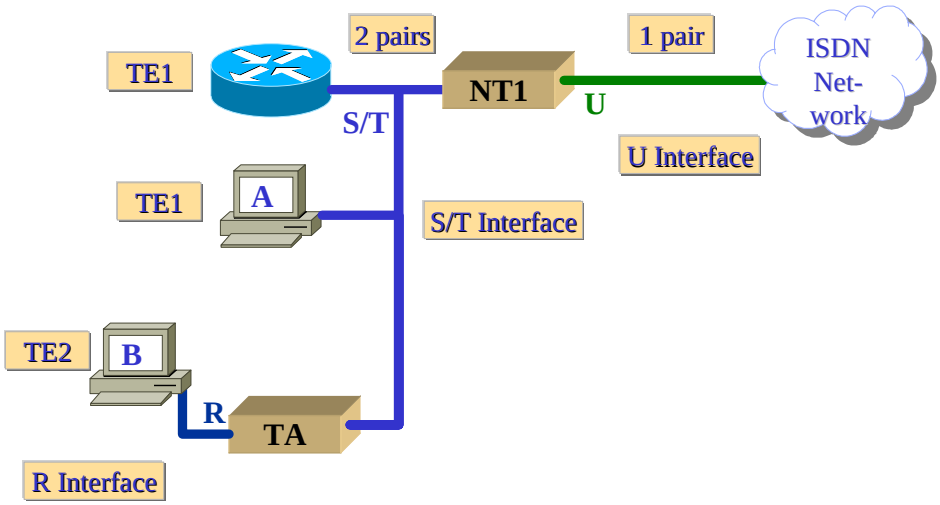
7.18.5 **Type 2 network termination (NT2) —** Directs the traffic to and from different subscriber devices and NT1. NT2 is an intelligent device that performs the switching and concentration (a PBX, for example).

7.19 Reference points separate the ISDN functional groups and define the boundaries of the following interfaces:

7.19.1 The S/T interface defines the functional boundary between a TE1 and the NT. The S/T is also used to define the interface between the TA and the NT.

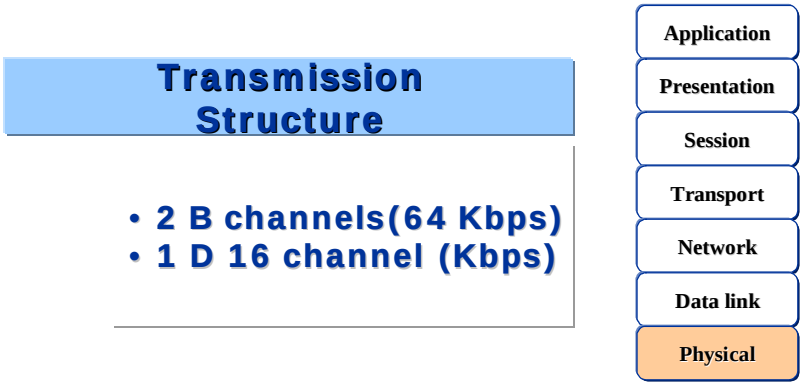
7.19.2 The R interface defines the interface between a TE2 and the TA.

7.19.3 The U interface defines the 2-wire interface between the NT and the ISDN “cloud”.

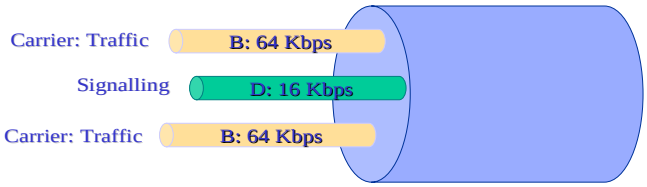


ISDN transmission structure

7.20 The transmission structure corresponds to the organization of the channels over the local loop for access to support services. There are two structures between the user and the ISDN center: the basic access interface (BRI) and the primary access interface (PRI).



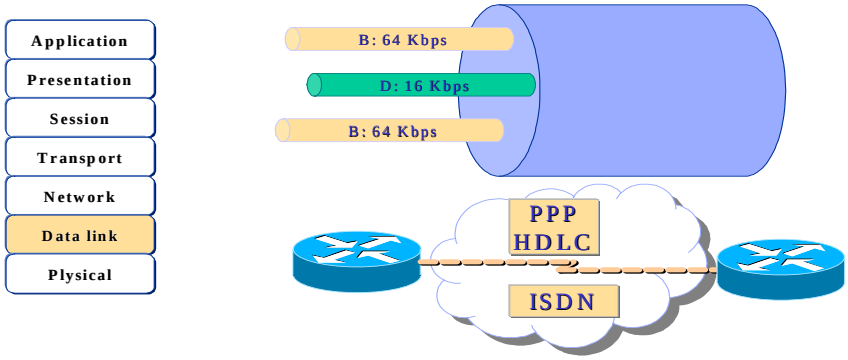
7.21 ISDN BRI operates over most of the copper cabling of today's exterior telephone facility and delivers a total bandwidth of one 144-kbps line in three separate channels. Two of the channels, called B-channels (carriers), operate at 64 kbps and are used to transport voice or data traffic. The third channel, called D (data) channel, is a 16-kbps signalling channel used to carry instructions telling the telephone network how to manage each of the B-channels. ISDN BRI is often known as "2B+D."



7.22 ISDN gives the network designer a great deal of flexibility because of its capacity to use each of the B-channels for voice or separate data applications. A long document, for example, could be downloaded from the corporate network through one of the ISDN 64-kbps B-channels, while the other B-channel is being used to examine a page of the World Wide Web. PRI access with 30 B-channels (64 Kbps) and 1 D-channel (64 Kbps) could also be used.

ISDN data link encapsulation

7.23 There are several encapsulation options available with remote access solutions, the most commonly used one being the point-to-point protocol (PPP).

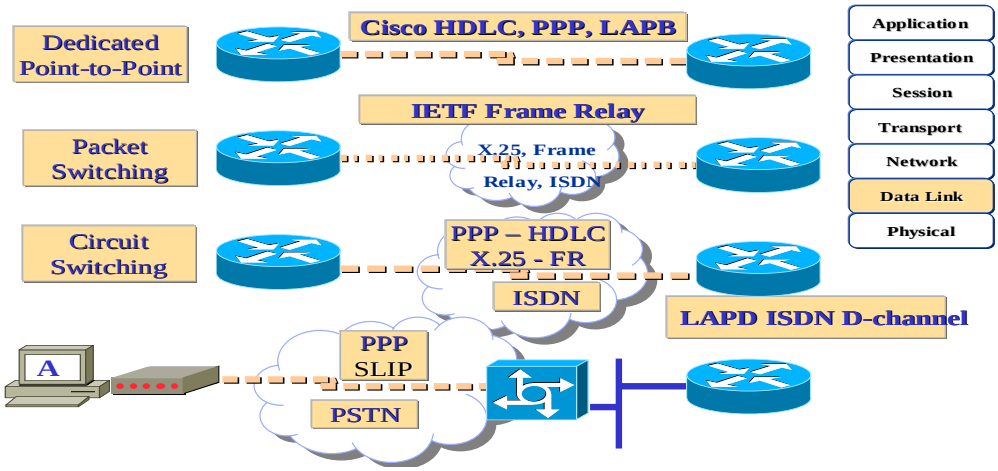


PACKET SWITCHING NETWORKS

7.24 Switched networks can transport varying sizes of frames (packets) or fixed-size cells. The most common type of packet switching networks is the Frame Relay. Frame Relay was designed for high speed and more reliable links. As a result, it has a limited number of error checking and reliability characteristics. Upper layer protocols are expected to deal with these problems.

WAN ENCAPSULATION PROTOCOLS

7.25 Each type of WAN connection uses a layer 2 protocol to encapsulate[4] traffic as it crosses the WAN link. The choice of encapsulation protocol depends upon the WAN technology and the communications equipment.



7.25.1 **HDLC—**The Cisco default encapsulation in point-to-point links. It is normally used in communicating with another Cisco device. If the communication is being made with a non-Cisco device, the most viable option could be synchronous PPP.

[4] **Encapsulation** – Data envelope in a particular protocol heading. For example, Ethernet data are encapsulated in a specific Ethernet heading before travelling over the network.

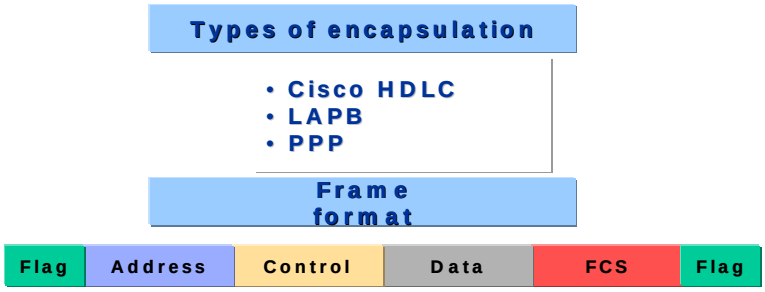
Tunneling – Architecture designed to provide the necessary services for implementing any standard point-to-point encapsulation system.

7.25.2 **LAPB** (X.25 protocol layer 2) – For packet switching networks. Can also be used on point-to-point links if the link is unreliable or there is an inherent delay associated with the link, as in the case of a satellite link. LAPB provides reliability and flow control on a point-to-point basis.

7.25.3 **PPP-** Usual for single user telephone dialling access to LAN or from LAN-to-LAN (router-to-router). PPP is standardized, allowing for interoperability among manufacturers. It also supports the encapsulation of several upper layer protocols, including IP and IPX.

7.25.4 **FR Cisco/IETF**- Used to encapsulate Frame Relay traffic. Cisco is a proprietary option and can be used only among Cisco routers.

7.26 There are, then, four different serial line encapsulation methods. Although their characteristics are different, they all share a common frame format, as shown for HDLC, LAPB and PPP –and in the next MD, which will be used for Frame Relay-.



7.27 The frame contains the following fields:

7.27.1 **Flag**—Indicates the start of the frame and is determined using the 7F hexadecimal standard.

7.27.2 **Address**—A one or two byte field to address the end station in multidrop environments.

7.27.3 **Control**—Indicates whether the type of frame is for information, supervision or unnumbered. It also contains specific function codes.

7.27.4 **Data**—The encapsulated data.

7.27.5 **FCS**—The frame check sequence.

7.27.6 **Flag**—The 7E trailer flag identifier.

CISCO HDLC ENCAPSULATION

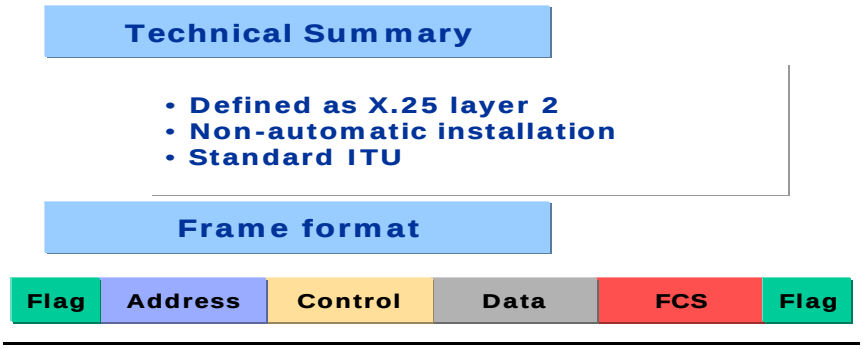
7.28 HDLC[5] is the Cisco default encapsulation method for serial lines. This is a very reduced implementation for optimization purposes; there is no windowing[6] or flow control[7], and only point-to-point connections are permitted (there are no multipoint connections).

[5] **HDLC** - High-Level Data Link Control. Bit-oriented and synchronous data link layer protocol developed by ISO. Derived from SDLC, HDLC specifies a data encapsulation method on synchronous serial links using frame characters and checksums. Also see SDLC.

[6] **Window** – Number of octets the sender wishes to accept or that the transmitter can send without any need for recognition.

[7] **Flow control** - Technique used to ensure that a transmitter unit, such as a modem, does not overload a receiver unit with data. When the buffers of the receiver device are full, a message is sent to the transmitter device to suspend transmission until the data in the buffers has been processed. In IBM networks, this technique is called *pacing.*

The address field is always defined as all-one. Furthermore, a 2-byte proprietary code is inserted after the control field, meaning that the HDLC frame is not interoperable with the equipment of other manufacturers.



LAPB ENCAPSULATION

7.29 LAPB (Link Access Procedure Balanced) is the standard layer 2 protocol defined by X.25.

7.30 It has two addresses that identify whether the frame is a command or a response. It has no Type field.

PPP ENCAPSULATION

7.31 The point-to-point protocol[8] (PPP) is a standard (RFC 1332, 1661) serial line encapsulation method that includes a protocol type field, together with a link control protocol. Among other things, this protocol can verify link quality during connection establishment.

7.32 There is also support for authentication through the Password Authentication Protocol[9] (PAP) and the Challenge Handshake Authentication Protocol[10] (CHAP).

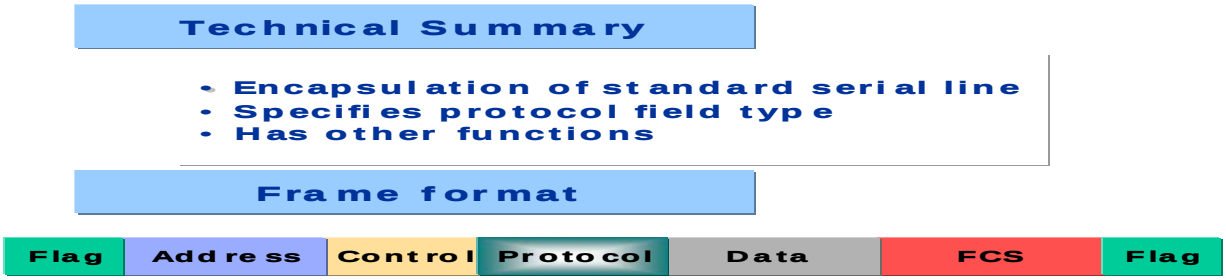
[8] **PPP** - Point-to-Point Protocol. A successor to SLIP, PPP provides router-to-router and host-to-network connections on synchronous and asynchronous circuits. See also SLIP.

[9] **PAP** - Password Authentication Protocol. Authentication protocol that allows PPP peers to authenticate each other. A remote router wanting to connect to the router must send an authentication request. Unlike CHAP, PAP passes the host or username and passwords in the free (non-coded) zone. It does not, of itself, prevent unauthorized access, but merely identifies the remote end. The router or access server then decides whether to permit this user's access. PAP is supported only by PPP lines. Compare with *CHAP*.

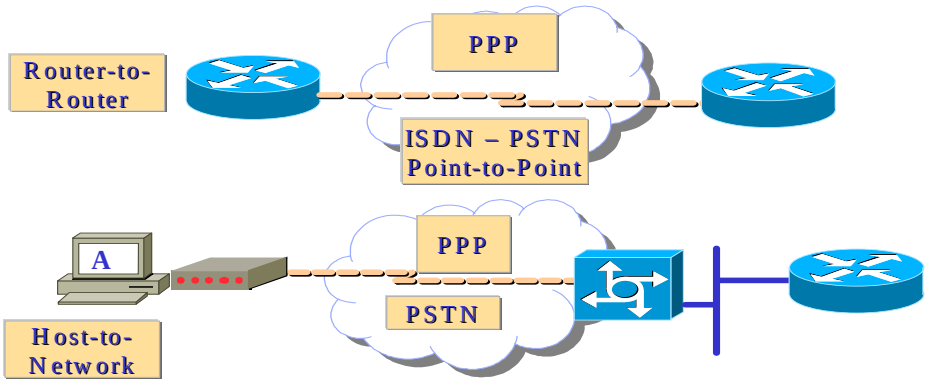
[10] **CHAP** *(Challenge Handshake Authentication Protocol)* – Security feature supported by lines using PPP encapsulation that prevents unauthorized access. CHAP does not of itself prevent unauthorized access, but merely identifies the remote end. The router or access server then decides whether to permit access to this user. Compare with *PAP*.

7.33 The point-to-point protocol (PPP) is generally considered the successor to the Serial Line IP (SLIP) protocol. PPP provides router-to-router and host-to-network connections through both synchronous and asynchronous circuits.

7.34 PPP emerged at the end of the 80s as an answer to the lack of encapsulation protocols for the Internet that was impeding the growth of serial line access. PPP was created basically to



resolve problems of remote connectivity with Internet. PPP supports the use of several network layer protocols, including Novell IPX, TCP/IP and AppleTalk.



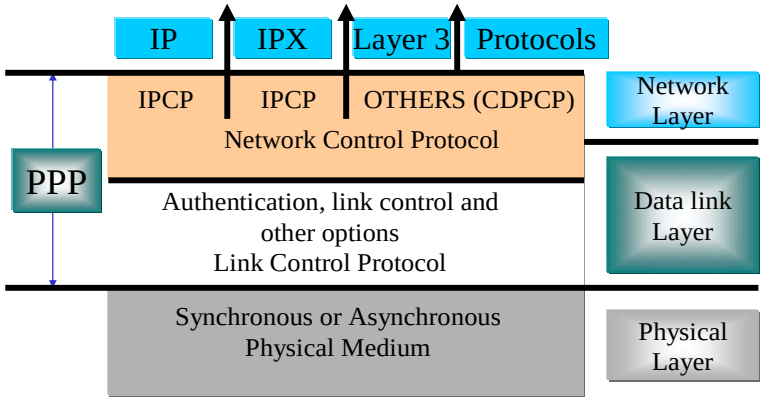
PPP Elements

7.35 PPP uses a layered architecture. With its lower level functions, PPP can draw on:

7.35.1 Synchronous physical media like those connecting to ISDN.

7.35.2 Asynchronous physical media such as those used by basic telephone service for telephone connections via modem.

7.36 PPP offers a wide array of services that control data link establishment.



7.37 These services are LCP options and consist mainly of frame negotiation and verification for the implementation of point-to-point controls specified by the administrator for the call.

7.38 With its higher level functions, PPP transports packets from several network layer protocols in NCPs. These are functional fields containing standard codes to indicate the type of protocol of each network layer that PPP encapsulates.

PPP Operation

7.39 PPP runs on the following types of WAN physical interfaces:

7.39.1 ISDN

7.39.2 Asynchronous series

7.39.3 Synchronous series

7.40 PPP uses another of its most important components, the link control protocol (LCP) to negotiate and establish WAN data link control options. It employs its network control programs (NCP) component to encapsulate different protocols.

7.41 PPP datagram transmission uses three key components for more effective data transmission:

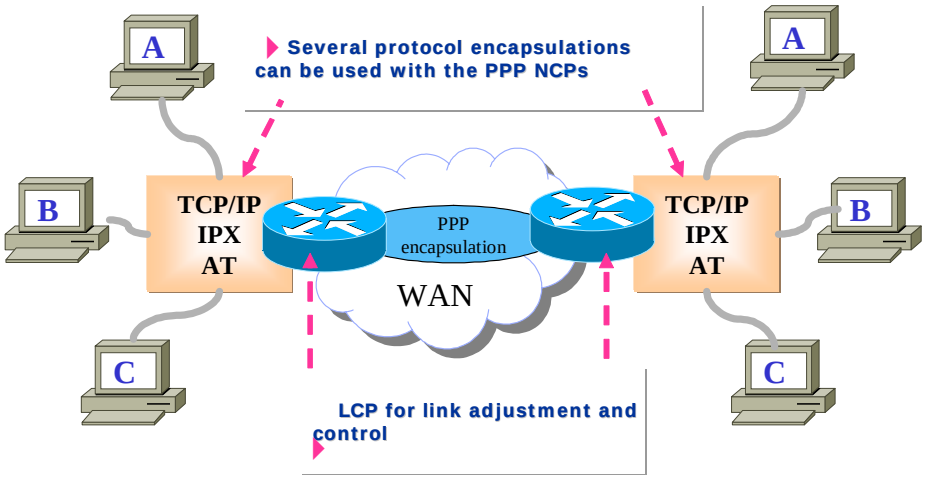
7.41.1 **Encapsulation** - PPP supports the high-level data link control (HDLC) protocol for encapsulation.

7.41.2 **Link control protocol (LCP)** – An extendable LCP is used to establish, configure and test the data link connection.

7.41.3 **Network control protocols (NCP)** – An NCP family is used to establish and configure different network layer protocols.

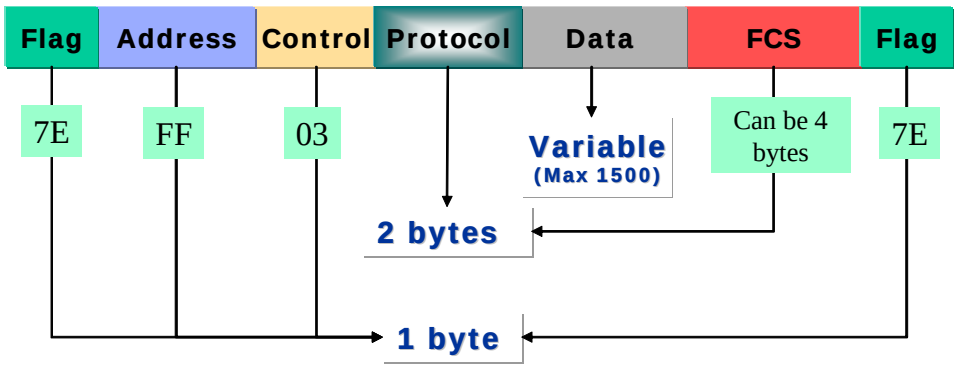
7.42 PPP connections are established by stages. An originating PPP node first sends LCP frames to configure and test the data link. The link is then established and the facilities negotiated.

7.43 The originating PPP node then sends NCP frames to choose and configure network layer protocols. The chosen network layer protocols, such as TCP/IP, Novell IPX and AppleTalk, are configured and the packets are sent from each network layer protocol.



PPP frame format

7.44 The PPP frame has the following field format:



7.44.1 **Flag** – Indicates the start or end of a frame and consists of the binary sequence 01111110.

7.44.2 **Address** - Consists of the standard broadcast address, the binary sequence 11111111. PPP does not assign individual station addresses.

7.44.3 **Control** - 1 byte that consists of the binary sequence 00000011, which calls for transmission of the user's data in a non-sequential frame. A link service without connection is provided similar to logical link control (LLC) type 1.

7.44.4 **Protocol** - 2 bytes that identify the encapsulated protocol in the frame information field. The most updated values in the protocol field are specified in the request for comments (RFC) of the most recently assigned numbers.

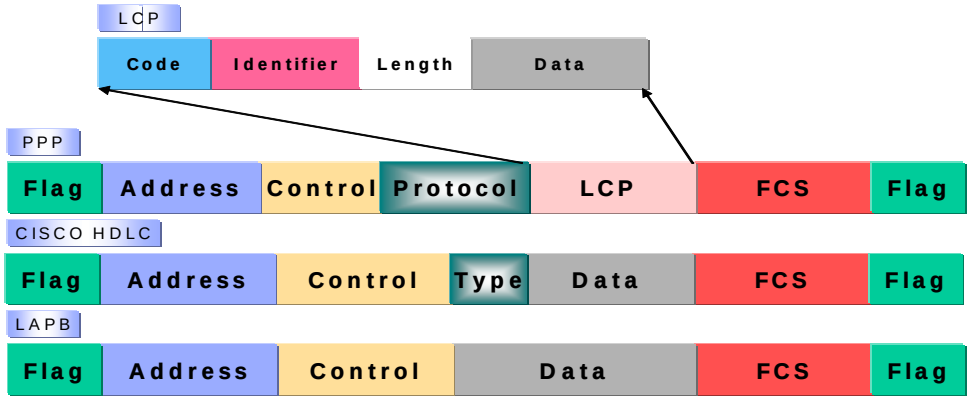
7.44.5 **Data** – Zero or more bytes containing the datagram for the protocol specified in the protocol field.The end of the information field is found by locating the closing flag sequence and allowing 2 bytes for the FCS field. The maximum default length in the information field is 1,500 bytes. By prior agreement, PPP consent implementations can use other values for the maximum length of the information field.

7.44.6 **Frame check sequence (FCS)** - Normally 16 bits (2 bytes). By prior agreement, PPP consent implementations can use a 32-bit (4 byte) FCS for improved error detection.

7.44.7 **Note** – The PPP link control protocol (LCP) can negotiate modifications to the standard PPP frame structure. Modified frames, however, will be clearly distinguishable from standard frames.

Summary of WAN frame formats

7.45 The diagram below summarizes the encapsulation protocol frame formats.



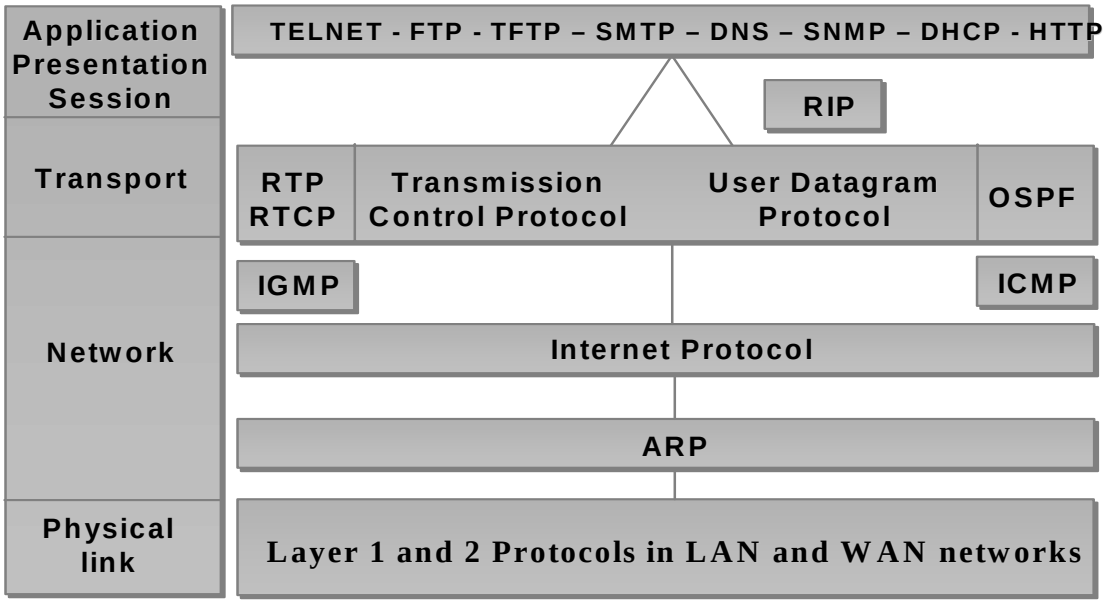
7.46 The following table offers a comparative summary of the most common data link protocols.

WAN Technology	Encapsulation Protocol	Notes
• Dedicated Point-to-Point	> HDLC > LAPB > PPP > Frame Relay	Can be any protocol that is configured at both ends.
• Packet switching	> Frame Relay > X.25 > ATM	Should be the same protocol as that of the carrier network.
• ISDN	> PPP > X.25 > Frame Relay	In D-channel: LAPD. In B-channel: any (similar to that of the point-to-point).
• PSTN	> Normally PPP > Formerly SLIP	Once established, it is a point-to-point. To accede to PPP Internet.

8. NETWORK FUNDAMENTALS

8.1 Networking evolves to support both existing and future applications. The OSI reference model organizes network functions into seven layers. The “RCP/IP reference model,” however, only has 4 layers, which can be mapped over the former.

8.2 Data flow from the highest level user applications to lower level bits transmitted through network media. The peer-to-peer functions use encapsulation and dis-encapsulation in the interfaces of the different layers.



8.3 The main characteristics of a LAN are:

8.3.1 The network operates within a building or within the same floor of a building (with coverage extending toward the metropolitan sphere).

8.3.2 LANs give the various connected devices (generally PCs) access to wideband media.

8.3.3 By definition, LANs connect computers and services on a common medium.

8.3.4 LAN devices include: *Bridges* (connect LAN segments and help filter traffic), *Hubs* (concentrate the LAN connection and make possible the use of braided copper media), *Ethernet Switches* (provide full-duplex dedicated bandwidth to segments or computers) and *Routers*, which offer many services including internetworking and broadcast control.

8.4 WAN **physical layer** protocols describe how to supply electrical, mechanical, operational and functional connections for WAN services, often obtained from WAN service providers (carriers).

8.5 WAN **data link** protocols describe how frames are transported between systems through a single data link. They include protocols designed to operate through dedicated point-to-point, multipoint and multi-access switched services, such as Frame Relay.

8.6 WAN standards have been defined and administered by different recognized authorities like the following:

8.6.1 International Telecommunication Union – Telecommunication Standardization Sector (ITU-T), formerly called International Telegraph and Telephone Consultative Committee (CCITT).

8.6.2 International Organization for Standardization (ISO).

8.6.3 Internet Engineering Task Force (IETF).

8.6.4 Electronic Industries Alliance (EIA).

8.7 WAN standards normally describe physical layer and data link layer (and at times network) requirements. The WAN physical layer describes the interface between the data terminal equipment (DTE) and the data circuit-terminating equipment (DCE). The DCE is usually the service provider, while the DTE is the connected device. In this model, the services offered to the DTE are available through a modem or CSU/DSU.

8.8 The figure below shows the relationship between layer 1 and 2 protocols in LAN and WAN networks:

<table>
<tr><th>OSI</th><th colspan="4">LAN</th><th colspan="4">WAN</th></tr>
<tr><td rowspan="2">Link</td><td rowspan="2">Ethernet</td><td colspan="3">802.2 LLC</td><td>HDLC</td><td>PPP</td><td>LAP B</td><td>SDL C</td></tr>
<tr><td>802.3</td><td>802.5</td><td>FDDI</td><td colspan="4" rowspan="2">V.24 – EIA/TIA232 – G703
V.35 - EIA/TIA449 - HSSI</td></tr>
<tr><td>Physical</td></tr>
</table>

8.8.1 **High-Level Data Link Control (HDLC):** an IEEE standard that is probably not compatible with the different providers, since each provider may have implemented it in its own way. HDLC supports point-to-point and multipoint configurations at a minimum cost.

8.8.2 ***Frame Relay*:** Uses high-quality digital facilities and simplified framing without error correction mechanisms, which means that it can send layer 2 information far more rapidly than other WAN protocols.

8.8.3 ***Point-to-Point Protocol (PPP)*:** Described by RFC 1661. Two standards developed by the IETF. It contains a protocol field to identify the network layer protocol.

8.8.4 ***Simple Data Link Control Protocol (SDLC)*:** WAN data link protocol designed by IBM for systems network architecture (SNA) environments. It has been largely replaced by the more versatile HDLC.

8.8.5 ***Serial Line Internet Protocol (SLIP)*:** Very popular WAN IP packet transport data link protocol. It has been replaced in several applications by the more versatile PPP.

8.8.6 ***Link Access Procedure Balanced (LAPB)*:** Data link protocol used by X.25 that has extensive error verification capabilities.

8.8.7 ***Link Access Procedure for D-Channel (LAPD)*:** WAN data link protocol used for signalling and for RDSI Channel-D call configuration. Data transmissions are made in RDSI Channel-B.

8.8.8 ***Link Access Procedure Frame (LAPF*):** A WAN data link protocol for carrier services in frame mode, similar to LAPD, used for Frame Relay technologies.

9. IP PROTOCOL (RFC791-RFC760)

9.1 IP (Internet Protocol) is an OSI model layer 3 (network) protocol designed to interconnect communication networks through packet switching, in order to form an internet.

9.2 Data blocks called datagrams are transmitted from a source computer to a destination computer.

9.3 Each datagram contains addressing and control information for packet routing, with the result that better *delivery service without connection* (no connection is established prior to the transfer of information) is provided between source and destination.

9.4 The device responsible for datagram routing among networks with different address systems is called a *router*. The router is basically a traffic manager (tell it where you want to go and the router will tell you the proper way).

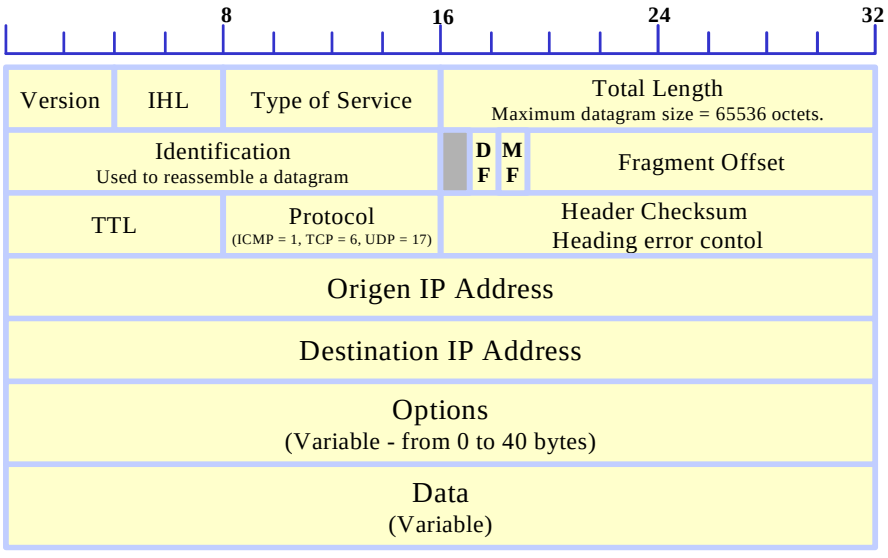
9.5 Routers have ports, which are physical connections to the networks. A local address should be assigned to each of these ports. If there are several routers, each should contain the information configured in the rest in order to make datagram routing possible.

9.6 Although it is possible to statically configure all IP addresses and their associated ports for each router, this would be inefficient because of the large amount of time it would take.

9.7 The appropriate method is to use protocols specifically designed to distribute routing information among the routers, called *routing protocols.*

IP packet format (Version 4)

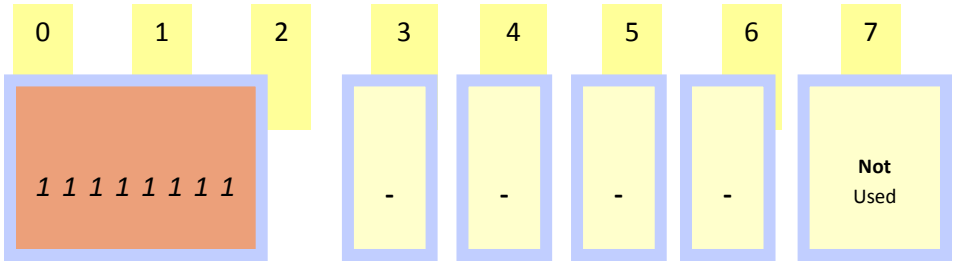
9.8 The following diagram illustrates the IP packet format version 4. The bits have been technically organized as usual–into 32-bit lines (equivalent to 4 octets).



9.9 **The first field, VERS (4 bits, 0 to 3),** defines the IP packet version (currently version 4), in order to check that sender, receiver and routers analyze the packet according to version 4 of the IP structure –in other words, it is the first parameter that should be checked before its analysis since, if there is any difference (between the packet received and the packet processing software), the machines will reject the packet to avoid incorrect interpretation of its format.

9.10 **HLEN field(4 bits, 4 a 7)**determines the length of the IP packet header and the amount is stated in bytes. All header fields have a fixed length, except the IP Options and Padding field.

9.11 **The Type of Service** is, in turn, divided into 5 subfields as follows:



9.11.1 **Priority** (3 bits): (o precedence) indicates packet priority, making it possible to control the information that will be more important in resending the data. For example, in VoIP (Voice over IP) transmission, the application software *marks* the packet in this field (with a certain value) so that routers will give it priority treatment over data packets.

9.11.2 **D** (1 bit): determines the type of transport required for the packet. When this bit is activated, it indicates processing with short delays.

9.11.3 **T** (1 bit): determines the type of transport required for the packet. When this bit is activated, it indicates high performance.

9.11.4 **R** (1 bit): determines the type of transport required for the packet. When this bit is activated, it indicates high reliability.

9.11.5 **Without use** (2 bits).

Assuming, for example, that a router can select between a low-speed leased line and a satellite link with a large bandwidth (but a long delay) and that some packets could have activated the D bit and others the T bit; in the latter case, the packets would be resent by the satellite link. It is also very important for the routing algorithms to select the underlying physical network technology with the low delay, high performance and high reliability characteristics so that the algorithm can choose, according to the status of those bits (D, T, R), the physical interface that meets the requirement defined by the type of transport.

9.12 **The Total Length field** determines the total length of the IP packet measured in bytes. Therefore, the length being 16 bits (16 to 31), the maximum packet size is 64 Kbyte (2^{16}=65.536).

9.13 **Fragmentation Control:** The fields that control the fragmentation of a datagram when transmitted over a network with an MTU (Message Transfer Unit)[11] smaller than the maximum IP datagram size are Identification, Flag and Fragment Offset.

[11] MTU (RFC 1191): NetBios: 512; X.25: 576;; 802.3/802.2: 1492; Eth 2.0: 1500; PPP: 1500; FDDI: 4352; IEEE802.4: 8166; 16M TR: 17914; EtherChannel: 65535

9.14 **The Identification field** determines which fragments form part of the same original datagram. As a result, all of them will have the same value in that field so that the receiver can "understand" (by analyzing the origin IP address, as well) that they are fragments of the same packet.

9.15 **The Flag and Flag Offset fields** determine the order in which those fragments should be reassembled. The least significant bit of the Flag field determines if there are more fragments (when its value is set to "0") and the Offset field, expressed in bytes, determines the position of the fragment within the original datagram.

9.16 **The Life Time field:** States the length of life of the datagram within the network. For example, when at packet reaches a router, a timer is activated that measures the length of time it remains within the router. Therefore, when the packet leaves that router, the equipment reduces its Life field by that period of time. When that value reaches zero, the packet is automatically expelled from the network and an error message is sent to the destination, thus avoiding the indefinite travel of such packets within the network.

9.17 **The PROTOCOL field:** Specifies the high-level protocol used to create the message transported in the data area.

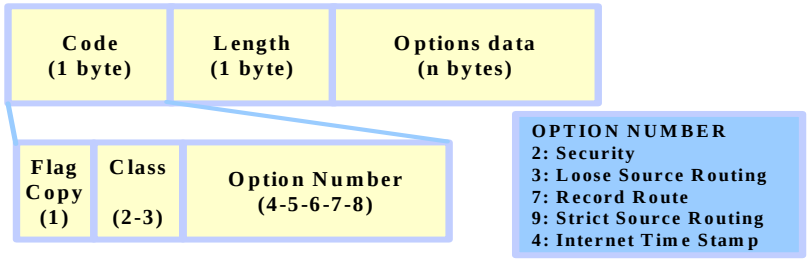
9.18 **The Header Checksum field:** Ensures the integrity of header values only.

9.19 **The Origin and Destination Address fields:** Determine the datagram transmission and reception addresses.

9.20 **The Data field:** Defines the data area, whose length varies.

9.21 **The Padding field:** Depends upon the content of the Options field, but can be used to ensure that the header length will be a multiple of 32 bits.

9.22 **The Options field:** It is not present in all datagrams and is included in network or debugging tests. Its length varies and depends upon the chosen option; for example, there is a byte that is broken down into three parts:



9.23 **Copy:**

9.23.1 1: routers should copy the option in all fragments

9.23.2 0: routers should copy the option in the first fragment and not in all fragments

9.24 **Option Class**

9.24.1 0: Network or datagram control

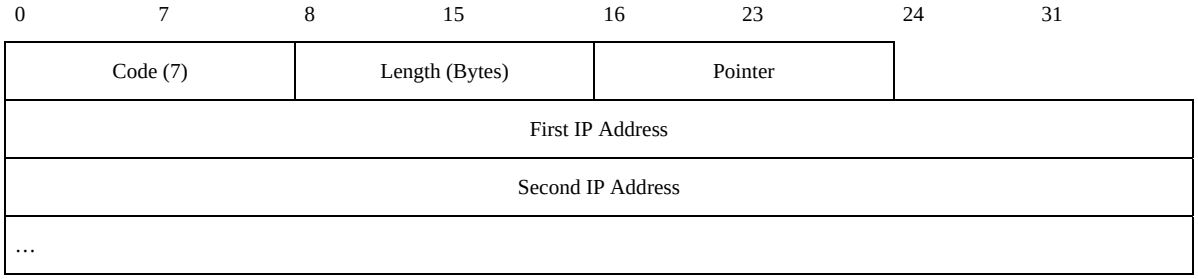
9.24.2 1: Reserved for future use

9.24.3 2: Debugging and mediation

9.24.4 3: Reserved for future use

Option Class	Option Number	Length	Description
0	0	-	End of the options list. Used if options do not finish at the end of the header
0	1	-	No operation. Used to align octets in a list of options
0	2	11	Security and handling restrictions. Military applications
0	3	Var	No strict source routing. Used for datagram routing by a specific path
0	7	Var	Route recording. Used to record the path of a route
0	8	4	Flow identifier.
0	9	Var	Strict source routing. Used to establish the route of a datagram in a specific path
2	4	Var	Internet time stamp. Used to record time stamps throughout a route

9.25 The most important options are the routing and Internet time stamp because they make it possible to monitor and control how the network handles datagram routes. The route recording option allows the source to create an IP address list and arrange for each router that handles the datagram to add its own address, in which case, the Option field would be formatted as follows:



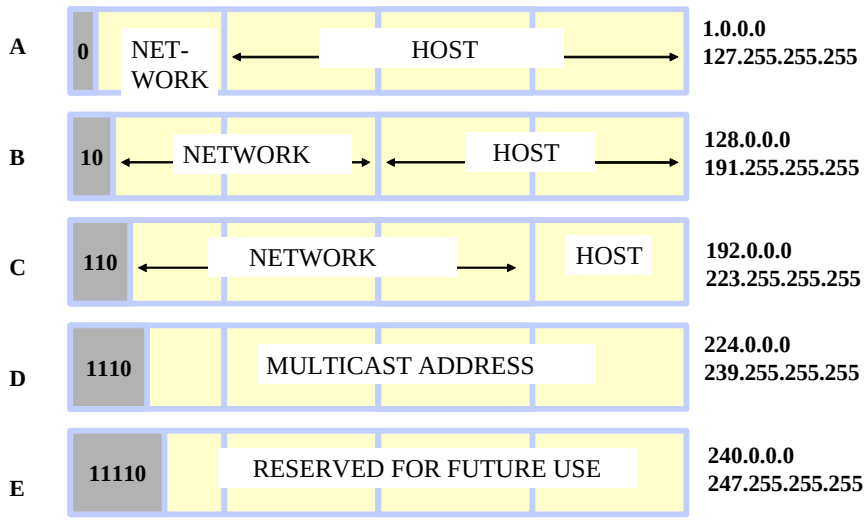
9.26 The Pointer field determines the next available slot in which the router can enter its IP address, but before it can do so it must compare the (stated) length value with the pointer value to see that there is enough "space." Only then will it enter its address and raise the pointer value; otherwise, it will send the datagram without including itself.

IP Addresses

9.27 Each host has as many IP addresses as it has network connection points. There are two kinds of network addressing systems:

9.27.1 **Classless:** Permits full use of the complete range of addresses, without any bit reservation for identifying different categories or classes.

9.27.2 **Classfull:** Original system (RFC 791) for segmenting 32-bit addresses into specific classes, in which the network number and the host number are identified.



9.28 Network numbers are assigned by the NIC (Network Information Center) to avoid conflicts. RFC 1597 assigns several addresses for use in private networks. There are protocols (NAT) for translating private addresses (unrecorded) into public ones and vice versa.

Address Class	Initial Address	Final Address
A	10.0.0.0	10.255.255.2555
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

Special values

9.29 If a machine receives a packet whose Net ID field of the destination address is equal to zero and the Host ID field of the destination address corresponds to its address, the receiver interprets the Net ID field as being this network. This address is used during the starting process –in other words, it allows a machine to communicate temporarily and once it has "learned" its correct network and IP address, it will again use the Net ID field = 0.

9.30 If a machine receives a packet whose Host ID field of the destination address is all ones, then the receiver interprets the Net ID field as being this network.

9.31 The Net ID network address=127 is reserved for the LOOPBACK function--in other words, it is a troubleshooting address for determining whether the TCP/IP protocol stack configured in the terminal operates correctly (ping 127.0.0.1).

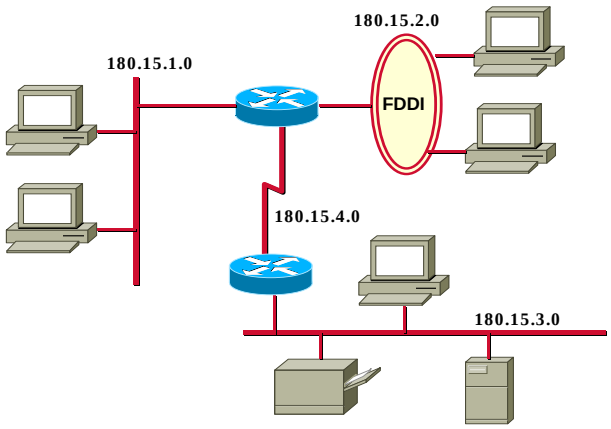
Subaddressing (Subnetting: RFC950)

9.32 IP networks can be divided into smaller networks called subnets. This procedure offers the administrator several benefits, including flexibility, efficient use of network addresses and the capacity to contain broadcast traffic (the broadcast does not cross the router). Subnets are locally managed and the organization is viewed as a single network by the rest of the world, which is unaware of the details of its internal structure.

9.33 One network address can be divided into several subnets. For example, 172.16.1.0, 176.16.2.0, 176.16.3.0, 172.16.4.0, etc., are all subnets within the network 172.16.0.0 (only zeros in the host number portion of an address denotes the entire network).

9.34 A subnet address is created by "stealing" bits of the host field to assign them to the subnet field. The number of "stolen" bits can vary and is specified in the mask.

9.35 In an organization whose IP addresses are not divided into subnets, any address within it will be routed according to its Net ID value. In the case of the address 180.15.0.0, for example, all packets will be routed based on 180.15 (this is a benefit for the size of routing tables). The drawback is that individual segments cannot be distinguished within the organization, resulting in low network performance, because all terminals "*would see*" the network broadcast.



9.36 The subaddressing/subnetting/subnetwork concept contributes to more efficient performance because externally all packets addressed to the organization will be routed in the same way, while subnets within the organization would restrict traffic to other segments.

9.37 In the example, the network address 180.15.0.0 was divided into 4 subnets: 180.15.1.0, 180.15.2.0, 180.15.3.0 and 180.15.4.0--in other words, in the address 180.15.1.0, 180.15 is the network address, 1 is the subnetwork address and the last field is the subnetwork terminal address. From the viewpoint of the address, a subnetwork is an extension of the network number. Network administrators will size the subnetwork according to the requirements.

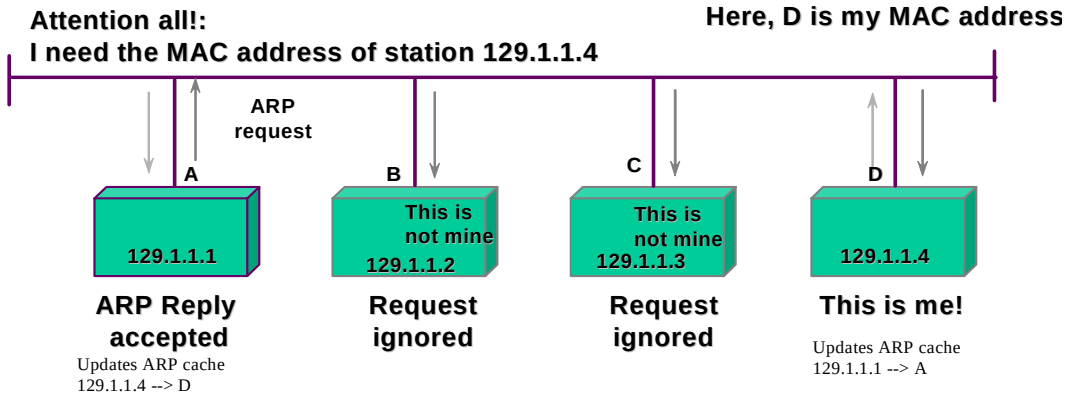
	Network		Host	
IP Address	**180**	**15**	**0**	**0**
	Network		Host	
Default Mask	**255**	**255**	**0**	**0**
	Network		Subnetwork	Host
Mask	**255**	**255**	**255**	**0**

9.38 The devices use a "subnetwork mask" to determine the part of the ID address dedicated to the subnetwork. The "mask" size is 32 bits, in groups of 8s as shown in the figure.

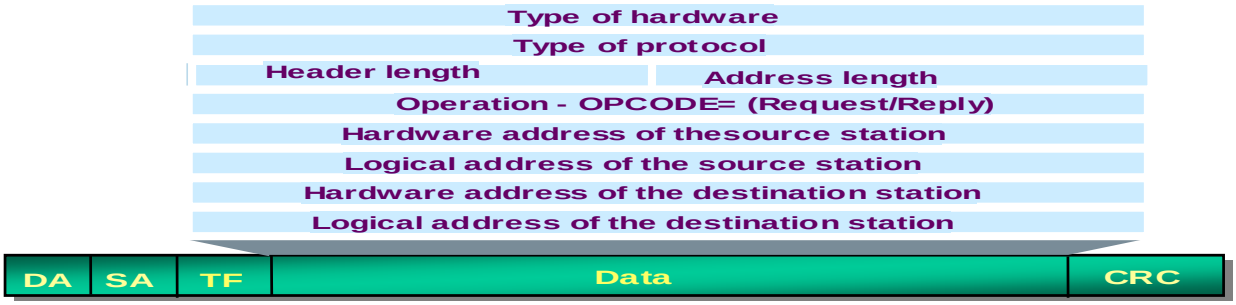
9.39 The mask is calculated as follows: both the network and subnetwork fields should consist only of 1's and the host of 0's--in other words, the subnetwork mask indicates those bits of the host ID field used to identify the subnetwork.

ARP (Address Resolution Protocol – RFC826)

9.40 The ARP protocol makes it possible to map the physical address of the network card with the host's IP logical address in order to route within a subnetwork (LAN segment) in accordance with the IP address. To accomplish this, it must establish an unequivocal relationship between the network physical address (MAC address) and the IP logical address of the terminal to be communicated with.



9.41 The figure below illustrates the ARP packet format:



9.41.1 **Type of Hardware**: indicates the LAN IEEE802 protocol and also other types of networks.

9.41.2 **Type of Protocol**: states the TCP/IP

9.41.3 **Header length**: determines the length of the header protocol

9.41.4 **Length of the logical address**: indicates the length of the logical address

9.41.5 **Operation**: indicates whether it is a question or a reply

9.41.6 **Logical address of the transmitting host**: indicates the logical address of the transmitting host

9.41.7 **Physical address of the transmitting host**: physical address of the transmitting host

9.41.8 **Physical address of the receiving host**: physical address of the destination host

9.41.9 **Logical address of the receiving host**: indicates the logical address of the destination host

9.41.10 **TF (Type Field)**: determines the type of data within the packet: TCP, Apple Talk, XNS

NOTE:

ARP does not run on IP and therefore has no IP header.

ARP requests are transmitted on broadcast.

The new EtherType defines 0x0806 for ARP requests and replies.

ARP replies are sent directly to the ARP requesting station (unicast, not broadcast).

ARP tables generally limit the validity of entries (age out).

Interface: 168.226.1.203

Internet Address	Physical Address	Type
168.226.1.1	00-00-0c-03-21-7a	dynamic
168.226.1.6	00-e0-8f-d7-b3-ff	dynamic
168.226.1.43	00-04-00-10-97-cc	dynamic
168.226.1.44	08-00-09-57-53-1e	dynamic

10. TCP[12]

10.1 **TCP (Transmission Control Protocol**) was especially designed to provide a reliable byte flow from end-to-end, on an unreliable internet. An internetwork differs from a single network because different parts of it have extremely different topologies, bandwidths, delays, packet sizes and other parameters.

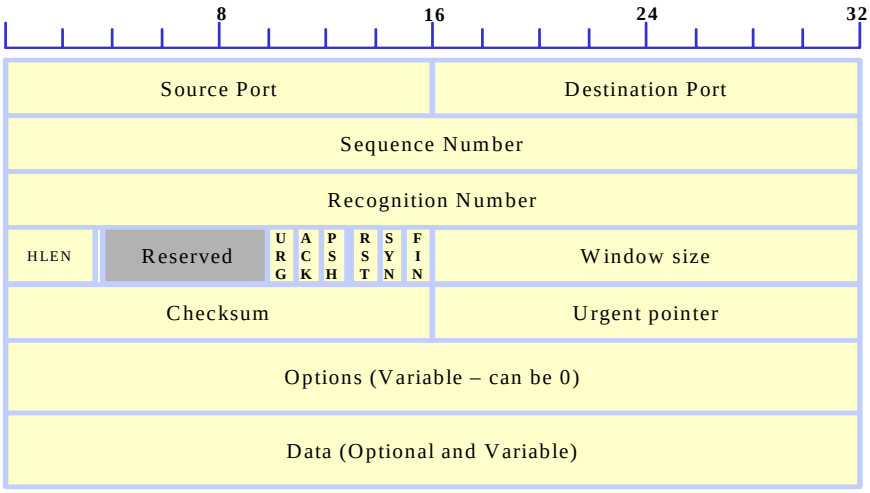
10.2 Each machine that supports TCP must have a TCP transport entity in the form of either a user process or part of the kernel that manages TCP flows and interfaces to the IP layer.

10.3 A TCP entity accepts local process data flows, fragments them into units no larger than 64 Kbytes (in practice some 1500 bytes), and sends each part as an independent IP datagram. When IP datagrams containing TCP data reach a machine, they are delivered to the TCP entity, which reconstructs the original byte flow.

10.4 The IP layer does not guarantee appropriate datagram delivery. For that reason, the TCP is responsible for implementing the necessary mechanisms to retransmit, order, recognize, time, etc. the segments in order to make the transmission reliable.

[12] There are approximately 7 TCP RFCs, the most important being RFC 793; RFC1122: updating of the former (793); RFC 813: window management; RFC 816: isolation and recovery failures, and others. The RFCs can be consulted in WWW.IETF.ORG

10.5 TCP does not support multicasting or broadcasting.



Source and destination ports

10.6 **The source and destination ports**: Identify the connection end points. Each host can decide how to assign its own ports, starting at 1024. A port plus the host IP address form a unique 48-bit TSAP (Transport Service Access Point), also called a socket. The pair of source and destination socket numbers identifies the connection.

TSAP Socket =	IP Address +	Port Number
[48 bits] =	[32 bits]	[16 bits]

10.7 Ports numbering from 0 to 1023 are called well-known ports and are reserved for standard services (for example, to use FTP services, a connection with source port 21 is usually requested in order to contact the FTP process; Telnet similarly uses port 23). The list of well-known ports can be obtained at RFC 1700.

Sequence Number

10.8 **Sequence Number and Recognition**: The numbers of segments being transmitted and received, which implement the usual connection procedure with recognition.

Header length

10.9 **HLEN** (Header Length): States the TCP header length in 32-bit units, since the options field has a variable length. Technically, the field indicates the start of the data within the segment (4 bits). Then comes an unused 6-bit field.

Flags

10.10 6 1-bit flags follow.

10.10.1 **URG**: Activated to 1 when the urgent pointer is in use. The urgent pointer is used to denote the displacement in bytes from the current sequence number where the urgent data are found.

10.10.2 **ACK**: Activated to 1 when the recognition number is valid. If the ACK value is 0, the Recognition Number field is ignored.

10.10.3 **PSH**: Way of indicating to the receiver that it should immediately deliver the data to the application layer, without any storage whatsoever (data are generally placed in a buffer to optimize their transfer to the upper layer).

10.10.4 **RST**: This flag is used to reset a connection that has become confused for some reason. It is also employed to reject an invalid segment or a connection attempt. Generally, segments with RST=1 represent a problem to be solved.

10.10.5 **SYN**: This flag is activated to establish connections. The connection request bears SYN=1 and ACK=0 to indicate that the piggyback field is not in use. The connection response supports recognition and for that reason bears SYN=1 and ACK=1. The SYN bit is essentially used as a Connection Request and Connection Acceptance (the ACK bit is used to distinguish between these two possibilities).

10.10.6 **FIN**: Used to terminate a connection. Specifies that the sender has no more data to transmit. In any case, after a connection is closed, a process can continue to receive data indefinitely. Both the SYN and the FIN segments have sequence numbers to guarantee processing in the correct order.

Window value

10.11 **Window Size**: Used to implement flow control through a variable-size sliding window. Specifies how many bytes can be sent after the recognition byte. A window size = 0 indicates that all bytes up to the Recognition Number -1 have been correctly received, but that no further data may be received for the moment.

Check Code

10.12 **Checksum**: Complete segment (including the *pseudo* header) error control. The *pseudo* header contains the IP addresses of the source and destination machines, the TCP protocol number (=6) and the computed number of bytes in the TCP segment, including the header. Inclusion of the TCP *pseudo* header in the checksum helps detect packets sent erroneously, but violates the protocol hierarchy because IP addresses belong to the IP, not the TCP, layer.

Options

10.13 This field was designed to provide a way to add facilities not covered in the regular header. The most important option permits each host to specify the maximum TCP segment load it is willing to accept. During the connection process, each host announces its maximum and analyzes that of its counterpart: the smallest wins! (if this option is not used, the assumed value is 536 bytes; for that reason, all Internet hosts must support TCP segments of 536+20=556 bytes).

10.14 Another important option is the negotiation of a window factor proposed in RFC 1323, which makes it possible to shift the Window Size field up to 16 bits to the left. A 64-Kbyte Window can be a problem for links with large bandwidths or delays, or both, (considering that an E3 line takes some 15 milliseconds to deplete a complete 64-Kbyte window and that the 2-way delay in transcontinental fibre is about 50 milliseconds. The sender would be left waiting for recognition 70% of the time.)

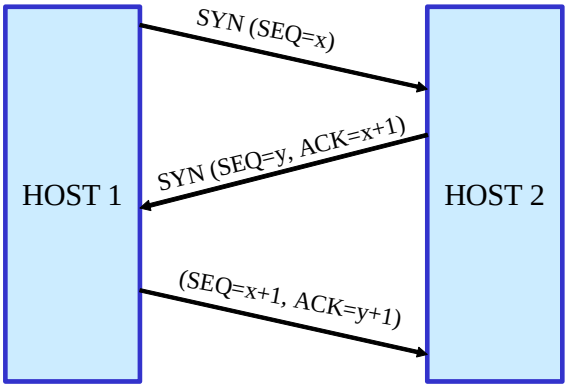
10.15 RFC 1106 proposes the use of selective relay (NAK), instead of the "fall back to N" protocol.

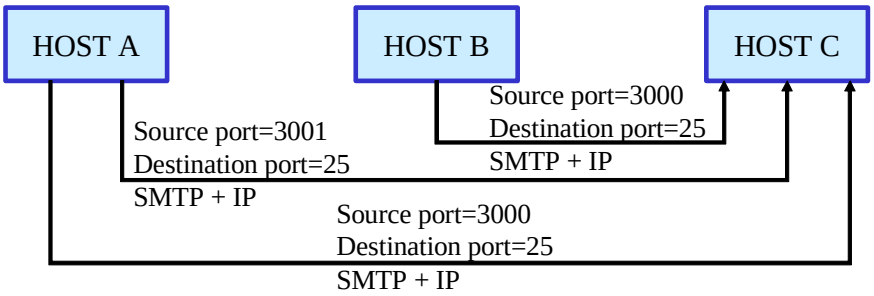
TCP Connection Management

10.16 TCP connections are established via a three-way handshake.

10.17 Before the establishment request, one side, the server, passively awaits the connection request, executing the primitive LISTEN and ACCEPT, whether or not indicating a specific source.

10.18 The other side, the client, executives a primitive CONNECT, specifying the IP address and the port to which it desires connection, the maximum TCP segment size it is willing to accept and, optionally, some user data (password).





10.19 The primitive CONNECT sends a TCP segment with the SYN bit activated and the ACK bit deactivated, and awaits a reply. When the segment reaches its destination, the TCP entity checks to see whether any process is executing a LISTEN at the indicated port in the Destination Port field. If not, it sends a reply with the RST bit=1 to reject the connection.

10.20 If any process is “listening” at that port, the TCP segment is delivered to it. It may accept or reject the connection. If it accepts it, it returns a recognition segment (SYN=1, ACK=1).

10.21 Although TCP connections are full-duplex, in order to fully understand the termination process, it is better to envisage them as a pair of simplex connections. Each simplex connection is terminated independently of its counterpart. To accomplish this, each part can send a TCP segment with the FIN bit activated, meaning that there are no more data to be transmitted. When that segment is recognized, it means that that transfer address has been closed to the sending of data, although the transfer can continue indefinitely in the other direction.

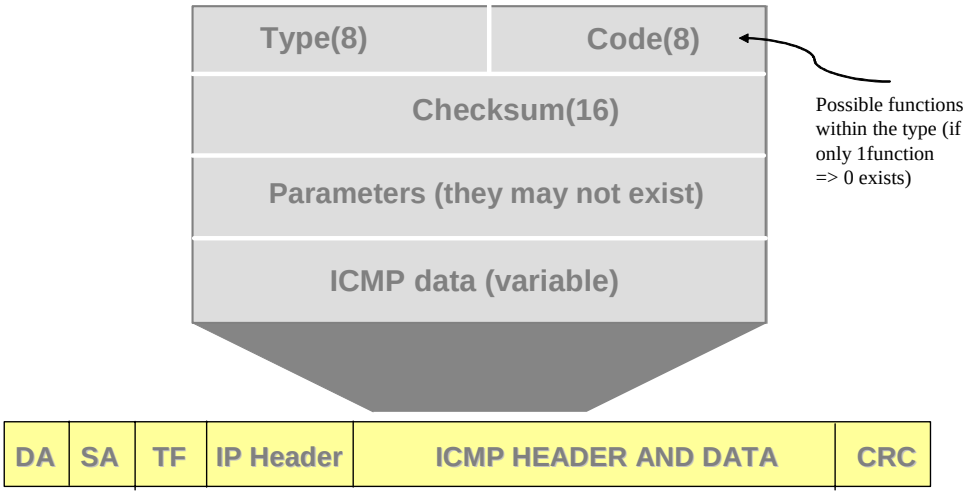
11. ICMP

11.1 Since there is no provision by IP for status control and error management, ICMP (Error and control messages) is the protocol that handles this for IP.

11.2 These messages are interpreted by the Internet Protocol in each piece of network equipment (host/routers).

11.3 Technically speaking, the protocol is an error reporting mechanism--in other words, it permits the equipment to send a message to the original source each time an error is found, but does not specify the action to be taken in the case of a certain error.

11.4 The only datagrams that do not generate error messages are those that bear error messages--in other words, if there is congestion, error messages are sent that could lead to more congestion, but in this latter case no ICMP messages will be generated, therefore avoiding messages about messages.



11.5 ICMP does not use a transport layer--it runs directly over IP--and consequently it is not reliable (there will be no ICMP error messages for an ICMP message). It is not the intent of ICMP to turn IP into a reliable protocol; it only seeks to report errors and provide feedback under specific conditions.

11.6 The Type field identifies the ICMP datagram and the Code field provides additional granularity.

Type (8 bits): indicates the type of message:

0: Echo reply

3: Destination unreachable

4: Origin reduction

5: Redirect (change route)

8: Echo request

11: Packet time exceeded

12: Packet parameter problems

13: Timestamp request

14: Timestamp reply

15: Information request

16: Information reply

17: Address mask request

18: Address mask reply

11.7 The code field indicates possible functions within each type (if there is only one function, its value is 0).

Code (8 bit): provides more information about the type of message

0: Network inaccessible

1: Host unreachable

2: Protocol unreachable

3: Port unreachable

4: DF configuration and fragmentation required

5: Source route failed

6: Destination network unknown

7: Destination host unknown

8: Source host isolated

9: Communication with destination network administratively prohibited

10: Communication with destination host administratively prohibited

11: Network inaccessible by service type

12: Host inaccessible by service type

11.8 Type 3, for example, indicates that the host is unreachable, but a code 1 provides a more specific reply, indicating that the destination host, and not the port, is unreachable (this could mean that although the network was reached, no host replied to the ARP REQUEST.

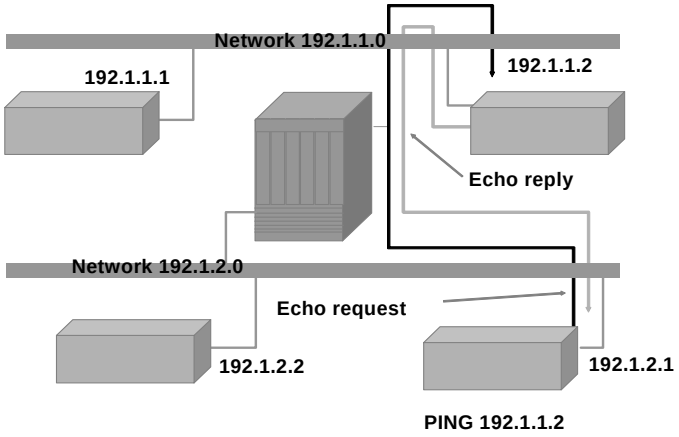
11.9 The checksum computes the ICMP message complement as "1". The header and the first 64 bits of user data of the datagram that motivated the message are transported in the data.

ICMP PING

11.10 The PING is one of the most common ICMP uses.

11.11 PING is used as a test and debugging tool

11.12 PING is an ICMP message that tries to locate other Internet stations in order to check whether they are active or whether a path has been enabled.



12. SWITCHING AND ROUTING

12.1 There are differences between and confusion over the strict application of the concepts of bridging, switching and routing and their practical implementation.

Layer 2 switching

12.2 Layer 2 switching uses the MAC addresses of the Ethernet interface cards (NIC) to filter network traffic and is based on hardware (ASIC). Bridges and switches perform the switching function. As there are no modifications in the frame during the switching process (unless bridging between heterogeneous networks like Ethernet and FDDI, for example), the operation is very efficient (low cost, high speed and low latency).

12.3 Layer 2 switches have the same limitations as bridges (they are essentially adapted to local 80/20 traffic patterns). Furthermore, although they segment collision domains, they cannot break the bc domains and can cause performance problems and limitations in network size. The main drawbacks switches represent for large network growth are the bc and mc and slow STP (spanning tree protocol) convergence.

Bridging

12.4 Bridging is fully analogous with switching. The difference in application stems from the high density of switch ports as compared with those of bridges (a switch is like a bridge with multiple ports).

Routing

12.5 Routers segment not only collision domains, but also broadcast domains. They provide optimum path determination because routers examine each packet that enters their interfaces, sending the information only to the known destination network (if the router does not know the destination network, the packet is discarded). Thorough packet inspection is used to control traffic and implement security policies. Routing is done based on Layer 3 (typically IP) logical addresses.

Layer 3 switching

12.6 Layer 3 switching is functionally similar to routing in all its effects and scope, differing only in the way it is implemented in the devices. It is a forwarding of packets based completely on ASIC hardware.

Layer 4 switching

12.7 Layer 4 switching is a technology similar to that of layer 3, into which routing functions relating to the applications (telnet, FTP, etc.) have been incorporated. In other words, the packet application ports are taken into consideration in routing decisions.

12.8 The main advantage of layer 4 switching is the possibility of implementing application- and user-based quality of service (QOS).

Multi-layer switching

12.9 Multi-layer switching combines the technologies of layers 2, 3 and 4 with characteristics of great scalability and reduced latency.

12.10 A multi-layer switch can make switching and routing decisions based on:

12.10.1 (MAC) frame source and destination addresses.

12.10.2 (IP) packet source and destination addresses.

12.10.3 The IP packet protocol field.

12.10.4 The segment source and destination ports (TCP or UDP).

Appendix 2- Description of a router

DESCRIPTION, COMPONENTS AND BASIC OPERATIONS

ROUTER DESCRIPTION

INTERNAL CONFIGURATION COMPONENTS

BASIC CONFIGURATION

ROUTER MODES

CONFIGURATIONS

PASSWORDS

ROUTER INITIALIZATION

IP ROUTING CONFIGURATION

1. DESCRIPTION OF A ROUTER

1.1 In order to describe the components of a router, we will take as an example the Cisco 1751 model router in the 1700 series.

Description of the basic components

1.2 Cisco 1700 series routers provide flexibility, security and functionality for small and medium-sized businesses, at the rate networks evolve.

1.3 See the Cisco 1700 series data sheet to supplement this information.[1]

1.4 Cisco 1700 series routers connect small businesses with various LAN Ethernets to several WANs through Integrated Services Digital Network (ISDN) synchronous and asynchronous connections.

1.5 The 1751 model is a modular router (it offers three slots in which to insert different interface modules). The location of the three slots can be seen in the figure above.

1.6 The figure shows the back of the router. Two of the slots are occupied by FXS voice interfaces.

1.6.1 **1** Kensington block slot.

1.6.2 **2** WIC or VIC card slot (SLOT 1) —Supports a Cisco WIC/VIC card.

1.6.3 **3** Console port (blue).

1.6.4 **4** VIC card spot (SLOT 2) —Supports a Cisco VIC card.

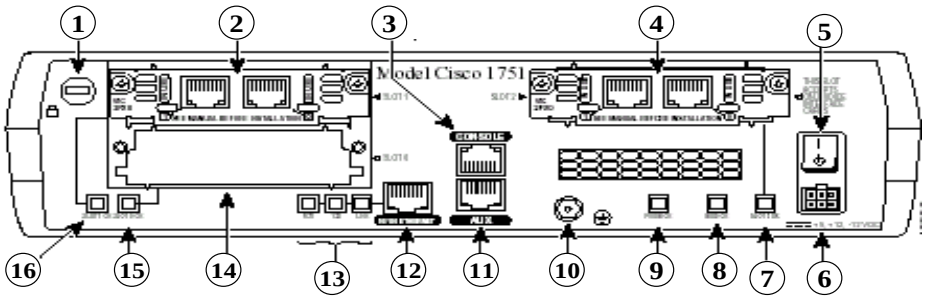
1.6.5 **5** Power switch.

1.6.6 **6** Power plug.

1.6.7 **7** Slot 2 status LED —On (green) when the VIC is inserted and operating properly.

[1] The 1700 replaced the 1600 series, for which EOS (end of sales) and EOL (end of life) were declared.

1.6.8 **8** MOD status LED—On (green) when the VPN encryption module (hardware) is installed and recognized by the IOS.



1.6.9 **9** PVDM status LED —On (green) when the PVDM module (internal hardware) is installed and recognized by the IOS.

1.6.10 **10** Ground screw.

1.6.11 **11** AUX port (black).

1.6.12 **12** 10/100 ETHERNET port (yellow) —Connects to the local Ethernet network. Speed and duplex self-sensing.

1.6.13 **13** Ethernet interface LEDs:

1.6.13.1 FDX—ON indicates the port is operating in full-duplex mode (OFF: in half-duplex mode).

1.6.13.2 100—ON indicates the port is operating at 100 Mbps (OFF: at 10 Mbps).

1.6.13.3 LINK—ON when the Ethernet link is active.

1.6.14 **14** WIC or VIC card slot (SLOT 0) —Supports a Cisco WIC/VIC card.

1.6.15 **15** Slot 0 status LED—On (green) when the WIC or VIC card is inserted and operating properly.

1.6.16 **16** Slot 1 status LED—On (green) when the WIC or VIC card is inserted and operating properly.

Router interfaces and connections

1.7 A router needs configuration in order to be able to operate within a network. Once it has been configured, network administrators will need to check the status of several of its components.

Console and Auxiliary Ports

1.8 All routers have a console port used to accede to the device directly from a terminal or a PC with terminal emulation. This port is frequently an RJ-45 interface called a “Console”.

1.9 Cisco provides the necessary cables with the following pin-outs:

ROUTER			ROLLOVER		RJ-45 to DB9		
SIGNAL	CONSOLE	AUXILIARY	RJ-45	RJ-45	RJ-45	DB9	SIGNAL
RTS	NO	1 (out)	1	8	8	8	CTS
DTR	2 (out)	2 (out)	2	7	7	6	DSR
TxD	3 (out)	3 (out)	3	6	6	2	RxD
SG	4	4	4	5	5	5	SG
SG	5	5	5	4	4	5	SG
RxD	6 (in)	6 (in)	6	3	3	3	TxD
DSR	7 (in)	7 (in)	7	2	2	4	DTR
CTS	NO	8 (in)	8	1	1	7	RTS

1.10 After establishing the physical connection from the terminal or a PC to the console port, the terminal must be properly configured to make communication with the device possible.

1.11 The router is then turned on and the boot banner will appear. The auxiliary port can be used to connect a modem, allowing for off band management if the other connections are lost. Both ports support asynchronous TTY lines.

Interfaces

1.12 They are the connections to the network through which packets enter and leave the router. Cisco supports a wide variety of interfaces, including Ethernet, Token Ring and serial interfaces. Some of the most common router interfaces are serial (for connection to WAN links) and LAN (like Ethernet, Token Ring and FDDI).

2. INTERNAL CONFIGURATION COMPONENTS

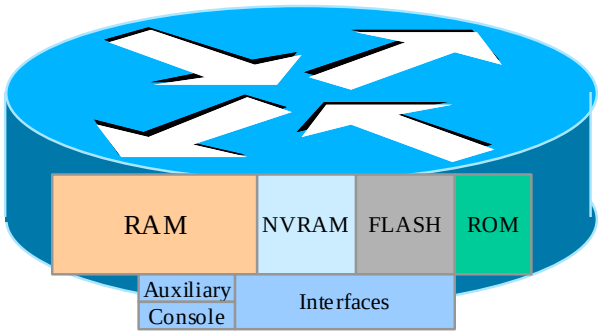
2.1 The router internal architecture (a router is a computer and, as such, has hardware elements similar to those of a conventional computer) supports components that play a very important role during the boot process. These components are:

2.1.1 Processor (*CPU*)

2.1.2 *Different* types of *memory* for storing information

2.1.3 An *operating system* that provides the operational functions

2.1.4 *Several ports and interfaces* to connect it to peripheral devices, or permit communication with other computers



Router elements

2.2 Router hardware components include: memory, processor, interfaces and lines.

Memories

2.3 There are basically 4 different types of memories:

2.3.1 RAM/DRAM

2.3.2 NVRAM

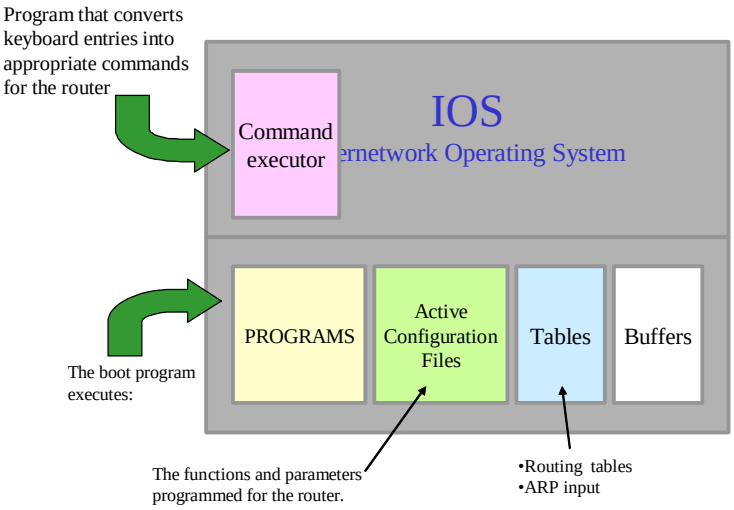
2.3.3 FLASH

2.3.4 ROM

2.4 **RAM/DRAM:** This is the main storage component for all router operations. It is called a working memory and contains information about the dynamic elements. Part of the IOS is also decompressed in the RAM. When the router is turned on, a bootstrap program is executed from the ROM memory. The program makes some checks and then loads the Cisco IOS software in the memory. The command processor, or EXEC, is part of the Cisco IOS software. EXEC receives and executes commands entered from the keyboard.

2.5 The router also stores an active configuration file, tables of network maps and routing addresses. If a version of this file is stored in the NVRAM, the stored file is reached and loaded in the main memory each time the router is started. The configuration file contains global, process and interface information that directly affects router operation and interface ports.

2.6 The operating system image cannot be seen on the terminal screen. This image is generally executed from the main RAM and loaded from one of several input sources. The operating software is organized into “routines” that manage tasks associated with the different protocols, data movement, table management, buffers, routing updates and user command execution.



2.7 **NVRAM**: This component is the non-volatile RAM (a special type of RAM that is not erased during the router reboot process) that contains a configuration backup copy. If power fails or the router is turned off, the configuration backup copy will enable the router to return to its operating conditions without any need for reconfiguration.

2.8 The router startup configuration file is stored in the NVRAM by default. When the router leaves the factory, it has no configuration file. This is the first file that is created during the configuration process. It also stores the virtual configuration register.

2.9 The NVRAM stores all of the router configuration information defined by the user, including, among other things: the host name for the router, the routing tables, the protocol configurations, the cache configurations, and the virtual configuration register.

2.10 **FLASH:** This component is a special class of programmable memory (like a ROM, but erasable and programmable, an INTEL EEPROM). Typically, the Flash memory cannot be modified during normal router operations, but can be updated or erased when necessary. The contents of the Flash memory are kept even after the router is rebooted.

2.11 This memory normally contains a copy of the IOS (Cisco Internetwork Operating System) software. The Flash memory has a structure that permits multiple copies of the IOS to be stored, making it possible to load new levels of the operating system into each network routers and then, at an appropriate time, to update the entire network to the new level.

2.12 The Flash memory contains the working copy of the current IOS software and is the component that initializes the IOS for normal router operations.

2.13 **ROM:** The Read-only memory stores the **bootstrap** program for the basic startup of the router hardware and the **POST (power-on self test)** programs that are used to check the basic workability of the hardware and determine the presence of interfaces.

2.14 ROM also contains the **ROM MONITOR**, a monitor boot program that can be used by the administrator to recover the system in the event of a boot failure. In some routers, the ROM contains a small version of the Cisco IOS software as an emergency backup. Series 7000 and 7500 Cisco routers have a complete version of the IOS in ROM.

2.15 In ROM monitor mode, the prompt symbol is the sign for greater (>).

2.16 Another ROM component is the Mini-IOS--called **RXBOOT** or bootloader--a small version of IOS that can be used to activate an interface and load a complete IOS in the FLASH memory, as well as to carry out other maintenance operations (it is like a fail-proof startup).

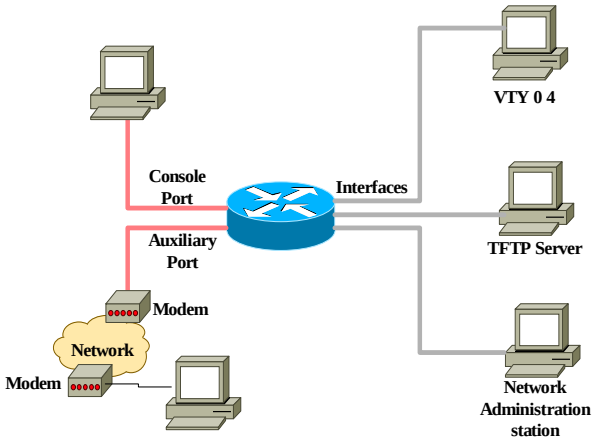
2.17 ROM components cannot be modified during normal router operations, but can be updated through special plug-in chips. ROM contents are kept even if rebooted.

Configuration sources

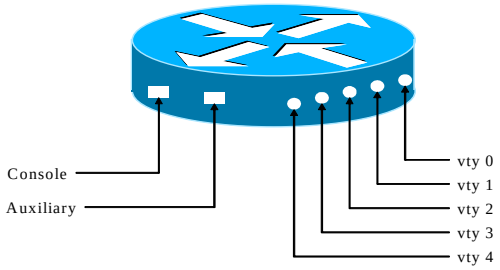
2.18 The router can be configured from different locations:

2.18.1 At the moment of initial installation, it is configured from the console terminal. The console terminal is a computer connected to the router through the console port. It can be connected by means of a modem using the auxiliary port. Once installed in the network, it can be configured from virtual terminals 0 to 4.

2.18.2 Files can also be downloaded from a network TFTP server or managed through a centralized management application.



2.19 The following figure illustrates the different modes of access to the router. For normal router traffic (Ethernet, serial, TR, etc.), access can be obtained to the virtual terminals (vty) from any of the interfaces.



2.19.1 The Console and Auxiliary ports are physically accessible through connectors (EIA-232).

2.19.2 The so-called VTYx (x= 0, 1, 2, 3 and 4) ports are virtual and do not exist physically. They are accessed from interfaces that handle normal router traffic (Ethernet, Serial, TR, ISDN, ATM, etc.), via the Telnet protocol. In other words, it is necessary to activate the IP protocol.

3. BASIC CONFIGURATION

3.1 One way to gain an understanding of how Internet operates is by configuring a router. Routers are complex devices that can have a variety of possible configurations.

3.2 After testing the hardware and loading the Cisco IOS system image, the router finds and applies configuration instructions. These inputs give the router details about specific attributes for the router, protocol functions and interface addresses.

3.3 If the router is in a starting situation in which it cannot locate a valid **startup-config** file, it will enter an initial configuration mode called **setup mode**.

SETUP MODE

3.4 The **setup** mode is the initial configuration routine. Its main purpose is to rapidly originate a minimum configuration for any router that cannot find its configuration elsewhere.

3.5 The **setup** does not aspire to enter complex protocol characteristics in the router. It is used only for minimum configuration. The command system configuration dialogue questions in **setup** mode are easily answered, because only basic configuration information is requested. The answers permit the router to use a sufficient configuration, but with minimum characteristics that will include:

3.5.1 An interface inventory

3.5.2 An opportunity to enter global parameters

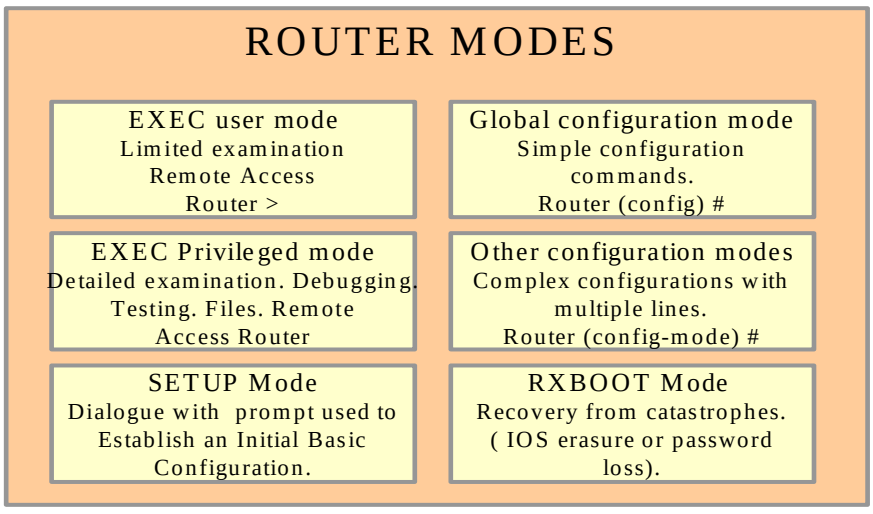
3.5.3 An opportunity to enter interface parameters

3.5.4 An information setup review

3.5.5 The opportunity to indicate whether use of that configuration is desired for the router

4. ROUTER MODES

4.1 Regardless of whether access is obtained from the console or through a Telnet session via an auxiliary port, the router can be placed in several modes. Each mode offers different functions:



4.1.1 **EXEC user mode**: “Look-only” mode in which the user can see certain information about the router, but cannot change anything.

4.1.2 **EXEC privileged mode**: Supports debugging and testing commands, detailed examination of the router, manipulation of configuration files and access to configuration modes.

4.1.3 **Setup mode:** Presents a dialogue with interactive prompts in the console that help new users create a basic configuration for the first time. Global configuration mode - Implements powerful on-line commands that carry out simple configuration tasks. Other configuration modes – Provide more complex multi-line configurations.

4.1.4 **RXBOOT mode:** Maintenance mode that can be used to recover lost passwords, among other things.

4.1.5 EXEC modes: **EXEC interprets the commands that have been entered and carries out the corresponding operations.**

5. CONFIGURATIONS

5.1 The configuration of network devices determines the behavior of the entire network.

5.2 Careful device configuration administration should be sought: configurations must be backed up, maintained, and stored in network servers for shared access and the necessary software must be installed and updated.

Router identification

5.3 One of the first basic tasks is to give the router a name.

Banners

5.4 Routers provide support for different types of banners that will show information or warnings to different users under given circumstances.

5.4.1 Message of the day (motd)

5.4.2 Line

5.4.3 Incoming

5.4.4 Login

EXEC Banner:

5.5 The line activation (exec) banner is shown when an EXEC process (such as a line activation or an incoming connection in a VTY) takes place.

Banner Incoming

5.6 The banner incoming is shown in terminals connected to reverse Telnet lines. This mode is very practical for giving users information.

Banner Login

5.7 Shown in all connected terminals following the banner MOTD and before the login prompt. The command activates or deactivates the banner in all lines.

6. PASSWORDS

6.1 Routers require the configuration of passwords to protect four accesses:

6.1.1 Privileged EXEC (ENABLE)

6.1.2 Console (CONSOLE)

6.1.3 Auxiliary line (AUX)

6.1.4 Virtual terminals (VTY)

6.2 Unless the router is configured to reference an external authentication server, the passwords will be stored (in explicit or coded form, depending upon the security environment) in the router configuration file.

Password encryption

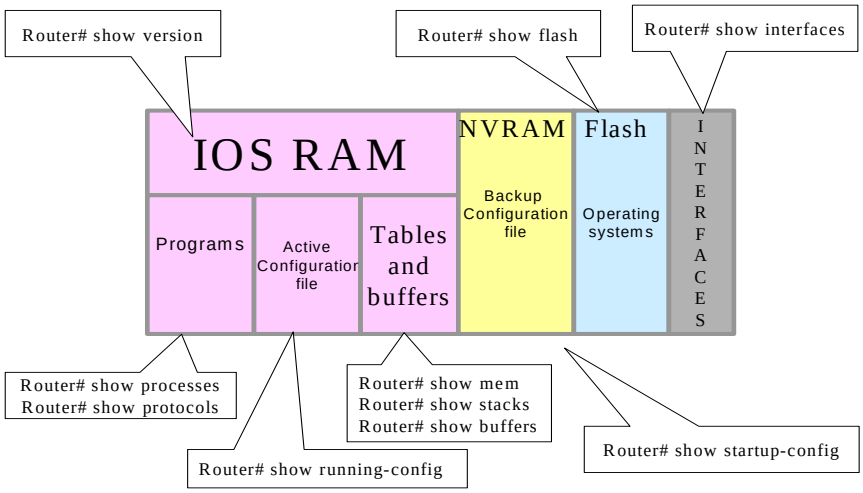
6.3 Cisco offers a password encryption service like those that are usually explicitly present in the configuration file (except “enable secret”).

6.4 Once the command has been entered, each password that is configured will be stored in coded form and cannot be recovered without a password cracking program (very simple and widely available).

6.5 Cisco uses the MD5 algorithm (there is no known way to reverse this algorithm) to code the “enable secret”. If the “enable secret” is used, it will not be possible to apply normal password recovery techniques (except through brute force), which depend upon visualizing the password in explicit form in the configuration file, making its resetting necessary.

7. ROUTER STATUS COMMANDS

7.1 The figure below illustrates the router status commands:



7.1.1 **show version:** Displays the system hardware configuration, the software version, the names and origins of the configuration files and the startup images.

7.1.2 **show processes:** Displays information about the active processes.

7.1.3 **show protocols:** Displays the configured protocols. This command shows the status of any network layer 3 protocol that has been configured.

7.1.4 **show mem:** Shows statistical data about the router memory, including statistical data about the free memory pools.

7.1.5 **show stacks:** Monitors the stack usage of processes and interrupt routines and shows the reason for the latest system reboot.

7.1.6 **show buffers:** Provides statistical data about the network server buffer pools.

7.1.7 **show flash:** Shows information about the flash memory device.

7.1.8 **show running-config:** Shows the active running configuration file.

7.1.9 **show startup-config:** Shows the backup copy of the configuration file.

7.1.10 **show interfaces:** Shows statistical data about all of the interfaces configured in the router.

7.2 **Show running-config and show startup-config commands:** These are perhaps the most used Cisco IOS software EXEC commands because they allow the administrator to see the current or running router configuration or the size of the images and the startup configuration commands the router will use the next time it is put into operation.

7.3 **Show serial interface command:** This command displays in real time the configurable parameters and statistics for the interface series.

7.4 **Show version command:** Shows information about the Cisco IOS version being used by the router.

7.5 **Show protocols command:** This command shows the overall status and the specific status of the interface of any configured Level 3 protocol (for example, IP, DECnet, IPX, and AppleTalk).

8. ROUTER INITIALIZATION

Startup Routines

8.1 IOS software startup routines are designed to start router operations. The router should perform reliably in the connection of user networks, having been configured for that service. To accomplish this, the startup routines should:

8.1.1 Ensure that all of router hardware has been tested.

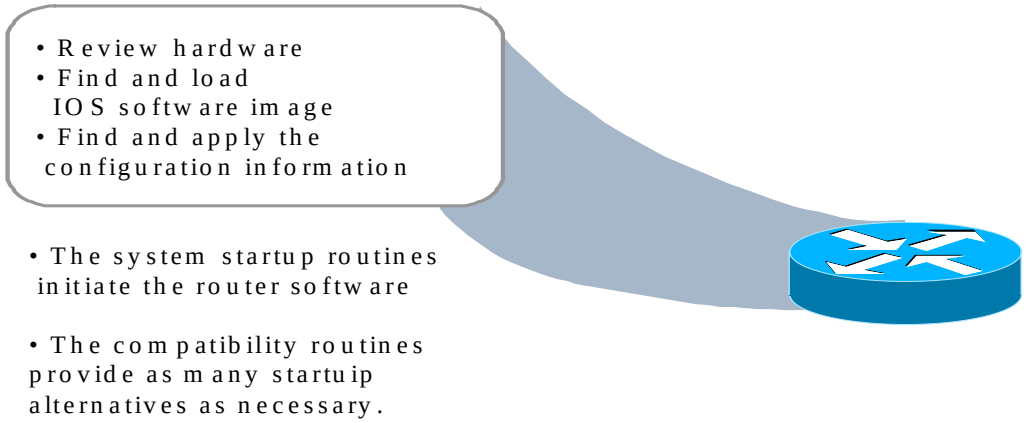
8.1.2 Search the memory and load the IOS software the router uses as its OS.

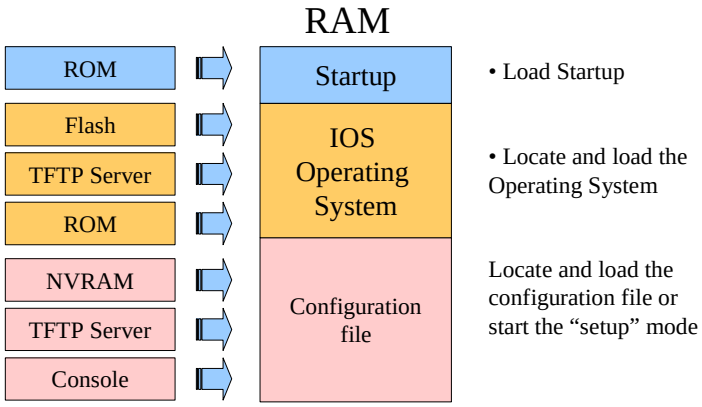
8.1.3 Search the memory and apply the router configuration information, including the protocol functions and interface addresses.

8.2 Immediately after startup, the router will make sure its hardware has been tested by executing a POST (Power-On-Self-Test).

8.3 The POST, which resides in and is executed from the ROM, performs a system self-test, during which it diagnoses all of the components. The presence and basic operation of the CPU, the memory and the network interface posts are all checked.

8.4 After the hardware functions have been checked, the router proceeds to initialize the software.





9. IP ROUTING CONFIGURATION

Initial IP Routing Table

9.1 The router initially possesses information about the directly connected networks or subnetworks. Each interface must be configured with an IP address and a mask. IOS software must receive this IP address and mask information from some source. The initial addressing source is the person who makes the first configuration. [2]

9.2 Of course, it is possible to start up the router from a zero condition--status lacking another source for an initial configuration--in setup mode and to reply to the prompts for basic configuration information.

[2] The global command "no ip routing" disables IP protocol routing.

Route Information

9.3 Routers learn about routes to destinations in three different ways:

9.3.1 **Static Routes:** Manually defined by the system administrator as the only route to the destination. They are useful for controlling security and reducing traffic.

9.3.2 **Default Routes**: Manually defined by the system administrator as the route to take when there is no known route to the destination.

9.3.3 **Dynamic routing**: The router finds out about routes to destinations on receiving periodic updates from other routers.

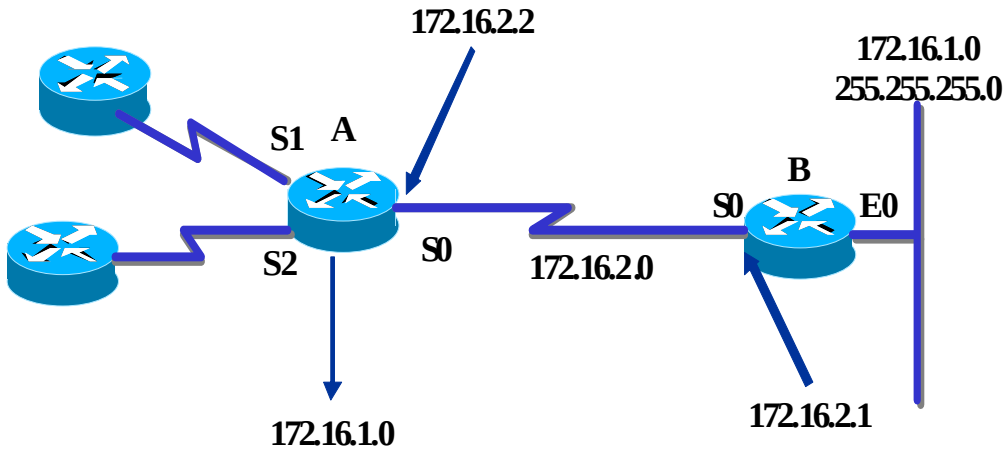
Static route configuration

9.4 A static route allows for manual routing table configuration. No dynamic changes will be made in a given table entry so long as the route is active and in general reflects a special knowledge of the networking situation known to the network administrator. No routing updates are sent by the links if only static routes have been defined, conserving the bandwidth.

9.5 In the example:

9.5.1 Assignment of a static route to reach the sole connection 172.16.1.0 network is appropriate for router A (ISP) because there is only one way to reach the network of the client.

9.5.2 Assignment of a static route from router B to undisplayed networks is also possible. However, a static route assignment is necessary for each destination network; therefore, a *default route could be more convenient.*




```
ip route 172.16.1.0  255.255.255.0  172.16.2.1
```

Command	Description
ip route 172.16.1.0	Specifies a static route to a destination subnet.
255.255.255.0	A subnet mask indicates that there are 8 bits of subnet connection in effect..
172.16.2.1	The router IP address of the next leap in the route to the destination.

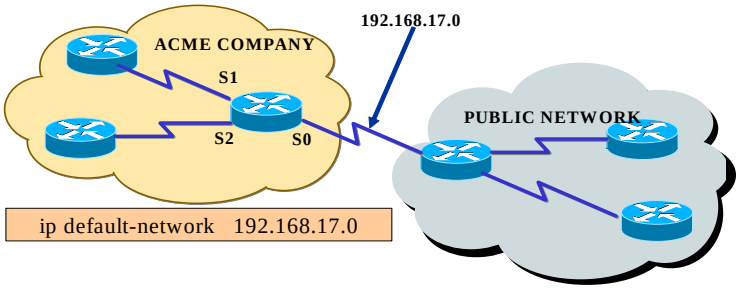
Default router configuration

9.6 When the routing table contains no entry for the destination network, the packet is sent to the default network. The routing table must contain the default network. Default routes keep the routing tables short.

9.7 The default network number must be used when a route is needed and information about the destination network is incomplete.

9.8 The router does not have complete information about all of the destination networks; therefore, it can use a default network number to indicate the address to be used for unknown network numbers.

9.9 In the example, default-network 192.168.17.0 defines the class C 192.168.17.0 network as a destination route for packets for which no entry has been made in the routing table.



Router(config)# ip default-network network-number

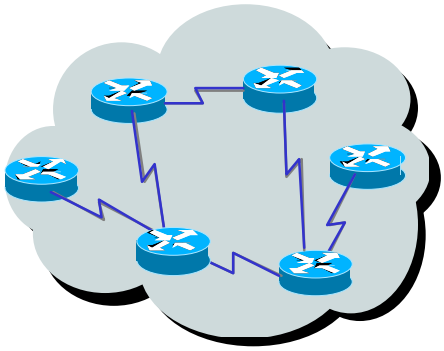
ip default network command	Description
network-number	IP network number or default subnet number.

Introduction to dynamic routing

Autonomous system

9.10 In the example above, Router A could need a firewall for routing updates. The administrator in Company X does not want updates from the public network. Router A could need a mechanism for grouping networks that will share the routing strategy of Company X. One of these mechanisms is an autonomous system number.

9.11 An autonomous system consists of routers administered by one or more operators that present a consistent standard for routing towards the outside world.

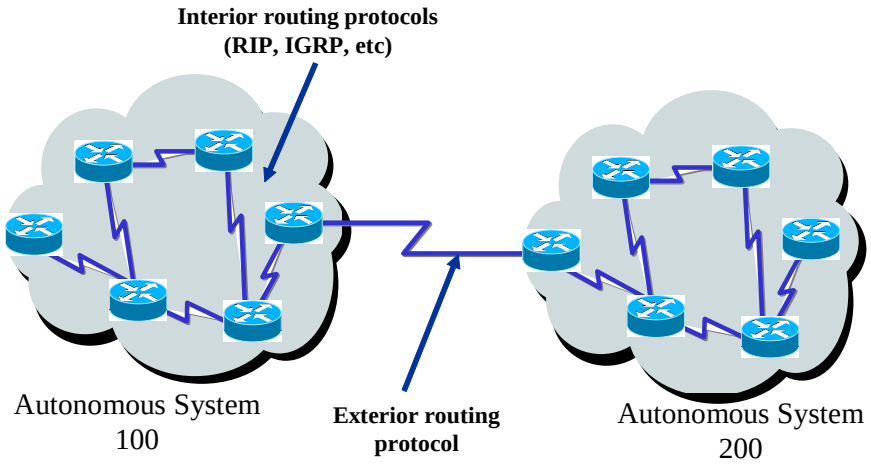


9.12 The Network Information Center (NIC) assigns an exclusive autonomous system number to each company. This autonomous system is a 16-bit number.

913 A routing protocol like the Cisco Interior Gateway Routing Protocol (IGRP) requires the specifying of this exclusive autonomous system number assigned in its configuration.

Interior or exterior routing protocols

9.14 Exterior routing protocols are used to communicate between autonomous systems, while interior routing protocols are used within a single autonomous system.



Interior IP routing protocols

9.15 Routers can use routing protocols--in the Internet layer of the TCP/IP protocol set--by applying specific routing algorithms.

9.16 Some examples of the most common IP routing protocols are:

9.16.1 RIP: Distance-vector routing protocol.

9.16.2 IGRP: Cisco distance-vector routing protocol.

9.16.3 OSPF: Link-state routing protocol.

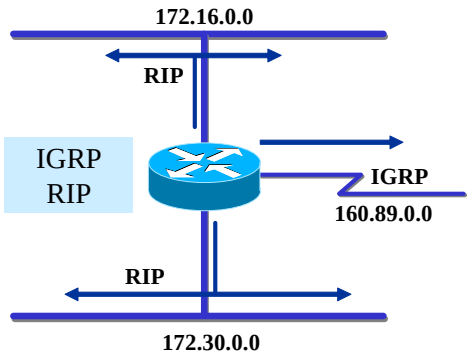
9.16.4 Enhanced IGRP (EIGRP): Balanced hybrid routing protocol.

Dynamic routing configuration tasks

9.17 As indicated in the figure, it is necessary to select the routing protocol to be used from the global configuration mode and then as many network subcommands can be entered as are necessary to activate protocol activities in the corresponding networks.

Global configuration
•Select routing protocol(s)
•Specify network(s)

Interface configuration
Check subnet mask/
address

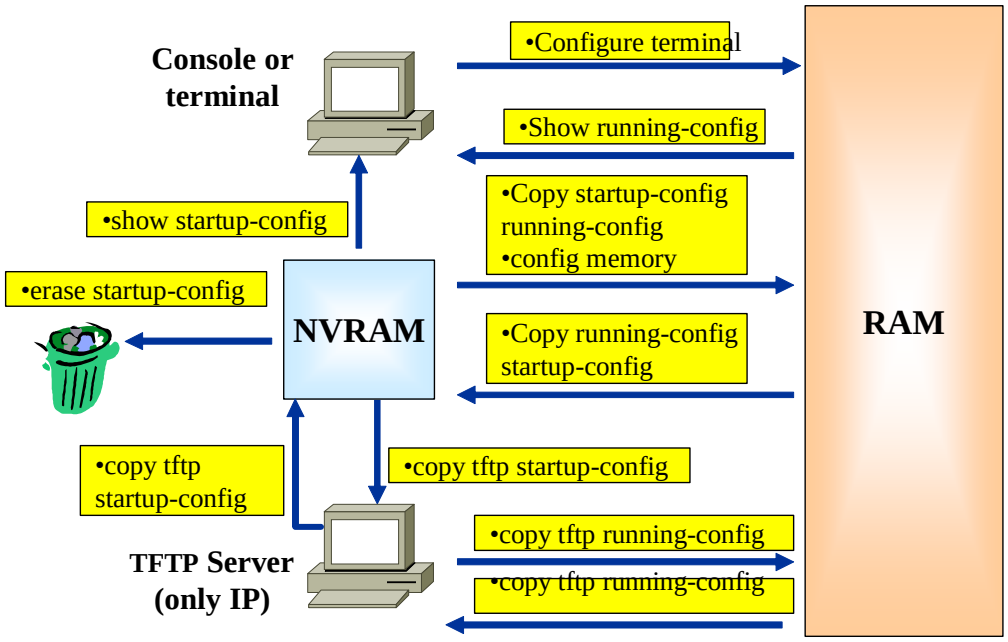


9.18 The figure shows the configuration situation of a router with 3 interfaces and different routing protocols.

9.19 The routing protocol to be activated must be specified through the global command "router".

10. ADMINISTRATION OF THE CONFIGURATION ENVIRONMENT

10.1 As the network grows and evolves, it becomes necessary to maintain control over the software and network device files from a centralized site.



Operation with a TFTP server

10.2 Device configurations can be stored and downloaded from a TFTP server.

Configuration backup

10.3 A copy of the running configuration can be stored in a TFTP server.

Configuration retrieval

10.4 The router can be configured by retrieving the configuration file stored in one of the network servers.

Cisco IOS name conventions

10.5 Cisco has developed many different images to optimize the way the software operates on the different platforms. These images adjust to the different platforms and the available memory resources and reflect the needs of its clients for network devices.

10.6 Thousands of IOS images and feature sets have accumulated over time. Cisco IOS software naming conventions, the meaning of the field name, the contents of the image and other details were always subject to change, making it necessary to frequently control the Cisco Connection Online (CCO) to obtain up-to-date data.

10.7 Starting with version 12.3, Cisco has drastically simplified the task of selecting the Feature Set, reducing the Feature Set alternatives to 8 (out of a total of 44 that existed for each version prior to the 12.3).

10.8 The table below illustrates the functionality included in each of the 8 IOS software packets.

10.9 As can be seen, IP BASE is the foundation on which the 7 other packets are constructed. Thus, for example, if voice is required, we should think of the IP VOICE packet.

10.10 But, if security functions (Firewall, IDS and VPN) were to be incorporated, as well, then the appropriate packet would be ENTERPRISE BASE (which incorporates support for ATM, VoATM and MPLS, not required in our case, but which are the consequences of packaging methodology applied by Cisco, in which priority has been given to simplicity).

Functionality **IOS Packaging**	Data Connectivity	VoIP and VoFR	ATM, VoATM and MPLS	AppleTalk, IPX, IBM Protocols	Firewall, IDS, VPN
IP Base	**X**				
IP Voice	**X**	**X**			
Advanced Security	**X**				**X**
Advanced IP Services	**X**			**X**	
SP Services	**X**	**X**	**X**		

Enterprise Base	X	X	X		X
Enterprise Services	X	X	X	X	
Advanced Enterprise Services	X	X	X	X	X

11. ACCESS TO A OTHER ROUTERS

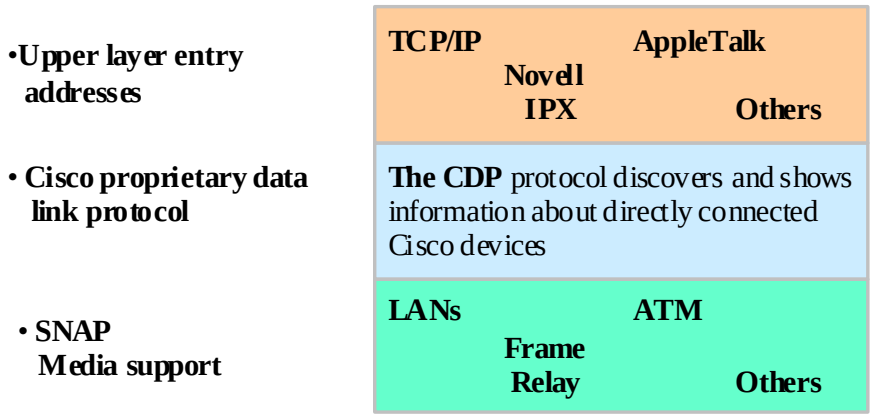
11.1 There are different ways to accede to other routers' information. One of these is by using the CDP protocol.

CDP

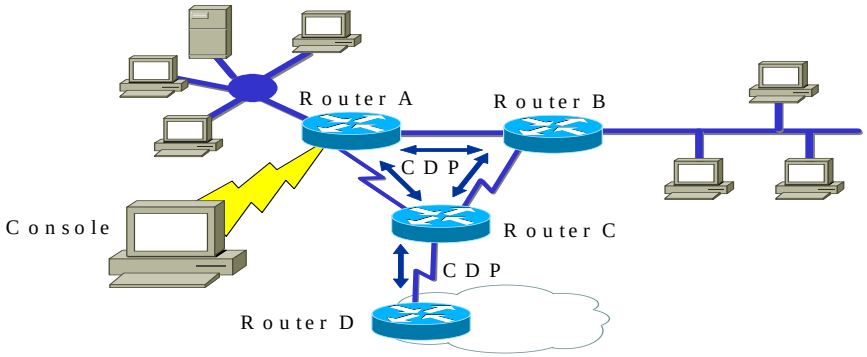
11.2 El Cisco Discovery Protocol (CDP) offers a Cisco proprietary tool that gives network administrators access to a summary of the configurations of other, directly connected, routers. CDP runs on the data link layer that connects the physical media and the upper layer protocols. As CDP operates at the low level, the CDP devices that support different network layer protocols are able to know each other--the data link address is similar to the MAC address concept.

11.3 When a Cisco device executes an initial sequence, CDP enters into operation by default and from that point on can automatically discover adjacent Cisco devices that are also using CDP.

11.4 The devices discovered extend beyond those that have TCP/IP, for CDP discovers the Cisco devices that are directly connected, independently of the layer 3 and layer 4 protocols they are executing.



CDP Information



11.5 The graph shows an example of how CDP offers its benefits to the system administrator.

11.6 Each router that executes CDP exchanges information about the data of any protocol with which it is familiar with its neighbors.

11.7 The administrator can see the results of this exchange of CDP information on screen in a console connected to a router configured to execute the CDP in its interfaces.

11.8 The network administrator uses a **show** command to display information about networks directly connected to the router. CDP provides information about each adjacent CDP device. Included among the possible data are:

11.8.1 **Device identifiers**: The host name and the domain name (if any) configured in the router, for example.

11.8.2 **Address list:** One address for each protocol being supported.

11.8.3 **Port identifier**: For example, Ethernet 0, Ethernet 1, Serial 0, etc.

11.8.4 **Capacities list**: For example, if the device acts like both a source route bridge and a router.

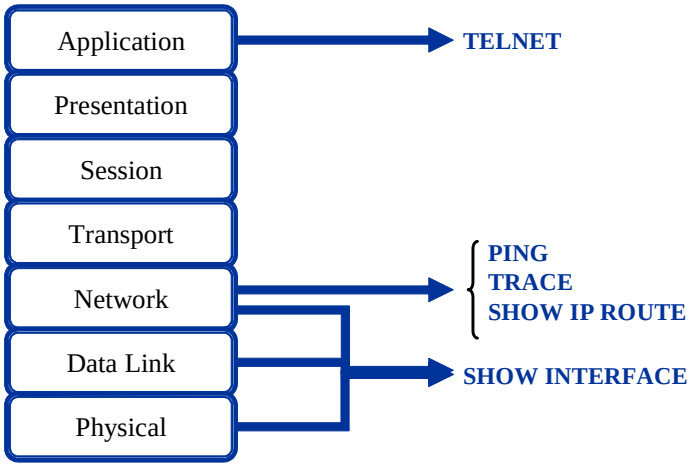
11.8.5 **Version:** Information like that offered by the locally executed “show version” command.

11.8.6 **Platform**: Device hardware platform: Cisco 7000, for example.

11.9 The bottommost router in the figure is not directly connected to the router of the administrator’s console. As a result, in order to obtain DCP information about this device, the administrator would need to make a connection via Telnet with a router directly connected to this target.

Testing Process

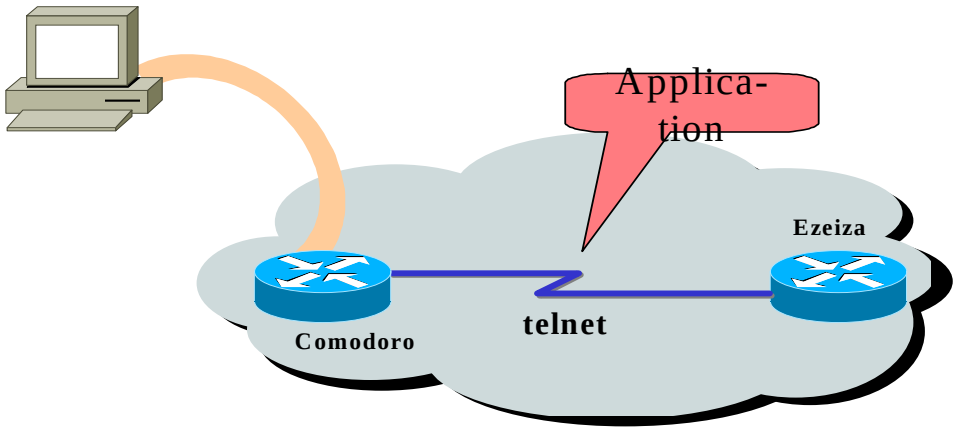
11.10 The basic test of a network should follow a sequence from one layer of the ISO/OSI model to the next. Each test presented in this section refers to the network operations of a specific layer of the OSI model.



Testing the Application Layer

11.11 Telnet offers a virtual terminal service, allowing the administrator to use Telnet operations to connect with other hosts using TCP/IP (through a client- server application).

11.12 The purpose of the test is to determine the possibility of acceding to the remote router. Successfully using Telnet to connect from the Comodoro router to the other router, Ezeiza, is a basic test for checking connectivity and accessibility.



11.13 If we can accede to another, remote, router through Telnet, not only will we verify that a TCP/IP application--upper layer application--can reach the remote router, but also that the lower layer services also function correctly.

11.14 If it is possible to communicate via Telnet with one router, but not another, it is likely that the Telnet failure is due to a specific address name or one with access permission problems. These problems can be traced to our router or to the router that failed as the Telnet communication target.

Testing the Network Layer

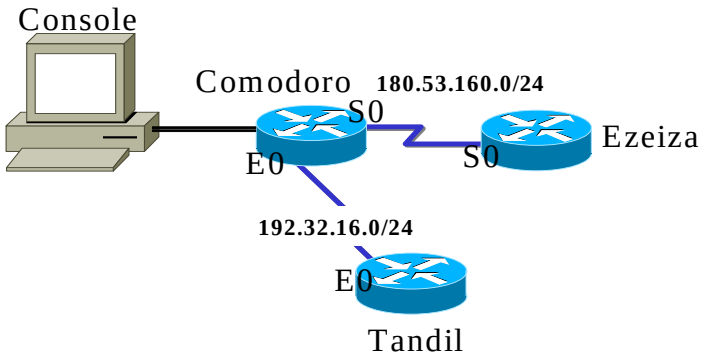
11.15 The following tools make it possible to determine the health of the network layer.

Ping Command

11.16 As an aid to diagnose the basic connectivity of the network, many network protocols support an echo protocol, which is a test to determine whether protocol packets are being routed correctly.

```
COMODORO>ping 180.53.160.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 180.53.160.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/3/4 ms
COMODORO>
```



11.17 The **ping** command sends a special packet to the destination post and then waits for a reply packet from that host. The results of this echo protocol may help evaluate the reliability of the route to the host, delays along the route, whether the host can be reached and whether it is operating.

11.18 The **ping 180.53.160.2** target in the figure replied successfully to four of the five datagrams sent to it. The exclamation marks stand for each successful echo. If one or more dots (.) were to be received instead of those marks, this would mean that the local router application timed out while waiting for a packet echo.

11.19 The EXEC user command **ping** can be employed to diagnose the basic connectivity of the network. ICMP (Internet Control Message Protocol) is the protocol that uses ping.

Trace command

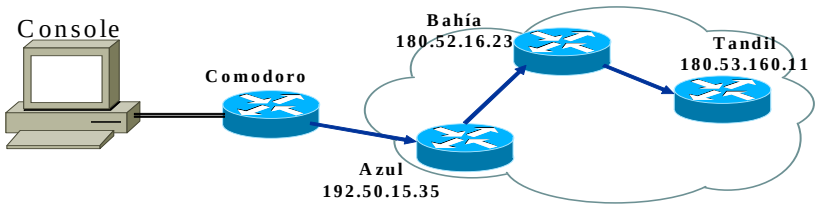
11.20 The trace command is the ideal tool for discovering where the data in your network are being sent. It uses the same protocol as the ping, except that instead of testing the connectivity from end to end, the trace command tests each step of the way.

11.21 This operation can be performed from either of the EXEC levels: user or privileged.

11.22 The trace command takes advantage of the error messages produced by the routers when a packet exceeds its time to live (TTL) value, to send several packets and display the time each packet takes to go and return.

11.23 The benefit of the trace command is that it tells us which is the last router reached along the route. This is called failure isolation.

11.24 In the example, the route from Comodoro to Tandil is traced. The route must cross Azul and Bahía along the way. If one of these routers is not reached, we would see three asterisks (*) instead of the router's name. The trace command would then continue trying to reach the next step, until stopped by an escape operation.




```
comodoro>trace azul

Type escape sequence to abort.
Tracing the route to azul (180.53.160.11)

  1 azul (192.50.15.35)   4 msec 8 msec   12 msec
  2 bahia (180.52.16.23) 6 msec 10 msec  14 msec
  3 tandil (180.53.160.11) 8 msec 14 msec  16 msec

COMODORO>
```

Show ip route command

11.25 The router gives us some powerful tools at this point in our search. We can effectively consult the routing table--in other words, the addresses the router uses to determine how to direct the traffic through the network.

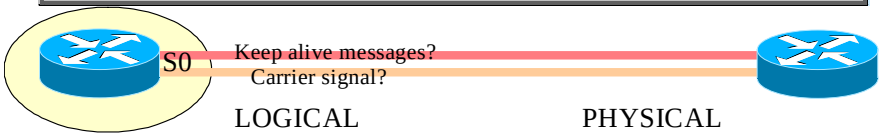
Workability of the link

11.26 While the hardware must make the actual connection between the devices, the software consists of the messages exchanged between adjacent devices. This information is made up of data that pass between two interfaces of the connected routers.

The interface has two components:

- **Physical (hardware)**
- **Logical (software).**

```
COMODORO>show interface serial 0
Serial0 is up, line protocol is up
  Hardware is HD64570
  Description: INTERFACE SERIES TOWARDS EZEIZA
  Internet address is 192.168.12.1/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
```



LOGICAL	PHYSICAL
Data Link Layer	Hardware (Physical Layer)
•KA Messages • Control Information •User Information	• Cable • Connectors • Interface

11.27 When the physical link and the data link are checked, these questions are asked:

11.27.1 Is there a carrier detect signal?

11.27.2 Is the physical link between devices operational?

11.27.3 Are the activity (KA) messages being received?

11.27.4 Can data packets be sent through the physical link?

Show interface serial command

11.28 One of the most important elements of the result of the **show interfaces serial** command is the display of the line and data-link protocol status. The Table indicates the key summary line to be checked and the meaning of the status.

INTERPRETATION OF THE INFORMATION: show interface serial		
PHYSICAL	**LOGICAL**	**STATUS**
UP	UP	Operational
UP	DOWN	Connection problem
DOWN	DOWN	Interface problem
Administrative DOWN	DOWN	Disabled

11.29 The line status in this example depends upon the carrier detect signal and refers to the status of the physical layer.

11.30 The line protocol, however, depends upon the activity fames--in other words, the data link frames.

Real-time traffic

11.31 The router includes hardware and software that make it possible to trace problems with the router itself or with other network hosts. The EXEC **debug** command at the privileged level starts up the console display of the events that have happened in the network as indicated in the debug command parameter.

Appendix 3 – Routing Protocols

ROUTING FUNCTIONS

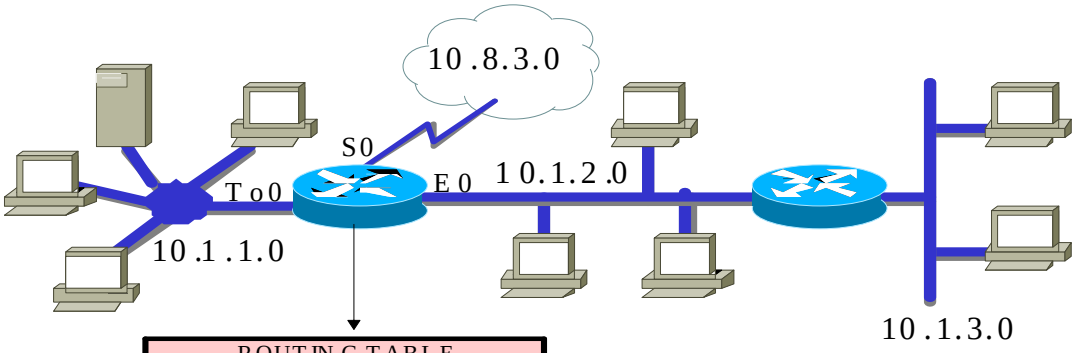
CLASSES OF ROUTING PROTOCOLS

1. ROUTING FUNCTIONS

1.1 Routers can be configured to use one or more IP routing protocols (or other network protocol). There is no single routing algorithm that meets the requirements of any network. Network administrators must analyse different (technical and political) aspects in order to select the best algorithm.

ROUTING CONSIDERATIONS

Initial IP Routing Table



ROUTING TABLE

NETWORK	INTERFACE
10.1.2.0	E0
10.1.1.0	To0
10.8.3.0	S0

1.2 Initially, a router must refer to the inputs of the networks and subnetworks that are connected directly. Each interface must be configured with a mask and an IP address. The Cisco IOS software must receive the IP address and the mask as configuration input from a source. The initial routing source is the person who does the first configuration.

1.3 Routers, by default, know the route to destination in three different ways:

1.3.1 Static routes – Manually defined by the system administrator as the only route to destination. They are useful for controlling security and reducing traffic.

1.3.2 Default routes – Manually defined by the system administrator as the route to take when there is no known route to destination.

1.3.3 Dynamic routing – The router learns about routes to destinations from periodic updates from other routers.

Static Route Configuration

1.4 The following command stablishes a static route:

IP route command	Description
network	Destination network or subnetwork
mask	Subnetwork mask
address	IP address of the router at the next hop
interface	Name of the interface to be used in the network of destination
distance	Administrative distance

1.5 The administrative distance is a reliability rating of a routing information source, expressed as a numerical value from 0 to 255. The higher the value, the lower the reliability rating.

1.6 A static route allows for manual configuration of the routing table. No dynamic changes will occur in a given table input as long as the route is active.

1.7 A static route may reflect a special knowledge of the networking status by the network administrator. Manually-entered administrative distance values are normally low figures.

1.8 Routing updates are not sent through a link if defined only by a static route, thus preserving bandwidth.

Example:

Command: ip route 172.16.1.0 255.255.255.0 172.16.2.1	
Command	**Description**
ip route 172.16.1.0	Specifies a static route to the subnetwork of destination.
255.255.255.0	A subnetwork mask indicates that an 8-bit subnetwork connection is in effect.
172.16.2.1	IP address of the router of the next hop in the route to destination.

Default Route Configuration

IP default network command	Description
network-number	IP network number or subnetwork number defined as default.

1.9 In the absence of an entry for the route of destination in the routing table, the packet is sent to the default network. The default network must exist in the routing table. Default routes keep routing table length as short as possible.

1.10 A default network must be used when only partial information is available on the network of destination. Since the router lacks full knowledge of all the networks of destination, a default network number can be used to indicate the direction to be taken for unknown network numbers.

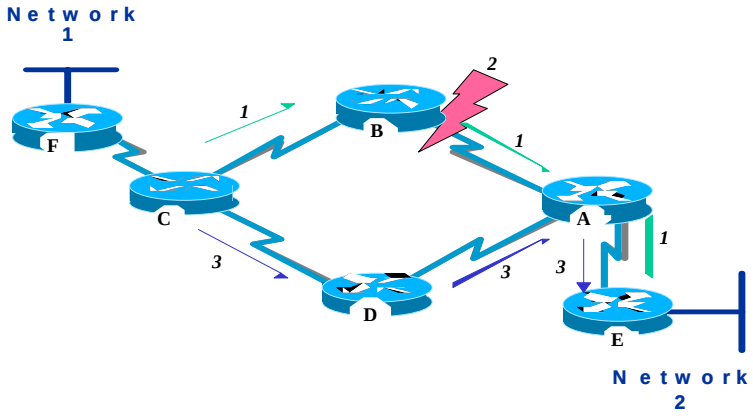
1.11 The global ip default-network 192.168.17.0 command, for instance, defines the C 192.168.17.0 class network as the destination route for packets lacking an entry in a routing table.

Static *versus* Dynamic Routes

1.12 Static knowledge is managed manually: a network administrator enters it in the router configuration. The administrator must manually update this static route[1] entry whenever a change in internetwork topology requires updating.

1.13 The dynamic knowledge works differently. After the network administrator has entered the configuration commands to start the dynamic routing[2], route knowledge is automatically updated through a routing process whenever new information is received from the internetwork. Changes in the dynamic knowledge are exchanged among routers as part of the updating process.

Adjustment to Changes in Topology



1.14 The network shown in the graphic adjusts in different ways to changes in topology, depending on whether it uses statically- or dynamically-configured knowledge. Static routing enables routers to properly route a packet from one network to another. The router consults its routing table and follows the static knowledge to send the packet to router F, C, B, A, and E, until the packet is delivered to the destination host.

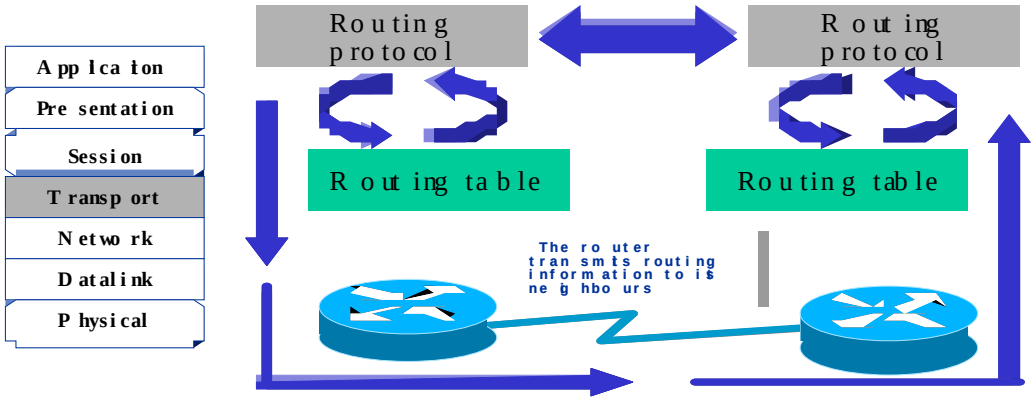
1.15 But, what happens if the route between router B and router A fails? Obviously, router B will not be able to send the packet to router A through a static route. Until router C has been manually reconfigured to send the packets through router D, communications with the destination network will be impossible.

[1] **Static route** – Route explicitly configured and entered in the routing table. Static routes have priority over routes chosen through dynamic routing protocols.

[2] **Dynamic routing** – Routing automatically adjusted to network topology and traffic changes. Also called *adjustable routing*.

1.16 Dynamic routing offers flexibility. According to the routing table generated by router C, a packet can reach its dstination following the preferred route through router B. However, there is an alternate route available through router D. When router B recognizes that the link to router A is down, it adjusts its routing table and sends the information to router C, which selects the route through router D as the preferred route to its destination. Routers continue to send packets through this link.

1.17 When the service in the route between routers B and A is restored, router C can again change its routing table and indicate its preference for the route clockwise, through routers B and A to the destination network. The dynamic routing protocols can also redirect traffic between the different routes of a network.



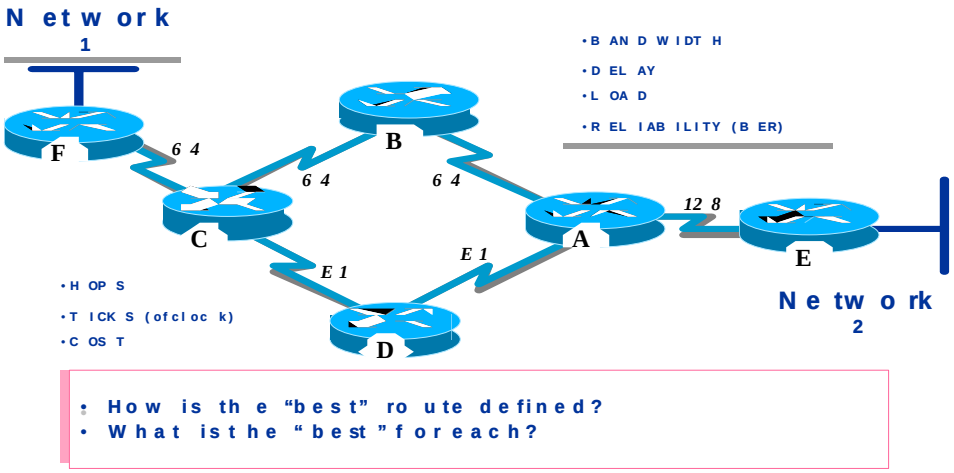
DYNAMIC ROUTING

1.18 The success of dynamic routing depends on two basic router functions:

1.18.1 Maintenance of a routing table

1.18.2 Timely distribution of knowledge--in the form of routing updates--to other routers.

1.19 Dynamic routing relies on a routing protocol for sharing knowledge. A routing protocol defines the set of rules used by the router to communicate with its neighbors.



1.20 For example, a routing protocol describes:

1.20.1 How updates are sent

1.20.2 What information is contained in said updates

1.20.3 When to send this information

1.20.4 How to locate update receivers

Distance representation using metrics

1.21 When a routing algorithm updates a routing table, its main objective is to identify the best information to be included in the table. Each routing algorithm interprets the term "best" in its own way. The algorithm generates a number--the so-called metrics value--for each route through the network. The lower the metrics number, the better the route.

1.22 Metrics can be estimated based on a single feature of the route. More complex metrics can be estimated by combining several features. Several route features are used to estimate the metrics. The most frequently used router metrics are the following:

1.22.1 **Bandwidth –** Data capacity of a link. For example, a 10 Mbps Ethernet link is normally preferrred over a 64 kbps leased line.

1.22.2 **Delay –** Time necessary to move a packet from its point of origin to its point of destination.

1.22.3 **Load** – Amount of activity in a network resource, like a router or a link.

1.22.4 **Reliability** – Generally refers to the error rate of each network link.

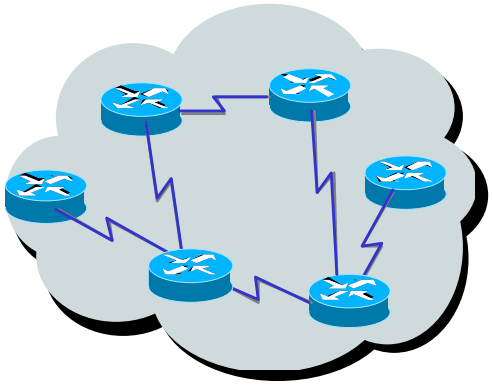
1.22.5 **Number of hops** – Number of routers that a packet must cross.

1.22.6 **Ticks** – Delay in a data link using the ticks of an IBM PC clock (approximately 55 milliseconds).

1.22.7 **Cost** – Arbitrary value assigned by the network administrator, generally based on bandwidth, expenditure in pesos, dollars, or other measure.

Autonomous system

1.23 An autonomous system consists of routers, administered by one or more operators, that present a consistent routing scheme to the outside world.

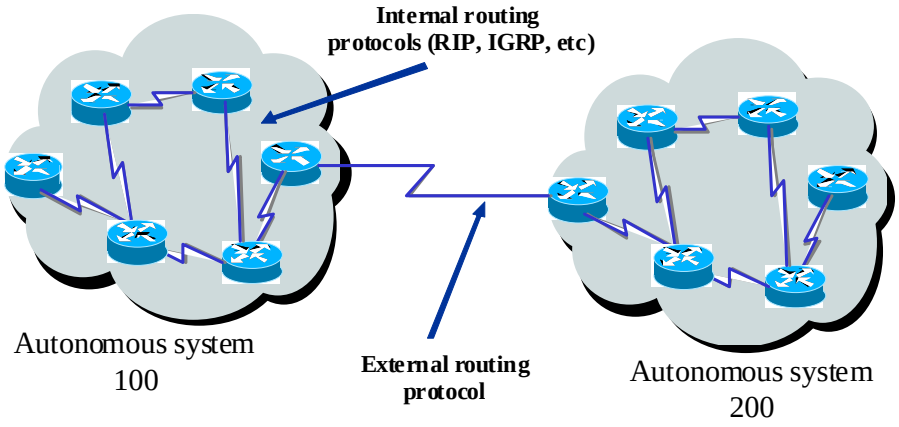


1.24 The Network Information Center (NIC) assigns a dedicated autonomous system to enterprises. This autonomous system is a 16-bit number. A routing protocol like the Cisco Interior

Gateway Routing Protocol (IGRP) requires that this assigned dedicated autonomous system number be specified in its configuration.

INTERNAL AND EXTERNAL PROTOCOLS

1.25 External routing protocols are used for communications between autonomous systems. Internal routing protocols are used within the same autonomous system.



Internal IP Routing Protocols

1.26 In the Internet layer of the TCP/IP protocol set, a router may use routing protocols through specific algorithms. Some examples of IP routing protocols follow:

1.26.1 RIP— A distance vector routing protocol.

1.26.2 IGRP— A Cisco distance vector routing protocol.

1.26.3 OSPF—A link state routing protocol.

1.26.4 EIGRP (Enhanced IGRP) —A balanced hybrid routing protocol.

2. CLASSES OF ROUTING PROTOCOLS

2.1 Most routing algorithms can be classified as one of two types of basic algorithms: distance vector[3] or link state[4].

2.2 The distance vector routing type defines the direction (vector) and distance to any link in the internetwork.

[3] **Distance vector routing algorithm (Bellman-Ford)** – Class of routing algorithms that iterate the number of hops in a route to find a shortest-path spanning-tree. Distance vector routing algorithms send their entire routing table to their neighbors in each update. Distance vector routing algorithms are prone to routing loops, but are more simple in computer terms than the link state routing algorithms.

[4] **Link state routing algorithm** – Routing algorithm where each router broadcasts or muticasts information to all internetwork nodes indicating the communication cost to each of its neighbors. Link state algorithms create a consistent network view and, therefore, are not prone to routing loops, at the cost of having relatively greater computer difficulties and a more disseminated traffic (as compared to distance vector routing algorithms).

2.3 The link state routing type (also called of the shortest path - SPF) recreates the exact topology of the whole internetwork (or at least of the partition where the router is located).

2.4 The balanced hybrid type combines aspects of the link state and distance vector algorithms.

Convergence

2.5 The routing algorithm is essential for the dynamic routing. When the network topology changes due to growth, reconfiguration, or failure, the basic knowledge of the network must also change.

2.6 The knowledge needs to reflect a precise and consistent view of the new topology. This precise and consistent view is called convergence.

2.7 When all internetwork routers work with the same information, it is said that the internetwork has converged.

2.7.1 Convergence occurs when all of the routers have a consistent perspective of the network topology.

2.7.2 Whenever the topology changes, routers must recalculate the routes, generating a state of transition.

2.7.3 The process and time required for convergence vary according to routing protocols.

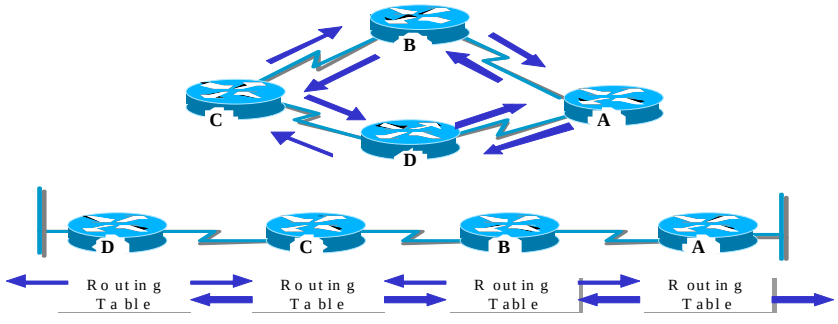
2.8 Quick convergence is a convenient network feature because it reduces the time during which routers have outdated information, which helps prevent making decisions that are incorrect, uneconomical or both.

DISTANCE VECTOR

2.9 Distance vector routing algorithms (also known as Bellman-Ford algorithms) periodically transmit copies of a routing table from one router to the other. Regular updates between routers inform of changes in topology.

2.10 Each router receives a routing table from its direct neighbor. In the following figure, for example, router B receives information from router A.

2.11 Router B adds a distance vector number (such as the number of hops), which increases the distance vector, and then transmits the routing table to its neighbor, router C. This same process, step by step, occurs in all directions between direct neighbor routers.

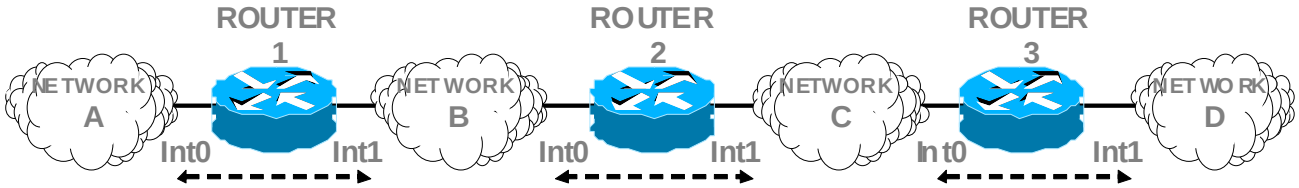


2.12 Thus, the algorithm accumulates network distances in order to keep a network topology data base.

2.13 Distance vector algorithms do not permit the router to know the exact topology of an internetwork.

Discovering the distance vector network

2.14 Every router that uses distance vector routing starts by identifying its own (directly connected) networks. In the graph, the distance of the port to each of the networks that are connected directly is 0.



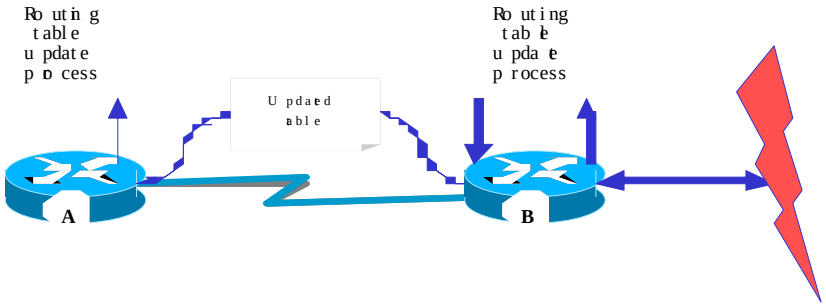
As the distance vector network discovery process proceeds, the routers discover the best route to the networks of destination, based on the information from each neighbor.

ROUTER 1	ROUTER 2	ROUTER 3
A → Int0 → 0 B → Int1 → 0	B → Int0 → 0 C → Int1 → 0	C → Int0 → 0 D → Int1 → 0
A → Int0 → 0 B → Int1 → 0 C → Int1 → 1	B → Int0 → 0 C → Int1 → 0 A → Int0 → 1 D → Int1 → 1	C → Int0 → 0 D → Int1 → 0 B → Int0 → 1
A → Int0 → 0 B → Int1 → 0 C → Int1 → 1 D → Int1 → 2	B → Int0 → 0 C → Int1 → 0 A → Int0 → 1 D → Int1 → 1	C → Int0 → 0 D → Int1 → 0 B → Int0 → 1 A → Int0 → 2

2.15 For instance, router A obtains knowledge about other networks from the information received from router B. Each of these inputs from other networks in the routing table has a cumulative distance vector to show the distance at which the network is in the given direction.

Changes in the Distance Vector Topology

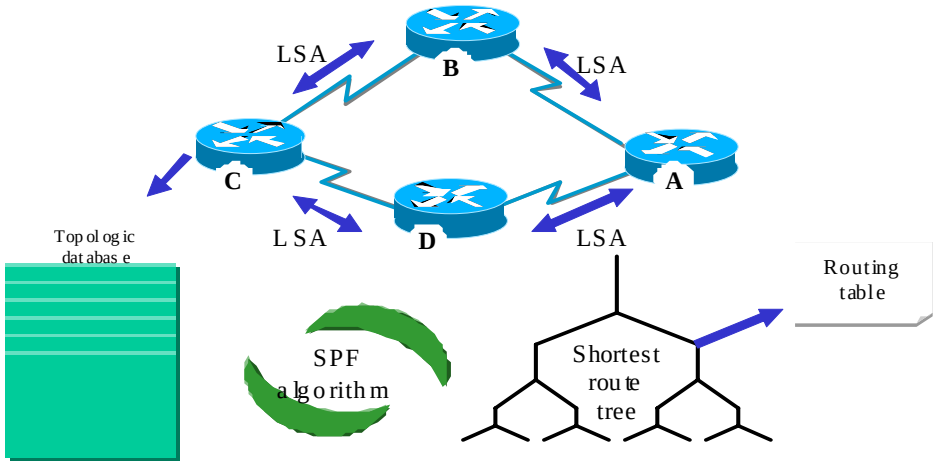
2.16 When a protocol topology changes by distance vectoring, the routing table must be updated. Like in the network discovery process, topology change updates occur step by step from one router to the other.



2.17 Distance vector algorithms require that each router send its entire routing table to each of its adjacent neighbors. Distance vector routing tables contain information about the total cost of the route (defined by its metrics) and the logical address of the first router in the route towards each network it knows.

LINK STATE

2.18 Routing algorithms based on the link state--also known as shortest-path-first algorithm (SPF) – keep a complex topology information database. While the distance vector algorithm has non-specific information about distant networks and has no knowledge about distant routers, a link state algorithm keeps complete data on distant routers and how they interconnect.



2.19 Link state routing uses link-state advertisements (LSAs)[5], a topologic database, the SPF[6] algorithm, the resulting SPF tree, and, finally, a routing table of routes and ports to each network. The following pages explain these processes and databases in more detail.

2.20 The engineers have implemented this link-state concept in the shortest free path first routing (OSPF). RFC 1583 contains a description of the OSPF link-state concepts and operations.

Link-state network discovery

2.21 Network discovery for link-state routing applies the following processes:

2.21.1 Routers exchange LSAs with each other. Each router begins with the networks connected directly on which it has direct information. Then, each router, in parallel with the others, builds a topologic database that includes all of the internetwork LSAs.

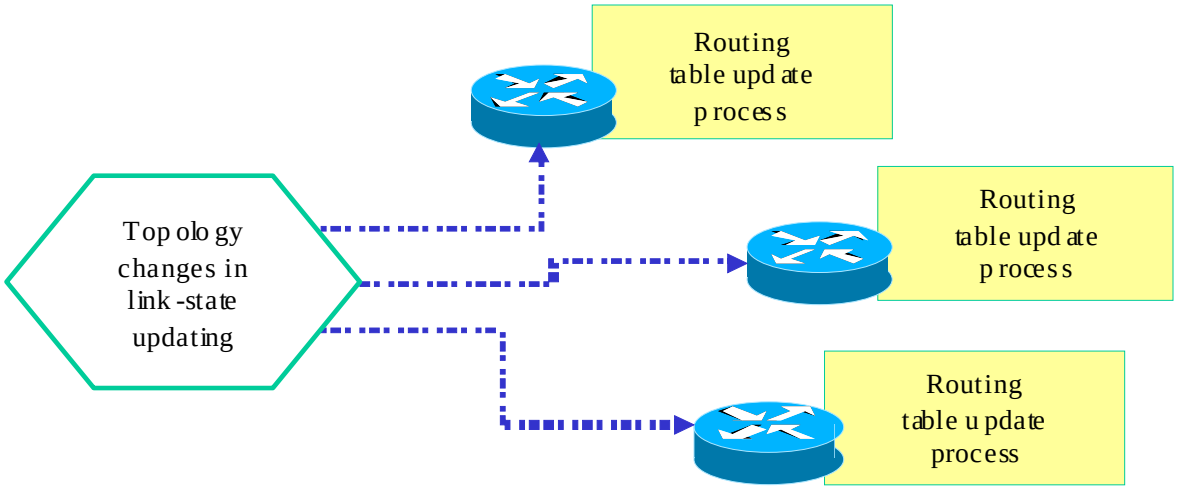
[5] **LSA** - *(Link-state advertisement) or Link-state packet (LSP).* Publication of the state of the link. Broadcast packet used by link-state protocols containing information about the neighbors and route costs. LSAs are used by receiver routers to maintain their routing tables.

[6] **SPF** - *(shortest path first algorithm)* Routing algorithm that iterates the route length in order to determine the shortest route spanning tree. *Dijkstra algorithm.*

2.21.2 The SPF algorithm determines the way to get to the network, identifying the shortest route to each of the other networks of the link-state protocol internetwork. The router builds this shortest route logical topology as an SPF tree. With itself as the root, this tree expresses routes from the router to all the destinations. The router makes a list with its best routes and with the ports to said networks of destination in the routing table. It also keeps other databases on topologic elements and state details.

Changes in link-state topology

2.22 Link-state algorithms are based on the use of the same link-state updates. Whenever a link-state topology is modified, the routers that are first aware of said modifications send information to the other routers or to a designated router that all the others can use for their updates. This includes the delivery of common routing information to all internetwork routers. To achieve convergence, each router does the following:



2.22.1 It keeps a record of its neighbors: name of the neighbor, whether it is active or down, and cost of the link to the neighbor. It builds an LSA packet containing a list of names and costs of links to its neighboring routers. This includes new neighbors, modifications of link costs, and links to out-of-service neighbors.

2.22.2 It sends this LSA packet so that it is received by all the other routers. When it receives an LSA packet, it registers the LSA packet in its database so that it can store the last packet generated by all the other routers.

2.22.3 Using the accumulated LSA packet data to build a complete internetwork topology map, it re-runs the SPF algorithm from that common starting point and estimates the routes to each network destination.

2.22.4 Whenever an LSA packet gives rise to a modification in the link-state database, the link-state algorithm re-calculates the best routes and updates the routing table. Then, all the other routers take this topology modification into account to determine the shortest route to be used for packet switching.

DISTANCE VECTOR - LINK STATE COMPARISON

2.23 Distance-vector routing may be compared to link-state routing in several key areas:

2.23.1 Distance-vector routing obtains all topology data from the information contained in the routing table of its neighbors. Link-state routing gets a broad view of the whole network topology by accumulating all the necessary LSAs.

2.23.2 Distance-vector routing determines the best route by increasing the value of the metrics it receives as tables move from one router to the other. For link-state routing, each router works separately to estimate its own shortest route to destinations.

2.23.3 In most distance-vector routing protocols, topology change updates are done in the form of periodic table updates. These tables are transmited from one router to the other, which generally results in a slower convergence.

2.23.4 In link-state routing protocols, updates are generally caused by changes in topology. The relatively small LSAs that are transmitted to all the other routers generally result in a faster convergence following any change in network topology.

DISTANCE VECTOR	LINK STATE
Sees the network topology from the perspective of the neighbors. **Adds distance vectors from router to router.** **Frequent periodic updates: Slow convergence.** **Sends copies of the routing table to neighbors.**	Gets a common view of the entire network topology. Calculates the shortest route to the other routers. **Event-triggered updates: faster convergence.** **Passes on link-state routing updates to other routers.**

3. DYNAMIC ROUTING CONFIGURATION

3.1 The selection of IP as routing protocol involves the definition of both global and interface parameters.

3.2 Global tasks:

3.2.1 Select a routing protocol, RIP or IGRP.

3.2.2 Assign IP network numbers, without specifying subnetwork values.

3.3 The interface task is to assign network/subnetwork addresses, as well as the correct network mask. A dynamic routing uses broadcasts and multicassts to communicate with other routers. The routing metrics helps routers find the best route to each network or subnetwork.

4. RIP

4.1 The RIP protocol was originally specified in RFC 1058. RIP key features include the following:

4.1.1 It is a distance-vector routing protocol.

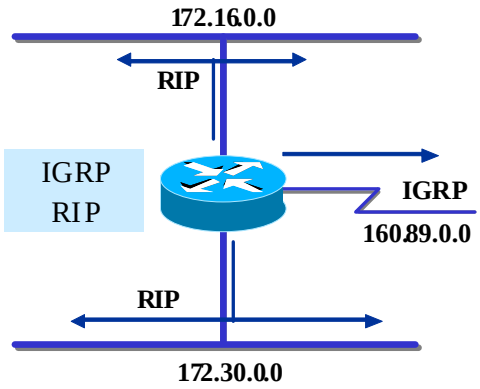
4.1.2 It uses hop calculation as metrics for route selection.

4.1.3 Maximum allowable hop calculation is 15 (16 is inaccessible).

4.1.4 Routing updates are issued every 30 seconds by default.

<u>global configuración</u>
- Select routing protocol(s)
- Specify network(s)

<u>Interface configuration</u>
- Verify subnetwork address/mask



Example of RIP configuration

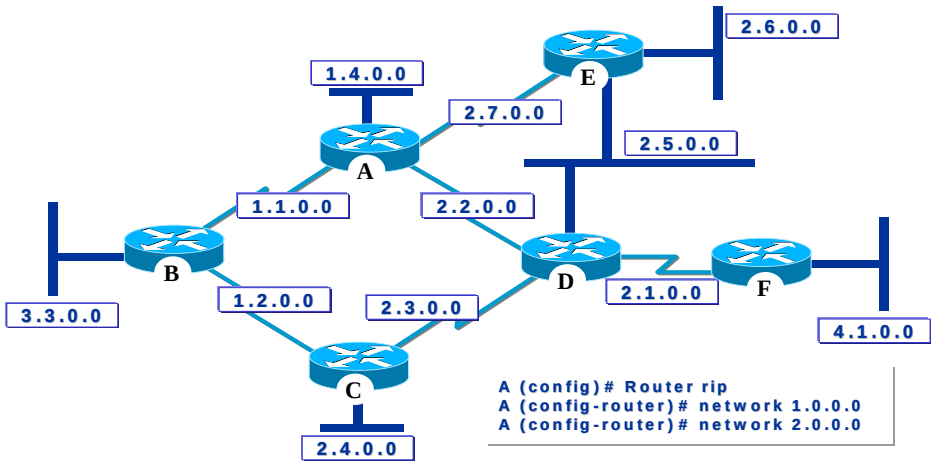
4.2 In the following example:

4.2.1 **router rip**—selects RIP as routing protocol

4.2.2 **network 1.0.0.0**—specifies a network connected directly.

4.2.3 **network 2.0.0.0**—specifies a network connected directly.

4.3 Cisco router A interfaces that are connected to networks 1.0.0.0 and 2.0.0.0 will send and receive RIP updates. These routing updates allow the router to be aware of the network topology.



<u>RIP MONITORING</u>

4.4 The **<u>show ip protocol</u>** command displays routing timer values and network information associated to the entire router. This information can be used to verify routing information. This router sends information about the updated routing table every 30 seconds (this interval is configurable). The next update will be sent after 9 seconds. The router injects routes for the networks mentioned following the router "network routing" line.

IP Routing Table

4.5 The **show ip route** command displays the content of the IP routing table. The routing table contains entries for all known networks and subnetworks, as well as a code showing how this information was obtained.

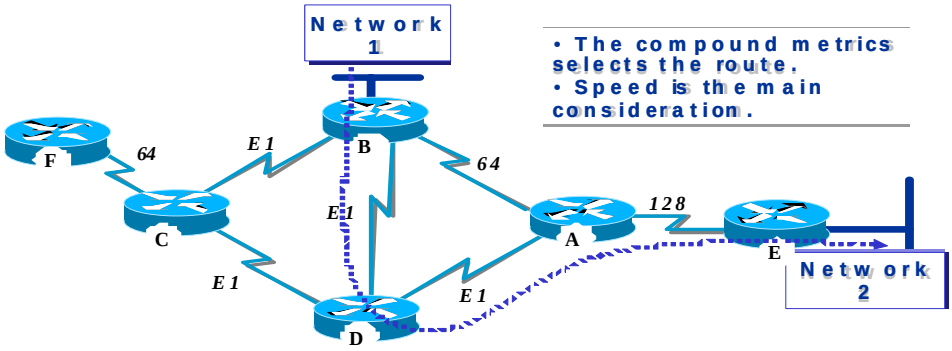
4.6 All routes to the networks that the router becomes aware of receive the mask that corresponds to the interface for which they were updated (RIP version 1).

DEBUG RIP

4.7 The command **debug ip rip** shows RIP routing updates while they are being sent and received. In this example, the update is sent and relayed by serial interfaces 0 and 2.

5. IGRP

5.1 IGRP is a distance-vector routing protocol developed by Cisco. Every 90 seconds, IGRP sends routing updates (which do not include subnetwork information) published by networks for a particular autonomous system. It runs directly over IP (protocol 88).



5.2 Some key IGRP features are shown below:

5.2.1 Versatility to automatically handle indefinite and complex topologies.

5.2.2 Flexibility for segments having different bandwidth and delay characteristics.

5.2.3 Scalability to operate in very large networks.

5.3 The IGRP routing protocol uses a combination of variables to determine a compound metric. Variables used by IGRP include:

5.3.1 Bandwidth (B)

5.3.2 Fixed delay between nodes (D)

5.3.3 Traffic load (L)

5.3.4 Reliability or error rate along the path (R)

5.3.5 Maximum transmission unit (MTU) [7]

5.3.6 Count of hops to destination (H)

IGRP METRIC

5.4 IGRP uses the indicated set of values to calculate routes. An algorithm is applied to these values, weighing them with coefficients K1, K2, K3, K4 and K5.[8]

$$Métrica = (K1 * B) + \frac{K2 * B}{256 - L} + (K3 * D) * \frac{K5}{R + K4}$$

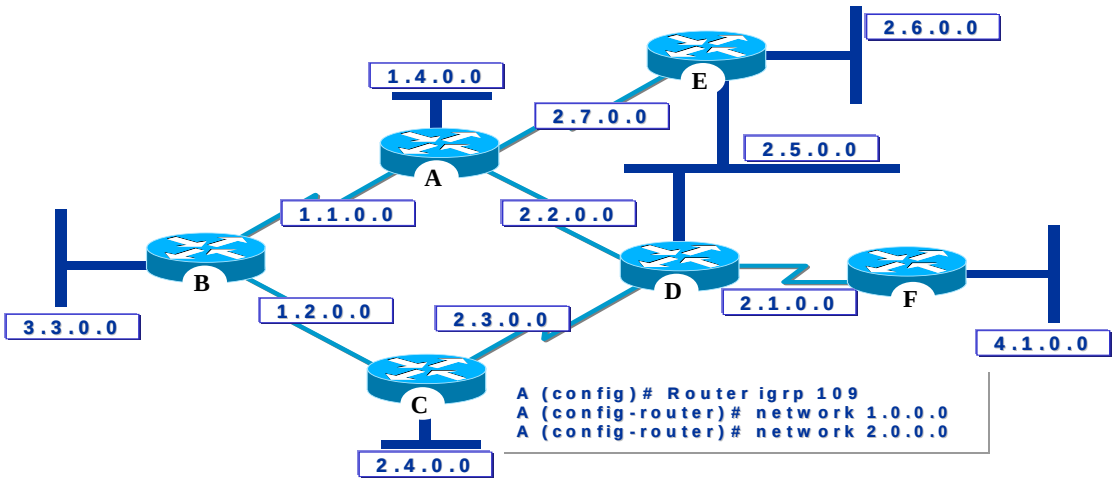
5.5 B is obtained by dividing 10 million by the least of all output interface bandwidths [in Kbps] (if Bw=1,544 Mbps ➔ 10000000/1544= 6476).

5.6 D is the sum of all output interface delays, divided by 10 [tenths of microseconds] (if delays are (20000 useg + 1000 useg)/10 = 2100)

5.7 The metric would then be 6476+2100= 8576. *The path with the smaller metric is the best path.*

Example of IGRP configuration

5.8 In the following example: IGRP is selected as the routing protocol for autonomous system 109. All interfaces connected to networks 1.0.0.0 and 2.0.0.0 will use IGRP to gather and distribute routing information.



5.8.1 router igrp 109—selects IGRP as the routing protocol for autonomous system 109.

5.8.2 network 1.0.0.0—specifies a network connected directly.

5.8.3 network 2.0.0.0—specifies a network connected directly.

[7] **MTU** - Maximum transmission unit. Maximum packet size, in bytes, that a given inerface can handle.

[8] Defaults are K1 = K3 = 1, K2 = K3 = K5 = 0.

IGRP MONITORING

5.9 The **show ip protocol** command displays the IP routing protocol, the routing timers, and the network information associated to the entire router.

5.10 The algorithm used to estimate the IGRP routing metric is also shown in this display. It also includes information on the routing metrics and the routing filters.

IP routing table

5.11 The **show ip route** command shows the contents of an IP routing table. The table contains a list of all known networks and subnetworks and the metrics associated to each entry.

DEBUG IGRP

5.12 The **debug ip igrp transactions** command displays RIP routing updates while they are being sent and received.

```
RouterA#debug ip igrp transactions
IGRP protocol debugging is on
RouterA#
00:21:06: IGRP: sending update to 255.255.255.255 via Ethernet0 (172.16.1.1)
00:21:06:       network 10.0.0.0, metric=88956
00:21:06:       network 192.168.1.0, metric=91056
00:21:07: IGRP: sending update to 255.255.255.255 via Serial2 (10.1.1.1)
00:21:07:       network 172.16.0.0, metric=1100
00:21:16: IGRP: received update from 10.1.1.2 on Serial2
00:21:16:       subnet 10.2.2.0, metric 90956 (neighbor 88956)
00:21:16:       network 192.168.1.0, metric 91056 (neighbor 89056)
```

Appendix 4 – Device Management

CISCOWORKS SMNS

INTRODUCTION

CISCO WORKS SERVER

WHATS UP GOLD

RME

1. INTRODUCTION

1.1 CiscoWorks Small Network Management Solution (CWSNMS) is an integrated network management solution for small to medium-sized networks with up to 40 Cisco devices. CWSNMS provides a powerful set of configuration and monitoring tools for managing Cisco devices.

Applications

1.2 CWSNMS includes the following applications:

1.2.1 CiscoWorks Server (In Common Services)

1.2.2 Resource Manager Essentials

1.2.3 CiscoView

1.2.4 WhatsUp Gold

CiscoWorks Server

1.3 CiscoWork Server is part of CiscoWorks Common Services. This server permits the execution of common network management tasks, such as managing user accounts, databases, starting and stopping CiscoWorks server processes, etc.

1.4 The connectivity and accessibility of devices can also be verified and faulty devices diagnosed.

Resource Manager Essentials

1.5 RME is a set of web-based applications that offers management solutions for Cisco switches, access servers, and routers. The RME browser interface provides easy access to critical information to maintain network operativeness, and simplifies the completion of tasks that are too time-consuming in manual mode.

1.6 RME is based on a client/server architecture that connects multiple web-based clients to a network server.

Cisco View

1.7 Basically, CV provides graphical views of front and back equipment panels. Dynamic displays and color graphs simplify the monitoring of devices, device-specific diagnostic components, and their configuration.

1.8 CV may be launched from both the CWSMNS desk Device Center or from Whats Up Gold.

Whats Up Gold

1.9 Whats Up Gold (WUG) is a network management software from another vendor (Ipswitch Inc). WUG allows for concurrent monitoring of multiple devices on a topologic map (while CV is only capable of monitoring one device at a time).

1.10 Consequently, WUG permits the discovery, mapping, monitoring, and tracking of alarms.

Desktop

1.11 The CW desktop is the interface to CWSMNS network management applications. It is a graphical user interface (GUI) that runs on a web browser. The desktop offers the following features:

1.11.1 Web clients

1.11.2 Desktop innovation

1.11.3 Logging In

1.11.4 Use of the desktop

1.11.5 On-line help

1.12 Whenever a network management application is invoked, CW checks that the required Plug-in Java is installed in the client system. If it is not, CW will require such installation.

Web Clients

1.13 The server may be accessed from any client that meets the appropriate system requirements. The only client software required is the Microsoft Internet Explorer web browser.

Use of the Desktop

1.14 The CW Desktop is the primary user interface and the starting point for all tasks. After doing the login, the desktop shows the following tabs:

1.14.1 WhatsUpGold

1.14.2 Essentials

1.14.3 Device Center

1.14.4 Admin

1.15 Each browsing tab contains a series of links that, in turn, contain groups of associated or similar tasks, tools, reports, and other options.

On-Line Help

1.16 Each CW application includes on-line help with conceptual and procedural information to facilitate its use. It also includes:

1.16.1 A search engine: Search of help topics by key word.

1.16.2 A table of contents: Presentation of typical network tasks.

1.16.3 A glossary: Definition of CW tasks.

1.17 If an option of the browsing tree is selected, help for that option will be displayed.

2. CISCO WORKS SERVER

Background

2.1 CW is a family of products based on Internet standards for managing Cisco networks and devices. All CW products use and depend upon the CW server. The CW server provides a common set of management services, which are shared by multiple network management applications.

2.2 It also provides management with information on user roles and privileges. With this feature, access to applications and specific functions within applications can be controlled. Control of roles and privileges is done through the authentication and control services included in CW, but can also be done using an external authentication server.

Server and Applications

2.3 Although many applications depend upon the CW server, not all of them use the services to the same extent.

2.4 The CW server basically provides two types of services:

2.4.1 Runtime Services: Desktop, process management, security and on-line help engine (enabled during installation).

2.4.2 System Services: Database engine and utilities, event distribution and job management services.

2.5 While Runtime services are always enabled by default, System services are enabled whenever an application software requiring these services is installed. Finally, the Desktop integrates all of the applications.

Completion of Jobs

2.6 Most jobs directly require administrator-level privileges because they affect the performance and behavior of the CW server. Only some jobs are accessible to all users.

Description
Server status check
Configuration of user accounts
Process status check
Log file status check
Connectivity check (Nslookup)
Connectivity check (Traceroute)
Connectivity check (Ping)
Connectivity check (station-device)

Server Configuration

2.7 The CW server includes tools to properly configure the server in order to support other Cisco applications.

2.7.1 Configuration of user accounts

2.7.2 Installation of Java Plug-in

2.7.3 Resetting of passwords

Configuration of user accounts

2.8 Several network and application management operations are potentially disruptive for the network or the applications themselves, and must be protected. To prevent such operations from being used accidentally or maliciously, CW uses a multilevel security system that gives access to certain functions only to users that can be authenticated at the appropriate level. CW provides two predefined access IDs (identifications), but the administrator can create additional IDs:

2.8.1 Guest (the password is specified during installation, user role = Help Desk)

2.8.2 Admin (the password is specified during installation, user role = combination of system administrator, network administrator, network operator, approver, and Help Desk). Equivalent to Windows administrator for CW. Has access to all CW jobs.

2.9 System administrators determine user security levels. When being configured, the user is assigned one or more roles.

2.10 The role, or combination of roles, of the user, determines which CW applications can be displayed.

Level	Description
0	Help desk
1	Approver
2	Network Operator
4	Network Administrator
8	System Administrator
6	Export Data
32	Developer

2.11 Users can perform other jobs on their own account, but most security jobs require privileges that correspond to the system administrator role.

2.12 When security jobs are performed, the following must be taken into account:

2.12.1 RME cannot retrieve forgotten/lost passwords. A system administrator level is required to change or delete the password and then add the user role again.

2.12.2 The user admin is reserved and cannot be erased.

2.12.3 If the admin password is forgotten, the utility indicated in “password reset” must be used.

Job	Purpose	Level
Change password	Modify the password on his/her own account.	All
Add user	Create new account and assign access level	Admin
Delete user	Remove account	Admin
Modify user	Update user information	Admin
See logged users	Show information on active users and send messages	Admin

Password resetting

2.13 The password resetting utility permits changes in a CW local user password from the line of commands. Administrator or super user privileges are required to execute this utility.

Server Administration

2.14 The CW server includes administrative tools to ensure proper operation, *inter alia*:

2.14.1 Basic tools

2.14.2 Maintenance of log files

2.14.3 Data management jobs

2.14.4 Back-end process management

2.14.5 Work and resource management

2.14.6 Network event management

Basic tools

2.15 Basic administrative tools permit the following jobs:

JOB	PURPOSE
Display installed software packages	List installed applications
Display log file status	Show logfile size and utilization

Log file maintenance

2.16 Log files can grow and use up all the space in the disk. CW includes a script to control this growth.

2.17 The script is designed to keep the following files:

2.17.1 Daemon manager

2.17.2 JRUN

2.17.3 Web server log files

Data management jobs

2.18 Storage management jobs must be regularly executed to ensure that there are database backups in case it becomes useless or corrupted.

2.19 When configuring the database backup strategy, the following guidelines must be considered:

2.19.1 Data protection and recovery are only supported within a same version (a database protected by another version cannot be recovered).

2.19.2 Check the size of the files stored in the backup directory. Some of them might require more disk space.

2.19.3 Database files are stored using the following backup directory structure:

2.20 The suite name used for the database files of the CW server is cmf. The .cmf database includes the data backup of the CW server applications.

JOB	PURPOSE
Database backup	Perform a backup job now.
Programming of regular backups	Perform programmed backup jobs
Database restoration	Replace the existing database with another version
Change of database password	Change the database password for security reasons

Data Backup

2.21 Data backup can be done on demand, instead of waiting for the next programmed backup, using the “Back up Data Now” option.

Back-end Process Management

2.22 CW applications use back-end processes to manage specific activities or jobs of the applications. Process management tools make it possible to control these processes in order to optimize or diagnose the CW server.

JOB	PURPOSE
Start process	Restart specific processes
Stop process	Stop specific processes
See processes	Show information about the processes, including status, ID, and other data.

JOB	PURPOSE
See process failures	Show faulty processes, information on failures, and time of occurrence of the failure.

Job and Resource Management

2.23 Job Management provides reporting services on jobs, resources, and events to the CW. Job Management is used to display jobs, release resources, and stop and/or remove jobs.

JOB	PURPOSE
Cancel a programmed job	Stop the execution of a job, while keeping it in Job Management
Remove a job	Removes a job from Job Management
Release an orphan resource	Releases resources locked due to system failures. Only to be used if no other options are available.

Network event management

2.24 There are two CW services for event management. Applications use one or the other.

2.24.1 Event Distribution Service (EDS)

2.24.2 Event Services Software (ESS)

Event Distribution Service (EDS)

2.25 With EDS, event sources and addressees can be managed. Event sources create network events, while addressees are the consumers of these events.

Source = originator = creator

Destination = consumer

JOB	PURPOSE
Enable or disable debugging or the generation of trace messages	Diagnose problems
Configure individual services	Enable the setup and configuration of event sources or event destination services, such as queueing parameters.
Associate event filters to a generic consumer.	Permit the use of a filter to specify the events that must be sent to each generic consumer.
See performance statistics of all internal data queues of event sources and consumers.	Show the work being carried out by the EDS. Based on these statistics, it can determine whether events are being lost, and the maximum value at which to set queue capacity.
See events received by EDS and the event logger.	Network monitoring or diagnosis.

Event Services Software (ESS)

2.26 ESS enables several CW processes to send broadcast messages to other processes in a distributed network environment. ESS uses a publication and subscription model where some processes broadcast messages while others selectively subscribe to the messages. In this model, each process subscribes to a host of topics, while other processes, when they need a process to receive the message, publish their messages to any of these topics. For example, if process 1 subscribes to topics a, b, and c, other processes will publish messages for process 1 on topics a, b, or c.

3. WHATS UP GOLD

3.1 Whats Up Gold (WUG) is a network management software from another vendor (Ipswitch Inc). WUG concurrently monitors multiple devices on a topologic map (while CV can only monitor one device at a time).

3.2 Therefore, alarms can be discovered, mapped, monitored and tracked using WUG.

User Roles

3.3 CWSNMS creates two priviledged users in WUG: admin and guest. These privileges permit the use of a single login for both applications.

3.4 The WUG admin user is mapped with the CW server Network Administrator and System Administrator roles.

3.5 The WUG guest user is mapped with the other CW roles, such as Help Desk, network operator, etc.

Mapping

3.6 The EssentialsmanagedDevices mapping contains the devices managed by the RME database. This mapping cannot be imported to RME, but is automatically created for the first time, when:

3.6.1 Devices are added or imported.

3.6.2 Devices using the WUG console are discovered and the “Export to Essentials” option is used.

3.7 Subsequently, the mapping shall be manually updated each time devices are added to RME using the “Recreate Map” option. The following jobs can be performed with WUG SNMS in the CW Desktop:

3.7.1 Recreate Map

3.7.2 Export to Essentials

3.7.3 Launch the Device Center and CiscoView applications

3.7.4 Change the passwords of *admin* and *guest* users.

Passwords

3.8 CW SMNS creates two privileged user accounts in WUG: *admin* and *guest*.

3.8.1 The WUG admin user is mapped with the CW server Network Administrator and System Administrator roles.

3.8.2 The WUG guest user is mapped with the other CW roles, such as Help Desk, network operator, etc.

3.9 These two user IDs can be used to access the web server:

3.9.1 *Admin* user ID: Has full access to all WUG functions and views. The *admin* password is generated during product installation.

3.9.2 *Guest* user ID: Has access to all WUG views, but cannot change any configuration. The *guest* password is generated during product installation.

Map Generation

3.10 Administration jobs include the discovery of network devices and the creation of the EssentialsManagedDevices map, using the WUG application (the WUG console and the WUG link are used on the CWSNMS desktop).

4. RME

Introduction

4.1 RME is a set of web-based applications that offers solutions for managing Cisco switches, access servers, and routers. The RME browser interface provides easy access to critical information for maintaining network operativeness, and simplifies the performance of jobs that are time consuming in manual mode.

4.2 RME is based on a client/server architecture that connects multiple web-based clients to a network server. As the number of devices increases, additional servers or data collection points can be added in order to handle network growth with a minimum impact on the browser application of the client.

4.3 Drawing on the inherent scalability of the intranet architecture, RME supports multiple users connected from any part of the network. The web-based infrastructure permits concurrent access to tools for managing networks, applications and services, operators, administrators, technicians, Hel Desk personnel, IS administrators, and final users.

4.4 RME allows network administrators to see and update the status and configuration of all Cisco devices from any point of the network, through a standard browser that acts as RME client. RME maintains a database with updated network information. It can generate a large variety of reports that can be used for capacity planning and diagnosis.

4.5 Although devices are added to the RME inventory at application startup, the administrator can program the exploration and periodic update of the information on devices to make sure that the information stored is the latest. Additionally, RME automatically records any changes made to network devices, facilitating the task of identifying changes and the person responsible for them.

4.6 RME applications provide monitoring and control of network failures, as well as practical tools for managing software images and router and switch configurations. RME applications, together with the links to Cisco.com services and support, automate software maintenance to facilitate network control and support.

Characteristics

4.7 RME works in conjunction with the CW server, which contains a set of administration services shared by multiple management applications. These management services are enabled when a suite is installed and an application that depends on any of these services is opened.

4.8 If a particular suite of applications does not use a service or does not use it to its fullest, this service might not appear on the CW Desktop.

4.9 RME uses the following CW services:

4.9.1 Database engine and utilities

4.9.2 Desktop for login and launching of applications

4.9.3 Event management

4.9.4 On-line help system

4.9.5 Job management

4.9.6 Process management

4.9.7 Security

4.9.8 Web server

RME components

4.10 The RME web-based infrastructure is made up by the following components:

4.10.1 *CiscoWorks Server*: RME depends on CW for common functions, such as the database engine, on-line help, security, login, launching of applications, job and process management, and the web server. It provides a common framework and interface for all CiscoWorks products. The CW server must remain constantly on line to probe devices, monitor events, and carry out the programmed data collection. If the server fails, the flow of information received and stored by RME will be interrupted.

4.10.2 *RME Database and Functions*: RME stores all critical network management information on a central database, including the inventory of devices, software images, configuration files, syslog messages, and a record of changes. RME functions interact with the database and with the network devices to collect information, display reports, and automate many repetitive jobs. Many RME functions can be configured so as to periodically probe devices and automatically update the database. RME uses common protocols such as SNMP, Telnet, TFTP, and RCP to access devices and retrieve configuration files and images.

4.10.3 *Cisco.com*: RME also connects to the Cisco.com system to obtain product updates and technical assistance information. Access to Cisco.com is not mandatory for RME, but it increases its capabilities. Software Management functions require access to Cisco.com.

Applications and Jobs

4.11 A large variety of jobs can be executed with the following applications supplied by RME:

4.11.1 Device Views

4.11.2 Change Audit

4.11.3 Configuration Management

4.11.4 Inventory

4.11.4 Job Approval

4.11.5 Software Management

4.11.6 AnálisSyslog Analysis

Views

4.12 RME provides device views—logical groupings used for specifying a device or group of devices. Views can be defined in order to group selected devices in a logical group.

4.13 For example, a device view quickly displays reports concerning devices of a certain type, or with specific characteristics, such as Catalyst switches, or devices under the responsibility of an operator.

4.14 Since almost all RME jobs require a definition of the set of devices on which they must be executed, views provide a convenient way of creating groups of devices. For example, before displaying an inventory report, the devices to be included in the report must be selected, and views can expedite this selection (instead of executing the report for each device). The performance of the RME graphic user interface (GUI) may be affected if the number of selected devices in the view is too large. The inclusion of "all devices" in the view must be avoided when the number of inventory devices is too large. It is better to use system views, or to create custom views to keep the number of devices in the views at a manageable level.

Types of Views

4.15 There are three categories of device views:

4.15.1 *System Views*: They are predefined and are immediately available after RME installation. They include most of the families of Cisco devices.

4.15.2 *Custom Views*: They are defined by users, and can be used by all the other users with access to the server.

4.15.3 P*rivateViews*: They are defined by users, but can only be used by the user that created them.

4.16 Furthermore, two different types of views can be created within the category of custom or private views:

4.16.1 *Dynamic Views*: These are logical groupings based on device attributes, such as class of device or software version. Devices in a dynamic view can change based on the value of the attributes in the inventory. For example, a dynamic view can include all devices with IOS version 12.0. All system views are dynamic.

4.16.2 *Static Views*: These are logical groupings based on user-defined characteristics. They include any device that is desired in the view. Group members do not change, unless devices are added or removed. Static views must be used when automatic changes in membership are not desired.

Change Audits

4.17 Change audit applications track and report changes in the network. They enable other applications to log information about changes in a central repository.

4.18 Inventory changes include any modification made to information on devices, such as chassis, interfaces, and system information, stored in the inventory database.

4.19 Software changes include updates to new software images.

4.20 Configuration changes include all modifications made to device configuration files, whether made using RME functionality or not.

4.21 Changes sent by configuration and software administrators cannot be filtered. Change logs can be displayed, and specific searches made by type, characteristic or time. The deletion of old change logs can be programmed.

4.22 It can also be configured to send change logs in the form of SNMP traps to remote servers in order to monitor and display changes from remote network management stations with event collection capabilities.

4.23 Logs are stored in the RME database until deleted, and continuous maintenance is required in order to delete old records from the database.

Configuration Management

4.24 The Configuration Management application stores the configuration files (the current one and a specified number of previous versions) of all Cisco devices contained in the inventory.

4.25 It also tracks changes and automatically updates the database. Sometimes, changes in the configuration of a device may lead to network performance failures or problems. Configuration Management helps to simplify and automate repetitive time-consuming jobs.

4.26 When a change is made to the configuration of a device, an automatic event is generated in the archive that keeps the latest configuration file.

4.27 For example, to improve NetConfig performance, Telnet could be used to download the configurations to the device and TFTP to explore the configurations.

4.28 The protocols used to download configurations are Telnet and SSH (in that order, although it can be changed).

4.29 The protocols used to browse configurations are: TFTP, Telnet, RCP, and SSH (in that order, although it can be changed).

4.29.1 Check device requirements to make sure RME can communicate with the devices.

4.29.2 Create approver lists (if prior approval of configuration changes is required) and define Configuration Archive preferences (update programming, number of copies kept, etc.).

4.29.3 Use the Configuration Archive to display device configurations and to identify/plan the necessary changes. Then, NetConfig and Config Editor applications can be used to implement and confirm the changes.

4.29.4 As a matter of continuous maintenance, check the Configuration Sync report to make sure that all running and startup configurations are the same for all devices.

4.30 The network administrator can use the Network Show commands and custom reports for diagnosing problems and collecting information.

Inventory

4.31 Networks are a combination of heterogeneous, geographically-scattered systems. Keeping inventory control of hardware and software assets is a critical task. Furthermore, most RME jobs are executed on device sets; consequently, the RME database must contain precise information on the devices.

4.32 The Inventory Manager is responsible for keeping the inventory. Since RME uses different management services to collect information on the devices (SNMP, TFTP, Telnet, RCP), each device contained in the database (inventory) must include management service (community chain, passwords) parameters (attributes). When this information exists in the inventory, it is considered that the device is an RME-managed object.

4.33 In other words, if the RME does not have information on the attributes, this device will not be under RME control. RME does not discover network devices on its own; they must be added manually or imported into the inventory database.

4.34 In order to simplify the process of populating the inventory database, information on the devices must be imported from a text-formatted file.

Software Management

4.35 The Software Management application automates the steps associated to the planning, programming, and downloading of software images, and the monitoring of the network.

4.36 It provides tools for storing backup copies of all images that run on network devices. It can also store additional copies if so desired, and plan and perform upgrades on several devices concurrently.

4.37 The application can check devices and software images for compatibility, and make recommendations prior to an upgrade. Software Management reports permit control over all network version upgrades.

4.38 Images must be imported to RME in order to be kept in the Software Image Library. Initially, images can be imported from the network devices themselves (or from another source) in order to create a base backup copy of all devices.

4.39 Furthermore, after import, Software Management can be configured to probe network devices in order to generate reports on the images running on the network that are not stored in the RME database.

Syslog Analysis

4.40 With the Syslog Analysis application, events can be recorded centrally and system error messages from Cisco devices can be controlled. Error messages are used to check device and network performance.

4.41 A maximum of 1 million messages can be stored for up to 14 days.

4.42 Purged messages can be backed up in a specified location (CSV format). The size of the backup file can be specified, as well as an e-mail address for receiving a warning if the backup exceeds the selected size.

4.43 Messages received by the RME server are periodically read (every 30 seconds) by the analysis process [Syslog Analyzer], where user-defined filters are applied and results are stored in the RME Syslog message database, and they remain available for reporting and initiating user-defined scripts.