

Aspire IP Requirements

1 Introduction

The purpose of this document is to outline performance and voice quality issues that need to be addressed for a successful implementation of VoIP on a converged IP network. In order to provide satisfactory voice quality, it is necessary to overcome the challenges of sending voice packets over a network designed for computers.

This document will present facts about the use of VoIP with the NEC Aspire telephone system. It will discuss network objectives to be met to achieve quality voice transmission and the requirements to meet these objectives.

Please note that if your network does not meet the minimum requirements below after VoIP is implemented, telephone calls across the network may experience poor voice quality or call connection and disconnect problems.

NEC will make every effort to assist and advise what measures should be taken to bring your network up to the minimum requirements. However, any network problem, lost IP calls or voice quality issues are not the responsibility of NEC.

This document describes “best practices” for providing quality voice over an IP network as recognized at the time of writing. Every effort has been made to ensure that the recommendations are up to date and accurate.

2 Transmission requirements

The most critical factors affecting the quality of voice transmission are delay, packet jitter and packet loss. These are packet transmission parameters that can be measured.

2.1 Packet Delay or Latency

Recommended Packet Delay is 80 milliseconds (ms) or less one way for toll quality voice

Required end-to-end Packet Delay is 150 ms or less.

2.2 Packet Jitter

Packet jitter is a measure of the variation in the delay between endpoints.

Suggested average Packet Jitter should be less than 20 milliseconds.

Required packet jitter is 50 ms or less.

2.3 Network Packet Loss

The maximum packet loss between endpoints

Desirable Packet Loss is 1% or less.

Required network Packet Loss is 2% or less.

2.4 Bandwidth Utilization

Bandwidth Utilization is the amount of available bandwidth used expressed as a percentage

Required combined Bandwidth Utilization for voice and data packets should not exceed 70% of available bandwidth.

This is to allow for control signals (that run in the background) and spikes in data traffic. Note that all segments of your network may not have the same bandwidth available so utilization measurements must be made for each segment.

3 Network Requirements

The following must be provided to meet the packet transmission requirements listed above.

3.1 Quality of Service (QoS)

QoS MUST be provided to insure timely delivery of voice packets.

On a converged network, where voice must share the network with data (where voice and data are competing for the same transmission resources), there can be no assurance of quality voice transmission without QoS.

3.2 Switched Network

A switched Local Area Network is required to avoid packet collisions on the Local Area Network. A hub based shared network is not acceptable for voice transmission.

Old style shared networks, networks using hubs, had a single transmission path that was shared by all terminals and hosts on the same section or collision domain. It was called a collision domain because collisions were inevitable. The access method used was “Carrier Sense, Multiple Access/Collision Detection” (CSMA/CD). The terminal that grabbed the transmission path first, controlled it. That is in fact no control.

A fully switched LAN network is a network where LAN switches are used instead of hubs. Switches split the LAN into very small segment to provide better bandwidth access for every endpoint on the LAN.

For optimum operations, the switch ports (and the connected devices) should be set to 100 Mbps and full duplex. These parameters should be set as “fixed” because speed detection errors can block communications. Connection speed auto-detection or negotiation should be turned off.

The LAN switch used should support IEEE 802.1p/Q. The VLAN portion of this protocol need not be implemented initially but may be used if LAN congestion is encountered.

An Aspire circuit card (SHUBU) is available with a limited number of switched ports for IP telephones. NEC BlueFire 200/24 switches are another excellent way of building a switched network. Both of these switch units are able to send power to IP telephones over the same cable used for voice. (see PoE discussion)

3.3 LAN Network Speed (Bandwidth)

The LAN speed MUST be 100 Mbps (not 10 Mbps) fixed.

You should force all devices (IP telephone sets, NTCPU, VoIP card and LAN switches) to 100Mbps full duplex, so there are no auto-negotiation issues.

It is permissible to use 10 Mbps in last section of a switched network containing only one IP telephone and one PC.

3.4 Virtual Private Network (VPN)

A Virtual Private Network MUST be employed when using public networks.

A Virtual Private Network provides a way for voice packets to pass through firewalls and routers without compromising the security of your network. To keep packet latency to a minimum, VPN encryption should be done with hardware and not software.

A Virtual Private Network (VPN) is not required for private networks that don't require a firewall. If a router is used for handling voice and data traffic to multiple sites, NAT must be disabled to allow voice traffic to pass through the router.

4 Recommendations to Ensure Quality Voice

4.1 Site Survey

It is strongly recommended that a Site Survey be conducted to evaluate your network's ability to support VoIP. You won't know if the network will support Voice over IP unless a survey is made. Professional help is available to make such surveys.

A site survey is a snapshot in time. The results are valid only until something changes on the network. Sometimes little things can have a large impact on the health of the network; new software, new network

equipment, adding employees or telephones. It is necessary to constantly monitor the network to ensure conditions do not change and negatively impact voice quality.

4.2 Codec (voice compression) Selection

It is recommended that G.729 codec (with 8 K bandwidth for one way voice signal) if the voice signal must travel over a WAN.

Use G.711 (with 64 K bandwidth for one way voice signal) local LAN based networks.

4.3 PoE

Recommend providing power to the telephones from LAN switch with PoE.

The Aspire SHUBU circuit card and BlueFire switches are capable of providing power to Aspire telephones. The power from a BlueFire switch is not currently compliant with IEEE 802.3af so other devices may require an In Line Power Adapter (ILPA) to receive power from these devices.

4.4 Emergency Power

Unlike traditional telephones, VoIP will not work when local power goes out. It is recommended that Battery backup or UPS be installed to provide power to the telephone system and all components of the network.

4.5 Router Selection

Some routers claim to support QoS but either they do not support it at all or they do a poor job of supporting it. This poor support may be due to lack of queuing configuration. Some routers provide only Weighted Fair Queuing (WFG) and do not have any other options. Some do not allow the user to adjust the bandwidth allocation.

The number of queues provided and the queue size is also important. Experience in the field indicates that 16 Meg of buffer memory is adequate. The router must have at least 2 queues to provide QoS. Most routers will provide 4 queues for QoS packet handling.

5 For Your Information

The following are things about VoIP implementation and usage that you need to be aware of.

5.1 Good Data Network Implementation

A data network that is functioning without problems is no guarantee that the network will support VoIP. You should perform a network survey to determine the current network condition. Then factor in the traffic that will be added by a VoIP installation to determine if the network will meet the network transmission requirements.

5.2 IP Network Voice Quality

– no guarantees

There are basic differences in the operation of traditional telephone networks and IP networks that have a bearing on the quality of the voice transmission. The purpose of the requirements and recommendations in this document should be followed to assure acceptable voice quality. However, the nature of IP networks is such that they cannot guarantee good voice quality 100 % of the time. There may be times when the IP voice quality is not acceptable to you.

5.3 Using the Internet Is a Challenge

The external network (WAN) must be managed to ensure delivery of voice packets. Standard Internet service is not a managed network and does not provide any QoS or guarantee bandwidth or delay. There are no assurances that it can deliver quality voice. QoS is recommended from end to end across the entire network to assure voice quality.

The same (single) connection to the Internet should not be used for both voice and World Wide Web access. To use both VoIP and web access simultaneously, install 2 connections to your ISP, 2 IP Addresses and 2 routers.

5.4 Echo May be a Problem

It is not uncommon for VoIP networks to experience echo. Some echo is present in standard telephone networks but is not a problem because there is no delay. In an IP network where transmission delays are common, the delay is significant and the echo becomes more noticeable. A change of hardware may be required to address this problem.

5.5 E911 Issues

Be aware of location identification problems with an IP implementation. When a 911 call is placed from a standard telephone, the location of the telephone is known. This is not true for an IP telephone. In theory, an IP telephone can plug into a network anywhere. That IP telephone can then connect to a PBX and call 911. There is currently no way to know where that IP telephone is located. If an IP telephone is always used from the same place, such as an employee working from home, the location information can be provided to the local public safety organization.

There are also power failure issues that must be addressed. When using IP telephones at the main site, always have battery backup (UPS). It is also a good idea to also have analog telephones strategically located so they can be used to call 911 in an emergency.

5.6 Voice Transcoding

Each time the voice signal is converted from analog to digital and back again, some fidelity is lost. The distortion added is usually not noticeable. Voice compression and decompression adds a little more distortion. Multiple encoding and decoding of voice signals can cause quality problems. If a telephone call must pass through multiple telephone systems there is a possibility that the signal will be encoded and decoded several times. This will result in poor quality. Voice Mail can also be a cause of transcoding distortion.

The network should be designed to avoid multiple encode, compress, decompress and decode cycles. There may be cases where multiple voice processing steps cannot be avoided and distortion will be encountered.

5.7 Reliability

We have all become accustomed to telephone service that is very reliable. VoIP is a relatively new technology and cannot provide the same level of reliability

Computers and computer networks have a history of reliability problems. For a variety of reasons, it is not uncommon to have a local network or wide area network to experience service interruptions. Even minor interruptions can cause telephone calls to be disconnected.

5.8 Security Issues

It is important that the network maintain a high level of security to protect it from hackers and virus. This is important for the IP telephone system as well as for your data network.

It is not likely that a virus will attack the telephone system but a virus could generate a great deal of traffic on the network, which would cause poor voice quality.

Hackers may try to access the telephone system to make telephone calls or to listen to telephone calls.

For these reasons, the IP ports of the telephone system should never be connected to the DMZ of the router. That would bypass the firewall and allow the outside world to access the telephone system IP port.

5.9 Be Aware of Aspire Configuration Limits

Do not install more equipment than the Aspire system is capable of supporting.

For example, the system cannot support more than 50 external IP locations (nodes) for voice. The system programming cannot accept more than 50 IP addresses. In IP networks with more than 50 nodes, it is possible to install a VoIP gatekeeper and route all voice calls to the gatekeeper.

Note that the number of Aspire systems connected together should not exceed 50 remote sites; otherwise the “Networking features” (feature transparency) will be lost.

Note that the selection of compression of each terminal may limit the usable ports on the Aspire gateway card. For example, the Aspire 32 port gateway card will support only 12 telephones that use G.711 64k compression.

It is recommended that the entire Aspire manual be read.

6 Discussion of Requirements

The following is a discussion of the requirements, recommendations and items listed above.

IP telephony is different than traditional telephony; different technology, different requirements and sometimes different results in a given situation. Using IP telephony, or VoIP, means adding telephone call traffic to your data network, combining the signals. This is referred to as convergence

For the successful implementation of VoIP, it is important to understand the issues (both positive and negative) that impact a VoIP network.

There are many factors influencing voice quality on an IP network (any one of which can degrade voice quality). There is no single thing that can be done to ensure good quality. For example, increasing the speed on the LAN will provide more bandwidth but it does not address how packets will be handled when congestion occurs.

6.1 Voice Networks and Data Networks are different

The objective of convergence is to move voice signals from the telephone network to a data (IP based) network. There are huge differences in these two networks, physically different, different modes of operation and different philosophy.

The Telephone Network

- Destination address sent only once during call setup
- A fixed path with dedicated bandwidth is setup from source to destination
- Only handles a fixed number of calls
- Traffic is not allowed to exceed capacity so services not degraded.
- Reliable real-time communications
- No need to retransmit signals

The Data Network

- Destination and source address must be included in every packet

- Able to take any path through a network of connections
- Scales – continues to accept packets during traffic overload. No access control.
- Service degrades (packets delayed or lost) as traffic increases
- Transmission protocols designed to send packets over an unreliable network. Best effort transmission
- Retransmits packets if lost or corrupted

6.2 Voice and Data Have Different Packet Handling Requirements

Voice data packets will require special handling to ensure the service quality meets user expectations.

The philosophy of data and voice packet transmission is very different.

Data Packets

- Not time sensitive. Tolerates delay (usually)
- Cannot tolerate loss of one packet or even one bit. Requires reliable transmission. Packet retransmitted if not acknowledged. Retransmitted messages add to data traffic.
- Data transmission is random and bursty. It is Unpredictable.
- Data packet size varies from very small to very large.
- Data transmission is asymmetrical, not the same in both directions.

Voice Packets

- Time sensitive. Requires timely delivery of packets.
- Can tolerate occasional packet loss. The ear cannot detect a single lost packet. Some Codecs able to compensate for lost packets.
- Regular transmission Consistent time interval for transmission of each packet.
- Each packet is the same size. Constant flow at given intervals. It is predictable.
- Voice transmission is symmetrical, the same in both directions

6.3 Voice and Data Packets Are Handled Differently

Different protocols are used for the transporting voice and data packets

Network protocol for data packets

- Uses connection-based transmission. Receiver acknowledges each packet sent. Acknowledge messages add to the network traffic.
- Uses TCP (connection based) protocol with time stamp, sequence numbers and error checking. Supports retransmission of lost or erroneous packets.

Network protocol for voice packets

- Uses UDP (connectionless) protocol with smaller packet header for efficient transmission. Does not support retransmission.
- Real Time Protocol (RTP) adds time stamp and sequence numbers not provided in UDP packet.

Data packets are transported on a “Best Effort” basis. As traffic is increased, packets contend for limited bandwidth. This causes traffic to slow down. It can cause packets to be lost or discarded. Lost packets or packets with errors are retransmitted creating additional traffic. Computer applications such as file transfer or e-mail can tolerate these conditions. It does not matter to a user if it takes a couple seconds longer to receive an e-mail.

On the other hand, voice quality depends on timely delivery of voice data. Most of the problems with voice quality are the result of packet delay or packet loss. There isn’t sufficient time to retransmit. If a packet doesn’t arrive on time, it is discarded. There’s no second chance to get it right.

From this it can be seen that voice packets will require special handling. Data packets can wait for service, but voice packets cannot wait.

7 Causes of Poor Voice Quality (Delay, Jitter and Packet Loss)

7.1 Congestion

Congestion is not listed above but it causes these conditions. Congestion is a concept and cannot be directly measured which may be why it is not discussed in technical papers about VoIP issues.

Congestion is usually thought of as heavy traffic or heavy usage. This kind of traffic can be addressed by adding bandwidth to the network. However, all network problems are NOT be solved by throwing bandwidth at them.

Network congestion also occurs at points where multiple channels are funneled into a single channel such as at a data switch. When two packets arrive at the same time, one must wait while the other is sent to the exit channel. It is desirable that some type of QoS be used to determine which packet should be sent first.

Congestion also occurs where a transition from a high speed to a low speed occurs such as at a router. A typical example is a 100 MHz LAN connected to a T1 line with only 1.5 MHz of bandwidth. Multiple packets can arrive on the faster high speed channel while one packet is sent on the slow channel. Here again, QoS needs to be employed so that voice packets will receive priority service.

7.2 Packet Delay

Packet delay is enemy number one of voice quality. Delay causes packets to be lost. If a packet does not arrive in time to be replayed at the receiving end, the packet is dropped.

Packet delay (latency) causes delays in a conversation. Delay does not distort the voice signal but delay can be very annoying, making normal conversation difficult for the speakers. The parties may start to talk at the same time or interrupt each other. As a result, the conversational quality is perceived as being poor.

Packet delay has an impact on all the other voice quality parameters. It is variations in delay that cause jitter. Packet delay makes echo objectionable. Levels of echo that would be acceptable in traditional telephones cause problems because of the increased delay.

As mentioned above, voice packets do not tolerate excessive delay and require special handling.

7.2.1 Packet Delay explained

Packet Delay is the time it takes for a packet to travel from sender's application to receiving application. The term "packet delay" usually refers to the delay in a section of the network while the end-to-end delay (from the mouth of the speaker to the ear of the listener) is called Latency.

There are 4 components of delay

- Voice collection time (sampling time)
 - This is the time it takes to collect the voice data to be placed in a packet. The packet cannot be sent until the voice data for each packet is collected. This is determined by the packet size setting, which is usually 10, 20 or 30 milliseconds.
- Voice Packet processing - Can take up to 75 milliseconds
 - Packet assembly / disassembly
 - Packet compression / decompression
 - Packet encryption / decryption
 - Packet encapsulation
 - Packet tagging (CoS)
- Propagation delay
 - Time it takes a packet to travel from source to destination
- Queuing delay – when 2 or more packets arrive at a switch or router in a network, they are placed in a queue to wait for processing.
 - Time spent waiting to be processed or transmitted
 - Layer 2 queues (LAN switches)
 - Layer 3 queues (routers and WAN switches)
 - Jitter buffer (a queue to compensate for packet jitter)

The ITU G.114 standard recommends that the delay be 150 ms or less for "good" quality voice.

It is impossible to eliminate all delay. Processing requires time and additional time is required to move the packet from place to place. Just these components of delay consume a considerable portion of the available "delay budget." Because of the limited "delay budget," it is important that measures are taken to reduce collisions, contention, congestion and queuing of voice packets. Only by taking such measures can you ensure an acceptable level of voice quality. Voice packets are special and require special treatment.

7.3 Packet Jitter

You may take the same route to work each day, but it doesn't always require the same time to get there due to traffic lights, stop signs, school buses, accidents, etc.

Jitter is the variation in inter-packet arrival time. Packets can take different times to travel the same route. Network causes of packet jitter are congestion, lack of bandwidth, varying packet size and routing changes (taking a different route due to congestion).

Packet jitter can cause voice audio to be choppy. Excess packet jitter can cause packet loss.

To compensate for packet jitter on the network, a jitter buffer is added at the receiving end where packets are stored for some short time to allow for the next packet to be received. Some packet jitter will always be present and a jitter buffer can compensate for this. Other documents have called this a de-jitter buffer because it's purpose is to remove jitter from the voice playback.

Most VoIP equipment today has dynamic jitter buffers. These compare the receive time with the send time stamp in the RTP header to calculate the jitter and automatically adjust the jitter buffer size. The installer has little control of the jitter buffer size and can only set the minimum and maximum size. The maximum jitter buffer size should be at least 2 times the voice sample collection time. When setting this, remember that the jitter buffer size directly affects the latency experienced by the user.

However, a jitter buffer cannot solve the problem of excessive packet jitter. Solutions for excessive packet jitter must be made in the network to reduce congestion and queuing time for voice packets.

7.4 Packet Loss

Causes of packet loss

- Overloaded queues in network routers – a packet is discarded if the queues are full when it arrives
- Overloaded jitter buffer – a packet is discarded if the jitter buffer is full when it arrives
- Excessive network delays – a packet is discarded if it arrives too late to be replayed
- Packets can be discarded if the subscribed CIR (Committed Information Rate) is exceeded.

Moderate loss of packets will not harm voice quality. However, the loss of several continuous packets will cause noticeable voice disruptions.

For voice, there is no time to retransmit lost packets. You have to get it right the first time.

7.5 Echo

Some echo is present on normal telephone calls but it is not perceived as a problem because there is no delay. The telephone industry calls this “sidetone” and convinced everyone it is a good thing. It gives users a sense that the telephone is working properly.

In the IP network, with delays due to the processing and transmission, echo becomes a serious problem.

There are two types of echo.

- Network induced echo
 - This is caused by a circuit mismatch, which causes some of the voice energy to be reflected back to the sender.

- Acoustically induced echo
 - This is caused by physical reflection of sound waves back to the sender. This can be audio coupling between transmitter and receiver of a handset or speakerphone.

Typically, one party of a conversation and not the other will hear echo. Analog trunks to the public telephone network are a common cause of circuit mismatch echo. Changing from analog trunks to digital trunks will usually eliminate this source of echo.

Echo canceling circuits in the endpoints usually do a good job of removing echo. It may take a short time for the echo canceling circuit to adjust for the delay of the echo. These circuits do not work in situations where there are significant variations in the packet jitter.

8 Addressing Voice Quality Issues

Congestion and Delay is the major causes of poor voice quality. Congestion and Delay can cause voice packets to be lost. Variations in delay cause packet jitter. The most important thing that can be done to ensure voice quality in a converged network is to reduce congestion and delay.

To minimize congestion and delay

- Provide sufficient bandwidth on both LAN and WAN
- Make smart use of bandwidth. Improve utilization of available bandwidth
- Use QoS to provide priority queuing for voice packets
- Replace all hubs on the LAN with Layer 2 switches to eliminate collisions and improve transmission efficiency

8.1 Addressing Delay

8.1.1 Bandwidth

Bandwidth is like money because you never have enough. On the other hand, bandwidth costs money so you want to use it efficiently.

Providing sufficient bandwidth to carry both voice and data traffic is the first step in providing quality voice.

The combined expected bandwidth of voice and data should not exceed 70 per cent of the available bandwidth. This is to allow for network broadcasts and control signals plus a cushion for bursts of data traffic. The traffic cannot be accurately predicted and has peaks and valleys. Having that little extra bandwidth at such times will make it less likely that voice traffic will be adversely affected.

Most LAN equipment now supports 100 MHz bandwidth and all NIC cards, switches and routers should be 100 MHz.

8.1.2 Bandwidth Usage

More efficient use of existing bandwidth is achieved by compressing data before it is sent. This is already done with data by putting it in ZIP files or using JPEG for pictures. There are also compression options available for voice data.

There are tradeoffs to be made in using data. Compressed data does use less bandwidth. However, the more a voice signal is compressed, the more difficult it becomes to restore it to its original form. Some fidelity is lost.

Another issue to consider when employing compression is latency. It takes time to compress and decompress the voice signal. This adds to the packet delay.

Compression options for voice:

- G.711 uses 64K bps bandwidth one-way. This is actually no compression. It uses the same digital signals as that used on traditional telephone systems (PCM).
- G.729 uses CELP (Code Excited Linear Prediction) encoding with 8K bps bandwidth one way.
- G723.1 uses MP-MLQ (Multi Pulse – Multi Level Quantization) encoding with 6.3K bps bandwidth one way.

See the table for the resulting bandwidth that can be produced by these codecs.

8.1.3 Packet Stuffing

Packet Stuffing is adding more voice data to each packet

In addition to compression to improve bandwidth efficiency, more voice data can be placed in each packet. This is because each packet has fixed number of bytes for addressing and control. These are referred to as the packet overhead. By putting more data in each packet, the fewer packets it takes to send a given amount of data. Fewer packets mean fewer overhead bytes to consume bandwidth.

IMPACT OF VOICE COLLECTION TIME ON BANDWIDTH AND LATENCY

Codec Type	Voice Collection Time	Packets Per Sec	Header Bytes	Voice Bytes	Layer 2 Bytes	One-Way Voice Bandwidth	Voice Processing Latency
G.711	20 ms	50 packets	40 Bytes	160 Bytes	26 Bytes	94.6 K bps	10 ms
G.711	30 ms	34 packets	40 Bytes	240 Bytes	26 Bytes	85.5 K bps	20 ms
G.729	20 ms	50 packets	40 Bytes	20 Bytes	26 Bytes	35.7 K bps	25 ms
G.729	30 ms	34 packets	40 Bytes	30 Bytes	26 Bytes	26.6 K bps	35 ms
G.729	40 ms	25 packets	40 Bytes	40 Bytes	26 Bytes	22.0 K bps	45 ms

*** Calculations for one way voice only with no control signaling. Must add 16 K bps per telephone for controls.

Adding more data to each packet also has tradeoffs and limitations. Adding more voice data to each packet increases the data collection time and thus increases the latency. The loss of a large voice packet has more of an impact on voice quality than the loss of a smaller packet. Usually, 20 or 30 milliseconds of voice signal are placed in each voice packet.

Aspire Note - the selection of compression of each terminal may limit the usable ports on the Aspire gateway card. For example, the Aspire 32 port gateway card will support only 12 telephones that use G.711 64k compression.

8.2 Using QoS to Assure Voice Quality

Voice packets cannot tolerate delays and need priority handling. This means that if there is a voice packet and a data packet in a router waiting to be sent, the voice packet will be sent first. In order to do this, Quality of Service (QoS) must be used. Quality of Service has two parts.

8.2.1 QoS and CoS

CoS is a way of marking (tagging) packets to identify a level of handling requirements. The Layer 3 header uses 3 bits in the Type of Service (TOS) Byte. For Layer 2, the VLAN tag has 3 bits for CoS (which is referred to as priority).

QoS is the ability to recognize a packet's special handling requirements and to provide the level of service required. The purpose of QoS is to ensure that time sensitive applications such as voice do not experience excessive delays during peak traffic.

Providing QoS is a 2-stage process.

- Network device (terminal or telephone) must mark priority of packets
- Packet handling devices (LAN switches and routers) must be able to recognize marked packets and provide the priority handling as required.

Standards used to mark packets for QoS are:

- IEEE 802.1p (layer 2 switches)
- DiffServ (Differentiated Service, layer 3 routers and switches)
- DSCP (Differentiated Service Code Point, layer 3 routers and switches)

8.2.2 Protocols for Providing CoS

IEEE 802.1p – layer 2 protocol

IEEE 802.1p provides a way to “tag” (mark) packets with a Class of Service designation before they are sent across the network. This enables network equipment to recognize high priority packets, such as voice packets, and send them first. There are 8 levels of “user priority” values (0 through 7). Class 7 is the highest level and it is reserved for network signals. Classes 5 and 6 are used for time sensitive packets such as voice.

DiffServ – an OSI layer 3 packet marking protocol

DiffServ (Differentiated Service) provides “forwarding class” information used by network devices for processing packets. DiffServ is usually implemented by WAN access devices and supported (on the backbone) by DiffServ compatible routers. This used to be called Precedence. An expanded version DiffServ that uses a 7-bit code is called Differentiated Serve Code Point (DSCP).

Packets are divided into “forwarding classes” identified by bits in the header called DiffServ Code Points (DSCP). Routers and gateways use this information to differentiate packet treatment.

QoS should be implemented even if bandwidth is abundant. It is difficult to predict traffic patterns on a network.

8.2.3 Queues and Queuing (What’s in a queue)

When a packet reaches a device and it cannot be served immediately, it is placed in a queue (a line) until service can be provided. In a device that supports QoS there are usually 3 or 4 queues for holding such packets. Each queue is for packets of a different CoS.

This is like the toll plaza on a highway (Garden State Parkway). Some lanes are for normal traffic. There are express lanes for “Easy-Pass” and there emergency lanes for police and ambulances. The speed that you get through the toll plaza depends on your class of service.

The way that packets are removed from these queues is as important as having multiple queues. There are several queue handling methods.

- Weighted Fair Queuing (WFC) – one packet is taken from each queue in round-robin fashion. It allots equal bandwidth to each queue.
- Custom Queuing (CQ) – can be configured to provide a percentage of available bandwidth to each queue (each class)
- Priority Queuing (PQ) – has 4 queues. Packets in the highest priority queue are serviced until the queue is empty.
- Class Based Weighted Fare Queuing (CBWFG) – Allows more flexibility for defining classes and allows definition of bandwidth allotted to each class. (BlueFire switches support CB-WFQ).

- Low Latency Queuing (LLQ) – A combination of PQ and CBWFQ creates a strict priority queue within CBWFQ for delay sensitive packets such as voice. This queue is managed so packets in other queues are not totally blocked by the priority traffic.

With no QoS, all packets are placed in a single queue and processed in the order in which they were received. This is called First In First Out (FIFO).

8.2.4 QoS without CoS

It is possible to configure routers or switches to prioritize packets based on a packet type or destination address. So, it is possible to prioritize packets with the IP address of the telephone system or UDP or RTP type packets.

For example, some routers have an option for “IP RTP Priority” which creates a strict-priority queue for RTP packet flows belonging to a range of UDP destination addresses. All RTP packets having a destination address in the designated range will be placed in this queue. Packets placed in this queue will be sent before any other queues are serviced. This type queuing must be used with care. If voice traffic (RTP packets) volume is high, it can block all other packets. If the packets with telephone controls are blocked, calls may be dropped. It is better to use Low Level Queuing limiting voice packets to 80% of bandwidth but this is more difficult to set up.

8.3 The case for a switched LAN

Layer 2 switches must be used on the LAN to isolating terminals and provide QoS. In a layer 2 switch configuration, each terminal has its own isolated section of the network. A switch separates traffic and removes contention.

8.3.1 Hubs and Switches in the LAN

A network cannot be constructed by connecting devices together with plain wire. It's possible to do this with analog telephones, but not a data network. Devices on the network transmit on one pair of wires and receive on another pair of wires. A device is needed to take what a device send on its transmit wires and send it to the other devices on their receive wires. Devices that do this are hubs or switches. A Local Area Network can be constructed using either hubs or Layer 2 switches.

A hub is a passive device. It has no intelligence. It simply repeats everything gets on the transmit wires of a connected device and sends (retransmits) it to the receive wires of all connected devices. It is even sent back to the device that sent the packet. This is why full duplex communication is not possible on a LAN constructed using hubs.

On the other hand, a switch is an intelligent device. When a packet is received, the Layer 2 destination address is examined and compared with a lookup table (SAT – Source Address Table). When a match is found, the packet is retransmitted to the port that goes to that address. The packet is only retransmitted on the

port that goes to the destination address. The switch is able to transmit and receive on multiple ports simultaneously.

A switch can also provide QoS. Because a switch can receive packets simultaneously from multiple devices, it is possible to receive multiple packets destined for the router. They cannot all be sent at once and are buffered until they can be sent. QoS can be used to determine the order in which these stored packets are sent to the router. Some switches can be programmed to add CoS tags to packets for use by other devices.

8.3.2 Advantages of a switched LAN

Provides Quality of Service (QoS) within the LAN – able to provide priority service to voice packets. This is the primary reason for using switched networks.

Dedicated Collision Domain – each port on a switch is its own domain. This increases the effective bandwidth of the LAN. There can be no collisions when only a single device is connected to a port.

Traffic Filtering – a switch will only forward packets to the port where the destination resides. This reduces the unnecessary traffic and improves bandwidth efficiency and utilization.

Full Duplex (option) – because collisions are eliminated, data can be sent full duplex (both ways at the same time). The use of full duplex increases bandwidth efficiency.

Power distribution and backup – Using a Layer 2 Switch that provides power avoids the use of power bricks at each terminal and is also convenient for connecting to a central backup power source (UPS).

Port security – can be configured to add security to protect the network and terminals from tampering by unauthorized users. (VLAN, IEEE 802.1X)

8.3.3 LAN Layer 2 Switch Protocols

With the introduction of LAN switching, standards were needed for the special requirements of packet handling in a switched network. Two protocols were introduced to address these. A 4 Byte “tag” was added to the layer 2 (MAC) header for priority (CoS) and VLAN identification.

802.1p – is a standard for layer 2 CoS/QoS. Three bits of the layer 2 tag are used to provide 8 classes of service marks. This is sometimes referred to as VLAN Priority. A LAN switch may be configured to use these marks or use something else such as packet protocol type or destination address to provide QoS.

802.1Q – is the VLAN protocol. This provides a virtual LAN or logical subnet using LAN switched filtering. It reduces traffic on a switched section of the LAN by filtering (blocking) packets and broadcast messages from terminals on other VLANs. VLAN uses 12 bits of the 4 Byte tag as a VLAN Identifier. A LAN switch can be configured to ignore the VLAN ID, add it, strip it off or filter a packet based on it.

8.3.4 Delay on a Switched LAN

If voice packets experience any delay on a Switched LAN, it is usually because the QoS of the switches has not been configured properly.

9 VPN is Required for VoIP on Public Networks

A VPN is required so that VoIP communication can pass through NAT firewalls and routers connected to a public network. All VoIP (both H.323 and SIP) will experience problems with NAT routers and firewalls.

9.1 *What is NAT and what does it do*

Most routers and firewalls use Network Address Translation (NAT). The primary purpose of NAT is to allow multiple terminals on the LAN to share one or more public IP addresses. NAT also provides security by hiding the private addresses of terminals on the LAN from anyone outside the network. NAT also works in conjunction with the firewall to control access to the LAN.

9.2 *The Problems caused by NAT*

When a terminal on the LAN sends a packet to the public network, NAT replaces the terminal's source address and port number in the IP header with a public IP address and port number. It puts this information in a table so it knows where to send packets when a response is received. NAT changes the address in the IP header, but not in any upper layer headers. There is also a source address in the RTP header which is not changed by NAT. The sending terminal placed this address in the RTP header so the receiving terminal would know where to send a response.

The voice packet now contains 2 different source addresses, the private address of the sending terminal and the address added by NAT.

The receiving device sends its response to the address in the RTP header, which is the private address of the sending device. Because this is a private address it cannot be routed and there is a transmission failure. The response packet never reaches the originator.

The problem described above is not the only problem. For each VoIP telephone call there are multiple data streams for voice and control. These data streams use both TCP and UDP ports and the port addresses are not known in advance. Passing these data streams through a NAT firewall is also a problem.

9.3 *VPN Solves the Problems*

VPN receives the packet from the originator before it is sent to the router. It first encrypts the entire packet, data and headers with source and destination addresses. It places this information inside a standard IP packet,

which is like placing it inside a virtual envelope and sends it to the NAT router. NAT changes the source address of the virtual packet and sends it to the destination.

At the destination, the virtual packet is passed to the VPN, which stores the source address information so it knows where to send a response. It then opens the packet and decrypts it. The result is a packet that is exactly the same as that encrypted by the VPN at the originating site.

The connection between the VPN devices is referred to as a tunnel. Anything that is put in one end of the tunnel passes through the tunnel and comes out at the other end exactly as it was entered. VPN has security measures to ensure that it is exactly the same. All headers are unchanged and source addresses in the IP and RTP headers match.

Now, when the receiving device responds, the packet will pass through the VPN tunnel and will be received by the originating device.

The use of VPN allows VoIP communication to be conducted through a NAT firewall or router.

It is strongly recommended that the VPN device use hardware encryption and decryption because it is much faster than software encryption.

10 Router Selection

Some routers claim to support QoS but either they do not support it at all or they do a poor job of supporting it. This poor support may be due to lack of queuing configuration. Some routers provide only Weighted Fair Queuing (WFG) and do not have any other options. Some do not allow the user to adjust the bandwidth allocation.

If the WAN is on a public network, the router must support VPN.

The amount of memory that the router has available for queuing packets is important. If a packet arrives and a queue is full, the packet will be discarded.

In our experience we have found that 16 mega Bytes of memory for queuing is adequate

11 The WAN Connection

The WAN is the part of the network that connects the sites. This could be a private network such as a point-to-point T-1 or a public packet network such as Frame Relay or ATM. These are managed networks with a SLA (Service Level Agreement) where the provider agrees to provide assurances for bandwidth, latency, lost packets and downtime.

You should be aware that if the data rate on the WAN exceeds the “committed rate”, the carrier may discard packets if there is no available bandwidth

11.1 QoS on the WAN

End-to-end QoS is a desirable feature but not always achievable. In most cases, the interior of the WAN does not provide QoS.

Even in those cases where the WAN cannot provide QoS, a QoS router should be used to provide QoS at the edge of the network (at both ends of your connection). The router can use QoS to control what it sends to the network but has no control over what it receives. It is depending on the network or the router at the other end of the connection to control what it receives.

11.2 The Internet Connection

Typical Internet Service is not a managed network service. It is a network of networks with no assurances about bandwidth or packet delivery. It has no QoS. It provides only “Best Effort” packet delivery. This type service is acceptable for surfing the web but not recommended for voice.

It is recommended that standard Internet service **not** be used to transport voice data because it is not a managed network. If standard Internet service is used for VoIP, the same connection should not be used for both voice and PC access to the Web. If a single connection is used, you have no control of what is being received on that connection. An Internet web page or pop-up window download could block voice data and cause very poor voice quality. The solution is to install 2 Internet connections (with 2 public IP Addresses) and install 2 routers.

For those working from a one-man-office or working from home such a configuration may not be practical. These users will be required to perform “manual QoS” by not accessing the Internet while they are using a VoIP telephone.

Some Internet Service Providers have begun offering higher levels of service for carrying voice and data. Some companies referred to as Internet Telephone Service Providers (ITSP) are even offering VoIP service. The cost of these services is based on the level of service and the bandwidth available.

Another reason to use 2 connections to the Internet is because you are paying a premium for the business grade service or VoIP service and it doesn't make sense to use that bandwidth with PCs accessing the Internet. Install a cheap Internet access connection for PC Internet web surfing.

12 Site Survey

Site Survey of existing network

You would not think of adding another floor to your office building or factory without accessing the structural soundness of the building. Adding VoIP to your existing network is a similar situation.

The added voice signals are going to place a significant load on your network and you need to know if it will support it. If it won't support it, you need to know what must be done to enable it to support the added voice traffic.

13 The Question of Quality

Voice Quality on IP Networks

It is agreed that traditional telephone service provides good voice quality. The telephone industry has worked hard over the years to achieve this quality. The major reason such quality is possible is because there is an end-to-end connection with a fixed bandwidth between callers.

IP telephony is a relatively new technology. It is still striving to provide “Toll Quality” voice. The transmission philosophy is different. Instead of a dedicated path per conversation, users must contend for available bandwidth on a single path. Collisions and delays are common. Measures can be taken to reduce them but, the nature of the network is such that they cannot be avoided. The system works well when traffic is low.

In a traditional telephone network, if a path to the destination is not available, the caller receives Busy Tone. In an IP network, a new caller must contend for available bandwidth and possibly degrade the quality of existing calls. As the traffic increases, voice quality suffers. Carriers are beginning to add controls to the network to limit access when congestion occurs to address this problem.

There are no guarantees of 100% voice quality on an IP network. Even if every rule is followed, there still may be times when a heavy traffic load or equipment outages can disrupt voice traffic.

14 GLOSSARY

802.1p

Priority and VLAN Topology. A Layer 2 method for signaling network priority on a per-frame basis. There are two components:

- A prioritization component allows network managers to assign priorities to specific packets. It provides for 8 different priorities for Level-2 traffic based on a 3-bit .User Priority. field defined by 802.1Q

802.1Q

VLAN Tagging. Defines changes to Ethernet frames that enable them to carry VLAN information. It allows switches to assign end-stations to different virtual LANs, and defines a standard way for VLANs to communicate across switched networks. Four bytes have been added to the Ethernet frame for this purpose, causing the maximum Ethernet frame length to increase from 1518 to 1522 bytes. In these 4 bytes, 3 bits allow for up to eight priority levels and 12 bits identify one of 4,094 different VLANs. 802.3ac will define the specifics of these changes for Ethernet frames. 802.1p specifies a method for indicating frame priority based on the new fields -- see 802.1p.

The missions of 802.1p and 802.1Q are to provide a uniform method for conveying frame priority and VLAN trunking information across the network. NOTE: 802.1Q is technically a historical document because this work has been merged into 802.1d.

802.1x

Port-Based Network Access Control. A supplement to IEEE 802.1d (Spanning Tree Protocol) that defines the changes necessary to the operation of a MAC Bridge in order to provide port-based network access control capability and a standard way for logging onto networks. Port-based access control, such as a password, can determine whether a user is permitted to access a network and define what network services are made available to the user.

802.3ab

Gigabit Ethernet on Copper Twisted Pair. IEEE standard approved June '99 defining the 802.3 1000BASE-T specification for Gigabit Ethernet operation on up to 100m of 4-pair Category 5 (CAT-5) copper wiring. In addition, it defines operation, testing, and usage requirements for the installed base of CAT-5 copper wiring. 1000BASE-T is important because most of the installed building cabling is CAT-5 UTP, because it will allow much less expensive connections than fiber-based Gigabit Ethernet, and because it allows for auto-negotiation between 100 and 1000 Mbps to make migration easier. Beginning in late 2000 and early 2001, PC servers began shipping with 1000BASE-T NICs (Network Interface Cards) for network connections.

802.3ac

VLAN Tagging for Ethernet. Applies the VLAN tagging defined by 802.1Q to Ethernet frames

802.3af

DTE (Data Terminal Equipment) Power via MDI (Media Dependent Interface). The IEEE 802.3af task force has the objective of economically providing power through an RJ-45 connector to a single Ethernet device over a twisted-pair link segment. 10BASE-T and 100BASE-TX devices are the primary target; 1000BASE-T (Gigabit Ethernet) is being considered.

ARP

Address Resolution Protocol. Based on standard RFC826: a TCP/IP protocol used to obtain the physical address of a node when only its logical IP address is known. An ARP request with a desired IP (Layer 3)

address is broadcast onto the network, and the node having that address responds by sending back its hardware (Layer 2) address so that packets can be sent to it.

Reverse ARP (RARP) does the opposite, finding the Layer 3 address that corresponds to a Layer 2 address. See RARP and BootP.

BGP

Border Gateway Protocol. Based on IETF RFC1771: a TCP/IP routing protocol for interdomain routing in large networks. It is used in the Internet and enables policy-based routing between ISPs. It could be applicable to corporate intranets that attach to the public Internet at more than one point. It is an alternative to EGP (Exterior Gateway Protocol). The current version is BGP-4. The 1996 web page <http://joe.lindsay.net/bgp.html> contains links to related RFCs, links to tutorial pages, and tips for configuring BGP routing.

Internal BGP is used within one Autonomous System (AS). External BGP is used between two border routers that are in different Autonomous Systems. See MBGP (Multicast Border Gateway Protocol).

BootP

Bootstrap Protocol. Based on IETF RFC951: a low-level TCP/IP protocol used by a diskless workstation or a network computer to boot itself from the network. BootP enables the station to determine its own logical IP (Layer 3) address upon startup. It uses the UDP transport mechanism and is an alternative to the RARP protocol. See RARP.

DHCP (Dynamic Host Configuration Protocol) includes all the BootP functions, so a DHCP server can respond to BootP requests. See DHCP. A BootP Relay Agent in a router is a function that relays BootP requests from a workstation on one subnet to a BootP or DHCP server on a different subnet. BootP requests are broadcast requests, so without this function the requests will not cross subnet boundaries.

CLI

Command Line Interface. For routers and switches, this is a type of user interface for entering line-by-line commands for control and configuration, typically from a terminal that is either physically attached locally or attached remotely via a telnet network connection.

CSMD/CD

Carrier Sense Multiple Access/ Collision Detection. The access method used for Ethernet IEEE 802.3 protocol.

DES Data Encryption Standard

DES is the U.S. Government-approved encryption standard from the 1970s that has proven to be breakable because of its relatively small 56-bit key size. Most people wanting high security uses the Triple-DES version, based on a key size of 112 or 168 bits. FIPS standard 46-3 designates DES and Triple-DES. DES requires too much computing resources for high speed throughput, so the U.S. Government has recently chosen the Advanced Encryption Standard to replace DES. Also see IPsec.

DHCP

Dynamic Host Configuration Protocol. Based on IETF RFC2131: a protocol for dynamic IP address assignment and automatic TCP/IP configuration that provides both static and dynamic address allocation. Extensions are being added to support PC boot from the network: Network PC v1.0 Reference Design specifies using DHCP for network boot, and DHCP is likely to replace RPL. NetWare 5.0 will include support for DHCP. IBM's LAN Client Control Manager v2 uses DHCP, replacing RPL that was used in v1.

DHCP includes all the BootP (Bootstrap Protocol) functions, so a DHCP server can respond to BootP requests. See BootP. DHCPv6 is the version under development for IPv6 . See IPv6. See MDHCP (multicast version of DHCP) and DNS (static address allocation).

Background: Manually assigning static addresses to each network device has long been a problem. In the past, workstations used RARP and BootP to obtain IP addresses from the network. But these protocols support only static allocation, and BootP requires workstation information such as the IP host address to be set up manually in a server database. Dynamic address assignment using DHCP provides for easier initial configuration and changes, allowing plug and play network operation for workstations and PCs.

How it works When a DHCP client workstation boots, it broadcasts a DHCP request asking for IP address and configuration parameters from any DHCP server on the network. An authorized DHCP server for this client will suggest an IP address by sending a reply to the client. The client may accept the first IP address or wait for additional offers from other servers on the network. Eventually the client selects the offer made by a particular server and sends a request to accept it. That server sends an acknowledgment confirming the client's IP address and providing any other configuration parameters that the client asked for.

The client's DHCP-issued IP address has an associated lease time that defines how long the IP address is valid. The client can repeatedly ask the server for renewal. If the client does not request renewal or if the client machine is shut down, the lease will eventually expire. Then that IP address can be reused by giving it to another machine. DHCP servers can also assign static network addresses to clients. This is handled by giving addresses an infinite lease.

A DHCP Relay Agent in a router is a function that relays DHCP requests from a workstation on one subnet to a DHCP server on a different subnet. DHCP requests are broadcast requests, so without this function the requests will not cross subnet boundaries.

DiffServ Differentiated Services

The result of an IETF working group that is defining a new bandwidth-management scheme for IP networks. The plan redefines part of the existing Type-of-Service (ToS) byte in every IP packet header to mark the priority or service level that packet requires. See ToS; this byte is renamed the DS byte. DiffServ will work well with security protocols because the ToS byte is in the IP header and is therefore not encrypted.

The Diff Serv charter is defined at <http://www.ietf.org/html.charters/diffserv-charter.html>. Links to additional information are at www4.ncsu.edu/~kwu/diffserv/qosref.html. Information about proposed standards is contained in RFC2474 and RFC2475. DiffServ has extremely widespread support among equipment vendors and service providers. It is expected to be a key element of Voice Over IP service (see VOIP).

Traffic service requirements are marked in the DS byte in the IP packet header. A 6-bit field called the Differentiated Services Codepoint (DSCP) defines the per-hop behavior (PHB) that the packet will receive; 2 bits are currently unused. The DS byte determines how a multilayer switch or router will handle the packet. Setting the bits in the DS byte will typically be performed only at the network boundary.

The scheme is expected to scale well because the work of making these assignments, which involves examining Layer 3 or higher layers of each packet, is limited to edge routers. LDAP is the likely protocol that these routers will use for handling policies regarding how to mark each packet (see LDAP). Routers in the core of the network simply examine Layer 2 and give the same service to all packets that are marked the same way. ISPs, or potentially ISP customers, may be able to mark the packets based on service level agreements.

DNS

Domain Name System. Based on IETF RFC1033 DNS is a distributed database system for translating names of Internet host computers into IP addresses. A DNS server computer maintains a database for resolving host names into IP addresses so that client computer users can address a remote computer by its host name rather than its complicated numerical IP address. The DNS Resources Directory provides extensive online technical information and news about DNS. Also see DDNS.

DNS also allows a host computer that is not directly on the Internet to have the same style of registered name. DNS normally only works with static IP addresses. DHCP allows dynamically assigned IP addresses to be tracked by DNS servers. See DHCP.

DS

Digital Signal. A system of classifying digital circuits according to the rate and format of the signal (DS) and the equipment providing the signals (T). DS and T designations have come to be used synonymously so that DS1 implies T1, and DS3 implies T3. In SONET, STS is used for electrical formats and OC is used for optical formats.

Voice Channels in North America, Japan, Korea:

DS0	1 64 kbps
DS1	24 1.544 Mbps (T1)
DS1C	48 3.152 Mbps (T1C)
DS2	96 6.312 Mbps (T2)
DS3	672 44.736 Mbps
DS4	4032 274.176 Mbps (T4)

Voice Channels in Europe and the ITU:

E1	30 2.048 Mbps
E2	120 8.448 Mbps
E3	480 34.368 Mbps
E4	1920 139.264 Mbps
E5	7680 565.148 Mbps

DSCP

Differentiated Services Codepoint. See DiffServ (Differentiated Services).

FTP

File Transfer Protocol. An application protocol that is used for transferring files between network nodes. FTP is part of the TCP/IP protocol stack and is defined by standard RFC959. See TCP/IP.

GARP

Generic Attributes Registration Protocol. Defined by 802.1p. There are two versions of this protocol. The first version is the GARP Multicast Registration Protocol (GMRP), which lets workstations request membership in a multicast domain. This joining action is called a leaf-initiated join. GMRP provides a standard protocol for sending traffic to only those ports that have requested multicast traffic. It is compatible with 802.1Q because the protocol operates on a port basis.

The second version is the GARP VLAN Registration Protocol (GVRP). Under GVRP a workstation requests admission to a specific VLAN rather than to a multicast domain.

This protocol links 802.1p and 802.1Q

GVRP

GARP VLAN Registration Protocol. To establish VLANs in an environment of multiple switches, GVRP provides a protocol mechanism that lets the switches dynamically establish and update their knowledge of the set of Virtual LANs that currently have active members. See GARP.

H.323

An ITU standard for videoconferencing over LANs, other packet-switched networks, and the Internet. It provides for sending any combination of real-time voice, video, and data. Various standards within H.323 define how calls are set up, what audio and video compression (codec) schemes are permitted, and how to participate in conferences. H.323 runs on TCP.

ICMP

Internet Control Message Protocol. An IETF protocol based on RFC792 that provides a number of diagnostic functions including sending error packets to hosts and sending PING messages. ICMP uses the basic support of IP and is an integral part of IP. ICMP Redirect is a process whereby a router informs a host computer that there is a better route from that host to a specific destination than via that host's default router (default gateway). ICMPv6 (RFC1885) is the new version that is integral to IPv6. It includes functions from IGMP and is required in every IPv6 node.

IP

Internet Protocol. Based on IETF RFC791: the TCP/IP standard protocol that defines the IP datagram. It is used in gateways to connect networks at Layer 3. See TCP/IP. IPv4 (version 4) is standard today. See IPv6.

IP Address

The Layer 3 address of a host (computer) attached to a TCP/IP network. Every host must have a unique IP address. IP addresses are 32-bit values written as four sets of decimal numbers separated by periods; for example, 125.6.65.7. Each decimal number (0-255) represents 8 bits of the complete 32-bit value.

The TCP/IP packet uses 32 bits to contain the IP address, which consists of a network address (netid) and a host address (hostid). The 32 bits are divided in different ways according to the class of the address, which determines the number of hosts that can be attached to the network. If more bits are used for the host addresses (such as in Class A), fewer bits are available for the network address.

Network addresses are supplied to organizations by the InterNIC Registration Service.

IPSec

IP Security. A suite of protocols that handles encryption, authentication, and secure transport of IP packets such as for VPNs. It is described in RFCs 2401-2412 produced by the IETF IPsec working group (www.ietf.org/html.charters/ipsec-charter.html). The IPsec Developers Forum provides technical information and allows vendors to schedule interoperability testing. Microsoft will provide IPsec support for VPNs in

Windows 2000. IPSec will provide network-layer security for IPv4 and IPv6. The VPN Consortium (www.vpnc.org) has established an inexpensive test for conformance with basic IPsec protocols.

IPSec works at Layer 3 to transport data transparently to network applications. It is intended to provide more lower-level security than SSL (Secure Socket Layer). IPSec adds a header to packets being sent over a VPN to identify that those packets have been secured. It supports several types of encryption including the Data Encryption Standard (DES), supports several types of authentication including Message Digest 5 (MD5, RFC2403) and SHA-1 (RFC2404), and several key management schemes that

allow parties to agree upon parameters for the session. Current implementations mostly use the IKE (Internet Key Exchange) protocol, which requires each pair of nodes to be linked via a unique key and thus creates a need for a huge number of keys when there are many nodes. Support for the Advanced Encryption Standard still needs to be added (see AES).

Proposals call for adding additional security features. IPsec also provides for data compression, which partially compensates for the poor compression that modems are able to perform on encrypted data. IPsec does not provide support for NAT (Network Address Translation). IPsec requires every user to have a defined public IP address, so if IP addresses are shared using NAT the security privileges are also shared. SSL works differently by operating at Layer 4 and focusing on the upper layers of the OSI model. See SSL. Also see PPTP.

IPv6 Internet Protocol Version 6

Based on standard RFC1883 and RFC1752: a new version of the IP protocol (see IP) that was designed to provide a solution to the address space limitations of the current version IPv4. The 6BONE is a worldwide network begun around 1996 that runs IPv6 on an experimental basis: see www.6bone.net. The IPv6 Forum (www.ipv6forum.com) is a consortium dedicated to promoting IPv6. IPv6 was formerly known as IPng (IP Next Generation). IPv6-enabled devices will still forward IPv4 traffic, and there is a standard for encapsulating IPv4 information within a virtual tunnel between IPv6 devices.

IPv6 provides:

- 128-bit address space (increased from 32 bits)
- Automatic address configuration capability based on DHCPv6 that allows a host to discover automatically the information it needs to connect to the Internet or to a private TCP/IP network.
- A simplified packet header structure, with many fields optional
- Support for source-selected routes (like Token Ring's source routing)
- Scalable routing architectures
- Network-layer security
- Quality-of-service (QoS) levels
- Mobile computing capabilities
- Multicasting features.

L2TP

Layer 2 Tunneling Protocol. The first proposed IETF protocol for tunneling Point-to-Point Protocol (PPP) across a private or public network. L2TP is in IETF draft status, and is the result of a merger of Microsoft PPTP, Cisco Layer2 Forwarding (L2F), and IPsec. L2TP support for VPNs is planned in Windows NT 5.0 (Windows 2000). L2TP is expected to receive broad industry acceptance in VPNs as a replacement to current proprietary protocols that do not allow equipment from multiple vendors to interoperate. It enables support for multiple protocols and unregistered IP addresses, allowing existing non-IP protocol applications such as SNA to be used. In 8/98 Cisco announced support for L2TP in the Cisco IOS software.

L2TP is a data-link layer protocol that creates one or more tunnels through an IP network between an L2TP Access Concentrator (LAC) and an L2TP Network Server (LNS). The tunnels carry traffic sessions over Point-to-Point Protocol (PPP) links. An authentication protocol (PAP or CHAP) and an optional encryption protocol (such as PPP Triple-DES) provide security.

MAC

Media Access Control -

MTU

Maximum Transmission Unit. The longest physical packet size that can be sent over a specific network. The MTU of most Ethernet networks is 1500 bytes; the MTU of X.25 networks is 576 bytes. Path MTU

Discovery is a process defined by RFC1191 for dynamically discovering the smallest MTU of any link between two arbitrary network hosts.

NAT

Network Address Translation. Based on IETF RFC1631: Converts the internal private IP addresses of an enterprise back and forth from a single public IP address that is valid on the Internet. This allows the enterprise to be represented externally by a single public address while using different internal IP addresses that do not conform to global standards. NAT helps extend the limited public IP address space, provides important security by masking host addresses that are inside the enterprise, and simplifying organizational changes that result in overlapping IP addresses.

NAT provides VPN functions by translating private IP addresses to global IP addresses in order to traverse a global network. Two address ranges are set up: one for the internal (private) network and one for the external (global) network. A firewall maintains a table that maps the internal to external numbers.

NIC

Network Interface Card – a circuit card installed in a PC to interface with the network.

PoE

See 802.3af

PPTP

Point to Point Tunneling Protocol. A Layer 2 protocol that enables virtual private networking by encapsulating other protocols such as NetWare IPX for transmission over an IP network. PPTP is used as a VPN tunneling protocol; other such protocols are IPSec and L2TP. See IPSec, L2TP.

PPTP is also used to create a private network (VPN) within the public Internet by taking advantage of its RSA encryption or its Microsoft Point-to-Point Encryption (MPPE). Remote users can access their corporate networks via any ISP that supports PPTP on its servers. The protocol was developed by the PPTP Forum, which included Ascend, Microsoft, 3Com, and U.S. Robotics. It was first demonstrated in Spring 1996 by U.S. Robotics and Microsoft. U.S. Robotics developed the Windows NT PPTP driver, for integration into Microsoft's Windows NT Server 4.0. PPTP support is built into Windows 95 and 98. PPTP allows NT network clients to take advantage of the services provided by Microsoft's RAS (Remote Access Service). For remote access, over analog or ISDN lines, PPTP creates a tunnel directly to the appropriate network NT Server. By terminating the remote user's PPP connection at the NT server, rather than at the remote access hardware, PPTP allows network administrators to standardize security using the existing services and capabilities built into the Windows NT security domain.

QoS

Quality of Service. Network device capabilities that provide some guarantee of performance such as traffic delivery priority, speed, latency, or latency variation. Delivery of good-quality audio or video streams typically requires QoS capabilities. The www.employees.org/~ferguson/QoS.html page on "Delivering QoS on the Internet and in Corporate Networks" contains an extensive bibliography, tutorial information, and links to QoS-related draft standards. The QoS Forum (www.qosforum.com) is devoted to educating the market and accelerating the adoption of standards-based QoS technologies but is not a standards-setting group. Also see 802.1p and RSVP.

QoSR

Quality of Service Routing. Procedures being studied by the IETF (RFC2386) to select routing paths based on network resource availability and the quality requirements of the traffic flow. Current routing protocols (such as RIP, OSPF, and BGP4) do not consider the link capacity when making route assignments.

RARP

Reverse ARP. A standard defined by IETF RFC903 that performs the opposite of ARP, finding a Layer 3 address that corresponds to a Layer 2 address. It is used by diskless workstations that need to obtain unique IP addresses upon startup. A RARP server responds to a RARP broadcast from the workstation and sends back the IP address. See ARP and BOOTP.

RTP

Real-Time Transport Protocol. RTP provides end-to-end network transport functions suitable for applications transmitting real-time data such as audio or video over multicast or unicast network services. It is an IETF standard defined by RFC1889 and RFC1890. It does not establish connections or provide any guarantees of delivery or network availability. It includes the Real-Time Control Protocol (RTCP) for use in multicasting. RTP runs over UDP and IP, and is important for transporting Voice Over IP (see VOIP). See <http://www.cs.columbia.edu/~hgs/rtp/> for an overview of RTP and related topics.

SLA

Service-Level Agreement. An agreement between an Internet service provider and its customer (or between two service providers) regarding the types of networking services, including service-level guarantees, that it will provide for stated prices. It will be important for future multilayer switches and other network devices to provide tools for enforcing compliance with these service levels and means for measuring compliance with them.

TCP/IP

Transmission Control Protocol-Internet Protocol. Based on IETF standard RFC793: TCP is a reliable, connection-oriented protocol that first establishes a connection between the two systems that will exchange data. When an application sends a message to TCP for transmission, TCP breaks the message into packets, sized appropriately for the network. TCP provides flow control (to prevent overrunning the receiver) and congestion control (to prevent overrunning the capacity of the network.) For Ethernet networks, the maximum packet size is 1518 Bytes. Also see IP, UDP. TCP uses the IP protocol to address and send the packets. The IP protocol uses three key parameters: the IP address, subnet mask, and default gateway.

ToS

Type of Service. A byte located in every IP packet header that contains 6 bits intended to identify the packet's priority and throughput handling requirements but rarely used. The IETF DiffServ working group is defining a new scheme for using this byte. See DiffServ.

UDP

User Datagram Protocol. A connectionless mode protocol that is part of the TCP/IP family, defined by IETF RFC768. UDP allows an application to send a message to one of several other applications running on a remote or local machine. UDP operates much faster than TCP because it has much less overhead. Consequently, UDP is extremely important for many real-time video, audio, and storage networking applications where high speed and low latency are important. Wire-speed UDP processing is an important feature for switches or routers that must handle this type of real-time traffic reliably.

Data sent via the UDP protocol is not acknowledged and is thus less reliable than data sent via TCP/IP. Data can also be out of sequence and potentially duplicated.

VLAN

Virtual LAN. A group of independent devices that communicate as if they are on the same physical LAN segment but can actually be located anywhere on the network. VLANs typically allow each connected device to be placed into a logical group according to its physical point of connection (switch port), MAC address, or network protocol type.

802.1Q defines a numbering scheme that allows up to 4094 distinct VLANs on a network -- see 802.1Q.

VoIP

Voice Over IP. An extension of ITU-T standards to provide recommendations for supporting voice communications over IP networks such as the Internet with compatibility between products from different manufacturers. Typical scenarios are PC to PC, PC to phone, and phone to phone. Some incompatibilities exist now between various implementations due to the unfinished state of H.323 standards. VoIP is currently used mostly over private IP WANs so traffic priority can be assured. In the future, Differentiated Services (see DiffServ) are expected to be crucial for providing appropriate priority so that VOIP can be implemented effectively on the public Internet. VOIP rides over the Real-Time Transport Protocol (see RTP), typically using minimum-size packets with small payloads of 20 bytes.

The Voice over IP Forum was formed in 1996 by Cisco Systems, VocalTec, Dialogic, 3Com, Netspeak and others as a working group of the International Multimedia Teleconferencing Consortium (IMTC), which promotes the implementation of the ITU-T H.323 standard (see www.imtc.org). The Protocols.com web site maintains links to many VOIP references and standards (www.protocols.com/voip.htm).

VPN

Virtual Private Network. A private connection over the public Internet that enables secure communications from a remote site. The two major classes of VPNs are remote access (accessing an enterprise network remotely via a dial-up call to a local Internet service provider) and site-to-site (linking two or more portions of an enterprise's intranet or extranet over the public Internet). The most common protocols for IP-based VPNs are MPLS (see MPLS), Layer 2 Tunneling Protocol (see L2TP), and the collection of IP Security protocols known as IPsec (see IPsec). When high security is required, the security features of IPsec are more appropriate than those of L2TP. Also see PPTP.

Some VPNs employ connections using PPTP, which is currently the most popular VPN tunneling protocol. For more security VPNs can use IPsec or MPLS, which are generally safer and more scalable than tunneling. See PPTP, IPsec, and MPLS. Layer 2 Tunneling Protocol (L2TP) is likely to be supported heavily for VPNs in the future -- see L2TP.

WFQ

Weighted Fair Queuing. A system of scheduling packets that are waiting for transmission that separates the packets into classes of different priorities and guarantees that each class receives some portion of the available bandwidth. This ensures that both heavy and light network users receive consistent response times. WFQ dynamically adjusts bandwidth allocations based on the traffic parameters and the relative amounts of traffic, reducing jitter and producing more predictable round-trip delays.

15 Bibliography

The following articles discuss the challenges of implementing VoIP.

1. Communication News, March 2004, “The Five Key Questions You Should Ask before Deploying VoIP” (http://www.commnews.com/stories/articles/0304/0304five_key.htm)
2. Communication Convergence; March 5, 2004; “VoIP’s Seven Deadly Sins” (<http://www.cconvergence.com/shared/article/showArticle.jhtml?article=18201870>)
3. Communication News; March 2004; “Improve Your VoIP Deployment” (<http://www.comnews.com/stories/articles/0304/0304VOIP.htm>)
4. Gartner Consulting, White Paper, May 2002, “Convergence Challenges for Enterprise Networks”