NEC

UNIVERGE® SV9100

Voice Over IP Manual

Table of Contents

1 Part 1: VoIP Reference Manual

Voice Over IP Reference Manual

Rev 1.2 May 2015

1.1 1. What is Voice over IP? (VoIP)

Voice over IP (VoIP) is a technology that converts speech into data packets and transmits these packets over IP (Internet Protocol) networks. As most organisations already have existing data networks in place, considerable cost savings can be achieved by utilizing these networks for speech transmission.

There are many factors that should be considered when implementing VoIP. Without careful planning and installation there is the potential for poor quality speech, unreliability, and disruption to the existing data networks.

This document describes the potential problems and possible solutions to these problems. There is also a troubleshooting section to help with problems that can occur.

1.1 TDM to IP Conversion?

TDM (Time Division Multiplexing) is a technique used in traditional telephone systems to allow multiple channels of information to be transmitted over the same physical medium by allocating a different time interval ("slot" or "slice") for the transmission of each channel. This technique is used internally in the telephone system but cannot be used over IP based data networks.

Therefore, it is necessary for the telephone system to convert the TDM data to IP packets. This conversion is carried out by a DSP (Digital Signal Processors) on the GPZ-IPLE card. Each DSP can handle one TDM-to-IP conversion. For example, a licensed 32 voip channel GPZ-IPLE card allows 32 DSP resources to be used and can support 32 simultaneous TDM - IP calls.

1.2 VoIP Mode?

There are several methods of VoIP operation. These can be categorized as:

- Extensions (standards based phones)
- Extensions (proprietary – with greater feature transparency)
- Trunks (basic calls between multiple telephone systems or ITSPs)
- Networking (feature-rich networking between telephone systems)

The modes available depend on the model of telephone system and the hardware/software installed. Please refer to the specific manual for your product to determine which modes are available.

1.3 Protocols and Standards?

VoIP is commonly used to connect telephone systems and telephones from different manufacturers together. To allow this interoperability each system must adhere to the same standard and “talk the same language” (known as a protocol). There are various standards and protocols that are used. The most common types (and those used by NEC equipment) are:

Session Initiation Protocol (SIP)

SIP is a proposed standard, developed by the Internet Engineering Task Force (IETF) for setting up sessions between one or more clients. It is currently the leading signalling protocol for Voice over IP, gradually replacing H.323 in this role. SIP has been designed to be future proof and is very flexible.

H.323

H.323 is a recommendation from the International Telecommunication Union (ITU-T) that defines the protocols to provide audio-visual communication sessions on any packet network. It is a part of the H.32x series of protocols which also address communications over ISDN and PSTN. This signalling method is closely related to ISDN and is inflexible and difficult to implement new features.

Proprietary

Most telephone system manufacturers have developed their own protocols to transmit their own proprietary features between telephone systems. This method usually provides a very feature-rich and integrated VoIP network, but is limited to connecting systems from the same manufacturer. Usually, if one or more of the Telephone Systems (or IP Telephones) is supplied by another manufacturer it is necessary to use a standards- based protocol (i.e. SIP or H.323)

Please refer to the Compatibility section below

1.4 CODECs?

The term CODEC (COder/DECoder) describes the technology of encoding and decoding a signal. Within VoIP this specifically refers to the algorithm used to convert speech from the PBX to data for transmission on an IP network.

The CODEC’s supported by the SV9100 are: -

G.711

This is the ITU-T recommendation for coding of speech at 64kbps using PCM (pulse code modulation). This CODEC is often described as uncompressed as it uses the same sampling rate as the traditional telephony (TDM). G.711 has a MOS score of 4.4 but uses a large amount of bandwidth for transmission. This CODEC is not commonly used due to the amount of bandwidth required, although it can be acceptable in LAN environment (i.e. System IP Phones connected over a 100Mbps LAN).

G.722

This ITU-T standard codec provides 7 kHz wideband audio at data rates from 48 to 64 kbps. This is useful in a fixed network Voice over IP applications, where the required bandwidth is typically not prohibitive, and offers a significant improvement in speech quality over older narrowband codec’s such as G.711, without an excessive increase in implementation complexity.

G.726

This ITU-T standard codec provides transmission of voice at rates of 16, 24, 32, and 40 kbps. The most commonly used mode is 32 kbps, which doubles the usable network capacity by using half the rate of G.711. It is primarily used on international trunks in the PSTN and also in the DECT wireless standard.

The SV9100 uses the 32 kbps version.

iLBC

The iLBC codec is an algorithm that compresses each basic frame (20 ms or 30 ms) of 8000 Hz, 16-bit sampled input speech, into output frames with rate of 400 bits for 30 ms basic frame size and 304 bits for 20 ms basic frame size. This codec is suitable for real time communications such as, telephony and videoconferencing, streaming audio, archival and messaging.

G.729A
This ITU-T recommendation describes the algorithm for coding of speech signals at 8kbps using CS-ACELP (conjugate-structure algebraic code-excited linear prediction). This codec samples the analogue signal at 8000Hz and uses a frame size of 10ms. This CODEC has a MOS score of 4.0. G.729 is the most commonly used CODEC for SV9100 VoIP installations. This is due to the fact that it offers high compression (and therefore low bandwidth) whilst maintaining good speech quality.

G.723
This ITU-T recommendation describes a very low bit-rate compression algorithm. The standard describes two versions 5.3Kbps and 6.4Kbps. SV9100 uses the lower bit rate. This CODEC offers low bandwidth speech transmission, but has a lower MOS score of 3.9. This CODEC is not commonly used on the SV9100, but is particularly suited to low bandwidth WAN connections.

MOS. The mean opinion score (MOS) provides a numerical measure of the quality of human speech at the destination end of the circuit. The scheme uses subjective tests (opinionated scores) that are mathematically averaged to obtain a quantitative indicator of the system performance.

Note: Not all CODEC's listed above are available for all applications.

1.5 Compatibility?

It should be noted that NEC does not guarantee that any third-party equipment will operate correctly with NEC equipment.

1.2 2. Factors Affecting Voice Quality

2.1 Quality of Service (QoS)?

Quality of Service (QoS) is one of the most important factors for VoIP. The term refers to the perceived quality of speech and the methods used to provide good quality speech transmission. There are several factors that affect speech quality, and several mechanisms that can be used to ensure QoS.

This section describes the problems that can occur and some possible solutions.

2.2 Latency (Delay)?

If at any point the usage on the network exceeds the available bandwidth, the users will experience delay, also known as latency. In more traditional uses of an IP data network, the applications can deal with this latency. If a person is waiting for a web page to download, they will accept a certain amount of wait time. This is not so for voice traffic. Voice is a real time application, which is sensitive to latency. If the round trip voice latency becomes too long (250 ms, for example), the call quality would usually be considered to be poor. Another important thing to remember is that packets can get lost. IP is a best effort networking protocol. This means the network will try its best to get your information there, but there is no guarantee.

Delay is the time required for a signal to traverse the network. In a telephony context, end-to-end delay is the time required for a signal generated at the talker's mouth to reach the listener's ear. Therefore end-to-end delay is the sum of all the delays at the different network devices and across the network links through which voice traffic passes. Many factors contribute to end-to-end delay, which are covered next.

The buffering, queuing, and switching or routing delay of IP routers primarily determines IP network delay. Specifically, IP network delay is comprised of the following:

Packet Capture Delay
Packet capture delay is the time required to receive the entire packet before processing and forwarding it through the router. This delay is determined by the packet length and transmission speed. Using short packets over high-speed networks can easily shorten the delay but potentially decrease network efficiency.

Switching/Routing Delay
Switching/routing delay is the time the router takes to switch the packet. This time is needed to analyse the packet header, check the routing table, and route the packet to the output port. This delay depends on the architecture of the switches/routers and the size of the routing table.

Queuing Time
Due to the statistical multiplexing nature of IP networks and to the asynchronous nature of packet arrivals, some queuing, thus delay, is required at the input and output ports of a packet switch. This delay is a function of the traffic load on a packet switch, the length of the packets and the statistical distribution over the ports.

Designing very large router and link capacities can reduce but not completely eliminate this delay.

2.3 Jitter (Delay Variation)?

Delay variation is the difference in delay exhibited by different packets that are part of the same traffic flow. High frequency delay variation is known as jitter. Jitter is caused primarily by differences in queue wait times for consecutive packets in a flow, and is the most significant issue for QoS. Certain traffic types-especially real- time traffic such as voice, are very intolerant of jitter. Differences in packet arrival times cause choppiness in the voice.

All transport systems exhibit some jitter. As long as jitter falls within defined tolerances, it does not impact service quality. Excessive jitter can be overcome by buffering, but this increases delay, which can cause other problems. With intelligent discard mechanisms, IP telephony/VoIP systems will try to synchronize a communication flow by selective packet discard, in an effort to avoid the "walkie-talkie" phenomenon caused when two sides of a conversation have significant latency. SV9100 incorporates a Jitter Buffer to avoid these problems.

2.4 Packet Loss?

IP is an unreliable protocol which means that in some circumstances packets of data can be discarded (dropped) by the network. This usually occurs when the network is particularly busy.

Loss of multiple packets of a voice stream may cause an audible pop that will become annoying to the user. To maintain voice quality, packet loss should not exceed around 1% of all packets. Obviously this figure should be as close to 0% as possible.

2.5 CODEC Selection?

The CODEC used will affect the voice quality due to the different compression algorithms used, and the amount of bandwidth required (see: Bandwidth and CODECs).

For example, on a low bandwidth WAN link, using a high bandwidth CODEC (such as G.711) may cause “choppy” speech as the WAN link will suffer from congestion. In this case, a lower bandwidth CODEC (such as G.729) may be more appropriate.

2.6 Bandwidth?

Available bandwidth has a major influence on voice quality in VoIP networks. Bandwidth is usually expressed in the number of bits per second (bps) that can be transmitted over a network link. The amount of bandwidth is usually limited by the service provider or the physical cables that are used for transmission.

Examples of bandwidth:
Ethernet LAN 100Mbps
ISDN (one B-Channel) 64Kbps
ADSL 512Kbps/8Mbps (see asymmetric bandwidth section)

Unit of Bandwidth	Abbreviation	Equivalence
Bits per second	bps	1 bps = fundamental unit of bandwidth
Kilobits per second	kbps	1 kbps = 1,000 bps = 10^3 bps
Megabits per second	Mbps	1 Mbps = 1,000,000 bps = 10^6 bps
Gigabits per second	Gbps	1 Gbps = 1,000,000,000 bps = 10^9 bps
Terabits per second	Tbps	1 Tbps = 1,000,000,000,000 bps = 10^{12} bps

Bandwidth is typically shared between VoIP and other data applications. It is important to take into account the amount of bandwidth required for voice and data applications. The amount of bandwidth required for VoIP calls depends on several factors, including:

- Number of simultaneous calls
- CODEC used
- Frame Size
- Data Networking Protocol used

The more frames we encapsulate into each packet, the less bandwidth is required. This is because each packet transmitted has the same header size - therefore if lots of very small packets are sent we are also using bandwidth for lots of header information. If we add several frames to the packet, we have fewer packets transmitted and therefore have less header information sent.

If we add lots of voice frames to each packet we know that we are using less bandwidth, but this does have disadvantages. If we have a large packet size, and a particular voice packet is lost, this will have a greater impact on the speech quality. If we are using small quantity of voice frames per packet the effect of losing a packet is reduced.

As a general rule: The more frames we have per packet, the less bandwidth is used, but the quality is lower.

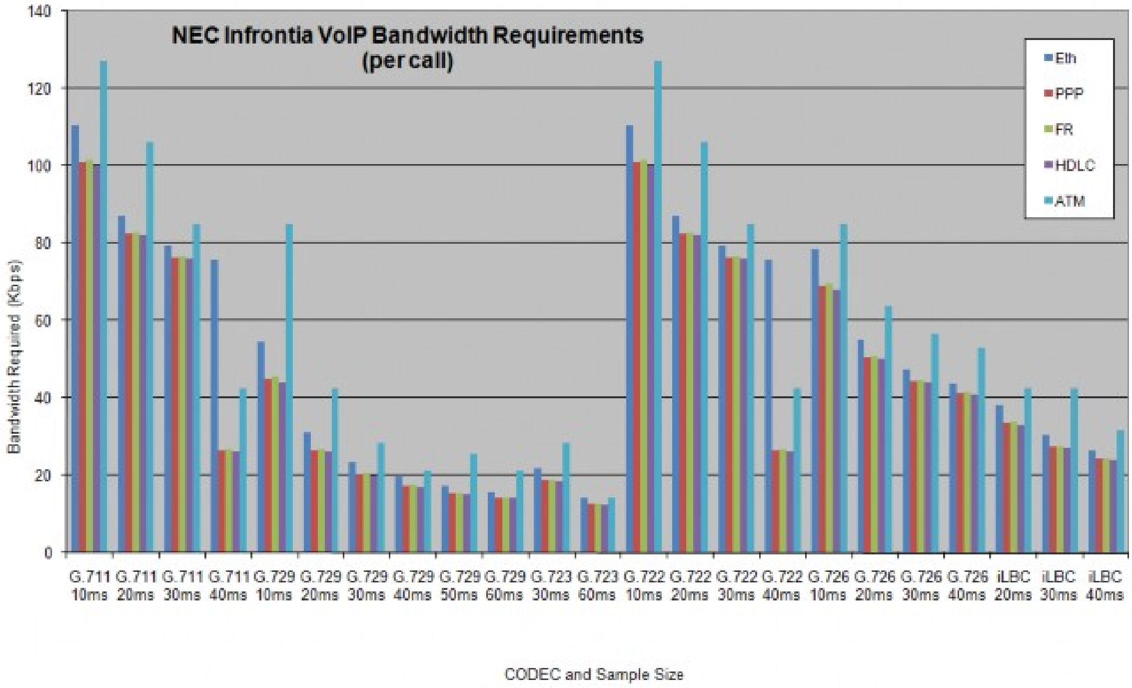
Example one:
CODEC: G.729
Frame Size: 10ms
Voice Frames per Packet: 2
Voice Sample Size: 20ms (frame size x Voice Frames) Bandwidth Required: 24Kbps

Example two:
CODEC: G.729
Frame Size: 80ms
Voice Frames per Packet: 8
Voice Sample Size: 80ms (frame size x Voice Frames) Bandwidth Required: 12Kbps

Note: Figures above do not take into account Layer 2 overhead. This varies dependant on the Layer 2 protocol used (e.g. Ethernet, Frame Relay, PPP).

The graph below shows the bandwidth requirements for 1 VoIP call using the CODECs and Networks specified. This can be used for an indication of the required bandwidth.

2.6.1 Bandwidth Graph



Increasing the bandwidth on a data connection can resolve some voice quality issues, however this is often impossible due to physical cable limitations, or more commonly, cost.

2.7 Frames per packet?

See explanation in the Bandwidth section above.

Increasing the amount of frames per packet (also described as VIF, Sample Size, and Fill Time) can reduced the bandwidth requirement and therefore improve voice quality. If the number of frames per packet increases too much the voice quality can deteriorate as the voice calls become more susceptible to packet loss and additional delay is introduced.

2.8 Layer 2 Protocol?

All VoIP packets are encapsulated into a Layer 2 protocol (e.g. Ethernet, PPP, Frame Relay) for transmission over the data network. Every Layer 2 protocol has different characteristics and header sizes. This means that the amount of bandwidth will vary dependant on the protocol used.

The bandwidth graph above shows the affect of different Layer 2 protocols on the bandwidth requirement. Unfortunately it is rarely possible to change the Layer 2 protocol to a less bandwidth-intensive protocol. The protocol is usually fundamental to the data network design and it is unlikely that this can be changed.

2.9 Type of data connection

The type of data network used will have a big affect on the voice quality. The reasons for this are described above (e.g. Bandwidth, delay, etc).

A brief description of some of the typical data network types is shown below.

Name	Typical Bandwidth (may vary)	Advantages	Disadvantages
Leased line - Kilostream - Megastream	64Kbps – 768Kbps 1Mbps – 2Mbps	- Guaranteed bandwidth - No contention - Reliable	- Expensive - Distance limitations
LES (LAN Extension Service)	10Mbp s 100Mb ps 1Gbps	- Guaranteed bandwidth - High throughput - Reliable - No contention	- Both ends must be located on same Telephone Exchange - Expensive
Frame Relay	Up to 2Mbps (UK)	- Widely available (commonly used for international connections)	- Expensive
ADSL (Asymmetric Digital Subscriber Line)	Upstream 512Kbps Downstream 8Mbps	- Inexpensive	- Contention (shared bandwidth) - No bandwidth guarantees - Delay varies dependant on Internet conditions - Unreliable - Asymmetric bandwidths

SDSL (Symmetric Digital Subscriber Line)	1Mbps – 10Mbps	- Symmetric bandwidth	- Availability – only certain areas are SDSL enabled - Contention (shared bandwidth) - No bandwidth guarantees - Delay varies dependant on Internet conditions - Unreliable
BT Baseband - EPS 8 (4-wire) - EPS 9 (2-wire)	Depends on cable quality and distance between endpoints (up to 2Mbps)	- Inexpensive - No contention	- Both ends must be located on same Telephone Exchange - Bandwidth depends on cable quality and distance between endpoints – can be relatively low
Wireless LAN	Typically up to 54Mbps	- Inexpensive (running costs)	- Can be unreliable - Limited distance - Difficult to implement QoS
ISDN (Integrated Services Digital Network)	64Kbps per "B" channel	- Inexpensive (install) - Guaranteed bandwidth - No contention - Reliable	- Not an "always on" solution - Limited speed - High call costs

Note: These services may not be available in your country

1.3 3. Implementing QoS

We have seen some of the problems associated with Voice Quality in Section 2. This section looks at how QoS can be implemented on data networks to provide the "best case" for VoIP traffic.

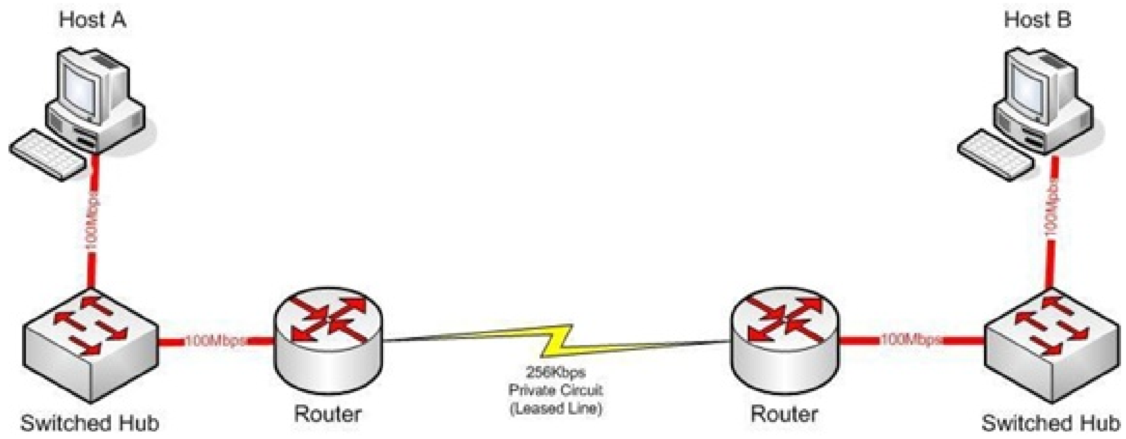
It should be noted that not all network hardware supports QoS and each manufacturer will have their own methods of implementing QoS. The explanations below are intended to be as generic as possible. The installer/maintainer of the data network should be familiar with the QoS characteristics of their equipment and should be able to configure the equipment accordingly.

The term Quality of Service is commonly used to describe the actual implementation of Prioritisation on network hardware. This prioritisation (at Layer 2 and Layer 3 of the OSI model) is described below.

3.1 What is Prioritisation?

When data is transmitted through a network it will typically encounter "bottlenecks". This is where the amount of available bandwidth is reduced, or the amount of data increases. This means that the packet delivery is affected.

Consider data communication between the two computers shown in the diagram below. The Hosts are capable of transmitting data at 100Mbps. When a packet from Host A (destined for Host B) reaches the router, the available bandwidth is reduced to 256Kbps and the packet flow must be reduced. This is an example of a bottleneck.



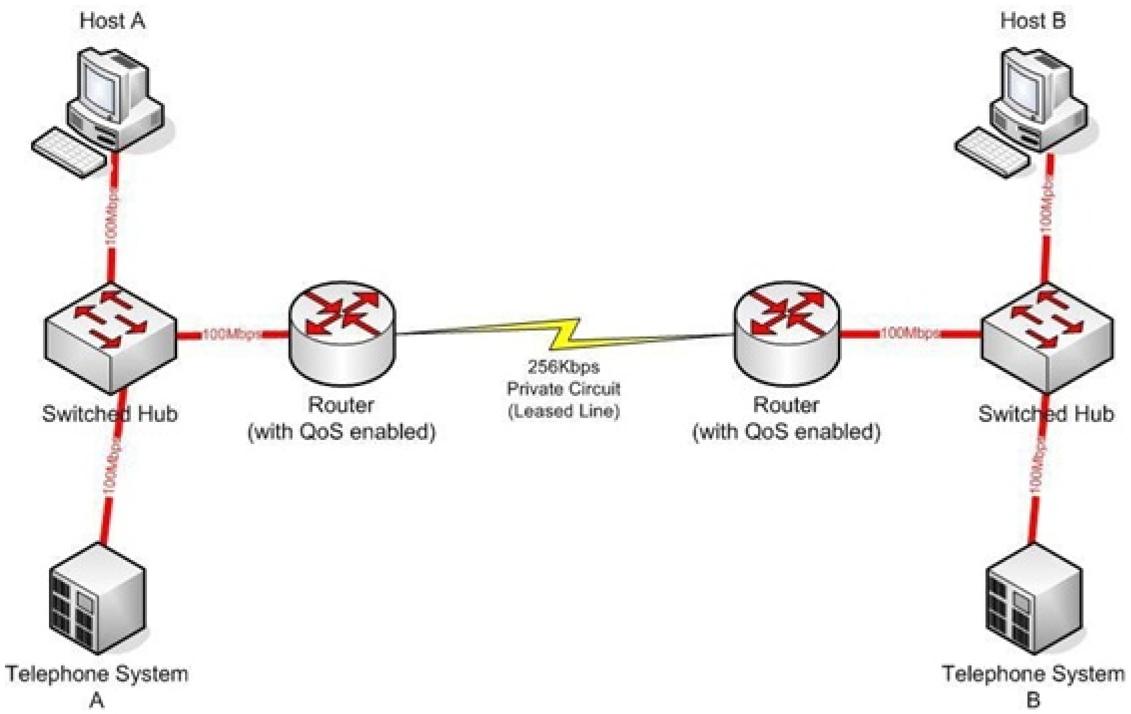
In this case there is only one host on each end of the network which is unrealistic. In reality there would be many hosts all sending data over the narrow bandwidth. This means that the routers must buffer the packets and transmit them over the Kilostream as efficiently as possible. When this occurs, certain packets will be dropped by the router and some packets will be delayed.

For most data applications this packet loss/delay is not critical. For example, it is unlikely to be noticed if an email takes 1 second or 5 seconds to be transmitted. When VoIP is implemented, this loss/delay has a massive impact on the voice quality. There will be gaps in speech, distortion and delay – all of which are unacceptable for voice traffic.

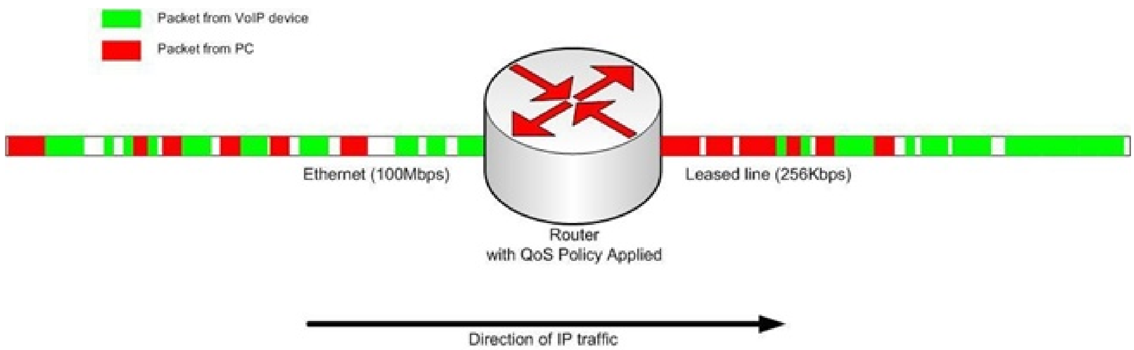
To avoid this problem, it is possible to prioritise the VoIP packets. This means that the router will examine all packets received, determine what priority level the packet has, and then forward it accordingly. This of course means that the "data1" will be assigned lower priority and the "voice" will be transmitted before it. This can have a negative impact on the "data" network if lots of "voice" is transmitted.

[1] Note that this description discusses "voice" and "data". These terms are commonly used when describing QoS, although in the case of VoIP, the voice is actually converted to IP and transmitted as data. Therefore, everything transmitted on a Data Network is data, but logically we think of this as "voice" and "data" traffic.

The diagram below shows how a "voice" and "data" network may be implemented.



Once the router has been configured for QoS, it will examine incoming packets and allocate the relevant priority to the packet. The diagram below shows the effect that Priority Queuing would have on "voice" and "data" networks. The packets arrive randomly and are processed and output according to the QoS policy – in this case VoIP traffic is output first.



To enable this type of queuing it is necessary to:

a) Configure the VoIP equipment to mark its packets with a specific value so that the switches/ routers can identify that it is "voice" - known as Marking
b) Configure the network equipment to recognise the difference between the different "Marked" packets – known as Classification. i.e. Inform the router what a "voice" packet looks like.
c) Configure the network equipment to give priority to the packets that have been classified as "voice" – known as Priority Queuing

3.2 Layer 2 QoS (802.1pq)

QoS is most commonly implemented at Layer 3 of the OSI model. This layer deals with IP addresses, and is usually handled by Routers. However, sometimes it is necessary to implement Layer 2 QoS – usually in large LAN environments with many IP phones.

Layer 2 devices work with Ethernet frames (encapsulated IP packets) rather than IP addresses. These devices are usually Switched Hubs (Switches). As the IP header information is encapsulated, the Switched Hubs are not able to reference the Type of Service (see: **Layer 3 QoS**) field in the IP header to determine the priority of a frame

Layer 2 QoS uses the Priority field of the Ethernet frame. This field is three bits long and can have 8 possible values (000 to 111 in binary). Some switches can be configured to prioritise traffic based on these values.
This field is only available if the Ethernet device is configured for VLAN (IEE802.1q) operation (VLAN is outside the scope of this document).

Protocol Structure - IEEE 802.1p: LAN Layer 2 QoS

The diagram below shows the format of an Ethernet frame, and the User Priority field that is used for Layer 2 QoS.

IEEE 802.1Q Tagged Frame for Ethernet:								
7 bytes	**1 byte**	**6 bytes**	**6 bytes**	**2 bytes**	**2 bytes**	**2 bytes**	**42 - 1496 bytes**	**4 bytes**
Preamble	SFD	DA	SA	TPID	TCI	Type Length	Data	CRC

Expanded view of TCI Field		
3bits	**1bit**	**12bits**
User Priority	CFI	Bits of VLAN ID (VID) to identify possible VLANs

Preamble (PRE) - The PRE is an alternating pattern of ones and zeros that tells receiving stations that a frame is coming, and that provides a means to synchronize the frame-reception portions of receiving physical layers with the incoming bit stream.
Start-of-frame delimiter (SFD) - The SOF is an alternating pattern of ones and zeros, ending with two consecutive 1-bits indicating that the next bit is the left-most bit in the left-most byte of the destination address. Destination address (DA) - The DA field identifies which station(s) should receive the frame.
Source addresses (SA) - The SA field identifies the sending station.
TPID - defined value of 8100 in hex. When a frame has the EtherType equal to 8100, this frame carries the tag IEEE 802.1Q / 802.1P.
TCI - Tag Control Information field including user priority, Canonical format indicator and VLAN ID.
User Priority - Defines user priority, giving eight priority levels. IEEE 802.1P defines the operation for these 3 user priority bits.
CFI - Canonical Format Indicator is always set to zero for Ethernet switches. CFI is used for compatibility reason between Ethernet type network and Token Ring type network.

VID - VLAN ID is the identification of the VLAN, which is basically used by the standard 802.1Q. It allows the identification of 4096 VLANs.
Length/Type - This field indicates either the number of MAC-client data bytes that are contained in the data field of the frame, or the frame type ID if the frame is assembled using an optional format.
Data - Is a sequence of bytes of any value. The total frame minimum is 64bytes.
Frame check sequence (FCS) - This sequence contains a 32-bit cyclic redundancy check (CRC) value, which is created by the sending MAC and is recalculated by the receiving MAC to check for damaged frames.

Example Ethernet Frame with Layer 2 QoS enabled

The example below shows an Ethernet Frame containing one RTP (speech) packet. The Frame has been VLAN tagged, has a VLAN ID of 99 and a VLAN Priority of 5. It is also possible to see that the Layer 3 QoS has not been set.

```
Source          Destination     Protocol

172.16.0.101
Payload type=ITU-T G.729, SSRC=701655963, Seq=28165, Time=21520


Frame 160 (78 bytes on wire, 78 bytes captured)

    Arrival Time: Jan 18, 2005 13:55:44.842738000

    Time delta from previous packet: 0.008241000 seconds
    Time since reference or first frame: 2.910072000 seconds
    Frame Number: 160

    Packet Length: 78 bytes
    Capture Length: 78 bytes

Ethernet II, Src: 00:60:b9:c6:6e:45, Dst: 00:60:b9:c1:ab:a3
    Destination: 00:60:b9:c1:ab:a3 (Nitsuko_c1:ab:a3)
    Source: 00:60:b9:c6:6e:45 (Nitsuko_c6:6e:45)

    Type: 802.1Q Virtual LAN (0x8100)

802.1q Virtual LAN

    101. .... .... .... = Priority: 5        (Layer 2 Priority = 5)

    ...0 .... .... .... = CFI: 0

    .... 0000 0110 0011 = ID: 99

    Type: IP (0x0800)

Internet Protocol, Src Addr: 172.16.0.101 (172.16.0.101), Dst Addr: 172.16.0.21 (172.16.0.21)

    Version: 4

    Header length: 20 bytes

    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)

        .... ..0. = ECN-Capable Transport (ECT): 0

        .... ...0 = ECN-CE: 0

    Total Length: 60

    Identification: 0x0086 (134)
    Flags: 0x00

        0... = Reserved bit: Not set

        .0.. = Don't fragment: Not set
```

3.3 Layer 3 QoS

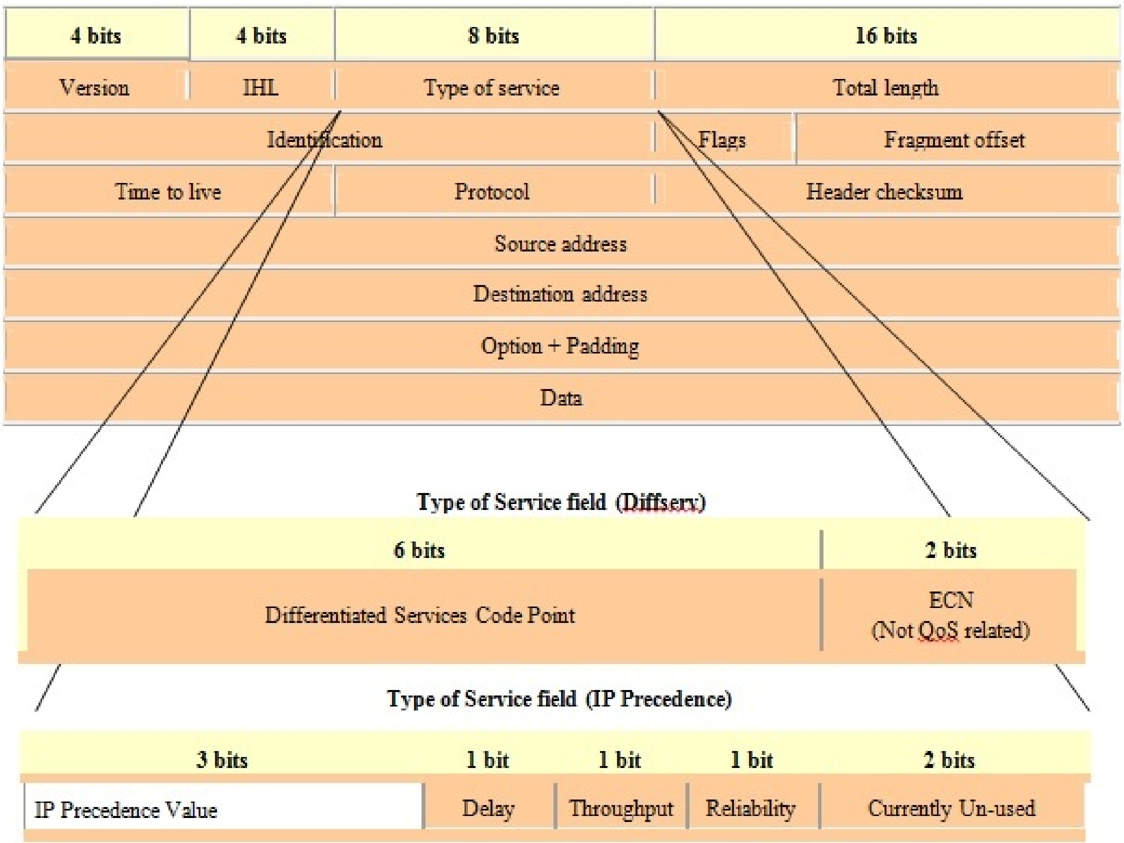
QoS is most commonly implemented at Layer 3. This allows the VoIP packets to be prioritised by routers, before they are forwarded to their next hop.

Layer 3 QoS uses the Type of Service (ToS) field of the IP packet. This is an 8 bit field in the header of the IP packet. The field can be used by Diffserv or IP Precedence. Although these are two different standards, the actual field in the IP packet is the same - it is just the value that differs.

Please note that by QoS will not function just by utilizing the ToS field (i.e. Marking the VoIP packets). It is an end-to-end process and requires configuration on all networking devices. Packet

Marking is the first step in this process and is often the only step that the NEC dealer will perform.

Protocol Structure - IP/IPv4 Header (Internet Protocol version 4)



Version - the version of IP currently used.
IP Header Length (IHL) - datagram header length. Points to the beginning of the data. The minimum value for a correct header is 5.
Type-of-Service - Indicates the quality of service desired by specifying how an upper-layer protocol would like a current datagram to be handled, and assigns datagrams various levels of importance. This field is used for the assignment of Precedence, Delay, Throughput and Reliability.
Total Length - Specifies the length, in bytes, of the entire IP packet, including the data and header. The maximum length could be specified by this field is 65,535 bytes. Typically, hosts are prepared to accept datagrams up to 576 bytes.
Identification - Contains an integer that identifies the current datagram. This field is assigned by sender to help receiver to assemble the datagram fragments.
Flags - Consists of a 3-bit field of which the two low-order (least-significant) bits control fragmentation. The low-order bit specifies whether the packet can be fragmented. The middle bit specifies whether the packet is the last fragment in a series of fragmented packets. The third or high-order bit is not used.
Fragment Offset - This 13 bits field indicates the position of the fragment's data relative to the beginning of the data in the original datagram, which allows the destination IP process to properly reconstruct the original datagram.
Time-to-Live - It is a counter that gradually decrements down to zero, at which point the datagram is discarded. This keeps packets from looping endlessly.
Protocol - Indicates which upper-layer protocol receives incoming packets after IP processing is

complete.
Header Checksum - Helps ensure IP header integrity. Since some header fields change, e.g., Time To Live, this is recomputed and verified at each point that the Internet header is processed.
Source Address - Specifies the sending node.
Destination Address - Specifies the receiving node.
Options - Allows IP to support various options, such as security.
Data - Contains upper-layer information.

3.4 IP Precedence

IP Precedence is a QoS method that combines a priority value with three different on/off parameters; Delay, Throughput, and Reliability.

Using the ToS bits, you can define up to 8 classes of service. Other devices configured throughout the network can then use these bits to determine how to treat the packet in regard to the type of service to grant it. These other QoS features can assign appropriate traffic-handling policies including congestion management and bandwidth allocation. By setting IP Precedence levels on incoming traffic and using them in combination with QoS queuing features, you can create differentiated service.

Type of Service Field (IP Precedence)

3 bits	1 bit	1 bit	1 bit	2 bits
IP Precedence Value	Delay	Throughput	Reliability	Currently Un-used

IP Precedence Values

Value	Binary Value	Description
0	000	Routine
1	001	Priority
2	010	Immediate
3	011	Flash
4	100	Flash override
5	101	CRITIC/ECP
6	110	Internetwork control
7	111	Network control

Delay

Value	Description
0	Normal delay
1	Low delay

Throughput

Value	Description

0	Normal throughput
1	High throughput

Reliability

Value	Description
0	Normal throughput
1	High throughput

3.5 Diffserve (Differentiated Services)

Differentiated Services (Diffserv) is a method of utilising ToS field in an IP header. Diffserv is now commonly used instead of IP Precedence as it provides greater flexibility. This method uses 6 bits of the ToS field to determine the priority – which provides up to 64 possible values. The combination of binary digits is known as the Diffserv Code Point (DSCP).

Type of Service Field (Diffserve)

6 bits	2 bits
Differentiated Services Code Point	ECN (Not QoS related)

The example below shows an Ethernet Frame containing one RTP (speech) packet. The IP Packet has the ToS field set to 101000 (binary) which is the equivalent of Class Selector 5. The router(s) in this network should be programmed to prioritise based on CS5.

```
Source           Destination        Protocol

172.16.0.21
Payload type=ITU-T G.729, SSRC=732771006, Seq=30885, Time=20560


Frame 159 (65 bytes on wire, 65 bytes captured)

    Arrival Time: Jan 18, 2005 13:55:44.834497000

    Time delta from previous packet: 0.000445000 seconds
    Time since reference or first frame: 2.901831000 seconds
    Frame Number: 159

    Packet Length: 65 bytes
    Capture Length: 65 bytes

Ethernet II, Src: 00:60:b9:c1:ab:a3, Dst: 00:60:b9:c6:6e:45
    Destination: 00:60:b9:c6:6e:45 (Nitsuko_c6:6e:45)
    Source: 00:60:b9:c1:ab:a3 (Nitsuko_c1:ab:a3)

    Type: IP (0x0800)

Internet Protocol, Src Addr: 172.16.0.21 (172.16.0.21), Dst Addr: 172.16.0.101 (172.16.0.101)

    Version: 4

    Header length: 20 bytes

    Diff Services Field: 0xa0 (DSCP 0x28: Class Selector 5; ECN: 0x00)
        1010 00.. = Diff Services Codepoint: Class Selector 5 (0x28)

        .... ..0. = ECN-Capable Transport (ECT): 0

        .... ...0 = ECN-CE: 0

    Total Length: 44

    Identification: 0x0069 (105)
    Flags: 0x00

        0... = Reserved bit: Not set

        .0.. = Don't fragment: Not set

        ..0. = More fragments: Not set
    Fragment offset: 0
```

3.6 Comparison of IP Precedence and Diffserv Values

As stated earlier, IP Precedence and Diffserv use the same field in the IP header to mark packets. It is possible to have the same ToS value for either method which means that the two methods can work alongside each other.

For example, if the VoIP equipment supports IP Precedence and the router can only prioritise using the DSCP they can be set to the same value, as per the table below:

DSCP Decimal	DSCP Binary	IP Precedence	Description
0	000000	0	Class Selector 0
1	000001		
2	000010		

3	000011		
4	000100		
5	000101		
6	000110		
7	000111		
8	001000	1	Class Selector 1
9	001001		
10	001010		AF11 (Assured Forwarding)
11	001011		
12	001100		AF12 (Assured Forwarding)
13	001101		
14	001110		AF13 (Assured Forwarding)
15	001111		
16	010000	2	Class Selector 2
17	010001		
18	010010		AF21 (Assured Forwarding)
19	010011		
20	010100		AF22 (Assured Forwarding)
21	010101		
22	010110		AF23 (Assured Forwarding)
23	010111		
24	011000	3	Class Selector 3
25	011001		
26	011010		AF31 (Assured Forwarding)
27	011011		
28	011100		AF32 (Assured Forwarding)
29	011101		
30	011110		AF33 (Assured Forwarding)
31	011111		
32	100000	4	Class Selector 4
33	100001		
34	100010		AF41 (Assured Forwarding)
35	100011		
36	100100		AF42 (Assured Forwarding)
37	100101		
38	100110		AF43 (Assured Forwarding)
39	100111		
40	101000	5	Class Selector 5

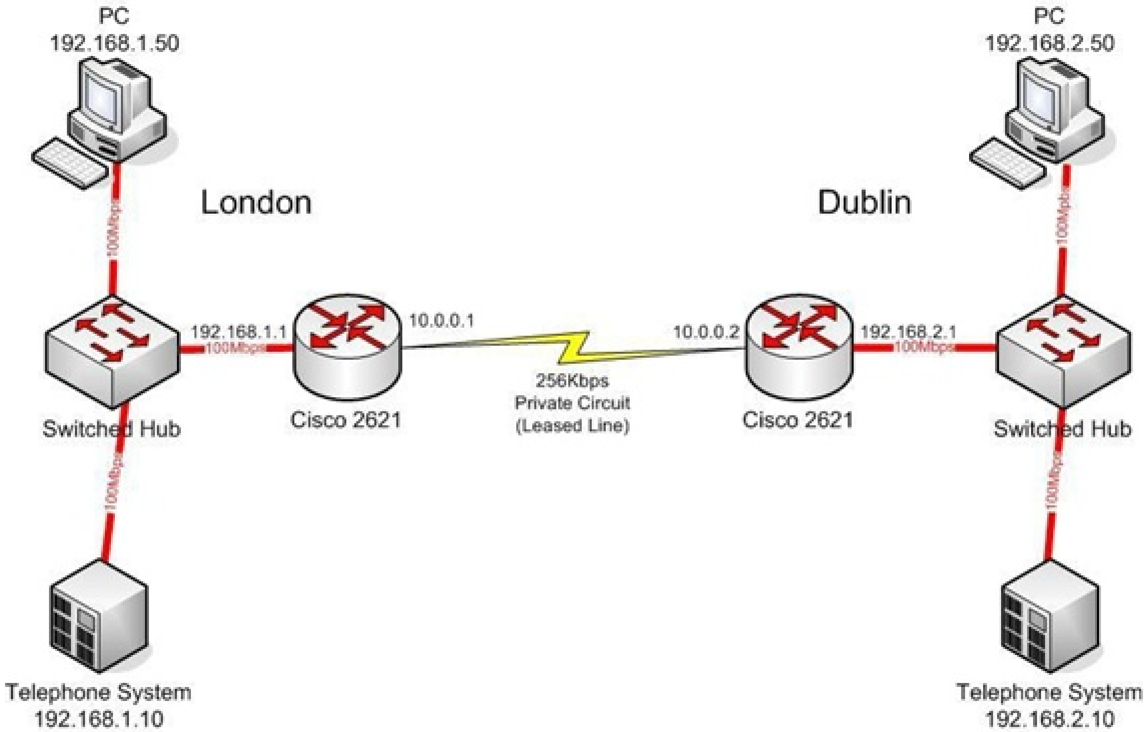
41	101001		
42	101010		
43	101011		
44	101100		
45	101101		
46	101110		EF (Expedited Forwarding)
47	101111		
48	110000	6	Class Selector 6
49	110001		
50	110010		
51	110011		
52	110100		
53	110101		
54	110110		
55	110111		
56	111000	7	Class Selector 7
57	111001		
58	111010		
59	111011		
60	111100		
61	111101		
62	111110		
63	111111		

3.7 Example Configurations

The diagram below shows a common network scenario and an example of a Cisco router configuration.

Note:
This document aims to provide a general description of VoIP technology without discussing individual manufacturer's solutions. However, this sample configuration has been provided as it is a common scenario and is a good example of how QoS can be implemented on a router.

NEC do not endorse or provide support on any third party equipment unless it is supplied by NEC.



The configuration file below shows the London Cisco 2621 router configuration. Some unrelated configuration has been removed. A description of some of the key commands can be found below the configuration.

```
Current configuration : 2023 bytes
!
version 12.3 hostname Cisco2621
!
class-map match-any VoIPClass         (1)
match ip dscp cs5                     (2)
policy-map VoIPPolicy                 (3)
class VoIPClass                       (4)
priority 50                           (5)
class class-default                   (6)
fair-queue                            (7)
!
interface FastEthernet0/0 description Connects to London LAN
ip address 192.168.1.1 255.255.255.0
!
interface Serial0/0
description Connects to Dublin via Kilostream
bandwidth 256                         (8)
ip address 10.0.0.1 255.255.0.0
service-policy output VoIPPolicy      (9)
encapsulation ppp
!
ip route 0.0.0.0 0.0.0.0 10.0.0.2
```

Explanation

1) Defines a Class Map called VoIPClass
2) Matches any packets that have the ToS field set to IP Precedence 5 / DSCP 40 and assigns them to VoIPClass

3) Defines a Policy Map called VoIPPolicy
4) Creates a Class called VoIPClass and assigns this to the VoIPPolicy
5) Allocates 50Kbps of bandwidth to the VoIPClass
6) and 7) Determines that any data that does not match VoIPClass should be processed using the "fair-queue" method (ie. No prioritisation)
7) Determines the amount of bandwidth available on the Serial interface – essential for the QoS calculations
8) Applies the VoIPPolicy to any packets that exit the serial interface. This means that data being received (input) will not use this policy.

1.4 4. Other Issues Affecting VoIP

4.1 Internet Based Connections

Internet-based connections are becoming increasingly popular. This is mainly due to the speed and cost of xDSL and cable modem connections. For data applications, these types of connection are generally acceptable. For Voice over IP applications there are several issues that should be taken into consideration.

Asymmetric data rates:
On many internet based connections, there are different data rates for upstream and downstream. For example 8Mbps down and 512Kbps up. This works well for internet access, as generally you download files from the internet to your PC and transmit less information in the other direction. For VoIP, speech uses the same amount of bandwidth in both directions, which means that the amount of simultaneous calls cannot exceed the amount of "upstream" bandwidth available.

Contention:
Most internet based connections specify a "contention ratio". This is typically 50:1 for home users or 20:1 for business users. This specifies the number of users subscribed to a single connection to the ISP. This means that you share the bandwidth with other users on the internet which means that the speeds that you are quoted are not necessarily accurate - you will receive less than these figures.

Note that it is unlikely that all of the subscribers will be using a connection at any one time, so these figures are not quite as bad as they first seem.

NAT:
Usually, the equipment that your ISP provides (cable modem, ADSL router, etc.) will use Network Address Translation. This allows several devices to share one public IP address. The issues relating to the use of NAT are outlined in "Firewalls and NAT" below.

VPN:
Due to the use of NAT, and non-routable IP addressing, it is necessary to implement a VPN solution. This is outlined in "VPN Tunnelling" below.

QoS:
As discussed earlier, it is essential to have some form of Quality of Service implemented. With internet based connections, we are not in control of the many routers, switches and other network hardware that reside between our two VoIP endpoints. This means that we are unable to specify any QoS parameters on these devices.

The only point in which we can control the QoS is at the VPN or firewall. This allows us to prioritise VoIP traffic over any other data that we send out to the internet. This helps to maintain reasonable quality speech - but once the data has exited the local router/cable modem it is at the mercy of the internet.

Summary:
When implementing VoIP using internet based connections it is very important that these factors are considered, and that the customer is made aware that you (the installer) or NEC cannot be held responsible for any quality issues experienced.

4.2 Firewalls

Network security is always a concern when connecting the LAN (Local Area Network) to the WAN (Wide Area Network). There are many ways to integrate security within the network - the most popular of which at Firewalls and Proxy servers.

Firewalls
Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorised Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

Proxy Server
Proxy server intercepts all messages entering and leaving the network. The proxy server effectively hides the true network address.

What should be noted is that no matter which security measure is implemented, the VoIP will have to have TCP/UDP ports open within the security wall (e.g. firewall/proxy) in order for the media and control streams to flow. If any of the points within the network prevent the ports from flowing from end to end, the VoIP application will not work.

The ports that need to be “open” on the firewall/proxy vary depending on the particular application being used, and the manufacturer of the equipment. A list of these ports is available in the relevant NEC product manual, however it should be noted that the preferred solution would be to allow all ports for the VoIP device to be open, or for the VoIP device to be located outside of the firewall.

4.3 Network Address Translation (NAT)

Network Address Translation is a technology that has been developed to enable several users to share one single Public IP address. This is partially in response to the lack of Public IP addresses.

Most of our home networks are NAT enabled. For example, you may have a DSL connection with one Public IP address, but want to have multiple computers/devices connected to the Internet. NAT integration within your switch or router provides a mapping of internal (private) IP addresses to public addresses (routable addresses) therefore allowing you the capability of having a multitude of different devices (nodes) connected to one routable address.

This re-routing of IP address from one address (Private Address) to another (Public Address) and the allowing of only selected ports to be opened create problems for the VoIP.

When a VoIP terminal receives a VoIP packet from a far-end site, the voice application routes information back to the far-end based on the embedded address. With the ports and addressing for the VoIP packets being defined at a layer to which the NAT device doesn't operate, a problem is created due to the addresses not matching and the correct ports not opening in the NAT device.

In order to resolve the NAT issues mentioned, the VoIP communication packets must be preconditioned for a VPN protocol before exiting from a NAT enabled network.

- SIP MLT (DT700 or DT800) and standard SIP extensions are able to traverse NAT routers without using a VPN. See the relevant section of the on line IP Manual for further information.

The Virtual Private Networks (VPN) section below describes how VPNs achieve this.

4.4 Virtual Private Networks (VPN)

A Virtual Private Network is a private data network that maintains privacy through the use of a tunnelling protocol and security procedures. Allowing for remote networks (including VoIP devices), which reside behind

NAT's and/or Firewalls to communicate freely with each other. In SV9100 VoIP networks, implementation of VPNs can resolve the issues with NAT that are described in the previous section.

The idea of the VPN is to connect multiple networks together using public (i.e. internet) based connections. This type of connection is ideal for those commuters, home workers, or small branch offices needing connectivity into the corporate backbone. It is possible to connect these remote networks together using private links (such as leased lines, ISDN, etc.) but this can be very expensive and there is now a high demand for low cost internet connectivity.

Companies today are looking at using a VPN for a variety of connectivity solutions, such as:

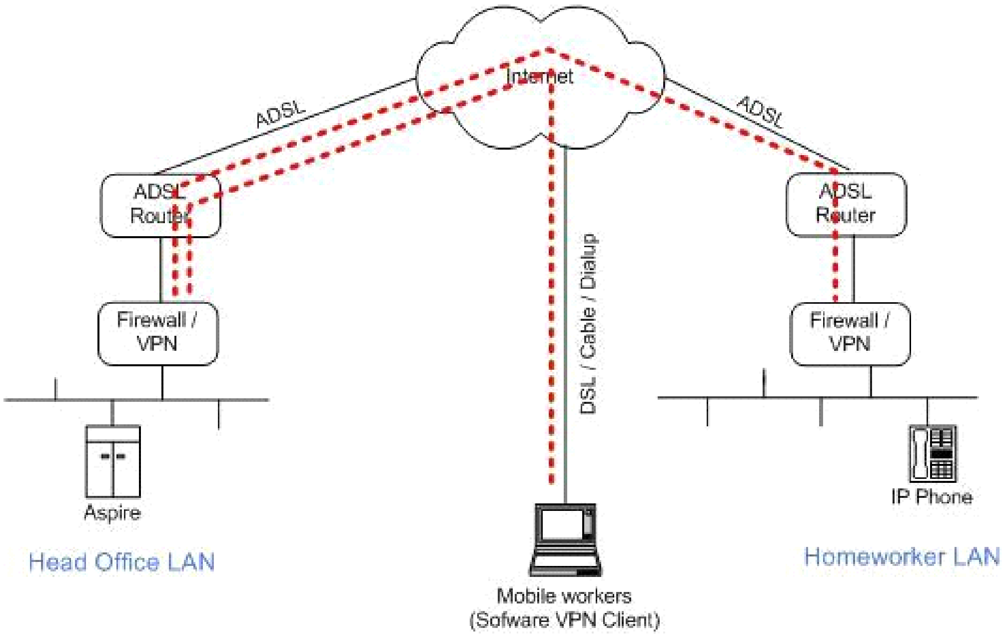
Remote User to Corporate Site VPN
Allows employees to use their local ISP's fastest connection such as cable modems or DSL. For travelling users, all they would need to do is dial into their ISP's local phone number.

Site-to-site VPN
Allows companies to make use of the Internet for the branch-to-branch connections, cutting the cost of the expensive point to point leased line service.

Extranet
Extranet describes one application using VPN technology. The concept is that a company and a vendor/supplier can access network resources at each site. For example, a customer may have access to a supplier’s intranet for access to product information

VPNs can be implemented in hardware or software. For single users, such as travelling sales personnel may have a software based VPN client on their laptop computer. This would connect back to the Head Office VPN server. For larger sites, the VPN would typically be implemented using a hardware VPN - this is often incorporated in to a firewall solution.

The diagram below shows an example of how a VPN tunnel may be implemented. The dotted lines show the tunnels that have been created through the internet. Each network can connect to the others as though they are connected with private connections (kilostream, etc.), without the issues relating to NAT.



Conclusion
When IP address translation is applied to a VoIP packet, the application fails and the communication path is broken. VoIP packets contain the IP address information and the ports used as part of its payload. When NAT

(Network Address Translation) is applied, only the header parameter is changed, not the payload data that affects the process of data packets within the VoIP switch and terminal. In order to support the addressing and port fluctuation that occurs when system IP Phones are deployed in remote facilities, VPN services are required.

Three most common scenarios for remote IP deployment are as follows;

1) Implementation of a system IP Phone behind a NAT talking to an SV9100 that has a public IP address. This would be a scenario where a telecommuter or a branch office talking to the SV9100 at the central site.

2) Implementation of a system IP Phone with a public IP address talking with an SV9100 behind NAT. An example would be a telecommuter.

3) Implementation of a system IP Phone behind a NAT, which connects to the internet, terminating into an SV9100 behind a different NAT.

When selecting VPN equipment it is important to consider Quality of Service. Generally VPN hardware is connected to internet connections which are unreliable and out of the control of the customer. (See: **Internet Based Connections**). However, it is possible to set prioritisation on some VPN units for voice traffic. This does not solve the unreliability of the internet, but helps to ensure that the data traffic to and from your LAN do not impair the quality of the voice traffic. (QoS is discussed in the **Quality of Service** section above).

It is highly recommended that any VPN hardware used for VoIP has the facility to prioritise voice traffic.

1.5 5. Troubleshooting

This section aims to provide some helpful tips to perform Voice Over IP troubleshooting.

The first step in resolving any issues would be to read through the relevant manuals/documentation and refer to any example configurations. If you are unable to resolve the issue using the documentation it may be helpful to use the tools outlined below.

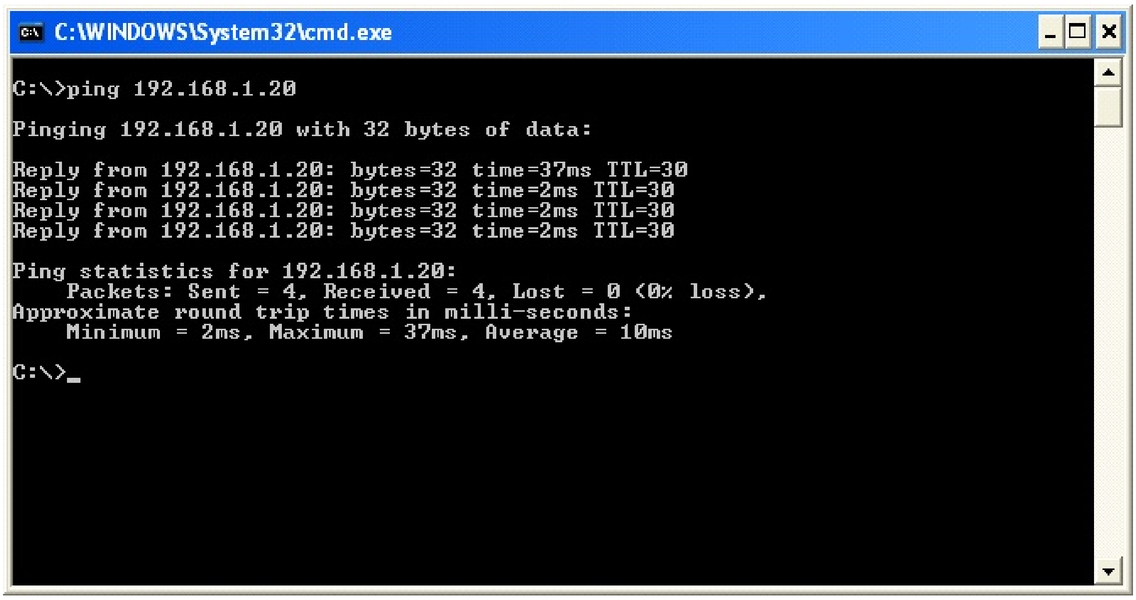
5.1 PING

This is one of the most useful tools available to troubleshoot IP connectivity. PING is a standard component of Microsoft Windows and is also implemented in the SV9100 SIP MLT IP Phones. PING sends a small IP packet to a specified destination and waits for a response back.

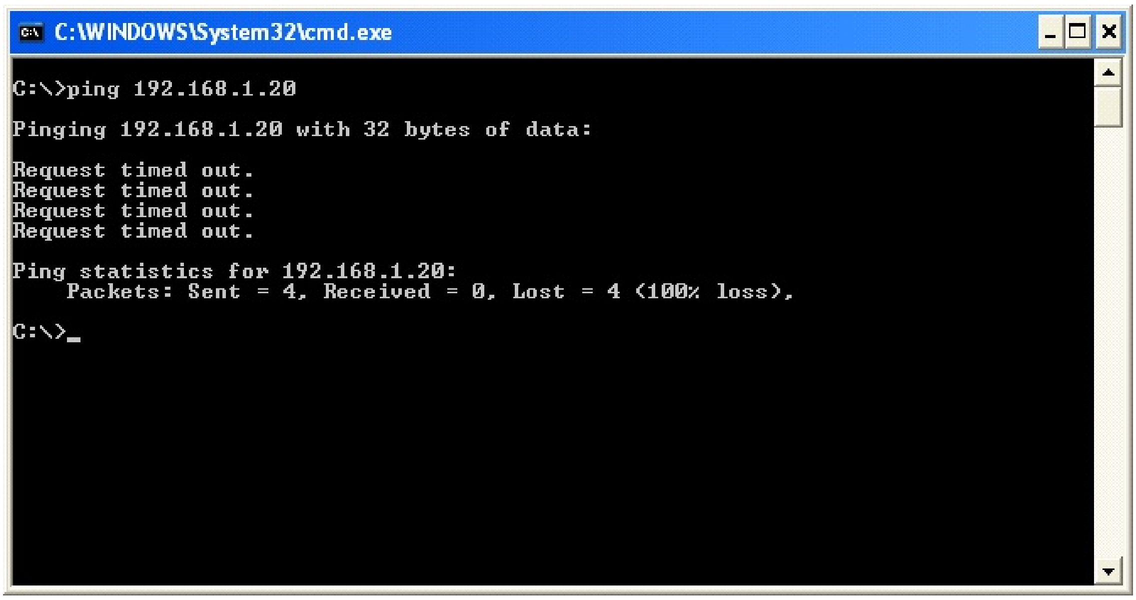
It should be possible to ping system IP Phones, the GCD-CP10, GPZ-IPLE and any other devices on the network. When you send a ping, you wait for a reply. If you do not receive a reply, the ping response “times-out”. This indicates a connection problem.

The ping traces below show these two conditions:

Successful PING



Unsuccessfull PING



If you are unable to ping a device it may mean that either the source or destination device:

- is not configured correctly
- is not connected to the LAN (e.g. cable disconnected)
- has a developed a fault

or any device in between the source or destination may be faulty (e.g. routers)

Pinging from a PC

The command syntax for ping is: ping [-t] [-n count] [-l size] target

-t (optional)	continually sends PING requests until Ctrl-C is pressed to cancel
-n (optional)	sends a specified number of PING requests
-l (optional)	sends packets of a specified size (bytes)
target	the destination IP address or host name

Note that there are other options available with the Microsoft Windows implementation of ping. The most commonly used options are listed above.

Examples:

ping 192.168.2.100 -t	Continually pings 192.168.2.100 until Ctrl-c pressed
ping 192.168.2.100 -n 10 -l 40	Sends ten 40-byte packets to 192.168.2.100
ping 192.168.2.100	Sends four 32-byte packets (default) to 192.168.2.100

Pinging from an DT700 or DT800 IP Phone

The IP Phone has a version of ping within the Maintenance Menu.

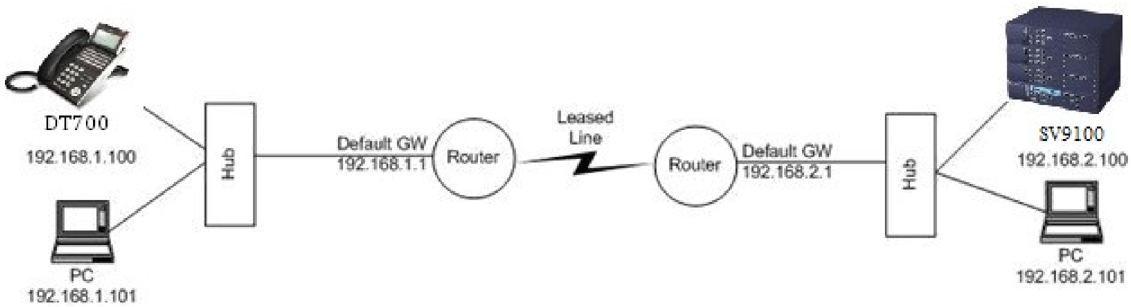
- Enter Maintenance Menu (Press Help key for 2 seconds)
- Press 3 (Ping)
- Enter the Destination IP Address that you wish to ping. (Use * for .)
- Press OK.

If the ping is successful you see OK after each ping. If it fails you will see NG

- Press the Exit button to return the phone to normal operation.

An example of ping usage:

A DT700 Phone unsuccessfully attempts to connect to the SV9100 as shown below:



From the diagram above we can see that there are several devices that could cause this connection problem:

- DT700 Phone (192.168.1.100)
- Local Hub
- Local router (192.168.1.1)
- Leased line
- Remote Router (192.168.2.1)
- Remote Hub
- SV9100 VoIPDB (192.168.2.100)

You will see that by pinging from the DT700 Phone and PCs, we can work out where the problem lies by process of elimination. We start by pinging the nearest device and working outwards towards our intended destination

Examples:

- The DT700 can successfully ping all devices up to and including the local router. Anything beyond that point fails. This would suggest that the Leased Line or remote router has a problem.

- The local PC (192.168.1.101) can ping all devices apart from the DT700. DT700 cannot ping anywhere. This would suggest that there is a problem with the DT700 or its connection to the switch/hub.

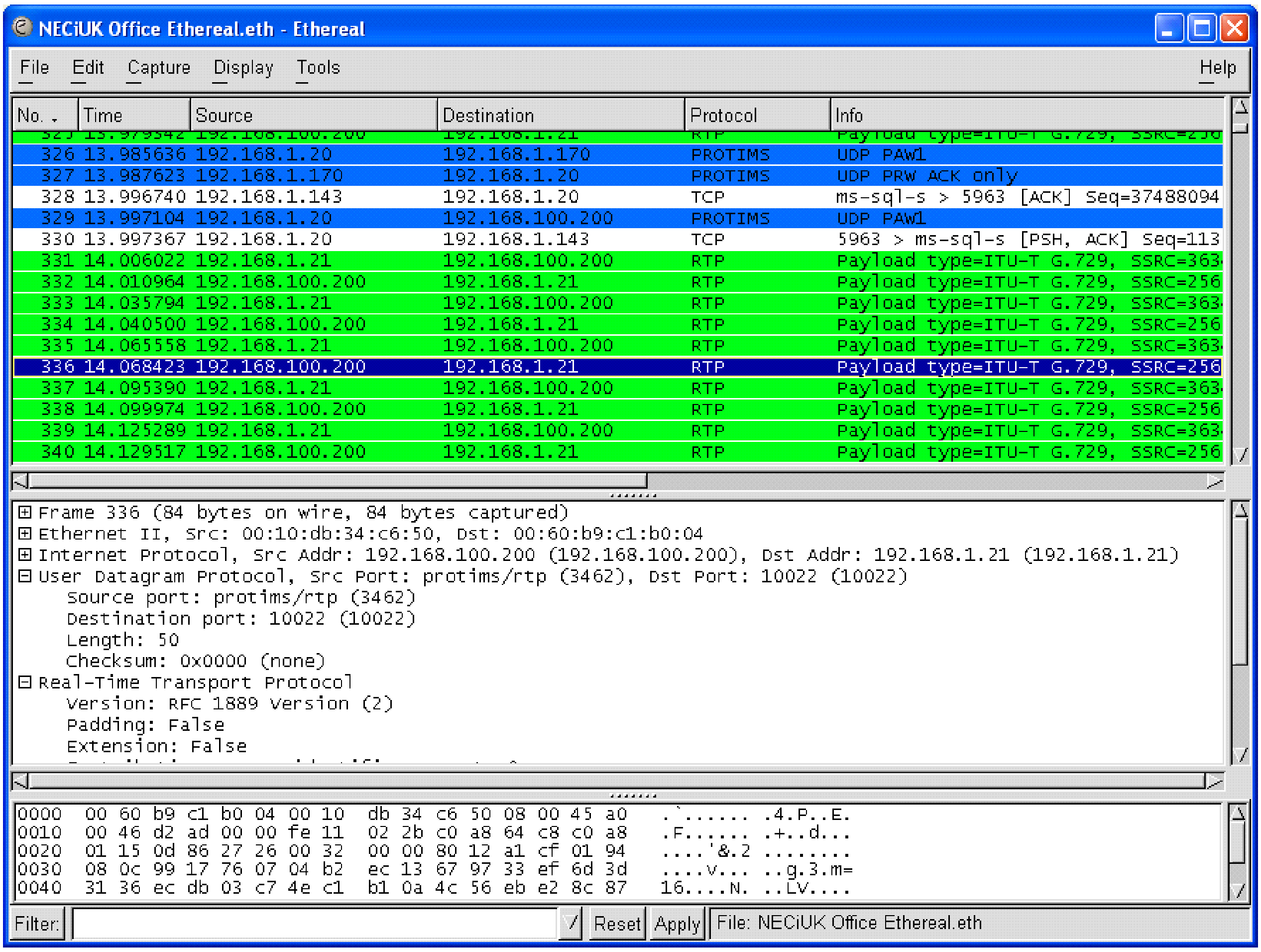
5.3 Packet Traces

It is possible to use a packet trace utility (also known as “Sniffers”) to determine what data is being transmitted and received on an Ethernet network. These can be particularly useful to determine the cause of connection issues or voice quality issues.

The packet trace utility has to be run on a PC connected to the same hub (not a switched hub) that the SV9100 or IP Phone is connected to.

There are many utilities available that will allow you to run a packet trace on a network. One such utility is Wireshark. This is a software application distributed under a GNU general public licence (see www.wireshark.org). This allows the files to be captured and saved in a standard format for analysis later. This utility is supplied on the Technical CD.

A sample trace file is shown below.



1.6 6. Glossary

802.1p
An IEEE standard for providing QoS using three bits (defined in 802.1q) to allow switches to reorder packets based on priority level.

802.1q
An IEEE standard for providing virtual LAN (VLAN) identification and QoS levels. Three bits are used to allow eight priority levels, and 12 bits are used to identify up to 4,096 VLANs.

ADPCM
Adaptive differential pulse code modulation. Process by which analog voice samples are encoded into high- quality digital signals.

Bit
Binary Digit. The smallest unit of data transmission (0 or 1)

Broadband
Descriptive term for evolving digital technology that provides consumers a single switch facility offering integrated access to voice, high-speed data service, video demand services, and interactive delivery services.

BW
Bandwidth.

CBR
Constant Bit rate. Constant bit rate. QoS class defined by the ATM Forum for ATM networks. CBR is used for connections that depend on precise clocking to ensure undistorted delivery.

CELP
Code excited linear prediction compression. Compression algorithm used in low bit-rate voice encoding. Used in ITU-T Recommendations G.728, G.729, G.723.1.

Circuit Switching
Circuit switching is a WAN switching method in which a dedicated Physical circuit through a carrier network is established, maintained, and terminated for each communication session. Used extensively in telephone company networks, operates much like a normal telephone call.

CIR Committed Information rate
Rate at which a Frame Relay network agrees to transfer information under normal conditions, averaged over a minimum increment of time. CIR, measured in bits per second, is one of the key negotiated tariff metrics.

CODEC
In Voice over IP, Voice over Frame Relay, and Voice over ATM, a DSP software algorithm used to compress/decompress speech or audio signals.

Compression
Compression is used at anywhere from 1:1 to 12:1 ratios in VOIP applications to consume less bandwidth and leave more for data or other voice/fax communications. The voice quality may decrease with increased compression ratios.

Connection-oriented
Mode of communication in which a connection must be established between the transmitter and receiver before transmission of user data. This can be done by switching a circuit or by setting up a logical channel. A well- known connection-oriented protocol is TCP. Connection-oriented is the opposite of connectionless.

Connectionless
Mode of communication in which a connection (circuit or logical channel) does not need to be set up for data transmission between the transmitter and receiver. It is the underlying protocol for packet-switched transmission. The individual data packets can go from the transmitter to the receiver via different paths. A well- known connectionless protocol is UDP.

CRTP
Compressed Real-Time Transmission Protocol- See RTP

CS-ACELP
Conjugate Structure Algebraic Code Excited Linear Prediction. CELP voice compression algorithm providing 8 Kbps, or 8:1 compression, standardized in ITU-T Recommendation G.729.

CSMA/CD
Carrier Sense Multiple Access/Collision Detection This is the access procedure to the Ethernet in which the participating stations physically monitor the traffic on the line. If no transmission is taking place at the time the particular station can transmit. If two stations attempt to transmit simultaneously this causes a collision which is detected by all participating stations. After a random time interval the stations that collided attempt to transmit again. If another collision occurs the time intervals from which the random waiting time is selected are increased step by step. Networks using the CSMA/CD procedure are simple to implement but do not have deterministic transmission characteristics. The CSMA/CD method is internationally standardized in IEEE 802.3 and ISO 8802.3.

DID
Direct Inward Dialling; The ability to make a telephone call directly into an internal extension without having to go through the operator. Called DDI in some territories (Direct Dial In)

Diffserv
Differentiated Services; The Diffserv model divides traffic into a small number of classes to provide quality of service (QoS).

DTMF
Dual-Tone Multifrequency; The type of audio signals generated when you press the buttons on a touch-tone telephone.

DSP
Digital Signal Processor

G.711
Describes the 64-kbps PCM voice coding technique. In G.711, encoded voice is already in the correct format for digital voice delivery in the PSTN or through PBXs. Described in the ITU-T standard

in its G-series recommendations.

G.723.1
Describes a compression technique that can be used for compressing speech or audio signal components at a very low bit rate as part of the H.324 family of standards. This CODEC has two bit rates associated with it: 5.3 and 6.3 kbps. The higher bit rate is based on ML-MLQ technology and provides a somewhat higher quality of sound. The lower bit rate is based on CELP and provides system designers with additional flexibility. Described in the ITU-T standard in its G-series recommendations.

G.729
Describes CELP compression where voice is coded into 8-kbps streams. There are two variations of this standard (G.729 and G.729 Annex A) that differ mainly in computational complexity; both provide speech quality similar to 32-kbps ADPCM. Described in the ITU-T standard in its G-series recommendations.

H.323
Extension of ITU-T standard H.320 that enables videoconferencing over LANs and other packet-switched networks, as well as video over the Internet.

IETF (Internet Engineering Task Force)
One of two technical working bodies in the Internet Activities Board. The IETF meets three times a year to set technical standards for the Internet

IP
Internet Protocol

Jitter
The variation in the amount of Latency among Packets being received

Latency
(Also called Delay) The amount of time it takes a Packet to travel from source to destination. Together, Latency and Bandwidth define the speed and capacity of a network.

LAN
A local area network (LAN) is a group of computers and associated devices that share a common communications line or wireless link and typically share the resources of a single processor or server within a small geographic area (for example, within an office building).

Packet
In data communication, the basic logical unit of information transferred.

PBX
Private Branch eXchange; An in-house telephone switching system that interconnects telephone extensions to each other as well as to the outside telephone network.

PSTN
Public Switched Telephone Network; The worldwide voice telephone network.

Packet Switching
Packet switching is a WAN switching method in which network devices share a single point-to-point link to transport packets from a source to a destination across a carrier network.

PCM
Pulse Coded modulation.

QoS
Quality of Service. Measure of performance for a transmission system that reflects its transmission quality and service availability. Standards based QOS for VoIP usually involves the implementation of Ethernet standards 802.1p and 802.1q at layer 2 across an Ethernet. At layer 3, the IP standard Diffserv defines bits settings in the TOS (type of service) in the IP header which will identify packets as being associated with a specific service.

RSVP
Resource Reservation Protocol. Protocol that supports the reservation of resources across an IP network. Applications running on IP end systems can use RSVP to indicate to other nodes the nature (bandwidth, jitter, maximum burst, and so forth) of the packet streams they want to receive. RSVP depends on IPv6. Also known as Resource Reservation Setup Protocol.

RTP
Real-Time Transport Protocol. Real-Time Transport Protocol. One of the IPv6 protocols. RTP is designed to provide end-to-end network transport functions for applications transmitting real-time data, such as audio, video, or simulation data, over multicast or unicast network services. RTP provides services such as payload type identification, sequence numbering, time-stamping, and delivery monitoring to real-time applications.

RTCP
RTP Control Protocol. Protocol that monitors the QOS of an IPv6 RTP connection and conveys information about the on-going session. See also RTP.

SIP
Session Initiation Protocol; A protocol that provides telephony services similar to H.323, but is less complex and uses less resources.

TCP (Transmission Control Protocol)
Connection-oriented transport layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack.

TOS
Type of Service; A method of setting precedence for a particular type of traffic for QoS.

Trunk
A communications channel between two points, typically referring to large-bandwidth telephone channels between switching centres that handle many simultaneous voice and data signals.

TDM
Time-division multiplexing. In TDM, information from each data Channel is allocated bandwidth based on preassigned time slots, Regardless of whether there is data to transmit.

TOS
Type of Service.

VAD
Voice activity detection. When enabled on voice port or a dial peer, silence is not transmitted over the network, only audible speech. When VAD is enabled, the sound quality is slightly degraded, but

the connection monopolise much less bandwidth.

VBR
Variable bit rate. QoS class defined by the ATM Forum for ATM networks. VBR is subdivided into a real time (RT) class and non-real time (NRT) class. VBR (RT) is used for connections in which there is a fixed timing relationship between samples. VBR (NRT) is used for connections in which there is no fixed timing relationship between samples, but that still need a guaranteed QoS.

Note:
Not all items above are described in this manual.

2 Part 2: VoIP Manual

General Information

2.1 General Information

General Information

Introduction

The UNIVERGE SV9100 system uses IP for various applications.

This section describes the procedure for connecting the UNIVERGE SV9100 system to an existing data network and configuring TCP/IP. This is the first step in implementing VoIP and other IP applications.

Network Addressing Overview

Before connecting the system to a data network, it is necessary to obtain the relevant IP Addressing information. This information is supplied by the IT Manager or Network Administrator at the customer site.

IP Addressing
All equipment/devices used in the LAN setup must have an IP address assignment. An IP address assigns a unique address for each device. There are two types of IP addresses: Private and Global. A Private IP address is not accessible through the internet; a Global IP address can be accessed through the internet.

In most cases, a Private address is used, as LAN devices are not usually directly connected to the internet. Private addresses are usually taken from the following ranges:

- Class A 10.0.0.0 ~ 10.22.255.255
- Class B 172.16.0.0. ~ 172.31.255.255
- Class C 192.168.0.0 ~ 192.168.255.255

A Public address is normally only used when a device is directly connected to the internet. This is unlikely in the case of the equipment. If public addressing is used, the numbers are normally allocated by an ISP.

Subnet Mask

As the IP address includes information to identify both the network and the final destination, the Subnet Mask sets apart the network and destination information. The default subnet masks are:

- Class A 255.0.0.0
- Class B 255.255.0.0
- Class C 255.255.255.0

The Subnet Mask is made up of four groups of numbers. When a group contains the number *255*, the router ignores or masks that group of numbers in the IP address as it is defining the network location of the final destination.

For example, if the IP address is: 172.16.0.10 and the Subnet Mask used is Class B (255.255.0.0), the first two groups of numbers (172.16) are ignored once they reach the proper network location. The next two groups (0.10) are the final destination within the LAN to which the connection is to be made.

➢ For sub-netted networks, the subnet mask may be different from the default subnet masks listed above.

DHCP

Dynamic Host Configuration Protocol (DHCP) assigns a dynamic IP address. Network control may be easier with DHCP as there is no need to assign and program individual IP addresses for the LAN equipment. To use a dynamic IP address, a DHCP server must be provided. The UNIVERGE SV9100 system GCD-CP10 blade provides an internal DCHP server, enabling the ability to use DHCP.

When equipment, which is connected to the LAN (the DHCP client), is requesting an IP address, it searches the DHCP server. When the request for an address is recognized, the DHCP server assigns an IP address, Subnet mask, and the IP address of the router, based on UNIVERGE SV9100 system programming.

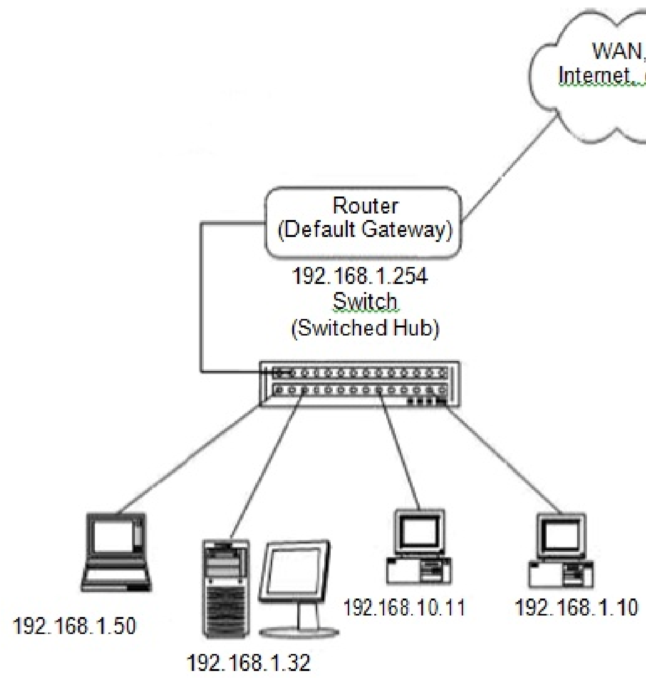
Note that the GCD-CP10 blade must always have a static IP address. This address is set in Program 10-12-01 : GCD-CP10 Network Setup – IP Address (default: 192.168.0.10).

Configuration Examples

Example Configuration 1 - Existing Network with Static Addressing

Each client device has a manually assigned IP address in the 192.168.1.0/24 network (i.e., 192.168.1.1 to 192.168.1.254 with a subnet mask of 255.255.255.0). They also have a default gateway address configured (192.168.1.254) this allows the device to route packets to destinations that exist outside of their own LAN.

Example Configuration 1 - Existing Network with Static IP Addresses



Assume that a UNIVERGE SV9100 is added to the existing data network. The Network Administrator (or IT Manager) should provide the following:

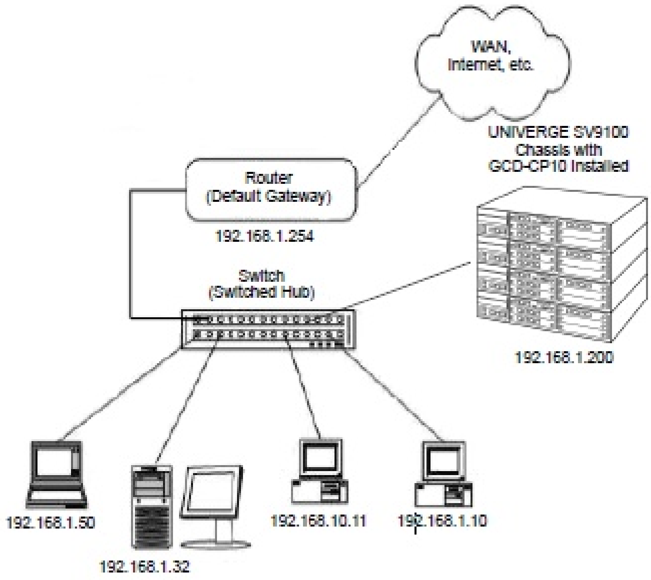
- IP Address (for the GCD-CP10 blade)
- IP Addresses (for the GPZ-IPLE daughter board)
- Subnet Mask
- Default Gateway
- A spare switch/hub port

First, program the UNIVERGE SV9100:

- 192.168.1.200
- 255.255.255.0
- PRG10-12-03: 192.168.1.254
- ***A system reset is required for the IP Address changes to take effect.***

Now connect the GCD-CP10 blade Ethernet Port to the switch/hub port, using a standard Cat-5 patch cable. The UNIVERGE SV9100 is now configured on the network and should be accessible by other devices on the network.

Example Configuration 1 - Adding the UNIVERGE SV9100 Chassis to the Network.



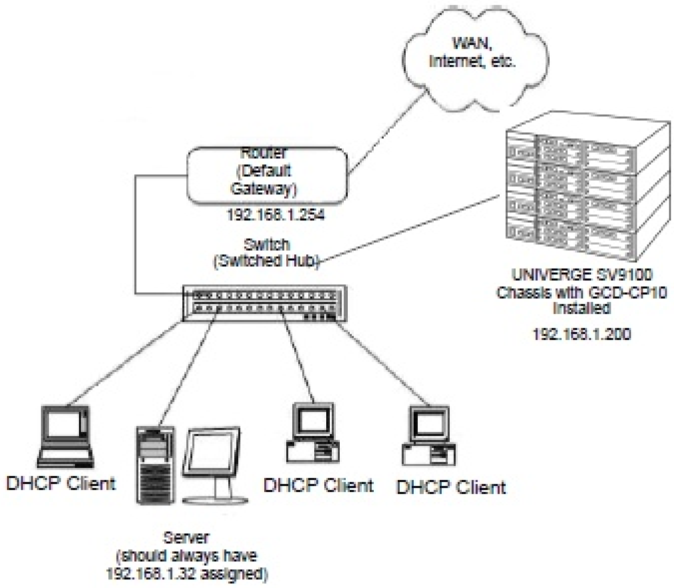
Example Configuration 2 - New Network with Dynamic Addressing

This shows a typical network configuration using Dynamic IP Addressing, and the UNIVERGE SV9100 Internal DHCP server. In most cases, the customer would use an external DHCP server (for example on a Windows Server) or static addressing (as illustrated in Example Configuration 1). However, if the UNIVERGE SV9100 is to be installed on a new network the Network Administrator may want to use the UNIVERGE SV9100 internal server (this is called inDHCP). In this example, the client PCs get an IP address, subnet mask, and default gateway from the inDHCP server. The server also uses DHCP, but should always be given the same IP address (192.168.1.32).

The Network Administrator (or IT Manager) should provide the following:

- IP Address (for the GCD-CP10 blade)
- IP Addresses (for the GPZ-IPLE)
- Subnet Mask
- Default Gateway
- Range(s) of IP Addresses to assign
- List of permanent IP addresses, with corresponding MAC Addresses
- A spare switch/hub port

Example Configuration 2 - New Network with Dynamic Addressing



Now connect the UNIVERGE SV9100 GPZ-IPLE Ethernet Port to the switch/hub port, using a standard CAT-5 patch cable. The UNIVERGE SV9100 is now configured on the network and its DHCP server is ready to allocate IP addresses. The client PCs should be set to *Obtain IP Address Automatically*.

General IP Configuration

The voice quality of VoIP depends on variables such as available bandwidth, network latency, and quality of service initiatives (QOS), all of which are controlled by the network and internet service providers. Because these variables are not in NEC control, it cannot guarantee the performance of the users IP based voice solution.

Therefore, NEC recommends connecting the VoIP equipment through a local area network using private IP addresses. For a network to be suitable for VoIP it must pass specific requirements. To make sure that the site meets these requirements an IP ready check and a site survey **must** be completed at each site before VoIP implementation.

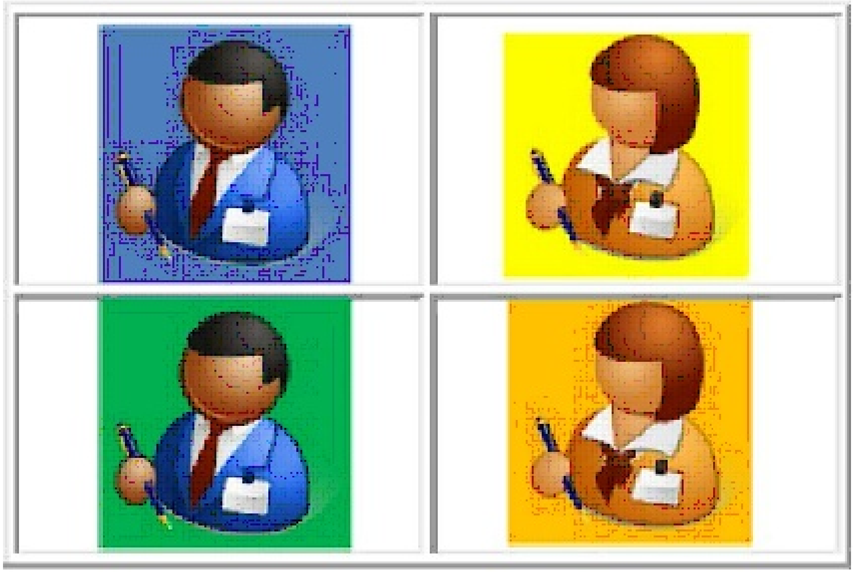
- One way delay must not exceed 100 ms
- Round Trip delay must not exceed 200 ms
- Jitter must not exceed 100ms
- Packet loss must not exceed 1%
- Data switches be full-duplex and manageable
- Routers must provide QOS
- Adequate bandwidth for estimated VoIP traffic (see bandwidth calculator)

Depending on how QOS policies are built into the network, assignments might be needed in the UNIVERGE SV9100 programming.

Simple MCU Video

The Simple MCU Video feature provides a built in video conferencing MCU for up to four standard SIP phones using the Remote Conference feature of the SV9100 system.

The video functionality can also be set to use system VoIP DSP resources for non-MCU video conferencing if peer-to-peer calls between standard SIP phones is disabled or not supported by the terminal used. If the system is set to allow peer-to-peer calls between standard SIP stations then no system DSP resources are required to support the video functionality between standard SIP phones.



Conditions

- CO calls cannot be transferred to a Remote Conference pilot and must directed to the conference pilot as a DID or DIL termination.
- If peer-to-peer is disabled the standard SIP video feature requires VoIP DSP resource be reserved for this function reducing the number of VoIP resources available for SIP phone calls.
- The system will always reserve 64 of the total 256 VoIP DSP resources for SIP voice calls.
- When set in programming the following tables show how many resources are reserved for each video mode. The total number of VoIP resources reserved for video cannot be higher than 192.

MCU Mode Video Channel VoIP Reservation (Peer-to-Peer Enabled Systems)

Program	Max simultaneous group (each group is 4 video channels)	1
84-27-22	MCU Mode 1 VoIP Reserved	64
84-27-23	MCU Mode 2 VoIP Reserved	160

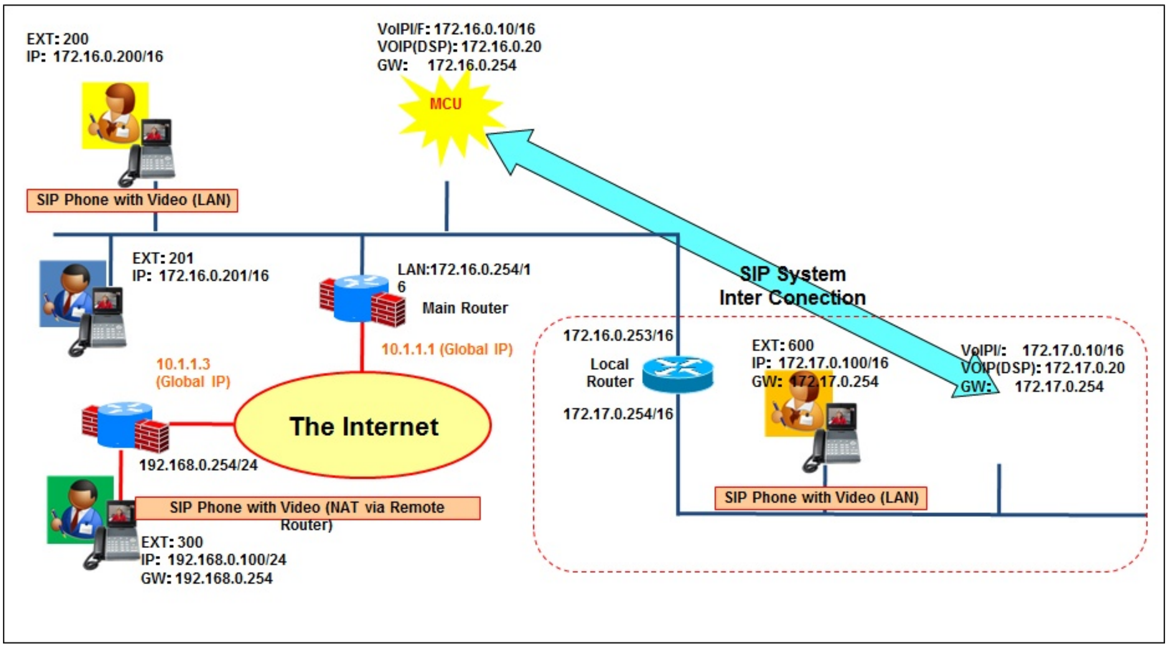
- Video over SIP trunks is not supported for version 1.00 software and will be supported in a later release.
- The combination of Programs 84-27-20, 84-27-21, 84-27-22 and 84-27-23 determine the total number of VoIP DSP resources reserved for video channels (not exceed 192).
- Mode 1 video quality is CIF (352x288).
- Mode 2 video quality is VGA (640x480).
- Video quality mode used depends on the standard SIP device support of that resolution.
- Setting Programs 84-27-22 or 84-27-23 to 1 will allow 4 video channels for MCU video mode type (1 or 2) if DSP resources are available.
- MCU group for mode 1 and mode 2 video cannot be enabled at the same time as it will try to reserve more than 192 VoIP DSP resources for video.
- The system will not allow more than 192 VoIP DSP resources to be reserved for video.
- After making setting changes to Programs 84-27-20, 84-27-21, 84-27-22 or 84-27-23 the VoIP

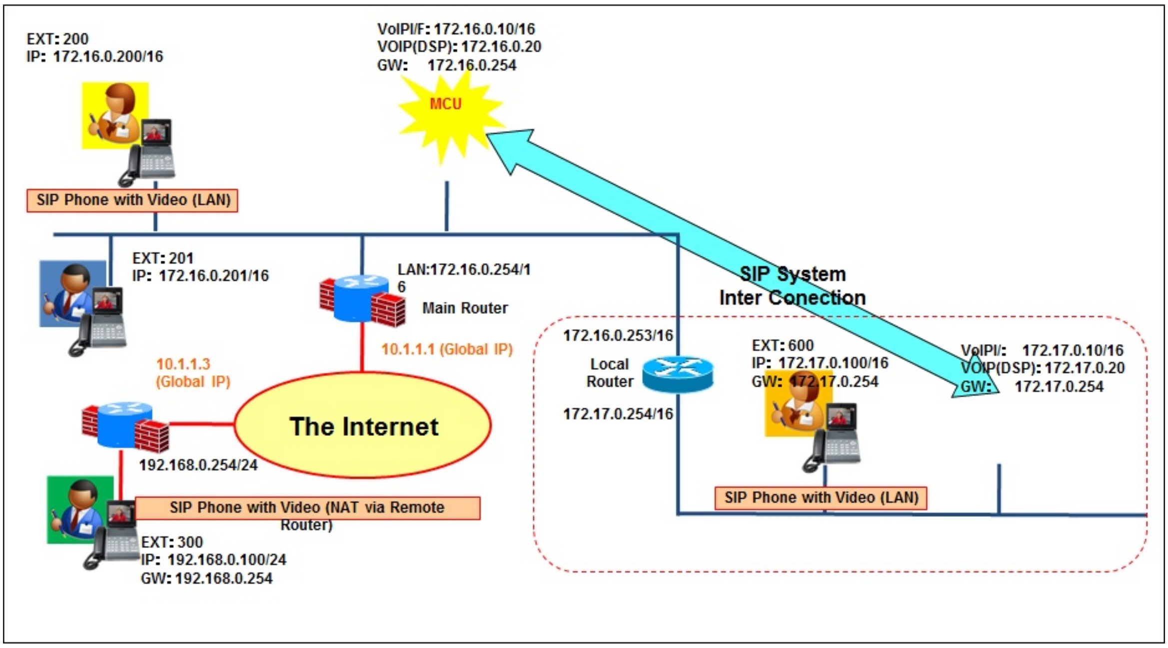
daughter board must be reset for the changes to take effect. This will happen automatically once all VoIP resources go idle.
- Up to 256 VoIP DSP resources are available when the SV9100 is properly licensed.
- Video streaming is not supported to SIP Terminal via Netlink.
- Simple MCU video is not supported for SIP Trunk calls.
- Once VoIP DSP resources have been reserved for video functionality, pressing Feature+4 on an idle display phone will show the number of VoIP DSP resources available for voice calls.

System Availability
Standard SIP Terminals with video capabilities that are compliant with RFC 3261, RFC 3262, RFC 3264 (Session Description Protocol), RFC 1889 (Real Time Protocol).

Required Components
- GCD-CP10
- GPZ-IPLE
- Video license (0042) BE114070
- Remote Conference license (0047) BE114073
- System Port License (0300) BE114042
- IP Telephone license (5111) BE114054

Example Usage





PRG No.	Description	Setting	Values	Default Value
84-26-01	DSP IP Address	172.16.0.20	**.**.**.**	172.16.0.20
84-26-12	Voice RTP Port	10020	0-65534	10020
84-26-13	Voice RTCP Port	10021	0-65534	10021
84-26-12	Video RTP Port	20020	0-65534	20020
84-26-13	Video RTCP Port	20021	0-65534	20021
84-27-22	Max MCU Group (mode1)	1	0-1	0
84-27-23	Max MCU Group (mode2)	0	0-1	0

IPLE Video Streaming Termination

Video functionality can be configured to use system VoIP DSP resources for non-MCU video calling if peer-to-peer calls between standard SIP phones is either disabled or video codecs not supported between the terminals being used.

If the system is set to allow peer-to-peer calls between standard SIP stations then no system DSP resources are required to support the video functionality between standard SIP phones.

Video CODEC support is currently for H.264/MPEG-4 AVC using either of the two video quality modes listed below.

Display Size (Pixel)	Frame Rate (fps)	Bit Rate (kbps)	CODEC Level
CIF (352x288)	15	384	1.2
VGA (640x480)	15	768	2.1

Example Video Streaming Usage

Licenses

License Code	Description	Notes
BE114042	SV9100 System Port License	System port license required for IP terminals and trunk ports
BE114054	SV9100 IP Phone License	Standard SIP Terminal license (per teminal)
BE114065	SV9100 IP Trunk License	IP Trunk license for SIP and H.323

Conditions

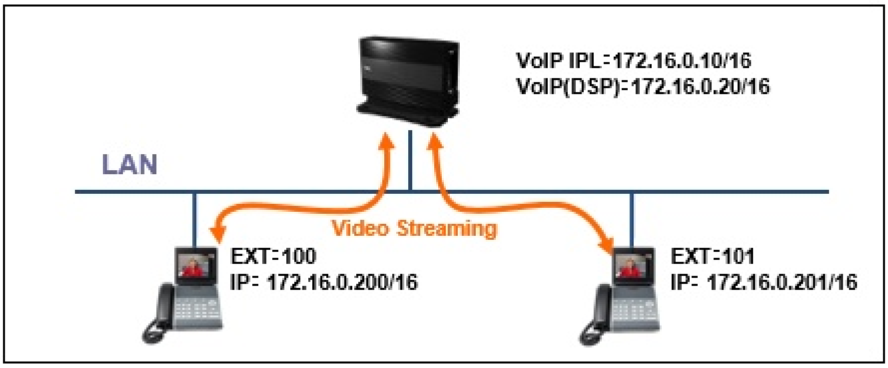
- The system will always reserve 64 of the total 256 VoIP DSP resources for voice calls.
- If peer-to-peer is disabled the standard SIP video feature requires VoIP DSP resource be reserved for this function reducing the number of VoIP resources available for SIP phone calls.
- When set in programming the following tables show how many resources are reserved for each video mode. The total number of VoIP resources reserved for video cannot be higher than 192.

Video Streaming Termination Channel VoIP Reservation

Program	Max simultaneous video channels	1	2	3	4	5	6	7	8
84-27-20	Mode 1 VoIP Reserved	32	32	64	64	64	96	96	96
84-27-21	Mode 2 VoIP Reserved	32	64	96	128	160	192	N/A	N/A

- Up to 256 VoIP DSP resources are available when the SV9100 is properly licensed.
- Video quality mode used depends on the standard SIP device support of that resolution.
- MCU group for mode 1 and mode 2 video cannot be enabled at the same time as it will try to reserve more than 192 VoIP DSP resources for video.
- The system will not allow more than 192 VoIP DSP resources to be reserved for video.
- After making setting changes to Programs 84-27-20, 84-27-21, 84-27-22 or 84-27-23 the VoIP daughter board must be reset for the changes to take effect. This will happen automatically once all VoIP resources go idle.
- Video streaming is not supported to SIP Terminal via Netlink.

Example Usage



VoIP LAN Link Speed Information (Release 3)

The SV9100 can now display the LAN link information for duplex and speed of either the CPU or VoIPDB interfaces.

Easy Edit – Advanced Items/VoIP/General Settings/VoIP Configuration/VoIP LAN Link Speed Information
LAN Link Speed of CPU - Displays the duplex and speed of the LAN connection between the CPU interface and network switch. *(PRG90-77-01)*
LAN Link Speed of VoIP - Displays the duplex and speed of the LAN connection between the VoIP interface and network switch. *(PRG90-77-02)*

Modifying MTU Size (Release 3)

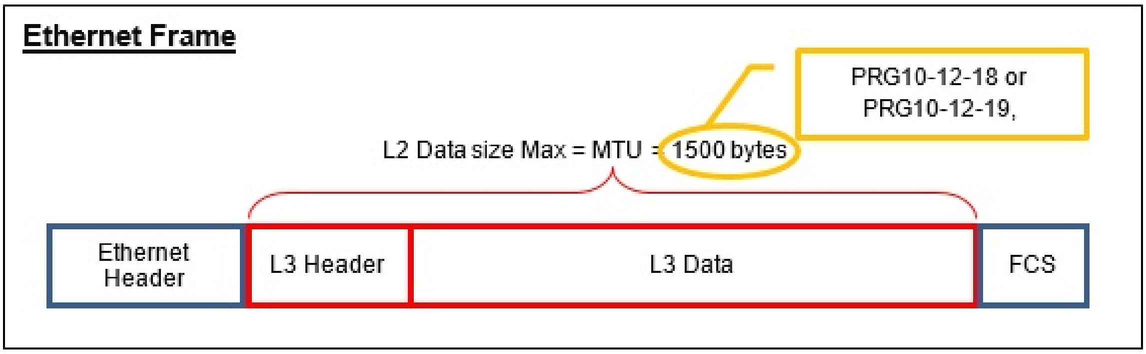
The MTU is the Maximum Transmission Unit. It means the size of the largest packet that a network protocol can transmit. When the quantity of data to send from the system exceeds the MTU, it will divide for each MTU and transmit in multiple steps.

Generally a larger MTU brings greater efficiency because each network packet carries more user data. But in some environments of low communication quality, a smaller MTU brings better efficiency since the resending of data by error decreases.

Therefore the MTU size for both the CPU and VoIPDB interfaces can be change depending on the environment, in order to improve the communication efficiency.

Easy Edit – Advanced Items/VoIP/General Settings/IP Addressing/CCPU IPL IP Network Setup
CCPU MTU - Allows the MTU size to be modified between 100-1500 bytes for the CCPU interface. Default value is 1450. *(PRG10-12-18)*
VoIPDB MTU - Allows the MTU size to be modified between 100-1500 bytes for the VoIPDB interface. Default value is 1450. *(PRG10-12-19)*

Service Condition
MTU is the maximum size of Layer 2 data. For IP packets, it is the total size of the IP header and IP data. MTU of the system was 1500 bytes fixed (*), but it will be variable by referring to this system data.
(*) If VLAN enabled, MTU was 1496 bytes fixed



This system data applies to packets sent from the IP addresses set in the PRG10-12-01 and PRG10-12-09.
Because this system data applies to OS of main software, it does not apply to the RTP / RTCP packets generated from DSP of VoIPDB.

Store Statistical Information of RTP (Release 3)

The SV9100 can now store statistical information of RTP on the SD Card. This information once stored on the SD Card can then either be retrieved using PC Pro to download or by saving to a USB stick using telephone programming.

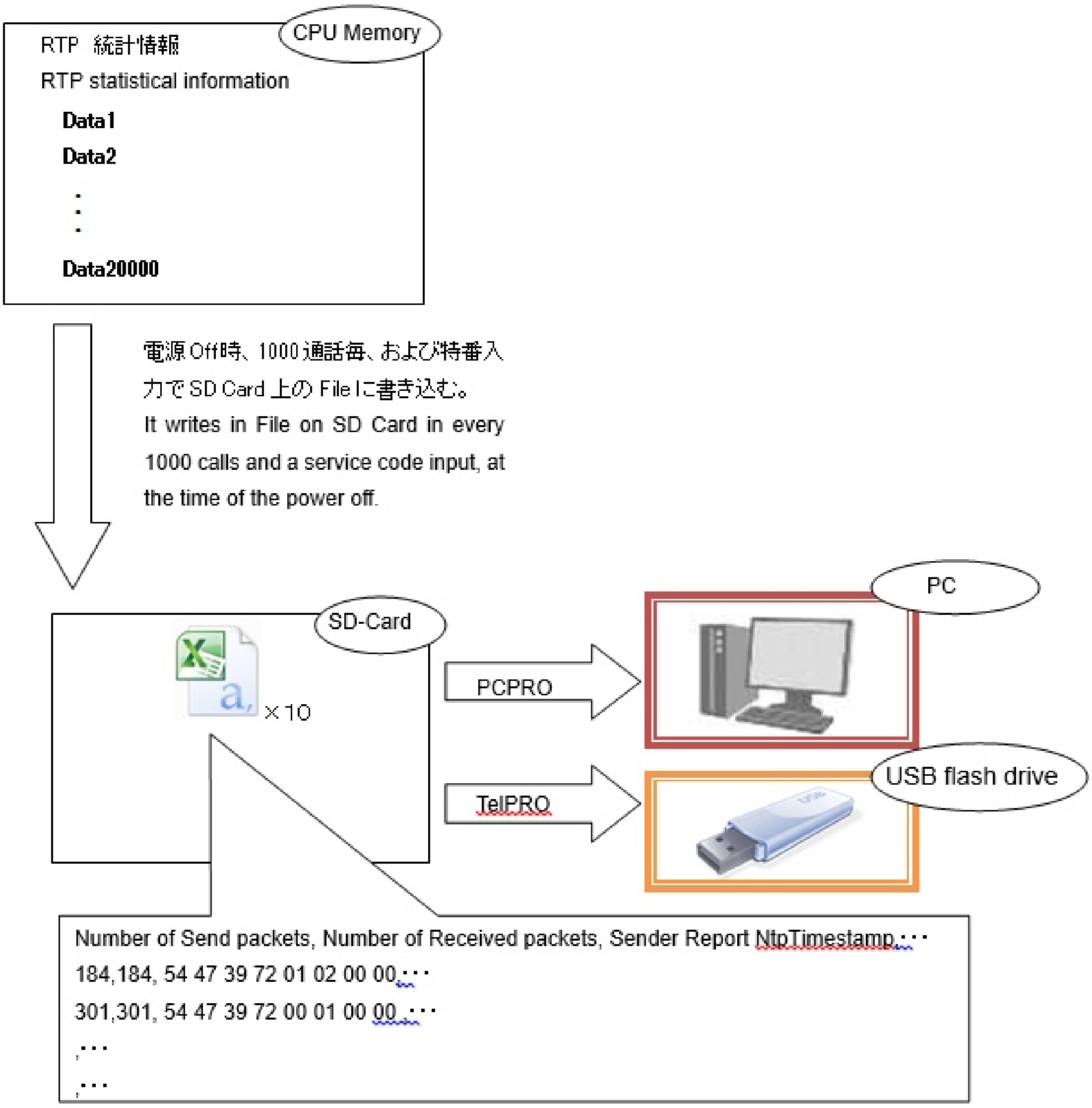
Easy Edit – Advanced Items/VoIP/General Settings/VoIP Configuration/Store Statistical Information of RTP

Save Statistical Information of RTP - This class of service option sets the availability of RTP statistical information being saved to SD Card. *(PRG20-07-35)*

Save Store Statistical Information or RTP - This sets the service code that when used RTP statistical information is saved on SD Card immediately. Normally the RTP statistical information is saved every 1000 telephone calls. Default value is 760. *(PRG11-10-54)*

Service Condition

- RTP Information is saved by considering the period as one call as it opens and closes. When closing an RTP stream and reopening by hold, transfer, etc., it saves as a separate call.
- Even if an RTP stream is not able to open, when an RTP Open Request is notified to the VoIP DB, then RTP statistical information is stored. Since the actual communication is not performed, all information is set to 0.
- The saved information is written in the file on SD Card every 1000 calls. However, the service code operation can only be performed, when the **Save Statistical Information of RTP** (PRG20-07-35) is On.
- When RTP statistical information is written to the SD Card, it is not concerned with the success or failure. The number of calls for the writing for every 1000 calls is returned to 0, and begins a count from 1 again.
- After saving onto the SD Card, the statistical RTP information in CPU memory is deleted.
- When a write error occurs during the writing to the file on SD Card. The RTP statistical information data being written is canceled including the RTP information in the CPU Memory.
- In order to perform the writing to the file on SD Card the task is set as a low priority, so as not to affect other services.
- Saves 20000 calls to a single file, and then saves from the next telephone call to another file.
- The number of files to save is to ten files, after that, the oldest file is erased and new information is saved. Old and new files are decided using the time of the creation date of a file. Therefore, it is dependent on the clock information on the system at the time of creating a file.
- About 4.6MB per file in memory is used. About 46MB memory is used by ten files. (230Byte/call.)
- When creating a new file, the system doesn't reserve the memory for 20000 calls, but file size increases during writing.
- When writing the RTP statistical information data , and the capacity of SD card is 30 MB or less, the oldest RTP statistical information file is deleted until 30MB or more availability is made to SD card.
- Even if all the RTP statistical information files are deleted, when sufficient capacity on the SD Card is not securable at the time of writing, then it becomes a write error and the RTP statistical information data being written is canceled.
- File format is csv.
- In the "DATA" folder on SD card, it saves by the name "MMDDhhmms.csv."
- When the remote terminal side is not supporting RTCP, only the information on the system side is obtained and all the information on the remote side is set to 0.
- IPLE requires transmission of RTP statistical information every 5 seconds after RTP is opened including from the remote side and updates to the newest information at the time.
- The timing which asks VOIP RTP statistical information is just before closing RTP.
- When a call is closed and RTP is closed before receiving the answer of the RTP statistical information from the remote side. Only the information on the system side is obtained and all the information on the remote side is set to 0.
- The statistical information of RTP on a secondary node of Net Link is also saved by the primary system



Limitations

- When the remote device does not support RTCP protocol, the statistical information of the RTP communication of the other party cannot be obtained.
- In Peer to Peer, the statistical information of RTP communication is not obtainable.
- When a write error occurs during the writing to file on the SD Card, the RTP statistical information data under writing is canceled.
- Video (SRTP) can not be supported.

RTP Statistical Information Format

Data Name	Data outline
Start Date	The date when a call has been begun
End Date	The date when a call has been ended

Ext/TRK Number	The Extension or Trunk Number on the system side.
Ext/TRK Number(Call partner)	The Extension or Trunk Number on the remote side.
Cumulative Lost Cnt	Receiving RTP packet loss total
Max Fraction Lost	The Max rate of packet loss When the max packet loss rate and the average packet loss rate are the same value, we can think a packet loss occurs constantly. When the max packet loss rate is high compared with an average packet loss, it's regarded as a temporary packet loss.
Average Fraction Lost	The average rate of packet loss When exceeding 1%, reconsideration of the network environment is needed.
Number of Sent RTP packets	Number of Sent RTP packets Transmission of RTP packet isn't done in case of 0. When there is no sound though a packet is being sent, It can think there is cause in the network environment, a system in a communication destination and a terminal.
Number of Received RTP packets	Number of Received RTP packets Transmission of RTP packet isn't done in case of 0. When there is no sound though speech packet is being received, It can think there is cause in a system of AspireUX or a terminal.
Cumulative Lost Cnt（Remote）	Receiving RTP packet loss total of Remote side(IP Terminal,IP trunk etc.).
Max Fraction Lost（Remote）	The max packet loss rate of the remote side
Max Round Trip Time（Remote）	It is the time concerning the round trip of the packet. A communication partner's “processing delay + network delay” are known.
Number of Sent RTP packets（Remote）	Number of Sent RTP packets（Remote Side）
Sender statistical information on system side	
Sent Sender Report NtpTimestamp	Sent Sender Report NtpTimestamp
Sender SSRC	RTP SSRC（Synchronization Source Identifier） It is used for a user's discernment. Synchronous sauce identifier. DSP of VOIPDB determines SSRC at random at the time of channel opening. When the SSRC same within the same session exists, it is changed.（It is hardly.） It is used for the judgment of being the same stream, etc.
Receiver statistical information on system side	

Max Inter Arrival Jitter	The max Interval of the arrival time of a RTP packet. Fluctuation between the arrival time of a RTP packet. Since it is dependent on a sampling frequency, a unit is set to ms by dividing by 8 in the case of G.711 (8-kHz sampling).
Average Inter Arrival Jitter	The average Interval of the arrival time of a RTP packet.
Remote Sender SSRC	Remote Sender SSRC It is used for a user's discernment. Synchronous sauce identifier.
Receiver Information of Remote Side	
Average Round Trip Time	Average Round Trip Time
Sender statistical information on Remote side	
Sent Sender Report NtpTimestamp	Sent Sender Report NtpTimestamp
Sender SSRC	Sender SSRC（Synchronization Source Identifier） It is used for a user's discernment. Synchronous sauce identifier.
Sender statistical information on Remote side	
Max Inter Arrival Jitter	The max Interval of the arrival time of a RTP packet. Fluctuation between the arrival time of a RTP packet. Since it is dependent on a sampling frequency, a unit is set to ms
Average Fraction Lost	The average rate of packet loss
Average Inter Arrival Jitter	The average Interval of the arrival time of a RTP packet.
Remote Sender SSRC	Remote Sender SSRC It is used for a user's discernment. Synchronous sauce identifier.
Additional Information	
type	0 : ICM MLT/STD SIP 1 : TRK SIP/H323 2 : VICM （VIDEO） 3 : VTRK （VIDEO） 4 : NET NETLINK 5 : CCIS CCIS(IP) 6 : ASP Aspire Net(IP)
Source System ID	Source System ID
Source Logical Port	Source Logical Port
Dest System ID	Destination System ID
Dest Logical Port	Destination Logical Port

Operation

Procedure to save Statistical Information of RTP to SD Card by Service Code.

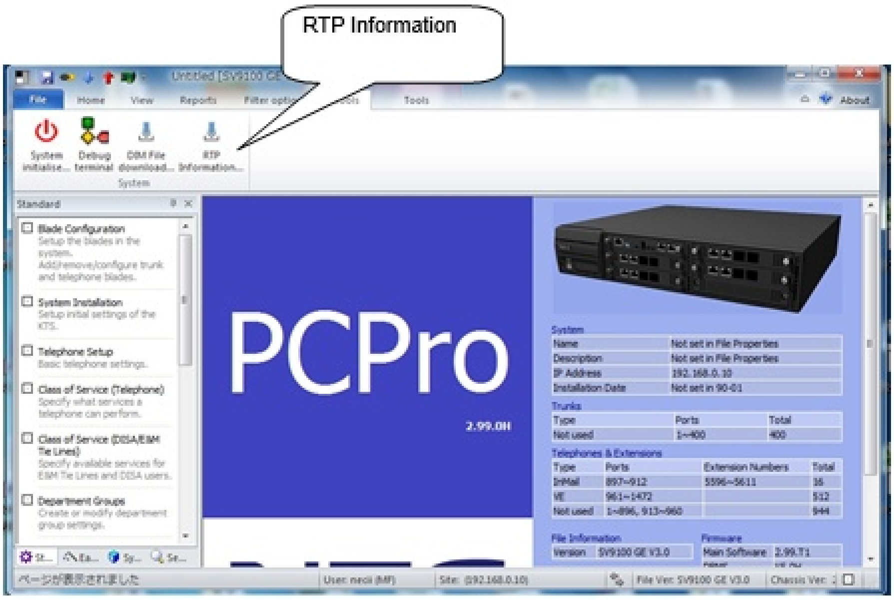
Operation	Note	LCD
No1 SPK + "Service Code" Service Code: PRG11-10-54	Enter speaker key, and enter the service code set up by PRG11-10-54.	
No2 Service Code check	Check Service code. If service code is not available, go to "No4". If there is no problem, go to "No3"	
No3 Start saving Statistical Information of RTP	Start saving Statistical Information of RTP. If save process is complete normally, go to "No5". If save process is fail (File access error etc.) , go to "No4"	012345678901234567890123 Saving Data
No4 Error display	If error occurs with No2, phone programming status is changed to error status, finish the process.	012345678901234567890123 Fail to write
No5 Complete saving Statistical Information of RTP	Complete saving Statistical Information of RTP.	012345678901234567890123 Data save complete !

Procedure of extraction Statistical Information of RTP (TEL Pro)

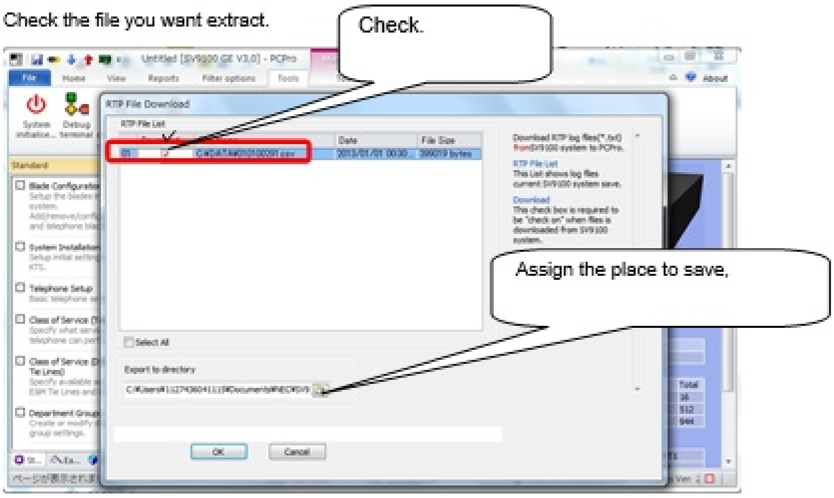
Operation	Note	LCD
No1 1 + TRF	Go to PRG90-03-03, and enter "1+TRF Key" to extract file to USB flash drive. No process is executed by just pressing TRF key(without dial 1) or any other keys	0123456789012345678901234 90-03-03 RTP Data Save YES:1 _ <- ->
No2 Check any other user is login.	Check any other station do the same operation. If that exists, stop the operation and go to "No7".	
No3 Start saving Statistical Information of RTP	Start saving Statistical Information of RTP to USB flash drive.	0123456789012345678901234 Saving RTP log
No4 USB mount check	Check USB is mounted. If USB isn't mounted, go to "No6". If there is no problem, go to "No5"	
No5 Complete saving Statistical Information of RTP	If saving is completed, LCD display is changed to next system data display.	0123456789012345678901234 90-04- M tenance Load Data |01 back ↑ ↓ select
No6 Error display	If error occurs with No4, phone programming status is changed to error status, finish the process.	0123456789012345678901234 90-03-03 Fail to write <- ->
No7 Error display	If error occurs with No2, phone programming status is changed to error status, finish the process.	0123456789012345678901234 90-03-03 Load fails [Login]

Procedure of extraction Statistical Information of RTP (PC Pro)

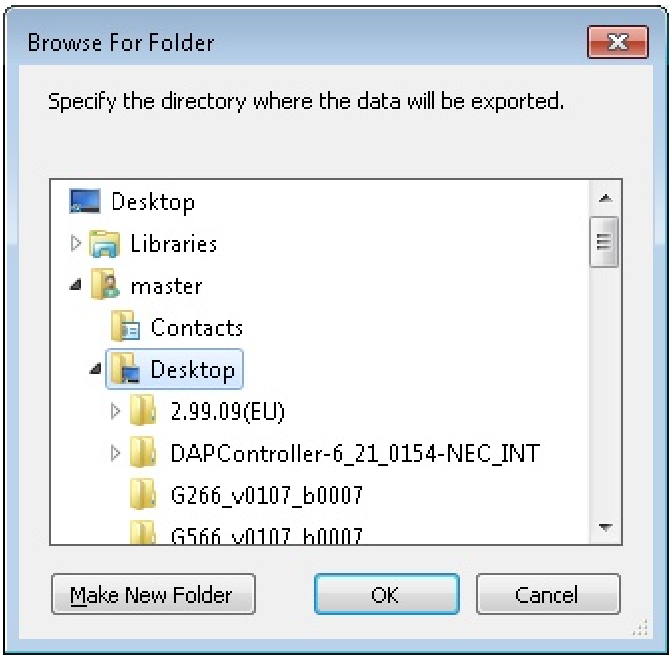
From the Tools menu click RTP Information.



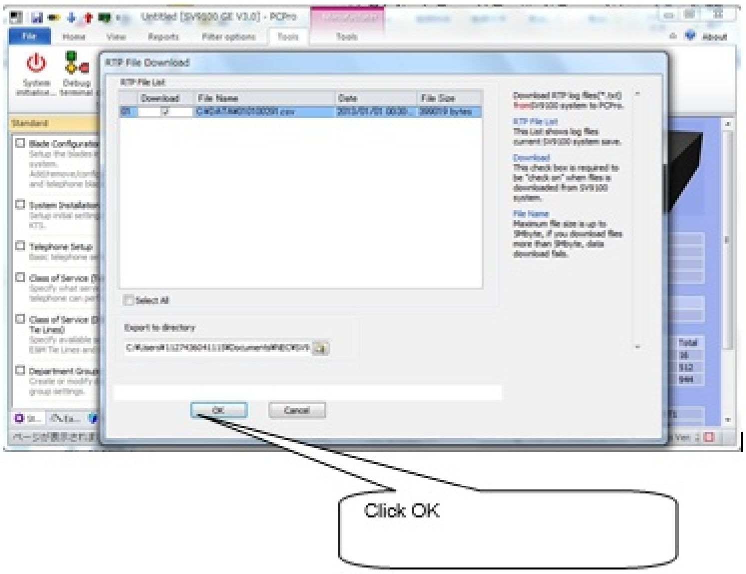
Check the file you want extract.



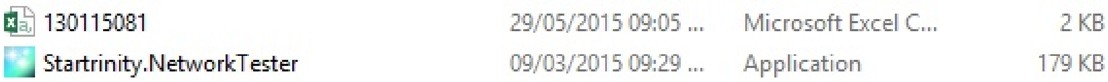
Specify the location the file(s) will be downloaded to and press OK.



Click OK



Saving will be completed and the files stored at the location selected.



2.2 QoS Settings

SV9100 QoS

When transmitting Voice over an IP network it is important to consider Quality of Service (QoS). This is the perceived quality of speech after being transmitted across the network.

It is recommended that you consult the "Voice over IP Reference Guide" as this discusses the issues that should be considered when implementing a VoIP network.

QoS is actually implemented on the network hardware such as switches and routers, and not the SV9100. The SV9100 can "mark" its data with appropriate tags and the network equipment has to be configured to prioritise that data over other (non VoIP) data. The Network Administrator should supply the SV9100 installer with the relevant QoS settings for their Network.

QoS can either be implemented at Layer 2 (within the Ethernet Frame Header) for Local Area Network (LAN) QoS policies or at Layer 3 (within the IP Packet Header) for Wide Area Network (WAN) point-to-point QoS policies.

Easy Edit – Advanced Items/VoIP/QoS Settings/Layer 2 QoS and VLAN. (PRG84-09)

QoS is implemented at Layer 2 by using VLAN (IEEE 802.1p/Q) tags.

Choose which interface needs to be programmed:
- Interface 1 = GCD-CP10 Ethernet connection
- Interface 2 = GPZ-IPLE VoIP connection

For any VoIP applications Interface 2 is used.

VLAN Mode - By default the system does not use VLAN tags, so these have to be enabled. Once enabled, all frames transmitted by the GCD-CP10 and GPZ-IPLE cards use the VLAN tags.
VLAN ID - This is the VLAN that the system belongs to. Valid values can be in the range 0 to 4094.
Priority - The priority should be configured between 0 (no prioritisation) to 7 (highest priority). Voice applications normally use a priority value of 5.

Easy Edit – Advanced Items/VoIP/QoS Settings/Layer 3 QoS. (PRG84-10)
This is the most common form of QoS. It utilises the Type of Service (ToS) field within the IP packets header, and can be configured based on two different QoS standards: IP Precedence and Differentiated Services (Diffserv).

Although IP Precedence and Diffserv are both supported on the UNIVERGE SV9100, it is becoming more common to use Diffserv only. The two methods of QoS are interoperable (for example IP precedence values can be mapped to Diffserv values and vice versa).

The ToS value can be set for each type of VoIP packet.

ToS Mode – Choose Disabled (Default), IP Precedence or Diffserv depending on the networks configured QoS policy.
IP Precedence Priority – Only use if the **ToS** Mode is set to IP Precedence. Enter the required IP Precedence value between 0 and 7.
IP Precedence Delay – Normally this value is not required. Use only IP Precedence Priority (above).
IP Precedence Throughput – Normally this value is not required. Use only IP Precedence Priority (above).
IP Precedence Reliability – Normally this value is not required. Use only IP Precedence Priority (above).
IP Precedence Cost – Normally this value is not required. Use only IP Precedence Priority (above).

Diffserv – Use only if the **ToS Mode** is set to Diffserv. Enter the required Diffserv value between 0 and 63.

Below is a table showing which QoS item is required for each particular VoIP feature of the SV9100.

	AspireNet	**Standard SIP Extensions**	**H.323 Trunks**	**SIP Trunks**	**SIP MLT Extensions (DT700/ DT800)**	**CCIS Networking**	**Netlink**
Voice Control (H.245) Sets up voice parameters for a voice call	X		X				
H.323 Used for H.323 signalling information, including GK registration	X		X				
RTP/RTCP Speech media packets	X	X	X	X	X	X	X
SIP Used for SIP signalling including registration		X					
CCIS Used for signalling of CCIS						X	
SIP MLT Used for singalling of SIP MLT (DT700/ DT800)					X		
SIP Trunk Used for signalling of SIP Trunk				X			
NetLink Used for signalling of Netlink							X
Video RTP/ RTCP Video media packets		X		X			

Be aware that the **RTP/RTCP** Layer 3 QoS setting is **common to all signalling protocols** so if there are several VoIP protocols being used on the same system, the speech cannot have different QoS values per protocol. i.e. If an SV9100 is programmed to use NetLink and SIP trunks, the speech will use the same RTP/RTCP QoS value whether a NetLink call is in progress or a SIP trunk call is in progress. The signalling for both protocols, however, can have different values.

2.3 IP Address Collision

IP Address Collision

Description

The system sends Gratuitous ARP (G-ARP) requests to check whether any other devices in the network have the same IP address as either the GCD-CP10, the GPZ-IPLE or the GPZ-IPLE Gateway IP addresses. If an IP address collision is detected an alarm can be triggered.

SV9100 Programming

The only programming required is for the Alarm setup, the Alarm Display Telephone and any email notification if required.
Set up the parameters of the Alarm using Alarm number 57 in *Easy Edit* – *Advanced Items/Maintenance/Alarms/System Alarm Setup* (PRG90-10).
Assign the extension number for the Alarm Display Telephone in *Easy Edit* – *Advanced Items/Maintenance/Alarms/System Alarm Display Setup* (PRG90-50-01).

SV9100 Requirements

The following information provides requirements for the IP address collision detection.

Hardware

The SV9100 requires the following hardware:
GCD-CP10
GPZ-IPLE

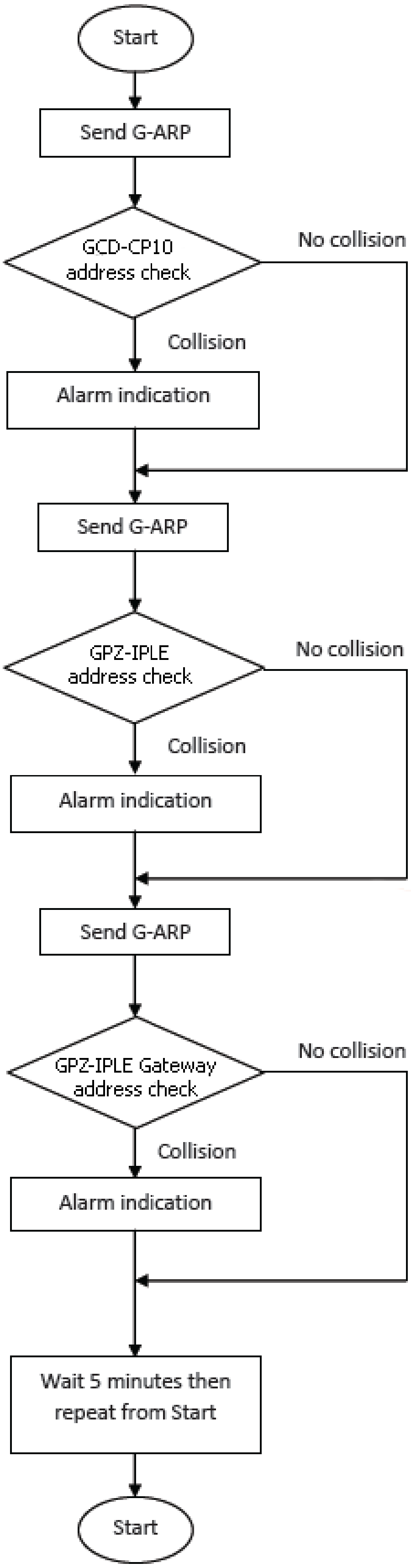
The Alarm can be displayed on the following terminal types:
DT300
DT400
DT700
DT800

Capacity

Up to 3 IP addresses can be checked for duplication using this feature. The 3 IP addresses are the GCD-CP10, the GPZ-IPLE and GPZ-IPLE Gateway address.

Operation

The diagram below shows the operational flow for this feature.


Start
Send G-ARP
GCD-CP10
address check
No collision
Collision
Alarm indication
Send G-ARP
GPZ-IPLE
address check
No collision
Collision
Alarm indication
Send G-ARP
GPZ-IPLE Gateway
address check
No collision
Collision
Alarm indication
Wait 5 minutes then
repeat from Start
Start

Conditions/Comments

- The collision alarm will continue until the IP address conflict is resolved.
- The collision detection will only occur in the same network subnet as the SV9100.
- The G-ARP packets are sent every 5 minutes, this timer is not programmable.
- If multiple IP address collisions are detected only one will be shown on the Alarm Display Telephone. The table below shows information about alarm priorities.

Command to be checked	Alarm display name	Alarm display priority
PRG 10-12-01	Collision(01)	10
PRG 10-12-09	Collision(02)	1
PRG 84-26-01	Collision(03)	2

2.4 IPLE Blade

GPZ-IPLE Blade

When assigning the IP addresses to the GPZ-IPLE and GPZ-IPLE Gateway, the addresses must be in the same network address range (subnet). The GCD-CP10 Ethernet connection requires a separate IP address in a different network address range (subnet).

When you have a GPZ-IPLE card attached to the GCD-CP10, the GCD-CP10 NIC is no longer required to be connected to the network. All applications that previously terminated to the GCD-CP10 NIC card can now be terminated through the GPZ-IPLE NIC.

For example, PC Pro, Web Pro, SMDR, etc. terminate to the GPZ-IPLE NIC card, when installed. Both the GPZ-IPLE and GCD-CP10 NIC share the same default gateway assignment. The default gateway command is used by both NICs, allowing only one device, GPZ-IPLE or GCD-CP10, to route outside of its own network address range (subnet).

The programming information can be found in the relevant section of the IP Manual.

When an IP Phone or IP Trunk calls a legacy device (Keyphone, SLT, trunk) the speech has to be converted from IP to TDM technologies. The GPZ-IPLE card provides this function. The GPZ-IPLE card has a maximum capacity of 256 DSP resources on board; each one can convert a speech channel from IP to TDM and vice versa.

Note: It is possible for IP phones to talk directly to other IP phones without using any DSP's on the GPZ-IPLE card. This method is referred to as Peer to Peer communication.

Available Codec's

A codec is a standard for converting an analogue signal to digital. This conversion process is handled by the DSP (Digital Signal Processors) on the GPZ-IPLE card.

Each codec has different voice quality and compression properties. The correct choice of CODEC will be based on the amount of bandwidth available, the amount of calls required and the voice quality required.

There are several different codec's available for use on the SV9100 as listed below.

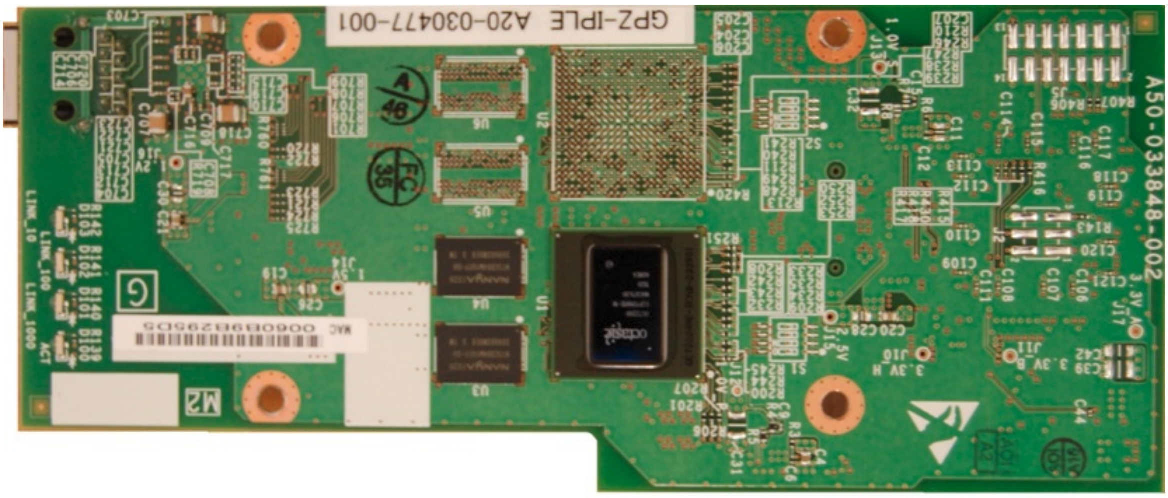
- G.711 (64kbps)
- G.722 (64kbps)
- G.726 (32kbps)
- G.729 (8kbps)

Not all of these codec's are available for all VoIP applications, refer to the relevant section of this manual for further information.

VoIP Gateways
The current GPZ-IPLE daughter board requires a single DSP IP address.

Ethernet Status
The connection status of the GPZ-IPLE Ethernet connection can be determined by observing the four LED's on the GPZ-IPLE VoIP card. The LED indications depend on whether there is an GPZ-IPLE VoIP card installed or an GPZ-IPLE VoIP card installed. Please refer to the GPZ-IPLE Differences page for further information.

GPZ-IPLE Daughter Board



The current GPZ-IPLE daughter board requires a single DSP IP address.

The IPLE daughter board provides:
- 256 (GPZ-IPLE) channels

Refer to the following tables for maximum upgrade capacities of the GPZ-IPLE daughter board:
- Table 2-6 SV9100 Maximum 9.5" Gateway and 19" System Capacities – Blades on page 2-12
- Table 2-7 SV9100 Maximum 9.5" Base and Expansion System Capacities – Blades on page 2-14

When installing an IPLE daughter board, the system allocates the maximum number of trunk ports for the blade being installed.
The IPLE does not have any DSP limitations based on CODEC settings.

2.4.1 IPLE Installation

GPZ-IPLE Installation

To install GPZ-IPLE on the GCD-CP10:

Do not remove or install the GCD-CP10 with the power on.

1. Turn off system power, and remove the GCD-CP10.

2. Install the IPLE daughter board on the GCD-CP10 blade.

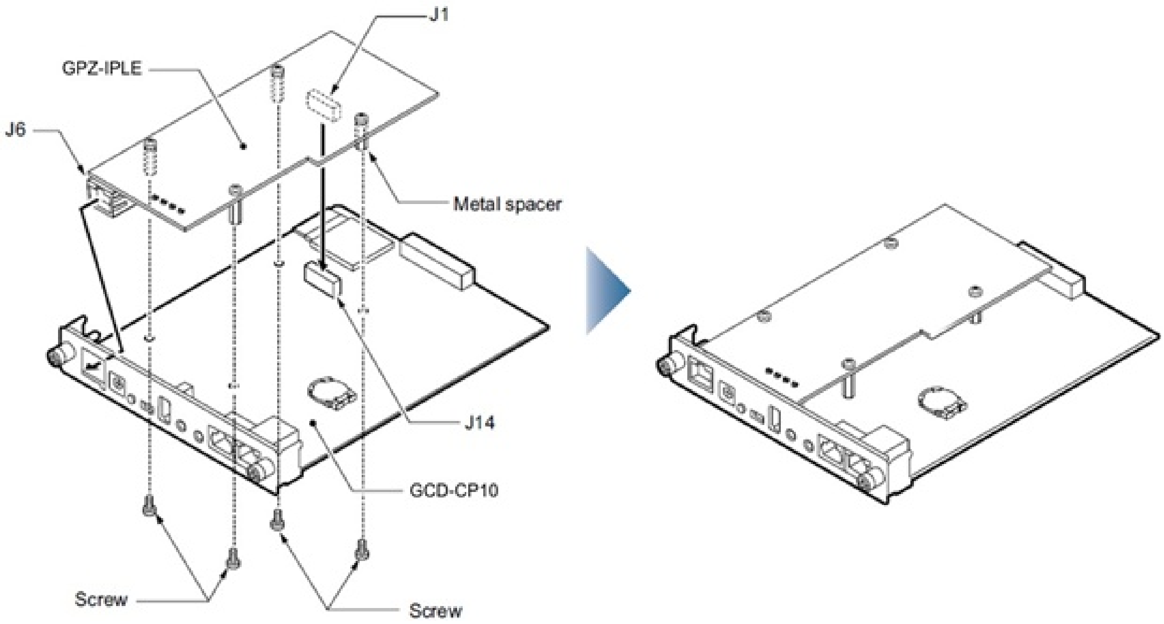


Figure 1 - Installing the GPZ-IPLE Daughter Board

3. Insert the GCD-CP10 into slot 1 in the Controlling Chassis.

4. Connect the IPLE daughter board to the CD-RTB or to an external switching hub using an Ethernet cable.

5. Refer to the UNIVERGE SV9100 Programming Manual for detailed programming instructions.

GPZ-IPLE Switch Settings

This daughter board does not have any switches that need to be set and does not require any hardware setting.

2.4.2 IPLE LED Indications

GPZ-IPLE LED Indications

LED indications for the GPZ-IPLE Daughter Board are indicated in Table 1 - IPLE Daughter Board LED Indications on page 4-29.

Each LED is listed with its associated function and LED and Operational status. Refer to Figure 1 - GCD-CP10 Blade with Daughter Boards Installed on page 4-16 for the location of the LEDs on the blades.

LED	Function	LED Status	Operation Status
LINK 10 (D103)	10 Base-TX link speed indicator	On Red	10 Base-TX link up
LINK 100 (D102)	100 Base-T link speed indicator	On Red	100 Base-T link up
LINK 1000 (D101)	1000 Base-T link speed indicator	On Yellow	1000 Base-T link up
ACT (D100)	Link activity or data transmission and reception	On Green	LED lights when link up is completed. LED flashes when data is transmitting or receiving.

Table 1 - IPLE Daughter Board LED Indications

Table 2 - IPLE Daughter Board LED CN1 Transmit/Receive Data Indications shows the LED indication when transmitting or receiving data on CN1.

ACT	LED			Operation Status
	Link1000	Link100	Link10	
Off	Off	Flash	Flash	Internal Error (Hardware Error)
Off	On	Flash	Flash	
On	On	Flash	Flash	
On	Off	Flash	Flash	State of half-duplex transmission (Not supported) Change HUB etc. to full-duplex transmission.
Flash	Blinking one by one			The firmware is being updated.

2.4.3 IPLE VoIP Channel Licensing

The GPZ-IPE VoIPDB installed in a SV9100 system has a maximum channel (DSP) capacity of 256.

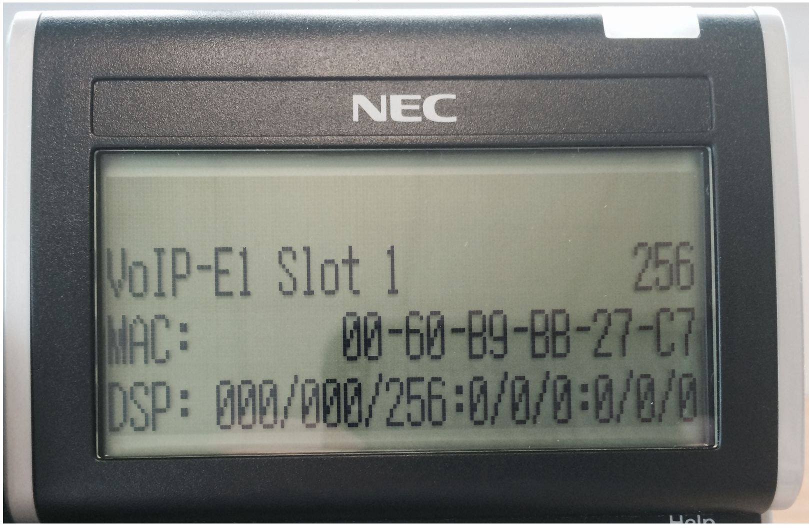
A default system with no free license enabled or additional licenses installed has 8 VoIP channels available. This means 8 IP devices could make calls through the GPZ-IPLE to TDM extensions and trunks. Alternatively 4 IP devices could make calls through SIP trunks as two VoIP channels would be required for this. One for the device and one for the trunk.

When IP devices are licensed on the SV9100, VoIP channels are automatically assigned in licensing but are not activated on the IPLE card until they have been assigned in programming.

You can check how many VoIP channels are available on a SV9100 from a keyset by pressing **Feature + 4**.

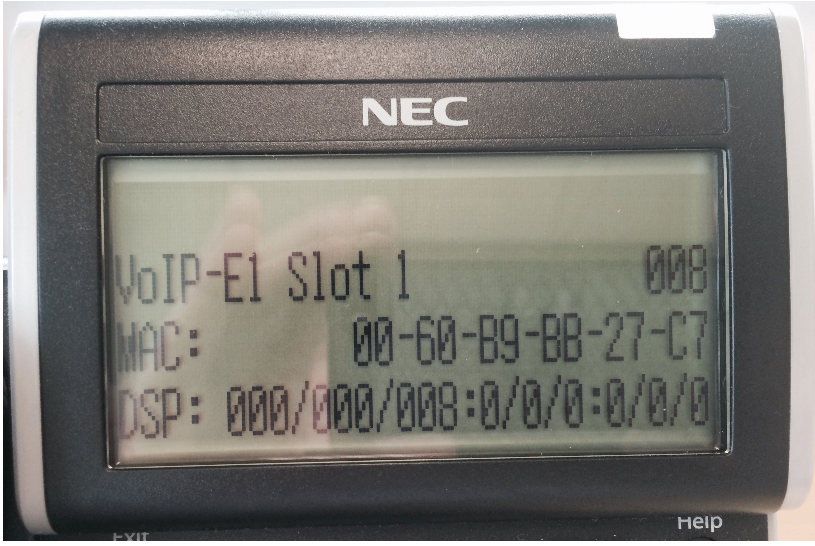
The DSP resources are displayed as ACTIVE/RESERVED/TOTAL AVAILABLE

Feature + 4 - SV9100 running Free License



The full 256 VoIP channels are available on this SV9100.

Feature + 4 - SV9100 Free License disabled and no additional licenses installed



The 8 free VoIP channels are available on this SV9100.

The below table illustrates the number of VoIP channels that are allocated in licensing with each IP device. These would be visible in the Feature Activation screen when licenses are installed as VoIP Channels (5103).

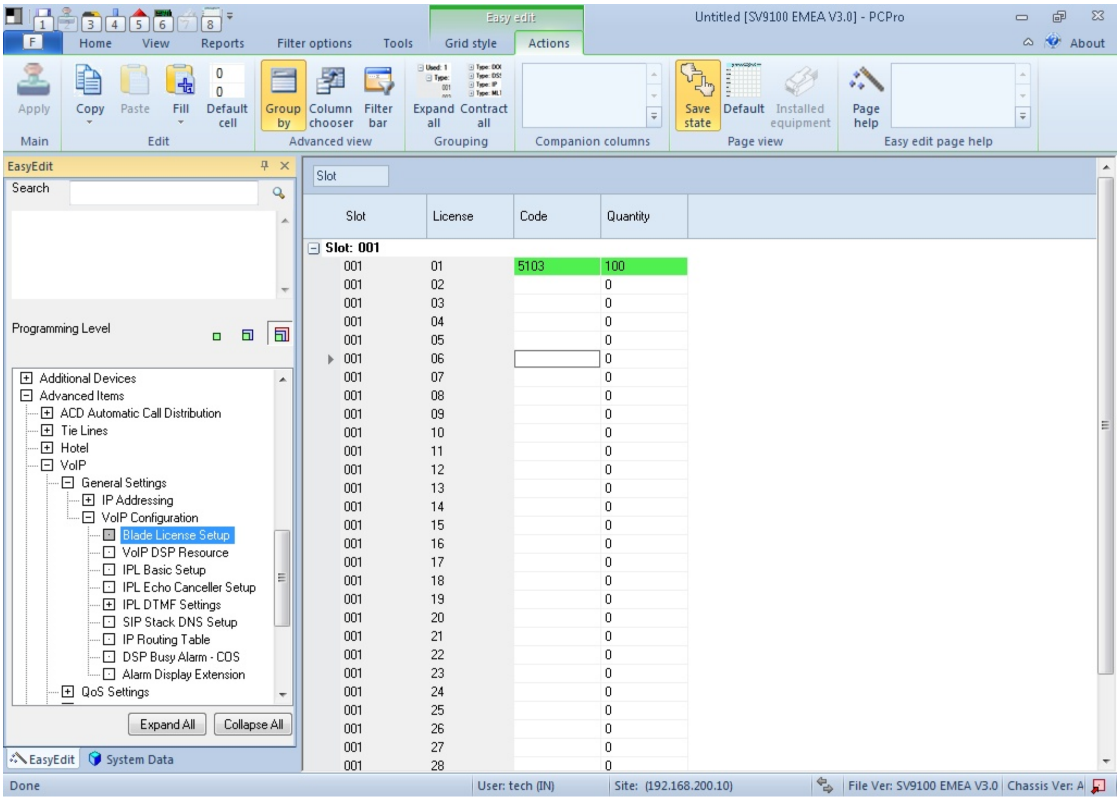
IP Devices Licensing

Product Code	License Description	Notes	Number of VoIP Channels
BE114497	SV9100 IP PHONE DT-01 LIC	SIP terminal license for DT700/DT800 terminal	1
BE114054	SV9100 IP PHONE-01 LIC	SIP terminal license for standard SIP extension including IP DECT terminal	1
BE114058	SV9100 SOFTPHONE-01 LIC	SP310 softphone license	1
BE114065	SV9100 IP TRUNK-01 LIC	IP trunk license used for SIP and H.323 trunks	1
BE114066	SV9100 NETWORKING-01 LIC	Network call channel license used for Aspirenet and K-CCIS	1
BE114067	SV9100 NETLINK NODE-01 LIC	Netlink secondary node license. Assigns additional 32 IPLE channel licenses.	32

Note: K-CCIS and Aspirenet Feature Networking use the same VoIP channels allocated

When SV9100 licenses are installed the VoIP channels must be assigned to the GCD-CP10 for a stand alone system and also when Netlink is configured for the Primary and Secondary nodes, otherwise if the free license is not enabled then the GPZ-IPE will be restricted to only use the 8 free VoIP channels and most likely cause speech issues and instanses of the DSP Busy Alarm being reported.

The VoIP channels can be allocated using *Easy Edit – Advanced Items/VoIP/General Settings/VoIP Configuration/Blade License Setup (PRG 10-54)*

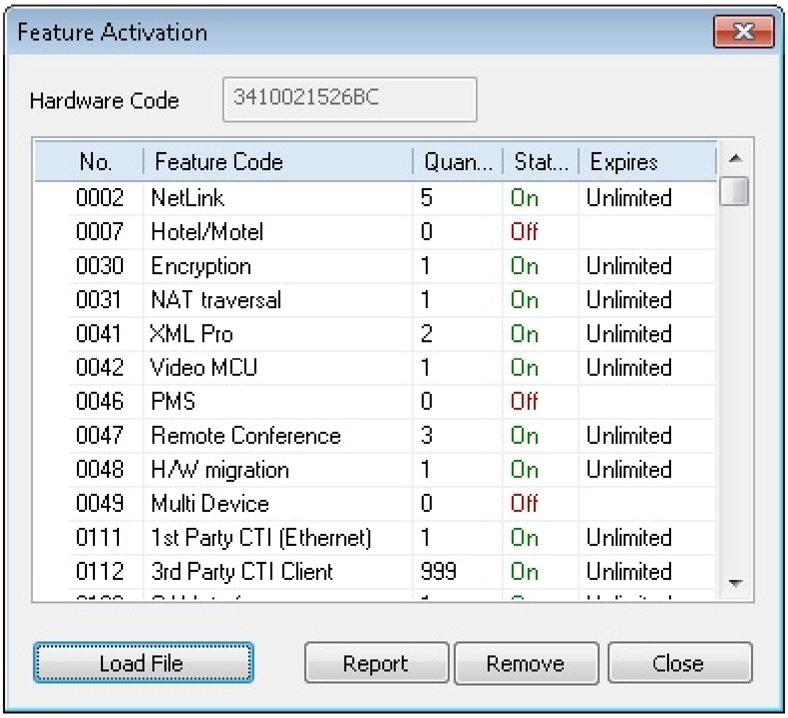


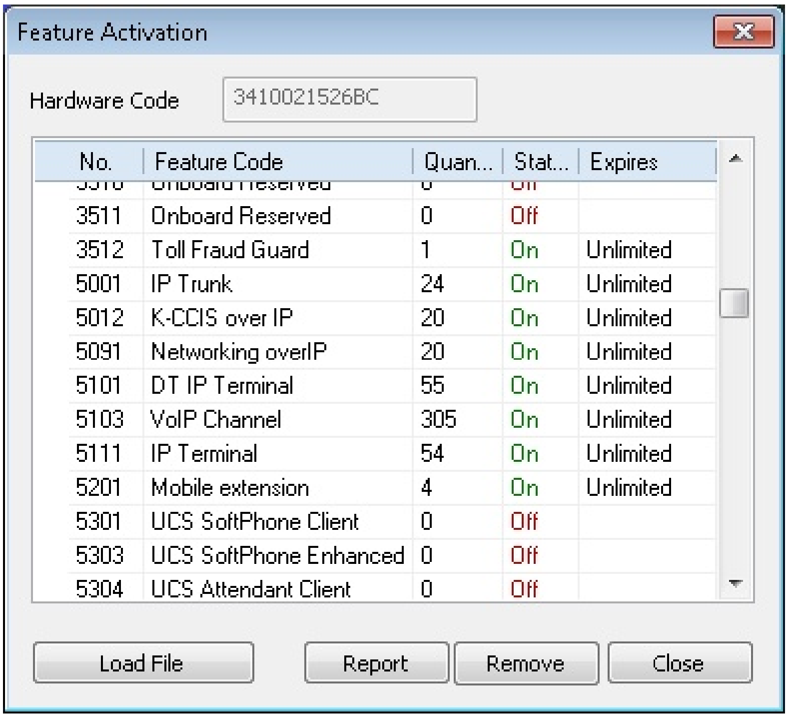
Select the GCD-CP10 slot for the standalone system. If Netlink is used then the Primary GCD-CP10 and Secondary GCD-CP10(s) will require VoIP channels allocated depending on the number of IP devices used at each node. This is flexible but most likely will match the number of IP devices used at each node.
Code - This is the VoIP channel license code and is always entered as **5103**. *(PRG 10-54)*
Quantity - The quantity of VoIP channels to allocate to this systems IPLE card. The maximum number you should enter is 248 because this with the 8 free VoIP channels will give you the maximum card capacity of 256.

Example Usage

This example demonstrates how to increase the VoIP channels allocated from 8 to 108 when additional IP licenses have been installed.

SV9100 system has the following IP licenses installed.





Based on the IP license table further up this means the SV9100 system will have the following VoIP channels allocated.

Feature Code	Feature	Quantity	VoIP Channels

0002	Netlink	5	160
5001	IP Trunk	24	24
5012	K-CCIS over IP	20	20[2]
5091	Networking over IP (AspireNet)	20	20[2]
5101	DT IP Terminal	55	51[1]
5111	IP Terminal	54	50[1]

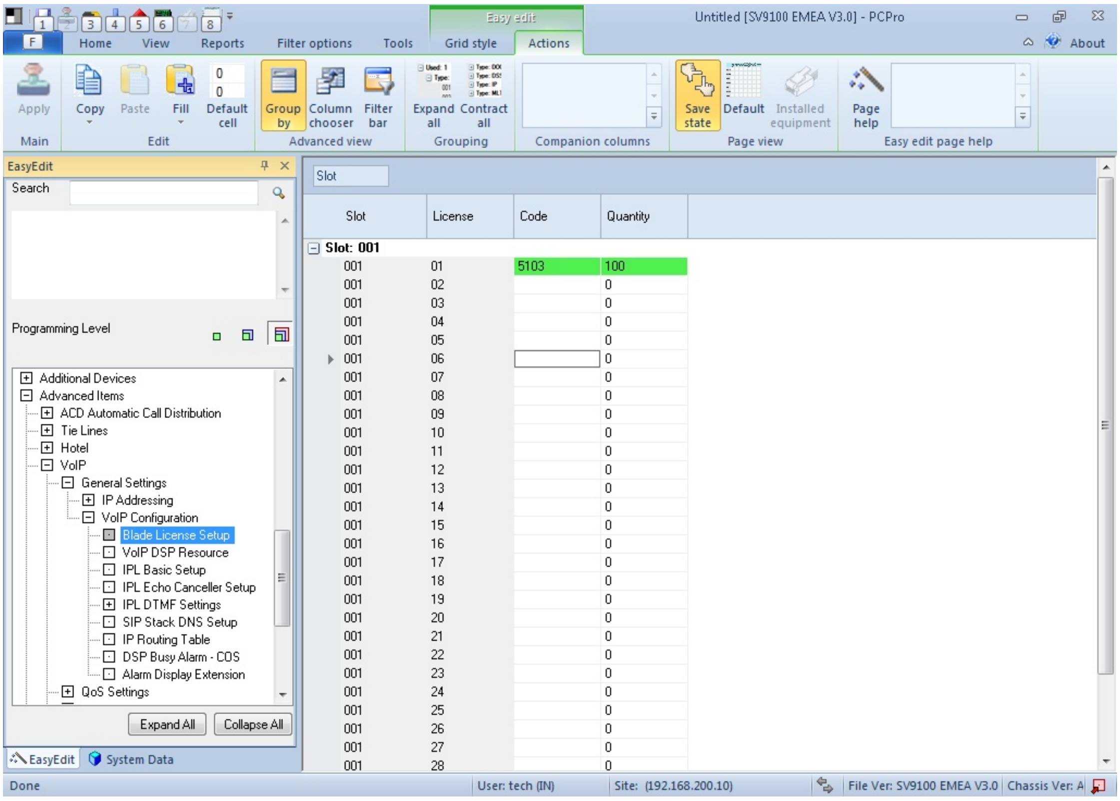
[1]There are 4 less VoIP channels allocated for DT IP Terminals (5101) and IP Terminals (5111) because the quantity displayed in the Feature Activation screen for each of these also includes the 4 free terminal licenses, however the 8 free VoIP channels (5103) are not displayed on this screen.

[2]K-CCIS over IP (5012) and Networking over IP (5091) use the same allocation of VoIP channels, so in this case it would not be 20 + 20 for each, there are just 20 available for both.

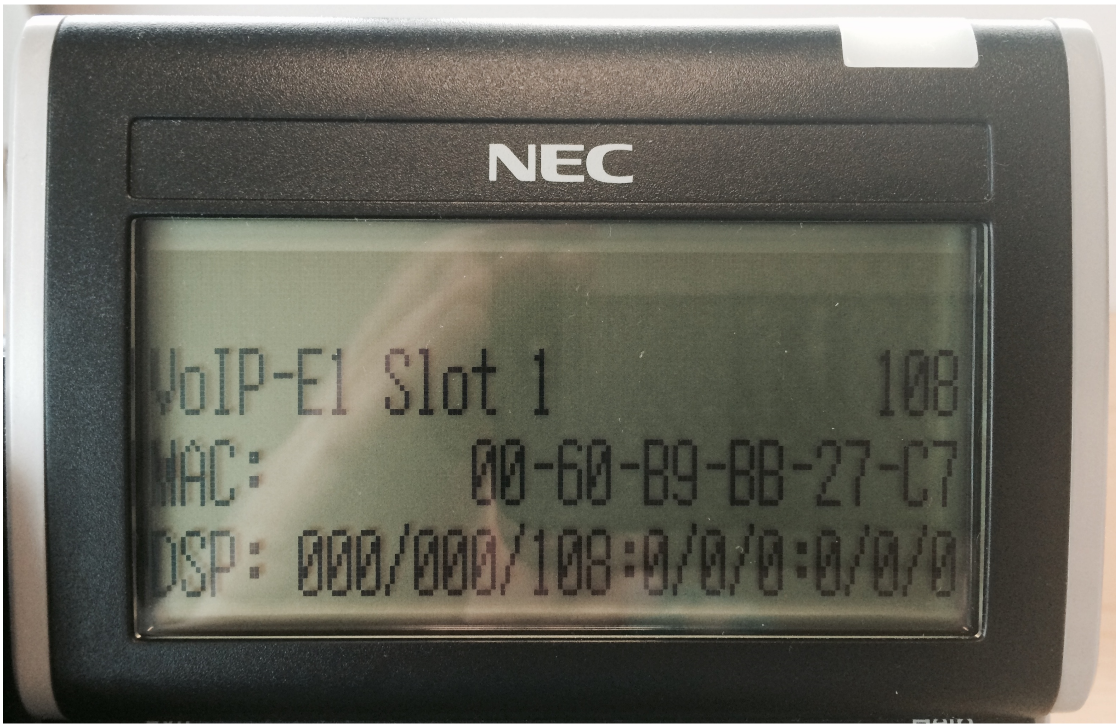
So to add the above up to the number of VoIP Channels available it goes like this:

160 + 24 + 20 + 51 + 50 = **305**

Now I determine that I want to allocate 108 VoIP channels to my GCD-CP10 at this time so back on the *Easy Edit – Advanced Items/VoIP/General Settings/VoIP Configuration/Blade License Setup (PRG 10-54)* page I allocate a quantity of 100 to code 5103. Apply, upload and then disconnect.



After the system has initialised the cards, the new VoIP channels should be allocated on the IPLE and can be confirmed by pressing **Feature + 4** on a keyset.



108 VoIP channels are now available.

2.5 Extensions

IP Extensions

This section gives an overview about the range of IP extensions that can be connected to the SV9100.
There are several different types of IP extensions that can be currently used:

- SIP MLT (DT800/DT00)
- Standard SIP (3rd Party)
- IP DECT

SIP MLT Overview

SIP MLT extensions use an enhanced version of the SIP protocol (iSIP) developed by NEC to communicate with the SV9100 system. This allows the phones to use most of the features available on a normal (TDM) keytelephone.

Use the links below for further information.
SIP MLT General InformationSIP MLT
SIP MLT Features
SIP MLT QoS
SIP MLT Models
SIP MLT Firmware Upgrade Procedure
SIP MLT IP Phone Manager
SIP MLT Auto Configuration
SIP MLT Factory Default

Standard SIP Overview

SIP is an industry standard protocol and therefore there are many different hardware and software based phones.
As these phones are not developed by NEC and are not designed specifically for use on the SV9100, they do not support majority of the features that you would find on an SV9100 Keytelephone.
The features available to SIP extensions are detailed in the SIP Extension Compatibility Report for the relevant SIP terminal.

Use the links below for further information.
Standard SIP General Information
Standard SIP available features

IP DECT Overview

IP DECT is an NEC product that combines the functionality of traditional DECT with the flexibility of the Standard SIP protocol giving a robust and reliable wireless solution.
The handsets use the traditional DECT protocol to communicate with the DECT Access Points (DAP’s) and the DAP’s use the Standard SIP Protocol to communicate with the SV9100.
Use the links below for further information.
IP DECT General Information

2.5.1 SIP MLT

The SIP MLT (DT700/DT800) Series offers a line up of modular telephones. This modular design allows the telephones to be upgraded and customized (except economy version) as required.

Optional LCD panels, keypads, handset cradles, face plates and coloured side panels can easily be snapped on and off. See the tables for compatible kits.

SIP MLT extensions use an enhanced version of the SIP protocol (iSIP) developed by NEC to communicate with the SV9100 system.
This allows the phones to use most of the features available on a normal (non-IP) keytelephone.
The phones cannot be used on any system other than the SV8000/SV9000 platforms.
The registration procedure for SIP MLT extensions is different to the SIP/H.323 Extensions, and is described in the **SIP MLT Extension Registration** section below.

To run SIPMLT extensions the SV9100 must have:

- GCD-CP10
- GPZ-IPLE
- SIP MLT License(s). Other licenses may be required for extra features/functionality.

Providing Power

SIP MLT's require power to function. This can be provided in various ways: -

a) Local Power
The SIP MLT's have a connector for external power. This is supplied by an AC adapter that has a 27V DC output. This means that a mains socket is required in the vicinity of each SIP MLT and loss of mains power in the building will prevent the phones from working.

b) Powered Patch Panel (Midspan)
A powered patch panel has two RJ-45 connectors per SIP MLT. One port connects to the switch/hub, and the other port connects to the SIP MLT. The patch panel has an integral power supply that adds power to the spare pins of the RJ-45.
When the SIP MLT is connected to the powered patch panel, it automatically receives its power via the spare pairs on the Cat-5 cable - there is no need for a local power adapter.

c) Power over Ethernet (PoE)
A PoE switch is a switched hub that also provides power over the spare pairs. The switch can be used with any device (not just SIP MLT's) and will detect if power is required or not. As all of the phones receive their power from one device, it is easy to protect the SIP MLT's from loss of power (by connecting the PoE switch to a UPS).
There are two industry standards for PoE:

- Cisco Inline Power – not supported by the DT800/DT700 range of SIP MLT’s
- IEEE802.3af – supported by the DT800/DT700 range of SIP MLT's

SIP MLT Extension registration

SIP MLT ports are allocated in blocks of 2.

For example

Insert a 16 port extension card (e.g. DLCA, LCA)

1st DT800 DT700 to register is set to 1 (default)

Configure an SIP MLT and connect to the LAN

The SIP MLT will take port 17 (ext 216 in default)

Port 18 will also be reserved for use by another IP extension.

If a second extension card (e.g. DLCA, LCA) is inserted, it will take ports 19 onwards.

When connecting a SIP MLT, the MAC address (ID) is automatically registered in *Easy Edit* – *Advanced Items/VoIP/Extensions/DT800 DT700 Setup/DT800 DT700 Terminal Settings. (PRG15-05-02)*
If the MAC address is entered manually, prior to connecting the phone, when the phone is connected, it may (depending on the Register Method) use the port number assigned.
The MAC address is printed on the barcode label on the base of the phone. It is a 12-digit alphanumeric number, ranging from 0-9 and A-F.

Note: If the port does not have a corresponding extension number assigned to it, the SIP MLT will be assigned to the next available port which does have an extension number.
If there are no ports with extension numbers available, the SIP MLT with show "Full Port" on the display.
If the extension number is removed from and already registered SIP MLT, it will re-register to the next available extension number.

If the SV9100 is being used as a DHCP server and has default IP addresses, no configuration is required on the SIP MLT.

Registration Procedure – Plug and Play

When the Register Mode is set as **Plug and Play** in *Easy Edit* - *Advanced Items/VoIP/Extensions/DT800 DT700 Setup./DT800 DT700 Hot Desk/DT800 DT700 Logon Type. (PRG10-46-01),* the following information will apply.

Set the Extension Number for the SIP MLT extension against an unused (no associated hardware) port in *Easy Edit* -*Advanced Items/VoIP/Extensions/DT800 DT700 Setup./DT800 DT700 Hot Desk/DT800 DT700 Logon Feature (PRG11-02)*

The SIP MLT should be programmed to register to the GPZ-IPLE card on the SV9100.

When an SIP MLT connects to the SV9100, it is assigned the first available port after the value set in *Easy Edit* – *Advanced Items/VoIP/Extensions/DT800 DT700 Setup/DT800 DT700 Setup/1st DT800 DT700 to register. (PRG10-46-10)*

If static IP addresses or external DHCP server is in use, follow these steps on the handset itself: -

Press Menu 0
User Name - ADMIN
Password - 6633222
OK
Press 1 1 - Choose DHCP on or off (depending on network requirements)Press OK
Press 2 - IP Address of phone (if not DHCP) Type in the required IP address using * for . Press OK.
Press 3 - Default Gateway of phone if required (if not DHCP) Press OK.
Press 4 - Subnet Mask of phone (if not DHCP) Press OK.
Press Exit.

Press 2 2 1 - Enter the IP address of the SV9100 GPZ-IPLE card Press OK.
Press Exit.
Press 4 1 - Enter 5080 (SIP Server port) Press OK.
Press Exit several times to get to the main menu.
Press Save.

The SIP MLT will now attempt to connect to the SV9100.

Registration Procedure – Automatic

When the Register Mode is set as **Automatic** in *Easy Edit* - *Advanced Items/VoIP/Extensions/DT800 DT700 Setup./DT800 DT700 Hot Desk/DT800 DT700 Logon Type. (PRG10-46-01),* the following information will apply.

Set the Extension Number for the SIP MLT extension against an unused (no associated hardware) port. *Easy Edit* -*Advanced Items/VoIP/Extensions/DT800 DT700 Setup./DT800 DT700 Hot Desk/DT800 DT700 Logon Feature (PRG11-02)*

The SIP MLT should be programmed to register to the GPZ-IPLE card on the SV9100.

Enter a Used ID and Password for each SIP MLT in *Easy Edit* - *Advanced Items/VoIP/Extensions/DT800 DT700 Setup./DT800 DT700 Hot Desk/DT800 DT700 Logon Password.* It is recommended to use the extension number as the User ID.

Take the Personal ID Index from the above command and enter it against the relevant extension number in *Easy Edit* -*Advanced Items/VoIP/Extensions/DT800 DT700 Setup./DT800 DT700 Hot Desk/DT800 DT700 Logon Feature*

If static IP addresses or external DHCP server is in use, follow these steps on the handset itself: -

Press Menu 0
User Name - ADMIN
Password - 6633222
OK
Press 1 1 - Choose DHCP on or off (depending on network requirements) Press OK.
Press 2 - IP Address of phone (if not DHCP) Type in the required IP address using * for . Press OK.
Press 3 - Default Gateway of phone if required (if not DHCP) Press OK.
Press 4 - Subnet Mask of phone (if not DHCP) Press OK.
Press Exit.
Press 2 1 1 – Enter the User ID associated with that extension programmed in the SV9100 (normally the same as the extension number) Press OK.
Press 2 – Enter the Password associated with that extension programmed in the SV9100 Press OK.
Press Exit
Press 2 1 – Enter the IP address of the SV9100 GPZ-IPLE card Press OK.
Press Exit.
Press 4 1 - Enter 5080 (SIP Server port) Press OK.
Press Exit several times to get to the main menu.
Press Save.

The SIP MLT will now attempt to connect to the SV9100.

Registration Procedure – Manual

This mode of registration gives the ability to 'Hot Desk' from one SIP MLT to another. This means you can move from one handset to another and keep the same extension number and relevant programming.

When the Register Mode is set as **Manual** in *Easy Edit - Advanced Items/VoIP/Extensions/DT800 DT700 Setup./DT800 DT700 Hot Desk/DT800 DT700 Logon Type. (PRG10-46-01),* the following information will apply.

Set the Extension Number for the SIP MLT extension against an unused (no associated hardware) port. *Easy Edit -Advanced Items/VoIP/Extensions/DT800 DT700 Setup./DT800 DT700 Hot Desk/DT800 DT700 Logon Feature (PRG11-02)*

The SIP MLT should be programmed to register to the GPZ-IPLE card on the SV9100.

Enter a Used ID and Password for each SIP MLT in *Easy Edit - Advanced Items/VoIP/Extensions/DT800 DT700 Setup./DT800 DT700 Hot Desk/DT800 DT700 Logon Password.* It is recommended to use the extension number as the User ID.

Take the Personal ID Index from the above command and enter it against the relevant extension number in *Easy Edit -Advanced Items/VoIP/Extensions/DT800 DT700 Setup./DT800 DT700 Hot Desk/DT800 DT700 Logon Feature*

If static IP addresses or external DHCP server is in use, follow these steps on the handset itself: -

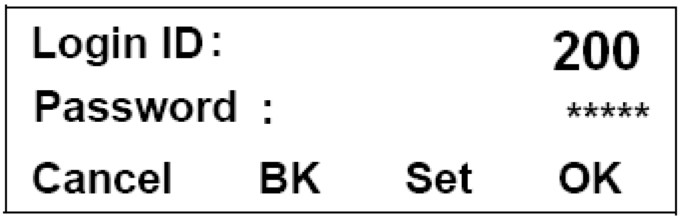
Press Menu 0
User Name - ADMIN
Password - 6633222
OK
Press 1 1 - Choose DHCP on or off (depending on network requirements)Press OK
Press 2 - IP Address of phone (if not DHCP) Type in the required IP address using * for . Press OK.
Press 3 - Default Gateway of phone if required (if not DHCP) Press OK.
Press 4 - Subnet Mask of phone (if not DHCP) Press OK.
Press Exit.
Press 2 2 1 - Enter the IP address of the SV9100 GPZ-IPLE card Press OK.
Press Exit.
Press 4 1 - Enter 5080 (SIP Server port) Press OK.
Press Exit several times to get to the main menu.
Press Save.

It is not necessary to enter the User ID and password into the handset programming, this is entered manually by the user each time they log on.

The phone will attempt to connect to the SV9100 but will show the following screen: -

Enter the User ID and press the 'Set' softkey

Enter the Password and press the 'OK' softkey



The SIP MLT will now attempt to register to the SV9100.
If the login information is accepted the display will change to normal idle status.

If the extension you are trying to log on as is already in use you may be prompted with ‘Override?’ On the display with a ‘Yes’ and ‘No’ softkey.
Choosing ‘Yes’ will log off the existing extension and give the extension number to you.
This option can be enabled or disabled on a per Personal ID Index using the **Log Off** option in *Easy Edit - Advanced Items/VoIP/Extensions/DT800 DT700 Setup./DT800 DT700 Hot Desk/DT800 DT700 Logon Password. (PRG84-22-04)*

Log the phone off
With the phone in an idle state, press the ‘Prog’ soft key four times, then press the ‘LOGOFF’ soft key
The display shows ‘LOGOFF THE SYSTEM?’ with a ‘Yes’ and ‘No’ soft key

Press ‘Yes’

The phone is now logged off and cannot be used until it is logged back on.

Alternatively you can press and hold the Exit key for 2 seconds.

The display shows ‘LOGOFF THE SYSTEM?’ with a ‘Yes’ and ‘No’ soft key

Press ‘Yes’

The phone is now logged off and cannot be used until it is logged back on.

SIP MLT Extension registration in a NetLink Environment

From Release 3 software it is possible to register a SIP MLT to any node in a NetLink environment.
If the SIP MLT is to register to the Primary system then all above information is correct and no changes are required.
If the SIP MLT is to register to a secondary node the only difference is that it should register to the relevant GPZ-IPLE IP address and port number.
The IP addresses of connected systems can be found in *Easy Edit – Advanced Items/VoIP/Networking/ NetLink/NetLink Systems* (PRG51-11-03).
The relevant port numbers can be found in *Easy Edit – Advanced Items/VoIP/Networking/NetLink/NetLink DT700 Registrar Ports* (PRG51-17).

Conditions
It is not possible for the DT800/DT700 to use the encryption feature when registered to a Secondary node.
This feature is not available for Standard SIP extensions.

SIP MLT Fail-Over Operation

In a NetLink environment it is possible to enter up to 4 registration destinations. This means that if the system that a SIP MLT is registered to is no longer available it can re-register to another node in the network. Furthermore, if the original system recovers the handset may revert back to its original registrar (software release 4 feature).

To set the registration destinations and port numbers for each SIP MLT follow these steps: -

Press Menu 0

User Name - ADMIN

Password - 6633222

OK

2. SIP Settings

2. Server Address & URI

Choose 1^{st}, 2^{nd}, 3^{rd} or 4^{th} Server Address in the order you wish to search

Enter the GPZ-IPLE IP address and press OK.

Press Exit

4. SIP Server Port

Enter the relevant port number for each Server (default 5080) and press OK.

Press Exit

Press Exit

Press Save.

The IP addresses of connected systems can be found in *Easy Edit* – *Advanced Items/VoIP/Networking/ NetLink/NetLink Systems* (PRG51-11-03).
The relevant port numbers can be found in *Easy Edit* – *Advanced Items/VoIP/Networking/NetLink/NetLink DT700 Registrar Ports* (PRG51-17).

Conditions
NetLink Replication must be enabled for this feature to work correctly.
DT800/DT700 NAT Terminals cannot use the SIP MLT Fail-Over Operation.
R3 software must be installed on all nodes.

Delete SIP MLT Registration

Before attempting to delete the registration of a SIP MLT, the IP Phone must be unplugged or powered off.
Enter Program 90-23-01 (handset programming or Web Pro only), and enter the extension number of the IP Phone. Press **1** and **Transfer** to delete the registration.

SIP MLT Codec Settings

SIP MLT's can use various CODECs. A CODEC is a standard for converting an analogue signal to digital. This conversion process is handled by the DSP (Digital Signal Processors) on the GPZ-IPLE card.
Each CODEC has different voice quality and compression properties. The correct choice of CODEC will be based on the amount of bandwidth available, the amount of calls required and the voice quality required.

Available Codecs for SIP MLT handsets

- G.711 64Kbps codec MOS 4.4
- G.722 64Kbps codec MOS 4.4
- G.729 8Kbps codec MOS 4.0

The bandwidth values quoted for these codecs are for the digitized speed in one direction only. The actual bandwidth required for a call will depend on many other factors and will be much higher than these figures.

The above MOS values are quoted for ideal network conditions. The value could be lower depending upon the network performance.

The codec is programmed against a Type (profile). Up to five Types (profiles) can be set up. The extension is then assigned to particular Type (profile).

1) Program the codec for each Type using the **Audio Capability Priority** option in *Easy Edit – Advanced Items/VoIP/Extensions/DT800 DT700 Setup/DT800 DT700 Codec (PRG84-24-28)*
2) Assign the Type number to the extension using the **Codec Type** option in *Easy Edit – Advanced Items/VoIP/Extensions/DT800 DT700 Setup/DT800 DT700 Terminal Settings (PRG15-05-15)*

Please be aware that this codec selection is only a *preferred* setting. It is possible that a SIP MLT will use one of the other available codecs depending on the destination of the conversation and also who was the originating party of the call.

RTP Alarm

RTP Alarm is an audible indication to a user that the RTP (speech) is not getting through to that user. It can be heard when using SIP MLT Extensions when there are problems on the network between the end points.
The alarm is indicated as several short beeps in the ear piece of the receiving user, the beeps may be repeated if the problem continues.

The RTP Alarm can be enabled/disabled on a per handset basis using the handset Menu: -

Menu
5. Setting
1. User Setting
2. Talk
1. RTP Alarm
Chose the required setting for the RTP Alarm and press OK
Press the 'Exit' key to exit the handset Menu

More information regarding packet loss may be obtained by using the 'QoS' option of the SIP MLT Maintenance Menu.

SIP MLT Maintenance Menu

There is a maintenance menu in the SIP MLT. To access it, press the "Help" button for 2 seconds.
This menu can only be accessed after the display shows "Connecting..." or the extension is operational. It is possible to use this menu during a call.
The menu options are as follows: -

1. QoS
2. System Information
3. Ping

The ‘QoS’ option gives information about lost packets, codec in use and the payload size.
The ‘System Information’ option gives various information about the network settings, SIP Settings, Audio & Visual Settings, Maintenance Settings and Terminal Information.
The ‘Ping’ option gives the ability to ping another IP address to check connectivity across the network.

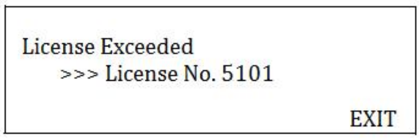
Note: The lost packet count can only be updated when the SIP MLT has connectivity with the SV9100, if connection is lost during the call the display will not be updated.

Peer to Peer

By default if two IP extensions are on an internal call together, the RTP will be sent directly between the two endpoints.
This reduces the DSP consumption, reduces delay on the VoIP packets and increases voice quality on the call.
There may be instances where this operation is not supported. May be the customers network does not allow it.
If this is the case it is possible to disable Peer to Peer for SIP MLT extensions. Use the **Peer to Peer** option in *Easy Edit – Advanced Items/VoIP/Extensions/DT800 DT700 Setup/DT800 DT700 Terminal Settings (PRG15-05-50)*

License

The SV9100 requires licensing to allow the registration of SIP MLT handsets. One license is required for each registration to the SV9100. If no license is available, the display of the SIP MLT shows:



Up to 896 SIP MLT licenses can be added.
License Code: BE114497

2.5.1.1 SIP MLT Models

There are several types of SIP MLT phone available for the SV9100. The system programming is the same regardless of the IP phone model.
The following SIP MLT models are available:

DT700 SIP MLT Terminals

- ITL-2E-1. This IP economy non-display Multiline Terminal has two programmable line keys. It does not support headset working
- ITL-6E-1. This IP economy Mutiline Terminal has six line keys with a display. It does not support headset working.
- ITL-8LDE-1. This IP economy Multiline Terminal has eight line keys with DESI-less display. It does not support headset working.
- ITL-8LD-1. This IP value Multiline Terminal has eight line keys with DESI-less display and a normal display.
- ITL-12D-1. This IP value Multiline Terminal has 12 line keys with display.

- ITL-12PA-1. This IP value Multiline Terminal with Analogue Power Failure adapter has 12 line keys with display.
- ITL-24D-1. This IP value Multiline Terminal has 24 line keys with display.
- ITL-32D-1. This IP value Multiline Terminal has 32 line keys (24 line keys plus an eight line key LK Unit) with display.
- ITL-320C-1. This IP sophisticated Multiline Terminal features a large colour touch panel LCD.
- ITL-12DG-3P This IP value Multiline Terminal has 12 line keys with display and Gigabit connectivity.
- ITL-12CG-3P This IP value Multiline Terminal has 12 line keys with colour display and Gigabit connectivity.

DT800 SIP MLT Terminals

- ITZ-8LDG-3P This IP value Multiline Terminal has eight line keys with DESI-less display and Gigabit connectivity.
- ITZ-12D-3P This IP value Multiline Terminal has 12 line keys with display.
- ITZ-12DG-3P This IP value Multiline Terminal has 12 line keys with display and Gigabit connectivity.
- ITZ-12CG-3P This IP value Multiline Terminal has 12 line keys with colour display and Gigabit connectivity.
- ITZ-24D-3P This IP value Multiline Terminal has 24 line keys with display.

2.5.1.2 SIP MLT Features

SIP MLT Encryption

It is possible to encrypt the signalling data and the speech data (RTP) between one or more DT800/DT700 extensions and the GPZ-IPLE card.

A 128 bit AES encryption technique is used.

If NetLink is in operation, the DT800/DT700 must be registered to the Primary system to be able to use the Encryption feature.

It is possible to set only the signalling to be encrypted or the signalling and the RTP together, it is not possible to encrypt only the RTP without encrypting the signalling.

If the call is between two DT800/DT700's with Peer to Peer enabled and both extensions are set to use encryption, the signalling and RTP will be encrypted regardless of the settings in system programming.

Only DT800/DT700 extensions can use the encryption feature, it is not supported for standard SIP extensions or any networking protocol.

If the speech is encrypted (sRTP) the number of available DSP's on the GPZ-IPLE card may be reduced (depending on the codec used). See the GPZ-IPLE DSP Information page for more information.

Encryption - System Programming

Easy Edit – Advanced Items/VoIP/Extensions/DT800 DT700 Setup/DT800 DT700 Encryption (PRG10-46)
Enable **Encryption Mode**
Enter a password in **One Time Password**
To enable RTP Encryption, enable **SRTP Mode** *(PRG84-27-03)*

Encryption - Handset Programming

On each DT800/DT700
Enter configuration menu (menu 0) followed by the password.
Option 2. SIP Settings.
Option 7. Encryption.
Option 1. Authentication Mode = Enable
Option 2. One Time Password = (As entry in PRG10-46-09) - Save

The handset will reboot and attempt to authenticate with the SV9100, if it is successful it will show 'Authentication Accepted'.
The handset will reboot again and show the normal display information once it has registered.
If RTP encryption is enabled, any call that has encrypted RTP will be indicated with the symbol of a key in the display during the call.

Encryption – CAUTION

The system and the handset use the one time password to create an authentication key. The authentication key is then used to encrypt the signalling and RTP packets.
In the unlikely event that this password or key is compromised it may be required to delete the key and create a new one.
The key can be deleted by using *PRG90-45-01*.
BEWARE, using this comand will remove the authentication key used by every IP extension that has encryption enabled. Each handset will then require reprogramming.
This programming command is only available through handset programming.

If encryption is in use, it may no longer be possible to troubleshoot any problems using network monitoring software e.g. Wireshark. If you need to use Wireshark to diagnose a problem it is recommended to disable encryption.

If NetLink is in operation, the DT800/DT700 must be registered to the Primary system to be able to use the Encryption feature.

SV9100 Requirements

The following information provides requirements for Encryption.

Handset Firmware

Encryption is supported with V2.2.1.0 DT700 handset firmware or later.

Hardware

The SV9100 requires the following hardware:
GCD-CP10
GPZ-IPLE

License

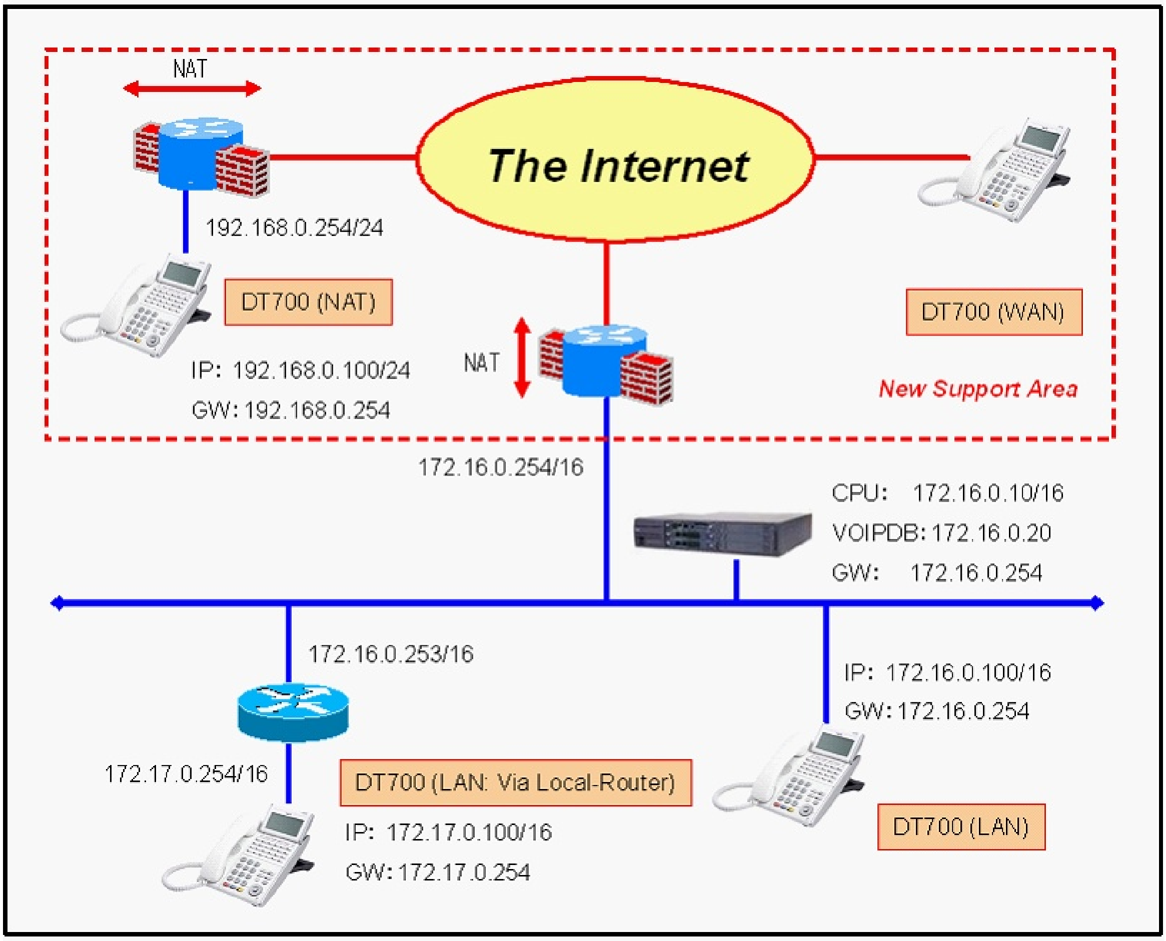
The system must be licensed for this feature with a BE114068 (License 0030).
The system must be licensed for DT800/DT700 ITL Terminals.

SIP MLT NAPT

The NAPT (**N**etwork **A**ddress **P**ort **T**ranslation) feature gives the SV9100 the ability to “traverse” its own subnet. With NAPT used in the SV9100, the network administrator can place the GCD-CP10 and the GPZ-IPLE in the customers LAN while still making it accessible to DT800/DT700 users outside the local LAN (e.g. via the internet).

This means a VPN is no longer required to place a DT800/DT700 on a remote network.
(This feature is not available for 3rd Party SIP devices (standard SIP))

A network configuration diagram is shown below



Depending on their locations, terminals are classified into the following four categories:

- LAN terminals

Terminals installed on the LAN where the main device is installed.

- WAN terminals

Terminals directly installed in the global address space.

- NAT terminals

Terminals connected to the main device through a NAT router.

- LAN terminal via local router

Terminals connected to the main device via a local router (non NAT)

DT700 NAPT System Programming – Additional programming for DT800/DT700 operation is still required.

Easy Edit – Advanced Items/VoIP/Extensions/DT800 DT700 Setup/DT800 DT700 NAT/DT800 DT700 NAT Setup
NAT Mode - On *(PRG10-46-14)*
NAPT Router IP Address - Static public IP address (system side). *(PRG10-12-07)*

Easy Edit – Advanced Items/VoIP/Extensions/DT800 DT700 Setup/DT800 DT700 NAT/DT800 DT700 NAT Exempt Networks. (PRG10-58)
Enter the network address and subnet mask of DT800/DT700 LAN terminal via local router (if connected – see below for further information).

Port forwarding system side

On the router connected to the SV9100 network, forward port UDP/5080 and UDP/5081 to the SV9100 GPZ-IPLE IP address.
Also forward the RTP ports (UDP/10020 - 10532) to the SV9100 VoIP gateway address. More entries may be required depending on the configuration and if NetLink is used.

Static or Dynamic NAT

There are two options available when programming the handset, Static NAT or Dynamic NAT. The choice depends on the capabilities of the router on the handset network. If UDP Session Detection is supported by the router then Dynamic NAT should be possible. It is recommended, where possible, to use Dynamic NAT.

Dynamic NAT

The router on the handset side must support dynamic address and port mapping for outgoing and incoming traffic.

Enter the Config Menu of the handset and Enable DHCP Mode in Network Settings/DHCP Mode. This should give an IP Address, Subnet Mask and Default Gateway to the DT800/DT700.

Be aware, when using NAT the handset does not use the normal SIP Server Settings. There is a new area for NAT addresses.

In SIP Settings/NAT Traversal/NAT Traversal Mode - set to **Dynamic**
In SIP Settings/NAT Traversal/WAN Settings/WAN Mate IP Address - Enter the **public IP address of the SV9100** *Easy Edit – Advanced Items/VoIP/Extensions/DT800 DT700 Setup/DT800 DT700 NAT/DT800 DT700 NAT Setup/NAPT Router IP Address. (PRG10-12-07)*
In SIP Settings/NAT Traversal/WAN Settings/WAN Mate Port - Set to **5080**.
In SIP Settings/NAT Traversal/WAN Settings/WAN Self IP Address – Leave this blank, the phone will get this address dynamically.

Exit and save, the handset will now try and register to the SV9100.

If it fails it may be because the router does not support dynamic address and port mapping. If this is the case Static NAT may have to be used.

Static NAT

The handset should have a static IP address or if using DHCP then reserve an address using its MAC address (if supported by the DHCP server).
Be aware, when using NAT the handset does not use the normal SIP Server settings. There is a new area for NAT addresses.
Set IP address, subnet mask and default gateway as usual in Config Menu/Network Settings.
In SIP Settings/NAT Traversal/NAT Traversal mode - set to **Static**
In SIP Settings/NAT Traversal/WAN Settings/WAN Mate IP Address - Enter the **public IP address of the SV9100** *Easy Edit – Advanced Items/VoIP/Extensions/DT800 DT700 Setup/DT800 DT700 NAT/DT800 DT700 NAT Setup/NAPT Router IP Address. (PRG10-12-07)*
In SIP Settings/NAT Traversal/WAN Settings/WAN Mate Port - Set to **5080**.
In SIP Settings/NAT Traversal/WAN Settings/WAN Self IP Address - Enter the **public IP address of the**

router on the network where the handset belongs.

Port forwarding handset side

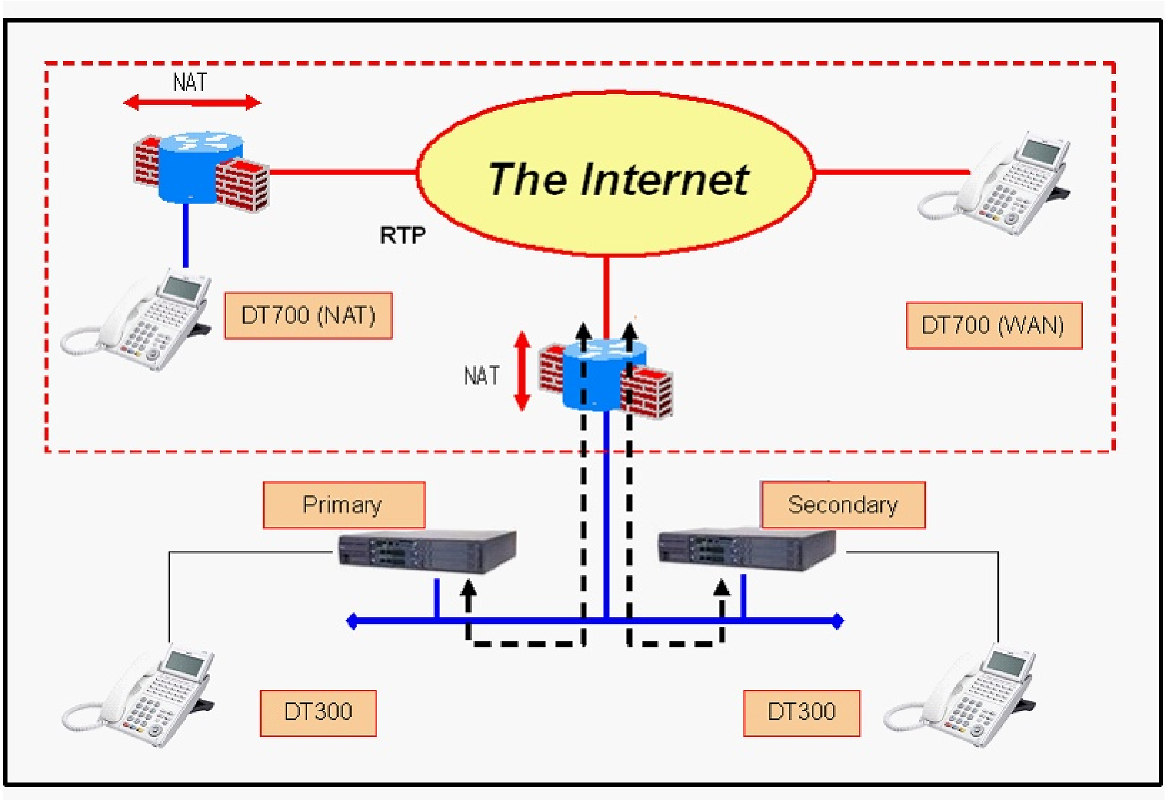
On the router connected to the handset network, forward port UDP/5060 to the IP address of the handset. Also forward port UDP/3462 to the IP address of the handset.

If you have multiple NAT handsets on the same remote network you will need to change the port numbers on each handset so that they are unique on the network. The first handset will be ok with default port numbers.
You can change the port numbers in Network Settings/Advanced Settings/Self Port Settings – The SIP Port can increment by one, recommend 5061, 5062 etc. The RTP ports must be an even number, recommend 3464, 3466 etc. The relevant port forwarding will then be required on the router on the handset network.

NetLink Considerations

When using NAPT in conjuction with NetLink the RTP/RTCP ports on the Primary and Secondary systems must be unique (see table below for an example).
This is to facilitate the correct port forwarding in the NAT router when the RTP should be forwarded to the Secondary VoIPU gateway rather than the Primary.

Index	PRG	Primary	Secondary	Remarks
1	10-12-03	172.16.0.254	172.16.0.254	LAN IP address of NAT router
2	10-12-09	172.16.0.10	172.16.10.10	IP address of GCD-CP10
3	10-12-10	255.255.0.0	255.255.0.0	Subnet mask of GCD-CP10
4	84-26-01	172.16.0.20	172.16.10.20	IP address of VoIPDB
5	84-26-02	10020	**20020**	RTP port number of VoIPDB
6	84-26-03	10021	**20021**	RTCP port number of VoIPDB



In this example there would be the following port forwarding rules in the NAT router connected to the SV9100: -

UDP/5080 -> 172.16.0.10 (DT800/DT700 signalling to SV9100)
UDP/5081 -> 172.16.0.10 (DT800/DT700 signalling to SV9100)
UDP/10020 – 10051 -> 172.16.0.20 (DT800/DT700 RTP/RTCP to Primary SV9100)
UDP/20020 – 20051 -> 172.16.10.20 (DT800/DT700 RTP/RTCP to Secondary SV9100)

DT800/DT700 Terminal via Local Router

If DT800/DT700 NAPT is programmed on an SV9100 it needs to know if there are any DT800/DT700 extensions connected via a local (non NAT) router or any remote DT800/DT700 which does not require passing through the NAT process. The network address of these extensions must be entered in *Easy Edit – Advanced Items/VoIP/Extensions/DT800 DT700 Setup/DT800 DT700 NAT/DT800 DT700 NAT Exempt Networks.*

An example of a DT800/DT700 via Local Router is if the SV9100 GPZ-IPLE card is in VLAN 10 and a DT800/DT700 extension is in VLAN 20. In this case the network address of VLAN 20 would need to be programmed on the SV9100.
These requirements also apply for a local routed network, not just VLAN operation.
These requirements **do not** apply for extensions connected via VPN's

Conditions

- "License Exceeded" will display on the DT800/DT700 terminal when trying to register a NAT phone, if the feature is not licensed.
- The NAPT Enhancement feature is only supported with GPZ-IPLE, not GPZ-IPLE.

- DT700 Terminals using NAPT Enhancement must be at firmware V3.0.0.0 or above.
- The NAT router on the SV9100 side must have a static WAN IP address, UPNP is not supported.
- UC Client softphone is not supported.
- Wireless phone (MH240) is not supported.
- If NAT enabled phones become unresponsive after being idle, the timer in Programs 84-23-01 and 84-23-02 may need to be changed to a shorter interval.
- It is necessary to set Program 10-46-14 to **OFF** when the GPZ-IPLE is assigned a global (public) IP address.
- When Program 10-46-14 is set to **ON**, it references programs 10-58-01 and 10-58-02 for terminals connected via a local router.
- NAPT can be used for SIP trunks and terminals on the same system.
- Multicast RTP packets cannot be set to an extension using the NAPT feature (ExMOH, BGM, and Room Monitor).

Restrictions – Static NAT

- A contract for static IP addresses is required for a WAN-side IP address specified for the NAT router on the terminal side.
- The NAT router on the terminal side must have the function for setting up static NAT.
- A conversion table must be manually set up for the NAT router on the terminal side.
- The table must be set up so that that the NAT router only converts IP addresses, not port numbers.
- IP addresses for terminals have to be specified statically. When allocating an IP address using DHCP, the IP address might change. NEC does not guarantee proper operation in this case.
- If installing multiple terminals in the domain of the NAT router on the terminal side, the SIP port number and RTP/RTCP port number for each terminal must be specified so as to avoid overlapping.
- The SIP server cannot be switched. (Only one address can be registered as the SIP server.)

Restrictions – Dynamic NAT

- The NAT router on the terminal side must have the function for setting up dynamic NAT.
-

Restrictions - Dynamic NAT

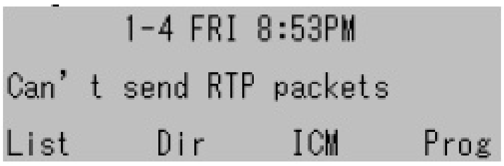
- The NAT router on the terminal side must have the function for setting up dynamic NAT.
- The beginning of the voice may cut depending on the network environment. And for this reason, a warning sound may rumble in the ear piece at the beginning of the call. If you want to avoid this warning, you must set program 15-05-3 to 0.
- It is assumed that port numbers are not changed by the NAT router on the terminal side.
- If a port number is changed by NAT router, NEC does not guarantee proper operation.
- If installing multiple terminals in the domain of the NAT router on the terminal side, the SIP port number and RTP/RTCP port number for each terminal must be specified so as to avoid overlapping.
- Peer to Peer is only possible for IP terminals under the same router.

	LAN	WAN	NAT
LAN	P2P	VoIPDB	VoIPDB
WAN	-	VoIPDB	VoIPDB
NAT	-	-	P2P(Only under the same router)

SV8100 R6

P2P was possible before SV8100 R6 enhance.

- When negotiation of a call has been completed. If GPZ-IPLE does not receive an RTP packet within 10 seconds of call setup, the call is disconnected. When this occurs the below message is displayed on the terminal LCD.

- 

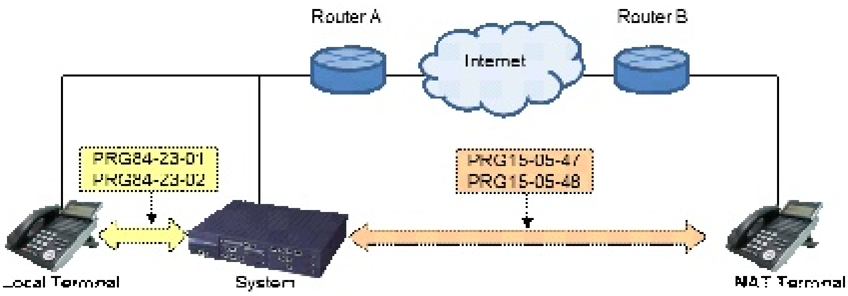
- The SIP server cannot be switched. (Only one address can be registered as the SIP server.)

SIP MLT NAPT Improvement for Registration Timers

Sometimes when a DT800/DT700 Terminal connects to the SV9100 via NAPT the intermediate router may have a firewall function, if there is no communication for a defined period the router may close the port used by the DT800/DT700. This will block the IP packets and the terminal will not function correctly.

A solution to this is to reduce the DT800/DT700 Registration and Subscription Expiry timers – however this could then cause unnecessary network load if a large quantity of DT800/DT700 terminals are also connected on the LAN since the same timers are used.

The Registration and Subscription timers for DT800/DT700 terminals connected via the LAN can be set to a longer duration than those connected via NAPT.



Easy Edit – Advanced Items/VoIP/Extensions/DT800 DT700 Setup/DT800 DT700 NAT/DT800 DT700 NAT Extension Plug and Play/Registration Expire Timer for NAT (15-05-47) - (0, 60 – 65535 Seconds) default = 180. A setting of 0 will disable the timer and a DT700 connected via NAPT will use the timer specified in 84-23-01.

Easy Edit – Advanced Items/VoIP/Extensions/DT800 DT700 Setup/DT800 DT700 NAT/DT800 DT700 NAT Extension Plug and Play/Subscribe Expire Timer for NAT (15-05-48) - (0, 60 – 65535 Seconds) default = 180. A setting of 0 will disable the timer and a DT700 connected via NAPT will use the timer specified in 84-23-02.

NetLink Operation
When a NAPT DT800/DT700 is registered to a secondary system the timer of the primary system from CMD 15-05-47 & 48 are used.
Timer setting and quantity of NAPT terminals
Since the network load will increase with the quantity of NAT terminals it is recommended that the following minimum settings are used.

PRG Commands	Quantity of terminals / minimum timer setting

	1~144	~192	~180	~512
15-05-47	60	90	180	180
15-05-48	60	90	180	480

SIP MLT NAPT Enhancement

The Dynamic NAPT (**N**etwork **A**ddress **P**ort **T**ranslation) feature has been enhanced to improve the performance of SIP MLT when used with a dynamic router connected at the terminal side.

Port forwarding on terminal side should no longer be necessary when using this feature with a suitable dynamic NAT enabled router. If using a Static NAPT router configuration then the setup details found in SIP MLT NAPT should still be used.

DT800/DT700 NAPT System Programming – Additional programming for DT800/DT700 operation is still required.

Easy Edit – Advanced Items/VoIP/Extensions/DT800 DT700 Setup/DT800 DT700 NAT/DT800 DT700 NAT Setup/NAT Mode. (PRG10-46-14) = On
Easy Edit – Advanced Items/VoIP/Extensions/DT800 DT700 Setup/DT800 DT700 NAT/DT800 DT700 NAT Setup/NAPT Router IP Address. (PRG10-12-07) = Static public IP address (system side).
Easy Edit – Advanced Items/VoIP/Extensions/DT800 DT700 Setup/DT800 DT700 NAT/DT800 DT700 NAT Exempt Networks. (PRG10-58) = Network address and Subnet mask of DT700 LAN terminal via local router (if connected – see below for further information).
Easy Edit – Advanced Items/VoIP/Extensions/DT800 DT700 Setup/DT800 DT700 NAT/DT800 DT700 NAT Extension Plug and Play/NAT Plug and Play. (PRG15-05-45) = Enabled per SIP MLT using NAPT.

Port forwarding system side

On the router connected to the SV9100 network, forward port UDP/5080 and UDP/5081 to the SV9100 GPZ-IPLE IP address.

Also forward the RTP ports (UDP/10020 - 10532) to the SV9100 VoIP gateway address. More entries may be required depending on the configuration and if NetLink is used.

Dynamic NAT

The router on the handset side must support dynamic address and port mapping for outgoing and incoming traffic.

Enter the Config Menu of the handset and Enable DHCP Mode in Network Settings/DHCP Mode. This should give an IP Address, Subnet Mask and Default Gateway to the DT700.

Be aware, when using NAT the handset does not use the normal SIP Server Settings. There is a new area for NAT addresses.

In SIP Settings/NAT Traversal/NAT Traversal Mode - set to **Dynamic**
In SIP Settings/NAT Traversal/WAN Settings/WAN Mate IP Address - Enter the **public IP address of the SV9100** *Easy Edit – Advanced Items/VoIP/Extensions/DT800 DT700 Setup/DT800 DT700 NAT/DT800 DT700 NAT Setup/NAPT Router IP Address. (PRG10-12-07)*
In SIP Settings/NAT Traversal/WAN Settings/WAN Mate Port - Set to **5080**.
In SIP Settings/NAT Traversal/WAN Settings/WAN Self IP Address – Leave this blank, the phone will get this address dynamically.

Exit and save, the handset will now try and register to the SV9100.

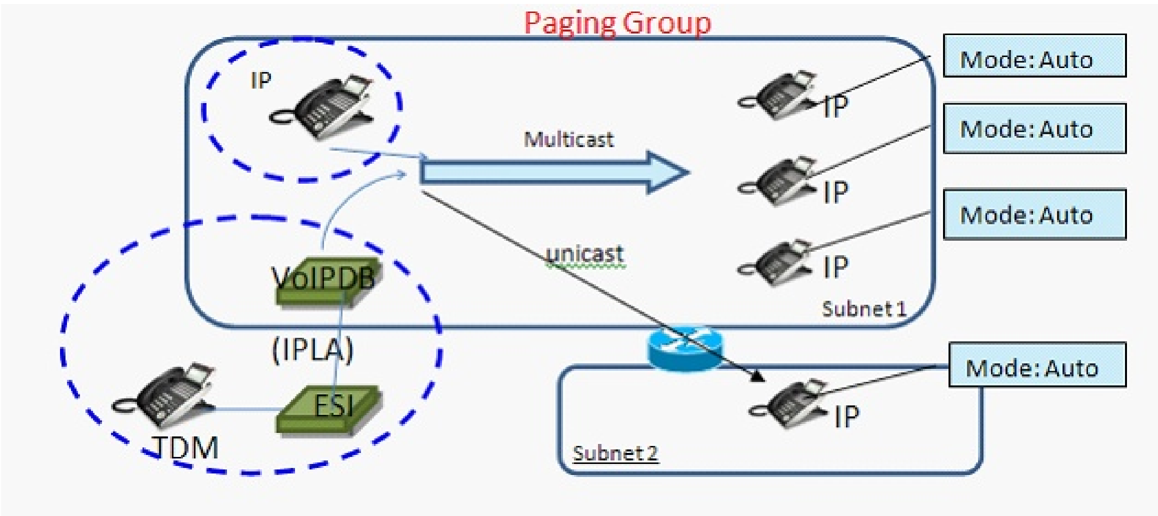
If it fails it may be because the router does not support dynamic address and port mapping. If this is the case Static NAT may have to be used.

SIP MLT Time Zone Offset

If a SIP MLT is located in a different time zone to the system it is registered to the time and date may be incorrect.
This can be resolved by offsetting the time and date on each handset compared to the system. Use the Time Zone(hour) and Time Zone(minute) options in *Easy Edit – Advanced Items/VoIP/Extensions/DT800 DT700 Setup/DT800 DT700 Terminal Settings* (PRG15-05-41/42).
The default hour setting is 12, this means 0 hours offset (equal to the system).
The default minute setting is 60, this means 0 minutes offset (equal to the system).
Possible entries are 0 to 24 hours (-12 to +12 hours) and 0 to 120 minutes (-60 to +60 minutes.

Unicast Paging

There is a choice between IP Multicast, Unicast or Automatic on a per extension basis.
This is of benefit when the DT800/DT700 extensions reside on a remote network where the routers do not support IP Multicast relay.



In the above example all extensions have the Paging Mode set to Automatic.
The system will reference the Subnet of the GPZ-IPLE and the Subnet of the extensions in the Paging Group.
If they belong to the same network then IP Multicast will be used. If they are in different networks then Unicast will be used and the router does not need to support Multicast relay.

SV9100 Programming
Use the **Paging Protocol Mode** option in *Easy Edit – Advanced Items/VoIP/Extensions/DT800 DT700 Setup/DT800 DT700 Terminal Settings. (PRG15-05-38)*

Set to **Multicast, Unicast** or **Auto** on a per extension basis.

Related programming
PRG10-19 GPZ-IPLE DSP Resource Selection.
Three new options, 6 – Common without Unicast Paging, 7 – Multicast Paging, 8 – Unicast Paging.

Limitations

- One DSP is required for ***each*** extension using Unicast Paging Mode where as only one DSP is required for ***all*** extensions using Multicast Paging Mode.
- Unicast Paging is not executed to an extension which can not get access to a DSP.
- Unicast can only be used for the Paging feature. Other Multicast features are not affected (MOH, Room Monitor, BGM).
- MH240 is not supported for Unicast Paging Mode.

LLDP

Description
Link Layer Discovery Protocol (LLDP) is used to transmit and receive information about neighboring network devices and IP telephones. Some SIP MLT settings can be automatically specified according to the LLDP data received from the network switch.
LLDP operates at layer 2 so the IP address of the terminal does not need to be specified until after the LLDP operation has completed.
LLDP uses IP Multicast to transmit/receive information so this must be taken into account on the customer's network.

LLDP Standards
The supported standards are:

- IEEE802.1AB:2005
- ANSI/TIA-1057 LLDP-MED (LLDP for media endpoint discovery).

The device class is "Endpoint Class III"

Requirements

- DT700 terminals must have firmware V4.0.0.0 or later to use the LLDP feature.
- The SIP MLT must be factory defaulted after the firmware upgrade to use the LLDP feature.
- The network switch must support LLDP and be configured accordingly.
- The network switch configuration varies depending upon the manufacturer and model. Consult the network administrator/maintainer for further information.
- If the LLDP information becomes unavailable from the network the terminal will continue to operate unless it is rebooted. It will then use the settings from the terminal's own configuration rather than the LLDP settings.

SIP MLT LLDP Menu
Default settings indicated in red

- Press Menu 0
- Enter the User Name and Password
- 1. Network Settings

- 6. Advanced Settings
- 6. LLDP Settings
    - o 1. LLDP Mode (Enable/Disable) (Enable)
    - o 2. Auto Setting Mode (Enable/Disable) (Enable)
    - o 3. RX Waiting Time (1 – 60 Seconds) (15 Seconds)
    - o 4. Transmit Interval (5 – 32768 Seconds) (30 Seconds)
    - o 5. Hold Multiplier (2 – 10) (4)
    - o 6. Fast Start Count (1 – 10) (3)
    - o 7. Transparent Mode (Enable/Disable) (Enable)
    - o 8. Asset ID (Input an Asset ID) (-)

Note:
Non-display IP Terminals should be configured using the Web interface or Auto Config.
All LLDP configuration items except 'Asset ID' are available via Auto Config in IP Phone Manager.

LLDP information sent from SIP MLT

Example:

Chassis id:	172.16.0.100	(Terminal IP address)
Port id:	0060.b9xx.xxxx	(Terminal MAC address)
Port Description:	LAN Port	
System Name:	NEC IP Phone	
System Description:	DT700 Series	
Time remaining:	xx seconds	
System Capabilities:	Bridge, Telephone	
Enabled Capabilities:	Bridge, Telephone	
Auto Negotiation:	supported, enabled	
Physical media capabilities:		
	100base-TX (Full Duplex)	
	100base-TX (Half Duplex)	
	10base-T (Full Duplex)	
	10base-T (Half Duplex)	
Media Attachment Unit type:	10	
MED Information:		
	H/W revision: 9.1.3.4	
	F/W revision: 4.0.0.0	
	S/W revision: -	
Serial number:		
Manufacturer:	NEC	
Model:	DT700 Series	
Asset id:	ASSET001	(Assigned in handset config)

LLDP information sent from Network Switch

Example (switch type and configuration dependant):

Chassis Subtype	18:EF:63:xx:xx:xx
Port Subtype	Fa 0/2
Time to Live	xx Seconds
System Name	Lab Switch
System Description	Cisco IOS V12.2 (55) SE
Port Description	Fast Ethernet 0/2
Capabilities	Bridge, Router
Management Address	172.16.255.254
Media Capabilities	LLDP-MED
	Network Policy

	Location Identification
	Extended Power
	Inventory
Hardware Revision	WS-C3560-8PC
Software Revision	12.2(55) SE
Manufacturer Name	Cisco Systems
Model Name	WS-C3560-8PC
Network Policy (Voice)	(VLAN ID, CoS, DSCP etc.)
Network Policy (Voice Signal)	(VLAN ID, CoS, DSCP etc.)
Extended Power Via MDI	Power priority
Location ID	Road, City, Post Code, Country etc.
Port VLAN ID	VLAN ID
MAC/PHY Configuration/Status	Speed, Duplex

SIP MLT Maintenance Menu

Received LLDP information can be viewed in the Maintenance Menu:

- Press and hold the ‘Help’ key for 2 seconds
- 2. System Information
- 6. LLDP Receive Information
  - LLDP Receive Data (Valid/Invalid)
  - Manufacturer Name
  - Model Name
  - System Name
  - System Description
  - Chassis ID
  - Port ID
  - Port Description
  - PHY Auto-nego status
  - Speed & Duplex
  - Unknown Flag (Voice)
  - VLAN Tag Flag (Voice)
  - VLAN ID (Voice)
  - L2 Priority (Voice)
  - DSCP Value (Voice)
  - Unknown Flag (VoiceSignal)
  - VLAN Tag Flag (VoiceSignal)
  - VLAN ID (VoiceSignal)
  - L2 Priority (VoiceSignal)
  - DSCP Value (VoiceSignal)
  - Location ID (Civic)
  - Location ID (ECS ELIN)
  - Asset ID

If the information received by LLDP changes whilst viewing this menu it will not refresh automatically. Exit and re-enter the Maintenance Menu to confirm the information is up to date.

Spare/Backup IP

Description

This facility allows the SIP MLT handset to use alternate network information which is used in the event of the DHCP server becoming unavailable.

There are two options for the alternate information:

1. **Spare IP**. This is where each terminal is preconfigured with static network information which is

used in case the DHCP server is unavailable.

2. **Backup IP**. This is where the terminal saves the network information that it receives from the DHCP server and uses it when the DHCP server is unavailable.

If **Spare IP** is used the network information that can be preconfigured is:

- IP Address
- Default Gateway
- Subnet Mask
- DNS Address
- 2nd SIP Server Address
- 3rd SIP Server Address
- 4th SIP Server Address
- 2nd SIP Server Port
- 3rd SIP Server Port
- 4th SIP Server Port

The above settings can be found in the handset Config Menu:

1. Network Settings
6. Advanced Settings
7. Spare IP Settings

If **Backup IP** is used the following information is saved to the handset flash memory:

- IP Address
- Default Gateway
- Subnet Mask
- DNS Address

The following information needs to be preconfigured (if required)

- 2nd SIP Server Address
- 3rd SIP Server Address
- 4th SIP Server Address
- 2nd SIP Server Port
- 3rd SIP Server Port
- 4th SIP Server Port

If Spare IP or Backup IP is being used by the handset because the DHCP server is unavailable the usual SIP server addresses programmed in to the handset are not used. Instead it uses the settings in:

2. Network Settings
6. Advanced Settings
7. Spare IP Settings
3. SIP Settings

At least the 2nd SIP Server Address and the 2nd SIP Server Port number needs to be configured if Spare IP or Backup IP is to be utilised.

SV9100 Requirements

Main Software

Spare/Backup IP is supported on any version of SV9100 software.

Firmware
Spare/Backup IP is supported on DT700 firmware V4.0.0.0 onwards

Conditions/Comments

- If using a spare or backup IP address, the same address might be used by a different device making it impossible to communicate with the SV9100.
- If using a spare or backup IP address, Auto configuration cannot be executed.
- If the Auto Configuration mode is enabled, the spare or backup IP address operating mode setting are initialised to the defaults. The backup IP service data previously acquired from the DHCP server is retained.
- The backup data previously acquired from the DHCP server is deleted when the configuration data clearing (initialisation of the terminal setting data) is executed.
- If using a spare or backup IP address, services other than the telephone function of programs such as XML applications might not work correctly.
- The backup data is also backed up or restored when the configuration data is backed up or restored.
- If the alternate IP address mode is “backup IP” data is saved to flash memory when the IP address is acquired from the DHCP server at the specified time.
- If the IP telephone is turned off while saving to flash memory, it might become impossible to start up the phone.

Configuration
Enter the handset Configuration Menu by pressing ‘Menu 0’ and enter the Username and Password.

- Press 1. Network Settings
- Press 6. Advanced Settings
- Press 7. Spare IP Settings
- Press 1. Spare/Backup IP Mode
  - Press 1. Disable
  - Press 2. Spare IP
  - Press 3. Backup IP
  - Press OK
- If using Spare IP Press 2. Network Settings
  - Press 1. IP Address and enter the static Spare IP address
  - Press OK
  - Press 2. Default Gateway and enter the IP Address of the Default Gateway
  - Press OK
  - Press 3.

2.5.1.3 SIP MLT QoS

SIP MLT Quality of Service

The SIP MLT handsets support Layer 2 (IEEE 802.1p/Q) or Layer 3 Quality of Service.
The programmable items are:

- VLAN tag for handset
- VLAN Priority for handset
- VLAN tag for PC port
- VLAN Priority for PC port
- ToS setting for RTP
- ToS setting for SIP signalling

VLAN Settings

It is possible for the SIP MLT to have specific VLAN and Priority settings. It is also possible for the PC uplink connection to have different VLAN and Priority settings.
The VLAN and Priority settings must be made by programming each individual handset.

Setting VLAN Values for the SIP MLT

1. Press **Menu**, then **0** (Config) to enter the terminal program mode.
2. At the Login screen, enter the user name (default = ADMIN) and password (default = 6633222) and press the **OK** softkey.
3. Press **1** for Network Settings.
4. Press **6** for Advanced Settings.
5. Press **1** for LAN Port Settings.
6. Press **2** for VLAN Mode.
7. Press **2** to Enable and press the **OK** softkey.
8. Press **3** for VLAN ID.
9. Enter the required VLAN information and press the **OK** softkey.
10. Press **4** for VLAN Priority.
11. Enter the require VLAN Priority information and press the **OK** softkey.
12. Press the **Exit** softkey three times.
13. Press the **Save** softkey.
14. The handset will reboot and reconnect to the SV9100.

Setting VLAN Values for the PC Port

1. Press **Menu**, then **0** (Config) to enter the terminal program mode.
2. At the Login screen, enter the user name (default = ADMIN) and password (default = 6633222) and press the **OK** softkey.
3. Press **1** for Network Settings.
4. Press **6** for Advanced Settings.
5. Press **2** for PC Port Settings.
6. Press **2** for Port VLAN Mode.
7. Press **2** to Enable and press the **OK** softkey.
8. Press **3** for Port VLAN ID.
9. Enter the required VLAN information and press the **OK** softkey.
10. Press **4** for Port VLAN Priority.
11. Enter the require VLAN Priority information and press the **OK** softkey.
12. Press the **Exit** softkey three times.
13. Press the **Save** softkey.
14. The handset will reboot and reconnect to the SV9100.

ToS Settings

It is possible for the SIP MLT to have specific Layer 3 QoS (ToS) values. It is possible to set the SIP signalling and RTP ToS values independently allowing for different values for each.
There are two ways to set the ToS values in a SIP MLT handset:

- By programming each handset through its menu.
- By programming the SV9100 which the SIP MLT then reads on registration.

In both cases the QoS value must be set by using a hexadecimal value.

Setting ToS Values using the SIP MLT Menu

1. Press **Menu**, then **0** (Config) to enter the terminal program mode.

2. At the Login screen, enter the user name (default = ADMIN) and password (default = 6633222) and press the **OK** softkey.
3. Press **1** for Network Settings.
4. Press **6** for Advanced Settings.
5. Press **4** for Type Of Service.
6. Press **1** for RTP.
7. Enter the hexadecimal value for the required ToS and press the **OK** softkey.
8. Press **2** for SIP.
9. Enter the hexadecimal value for the required ToS and press the **OK** softkey.
10. Press the **Exit** softkey three times.
11. Press the **Save** softkey.
12. The handset will reboot and reconnect to the SV9100.

Setting ToS Values using the SV9100 Programming

There are two items in system programming, one for SIP signalling and one for RTP.
For SIP signalling use the **Type of Service** option in:
Easy Edit – Advanced Items/VoIP/Extensions/DT800 DT700 Setup/DT800 DT700 Setup. (PRG84-23-06)
For RTP use the **Media ToS** item in:
Easy Edit – Advanced Items/VoIP/Extensions/DT800 DT700 Setup/DT800 DT700 Setup. (PRG84-23-13)

When the SIP MLT registers to the SV9100 it will read these ToS values and use them from that point onwards.
Using this method every SIP MLT registered to the SV9100 will have the same ToS values.

Considerations

If the SIP MLT is set to mark the frames/packets with QoS information this is only applied to the information being sent from the SIP MLT. The SV9100 must also be set to mark the frames/packets that it sends out to the SIP MLT.

For any type of QoS to function correctly the network that the devices are connected to must support the same protocol that the devices are using. The network must also be set up correctly to allow priority for this traffic over other traffic on the network. This must be done throughout the entire network.
Liaise with the network administrator to ensure this is implemented correctly.

2.5.1.4 SIP MLT IP Phone Manager

SIP MLT IP Phone Manager

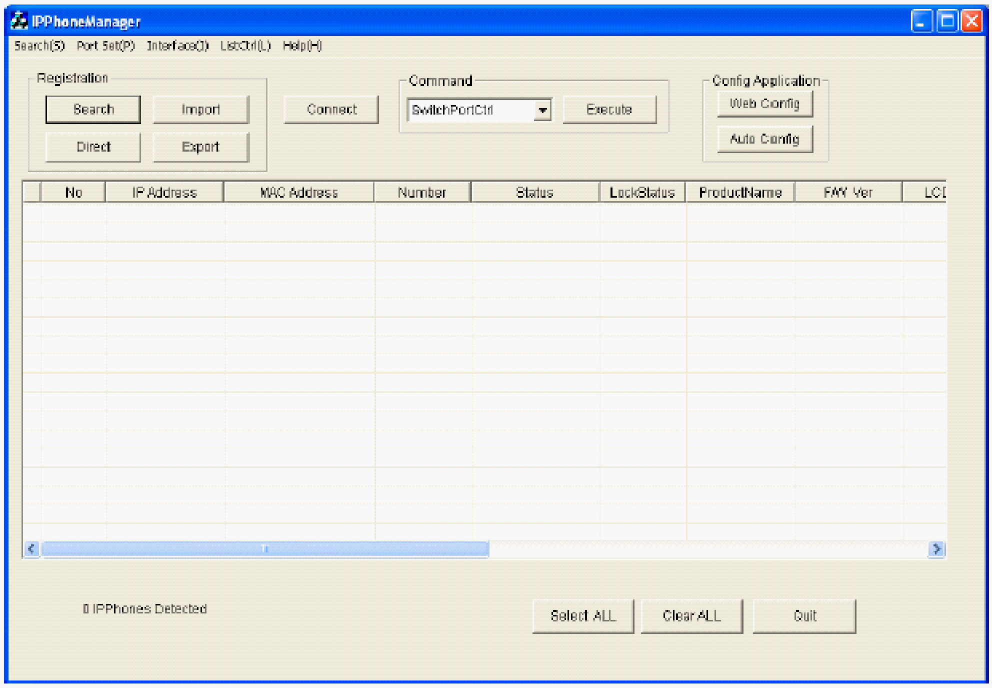
IP phone manager is a maintenance application for SIP MLT extensions.
It can be used for several functions such as initiating file downloads, creating configs, changing settings, backing up configs etc.

INSTALLATION

Follow these steps for installation of the IP Phone Manager.
1. Double Click Setup.exe icon to initiate the installation.
2. After installation, a Shortcut is placed on your PC Desktop. This icon can be used to run the IP Phone Manager application.
3. At the elect Interface Pop Up, select the active Network Interface Card that your PC is currently

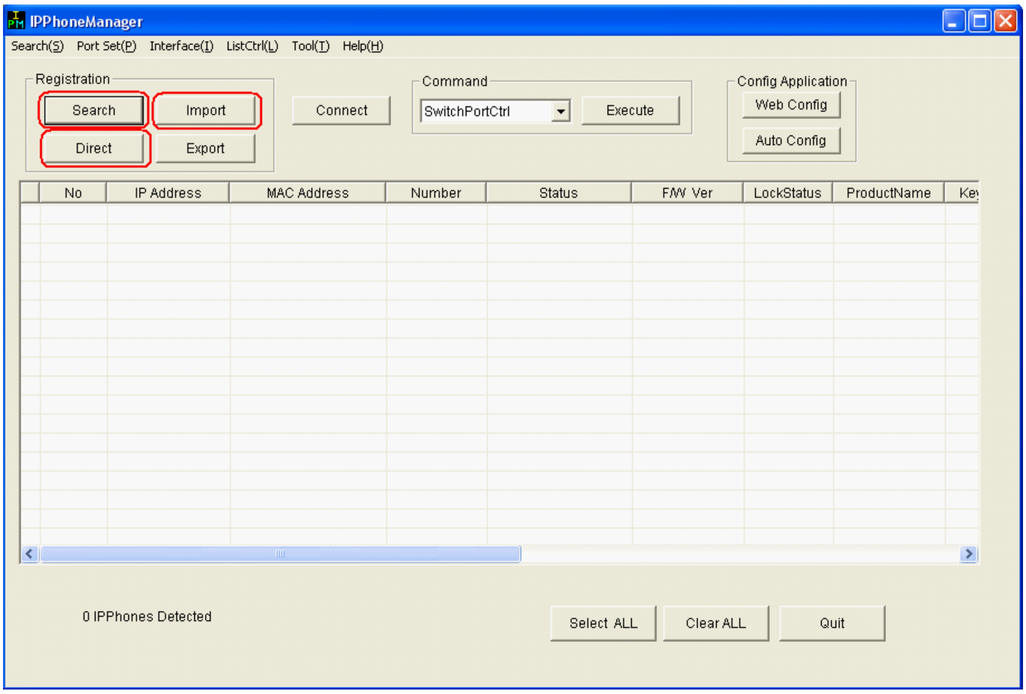
using.

4. IP Phone Manager now opens on your PC.



SEARCHING FOR TERMINALS

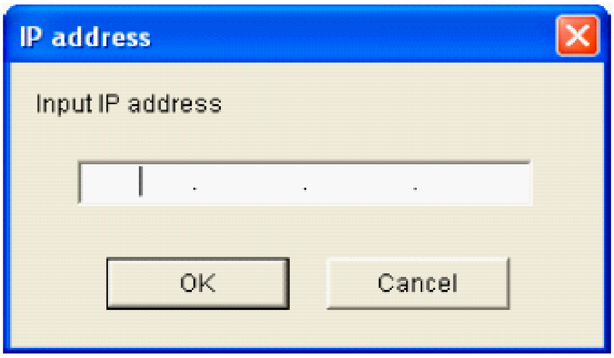
There are three methods to search for active terminals on your network.



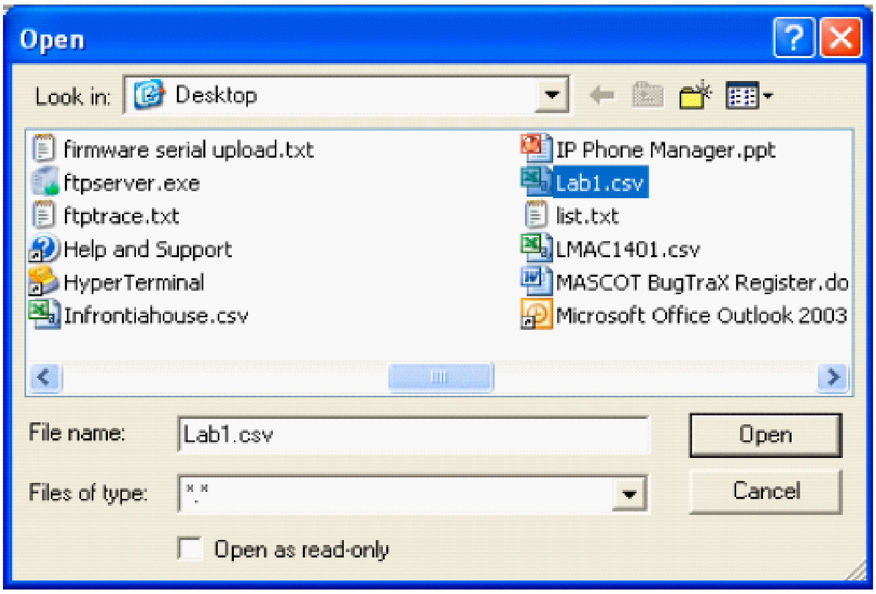
1. Search
The IP Phone manager sends a broadcast over the network in search of terminals. Active terminals respond to this broadcast with terminal information.

There are three settings that change the Search Frequency and timing of the IP Phone Manager broadcast.

2. Direct
When an IP Address of the terminal is known, it is possible to search for it independently. This is commonly used to for a quick search of a specific terminal or a terminal that may be in a different network or subnet.

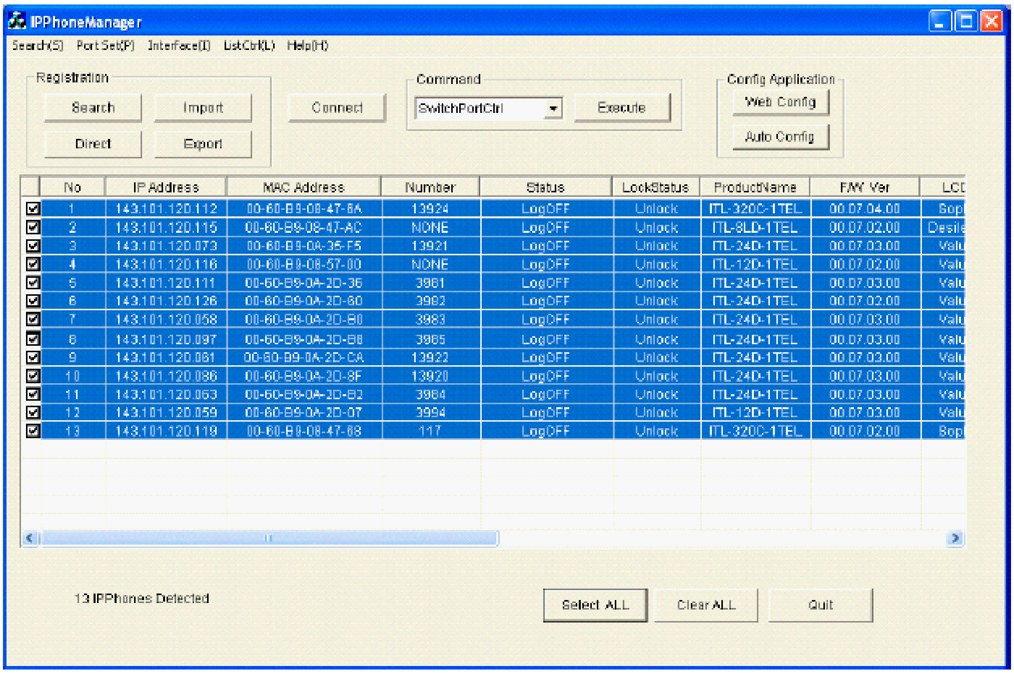


3. Import
PBX System configuration applications may export a list of registered terminals in a CSV file format. This CSV file can be imported to the IP Phone Manager Application. This import can now be used to Search and Connect the registered terminals indicated in the imported file.
The IP Phone Manager allows an active list of terminals to be exported in CSV format for later import or to save a current database for examination.

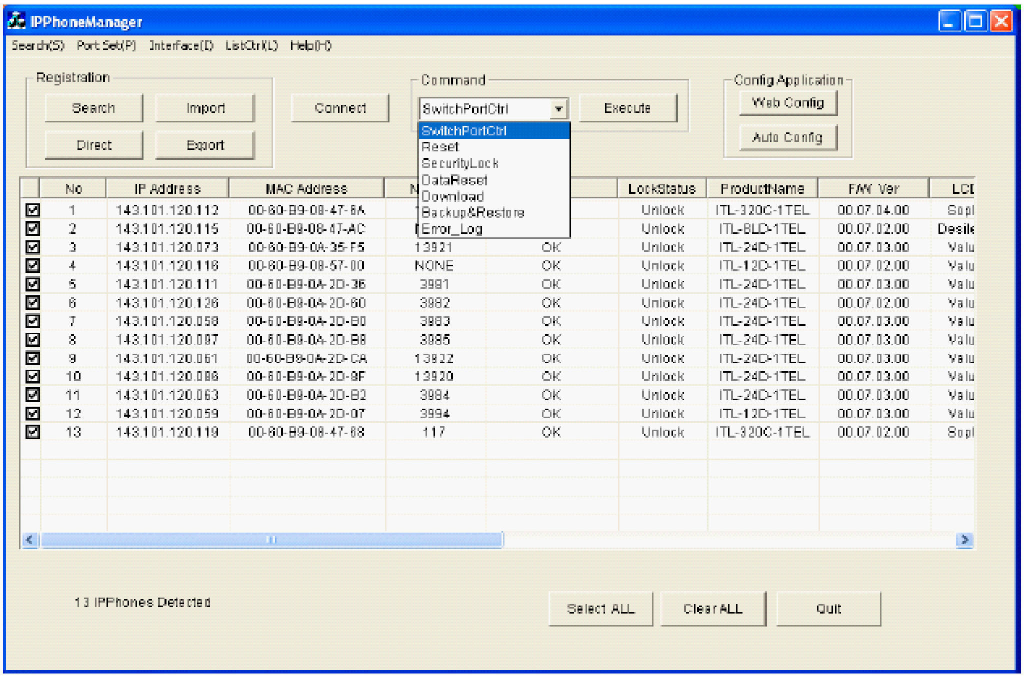


Terminal Connection

After terminals are discovered by the IP Phone Manger Search functionality, they must be connected to before any action can take place. For terminals that need maintenance or further information communicated between them, select the check box and press **Connect**. When the Status Field indicates OK, the terminal is in active communication with IP Phone Manager.



IP Phone Manager Commands



1. SwitchPortCtrl
   Switch Port Control can enable or disable the PC Port on the connected IP Terminal(s).
2. Reset
   This function resets the terminal(s) connected to the IP Phone Manager.
   Two options for resetting the Connected terminal(s) are available:
   - Soft Reset – Application layer of the terminal
   - Hard Reset – Full hardware reset of the terminal

3. SecurityLock
   This feature can lock or unlock the Connected Terminal(s), and has two modes:
   - **Enable** allows the user to change the status of the terminal security.
     - All Clear – Returns the terminal password to default value
     - Unlock – One-time security release on the terminal
     - Lock – Locks the Connected terminal(s)
   - **Disable** disables the SecurityLock feature from being set from the terminal.

4. Data Reset
   Data Reset erases the configuration stored in terminal memory. Three terminal memory locations can be reset.
   - IP Phone Settings – Terminal Configuration Data that is set in terminal programming under the **Config** menu tree
   - Personal Settings
   - Personal Data – Data that the user has personally set (holding tone, ring tone, and telephone book)
     - Factory Value resets all three data settings

5. Download

This feature downloads various file types via a FTP/TFTP server. Select the server type to be used for downloads and the parameters that are required (IP Address of server, authentication name and passwords).

Download Option:

- Use the Download Option Field to select the Terminal File type and enter a File name as required.
- Use the Simultaneous Downloads to select the quantity of terminals that access and attempt downloads at the same time. All remaining terminals are put into queue for the next available position. Some server applications can handle only limited simultaneous connections – consult your server documentation for any limitations.

IP Phone Information

- IP Phone Information is a search tool to help organize a large database of terminals into more manageable groupings. Terminals can be grouped in categories by **Type**, **Hardware Version**, or **Firmware Version**.

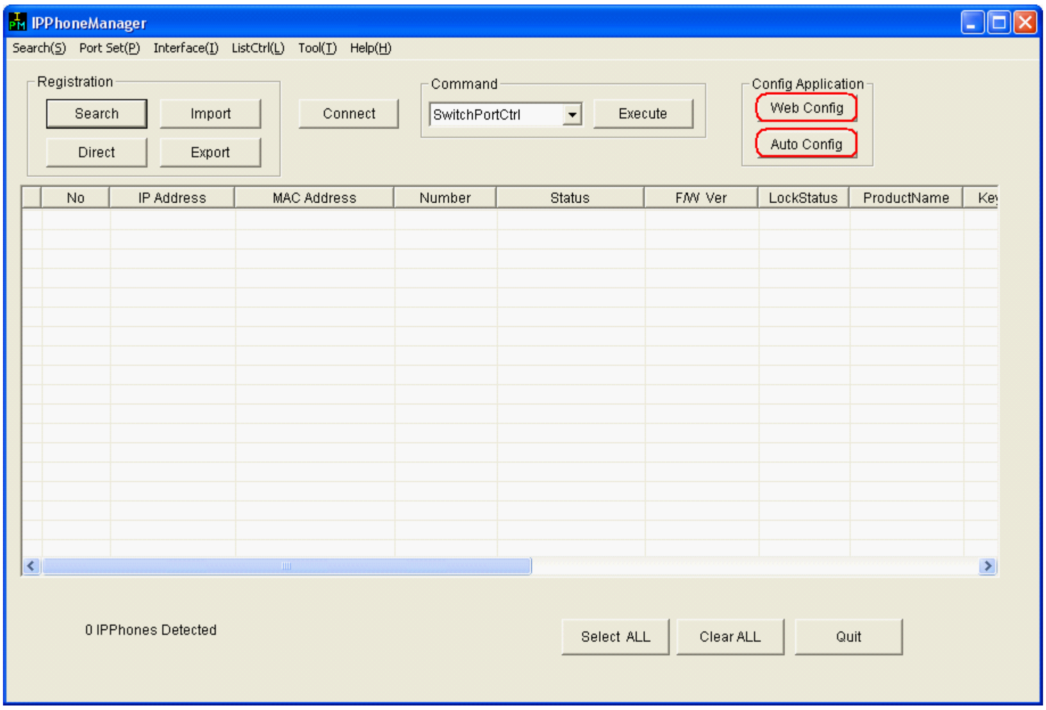
6. Backup & Restore
   Backup and Restore functionality allows terminal data to be sent to or received from a network server.
   - Data Backup is used to copy the current terminal data and configuration to an FTP/TFTP server for archiving. File names for the restored data can be saved as the terminal **MAC address**, **IP Address** or **Extension** number for easy user management.
   - Data Restore is used to copy a preexisting archived file to a terminal to restore its previous settings.

   Simultaneous Download can be selected according to the limitations of the FTP/TFTP server that you have selected to use.

7. Error Log
   Error Log information is a useful tool that can be used by developers for troubleshooting. Terminal log information can backup an FTP/TFTP server and is saved under the terminal MAC Address, IP Address or Extension number of the selected terminal(s).

   Simultaneous Download can be selected according to the limitations of the FTP/ TFTP server that you have selected to use.

Config Application



1. Web Config
   The IP terminal has an HTTP server for web programming. Selecting this button starts a session with Internet Explorer (or the default web browser installed on the local PC) for all the connected and selected terminals. You have one browser session started for every selected terminal – this feature is used on an individual terminal.

2. Auto Config
   The Auto Config button is a direct link to the Auto Configuration Tool. Auto Configuration Tool is used to build a master terminal configuration file for terminal initial setup Plug and Play purposes.

Toolbar Features

1. Search – Sets the frequency and timing that the IP Phone Manager attempts to search and discover IP terminals on the network.
2. Port Set – Port Set allows the customization for Port Numbers that the IP Phone Manager Application and IP Terminals use for communication.
   - Default IP Phone = 3530
   - IP Phone Manager = 20111
3. Interface – Select or change the active PC NIC card that IP Phone Manager needs to use.
4. ListCtrl – List Control is used to select and organize the fields to be viewed in the active IP Phone Manager home layout screen.

Select

5. Help – Displays Version information of IP Phone Manager.
6. Select ALL – Selects ALL discovered terminals.
7. Clear ALL – Unselects all preselected terminals on the home screen.
8. Quit – Terminates all communication between IP Phone Manager and closes the application.

Firmware Upgrade

Below is an example of how to use IP Phone Manager to upgrade the firmware of SIP MLT's

Conditions

1. The terminals must be operational.
2. The IPPhoneManager must be located in the same network segment the terminals are in (only if using the Search function).
3. Running FTP/TFTP Server containing correct firmware files.

Procedure:

1. Start up the IPPhoneManager
2. Press 'Search' in 'Registration' (Import or Direct may also be used)
3. Press 'Select ALL' (or individually select the phones to be upgraded)
4. Press 'Connect'
5. Select 'Download' in 'Command'
6. Press 'Execute'
7. Enter information in 'FTP/TFTP Server'
8. Select 'Boot&Program' in 'Download File Type'
9. Press 'Select All'
10. Press 'Download'.

The handsets will now download and save the firmware then reboot and reconnect to the SV9100.

2.5.1.5 SIP MLT Firmware Upgrade

SIP MLT Firmware Upgrade

From time to time it may be necessary to upgrade the firmware on the SIP MLT handsets, possibly to introduce new features.
There are several ways in which the upgrade can be performed, these are listed below.

- Using IP Phone Manager (TFTP/FTP server required)
- Using the SIP MLT menu (TFTP/FTP server required)
- Automatic upgrade whilst the phone is registering to the SV9100 (SV9100 programming and TFTP/FTP server required)

To show the current firmware version of a SIP MLT on its display use the following steps: -

1. Press and hold the **Help** key for two seconds.
2. Press **2** for System Information.
3. Press **5** for Terminal Information. The Hardware Version is displayed at this point.
4. Press the Down softkey several times until 'Firmware Version' is displayed.
5. To exit the menu press the **Exit** key or press the **Prev** softkey twice then the **Exit** softkey.

For instructions on using the IP Phone Manager please refer to the IP Phone Manager page.

Upgrade using the SIP MLT Menu

Before following the upgrade procedure, the firmware files must be loaded onto a TFTP/FTP server.
There are three firmware files depending on the type of handset being upgraded: -
itlisipe.tgz (for use with ITL-2E/6E handsets)
itlisipv.tgz (for use with ITL-8/12/24/32D handsets)
itlisips.tgz (for use with ITL-320C handsets)
itzisipvc.tgz (for use with ITZ-12CG handsets)
itzisipvg.tgz (for use with ITZ-8LDG,ITZ-12D,ITZ-12DG,ITZ-24D)
Each type of handset will request the correct file name by default.
This procedure must be performed on each handset that requires upgrading.

1. Press **Menu**, then **0** (Config) to enter the terminal program mode.
2. At the Login screen, enter the user name (default = ADMIN) and password (default = 6633222) and press the **OK** Softkey.
3. Press **3** for Maintenance Setting.
4. Press **1** for Download Menu.
5. Press **2** for Download Address and enter the IP address of the TFTP/FTP server
6. Press the **OK** softkey.
7. Press **3** for Protocol and choose either TFTP or FTP depending on what type of server you have available.
8. Press the **OK** softkey.
9. If using an FTP server press **4** for FTP Settings then enter the FTP User ID/Password/Folder and press the **OK** softkey after each entry.
10. Press the **Exit** softkey to get back to the Download Menu.
11. Press **1** for Download Files.
12. Press **3** for Boot & Program.
13. Leave the default file name as it is.
14. Press the **Exec** softkey.
15. The screen will flash ‘Downloading…’ whilst the file is downloaded from the TFTP/FTP server.
16. When the download is complete the screen will show ‘Saving…’ with a progress indicator.
17. When the save is complete the screen will show ‘Download Complete! Press the **Exit** softkey to Reset.’
18. Press the **Exit** softkey to reset the terminal.
19. The upgrade procedure is complete.

Automatic Firmware Upgrade

The following procedure should only be performed using Handset Programming or Web Pro
It is possible for the handset to check whether its firmware requires upgrading when it registers to the SV9100.
It does this by checking its firmware against the version set in system programming.
A TFTP/FTP server is required for this operation, see the information about TFTP/FTP server and firmware file names in the above method.

1. PRG84-07-01. Set to 0 to use TFTP or 1 to use FTP. If using FTP you must set the FTP Login Name in PRG84-07-03 and the FTP Password in PRG84-07-04.
2. PRG84-07-02. Enter the TFTP/FTP server IP address.
3. PRG84-28-02. Enter the firmware filename for each terminal type (see above). If using FTP you must enter the FTP directory in PRG84-28-01.
4. PRG90-42-01. Enter the firmware version that the handset should compare with. This is the version that the handsets will be upgraded to (e.g. 03.00.00.00).
5. PRG90-42-02. Enter the hardware version of each type of handset (see below for hardware

version information)
6. Reboot the SIP MLT to start the upgrade process.

SIP MLT Hardware Versions:
ITL-2E/6E – 09.01.03.00
ITL-8/12/24/32D – 09.01.03.03
ITL-320C – 09.01.03.04

WARNING: If the firmware version set in PRG90-42-01 is different to the actual version loaded onto the TFTP/FTP server, the download by the SIP MLT will be repeated in an endless loop.
WARNING: The firmware download feature does not support flow control so it is possible that the TFTP/FTP server may not be able to handle the number of download requests. To minimize this problem do not restart a large number of SIP MLT's at the same time. Also using a high spec PC or server may reduce the problem.

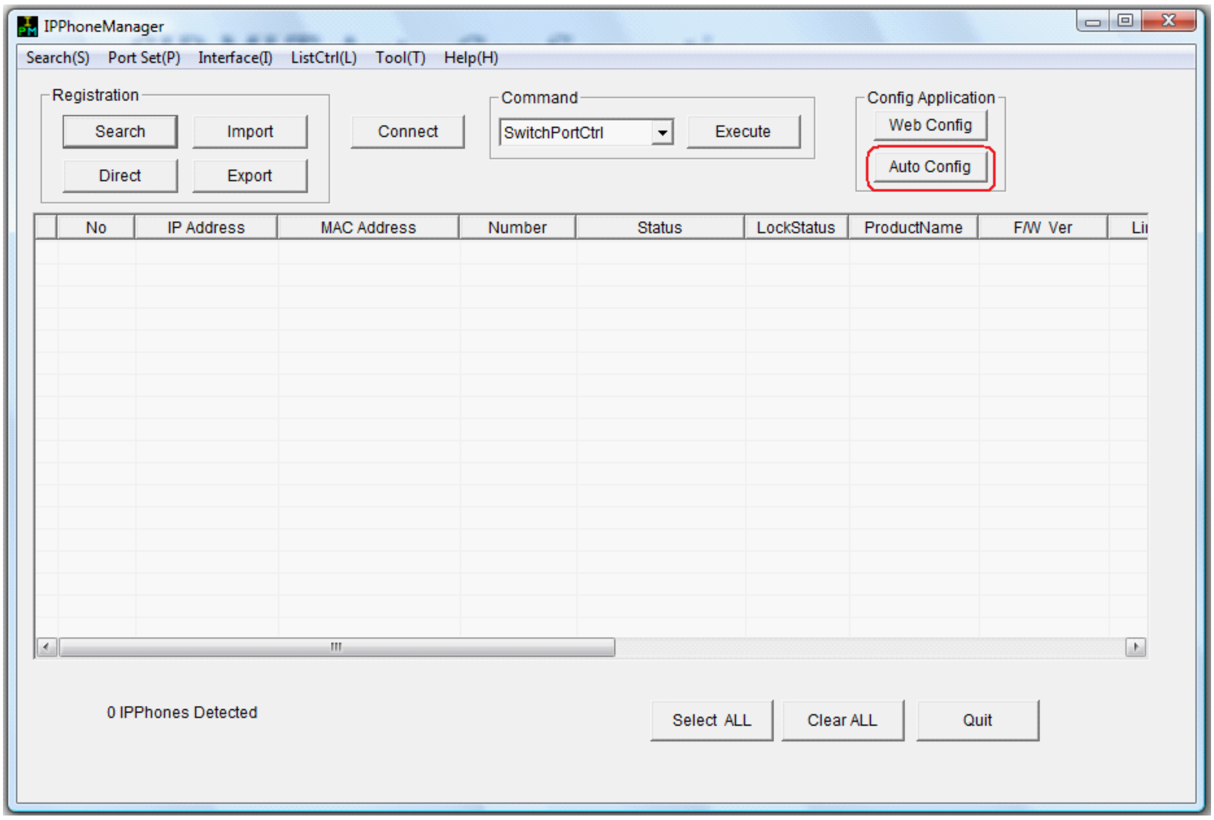
2.5.1.6 SIP MLT Auto Configuration

SIP MLT Auto Configuration

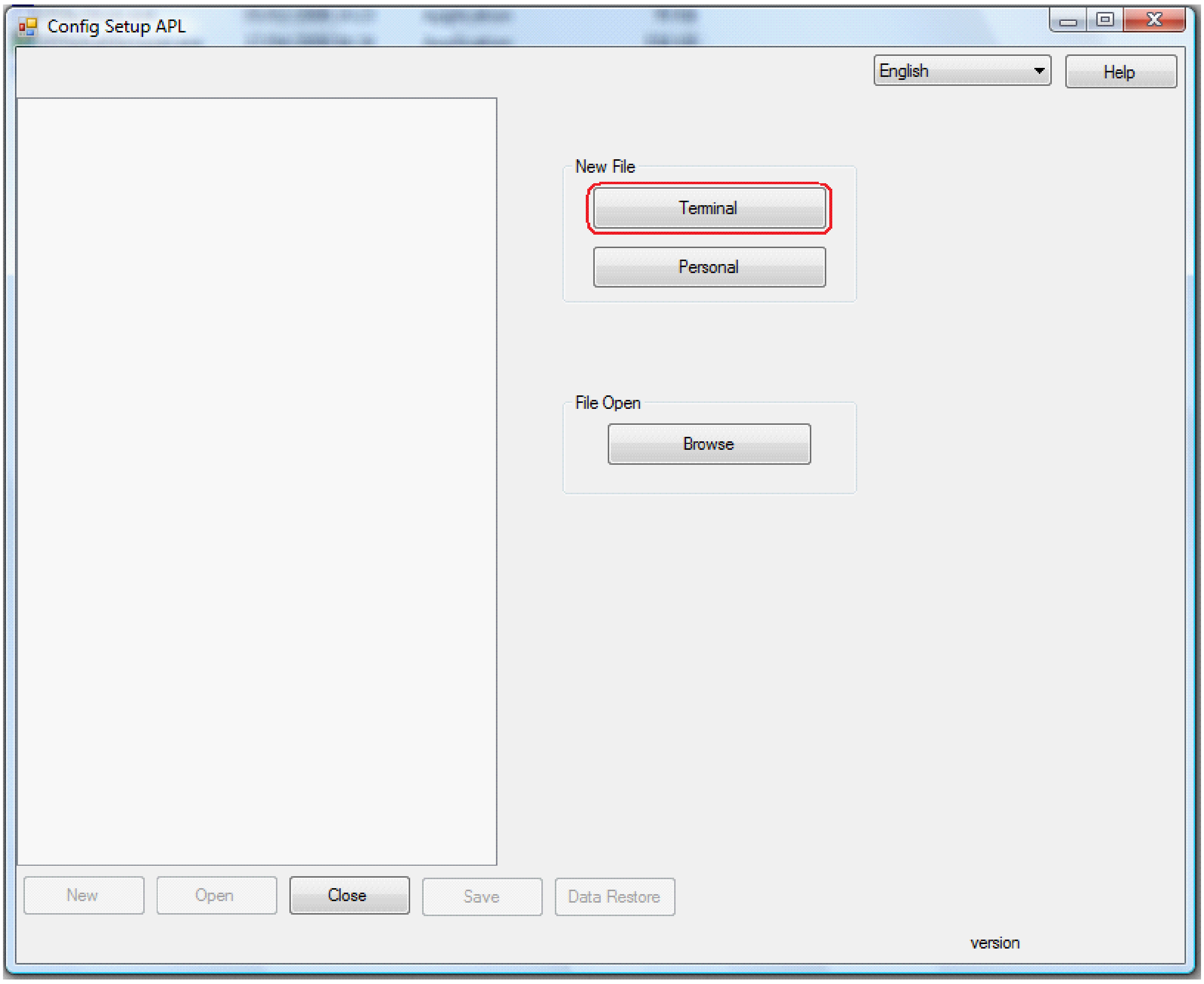
It is possible for a DT800/DT700 IP terminal to download a configuration file from an FTP server when it initializes.
To use this feature the following equipment is required: -

- IP Phone Manager software
- FTP Server
- DHCP Server supporting the following: -
  - Vendor Class
  - Option Codes

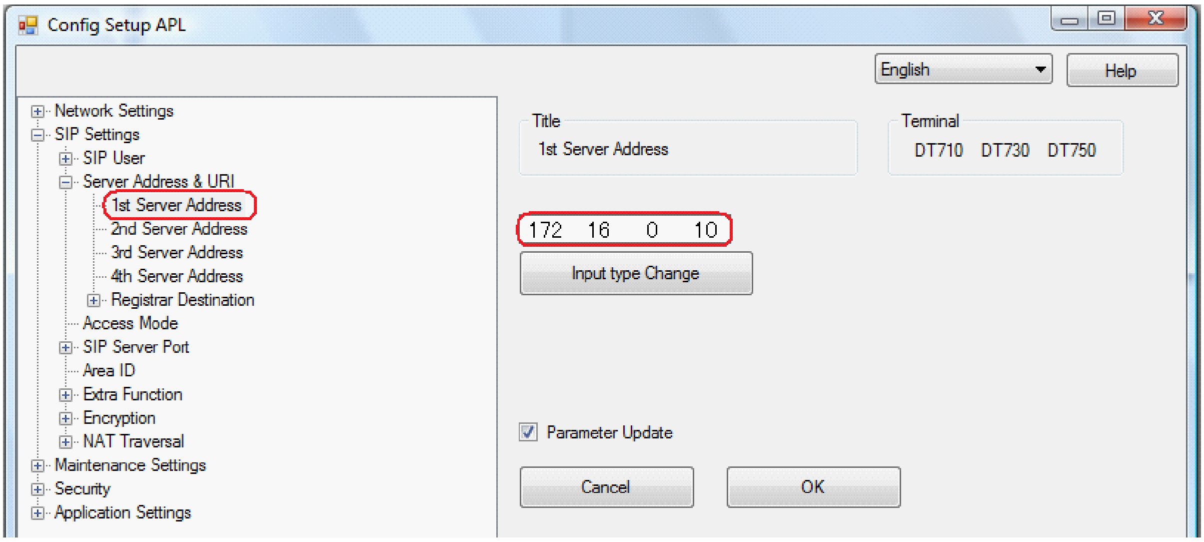
Building the Configuration File
1. Launch the IP Phone Manager software
2. Click **Auto Config**



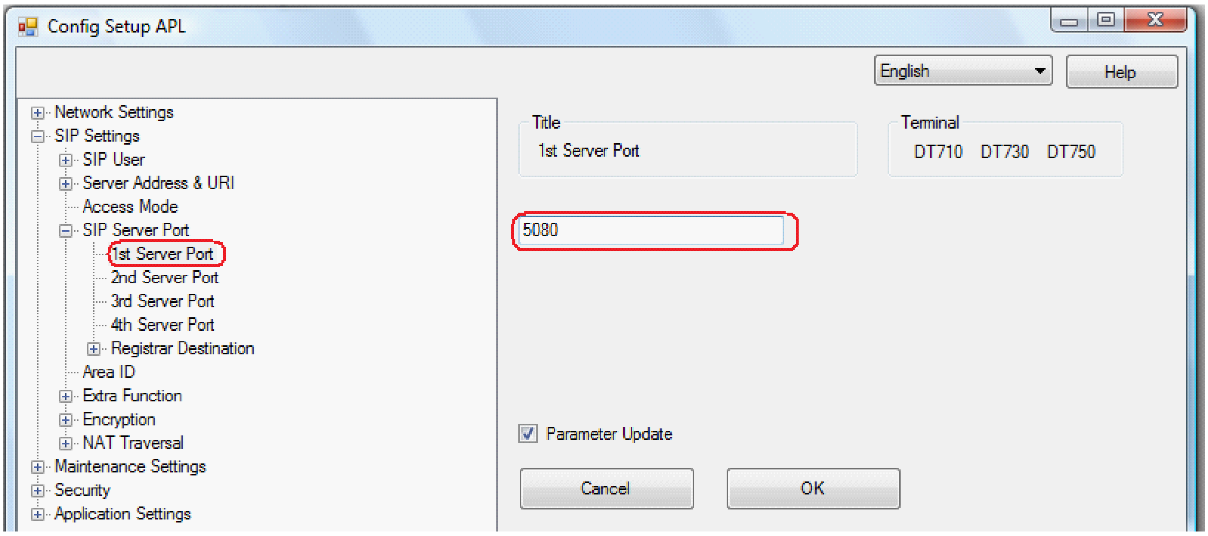
3. Click **Terminal**



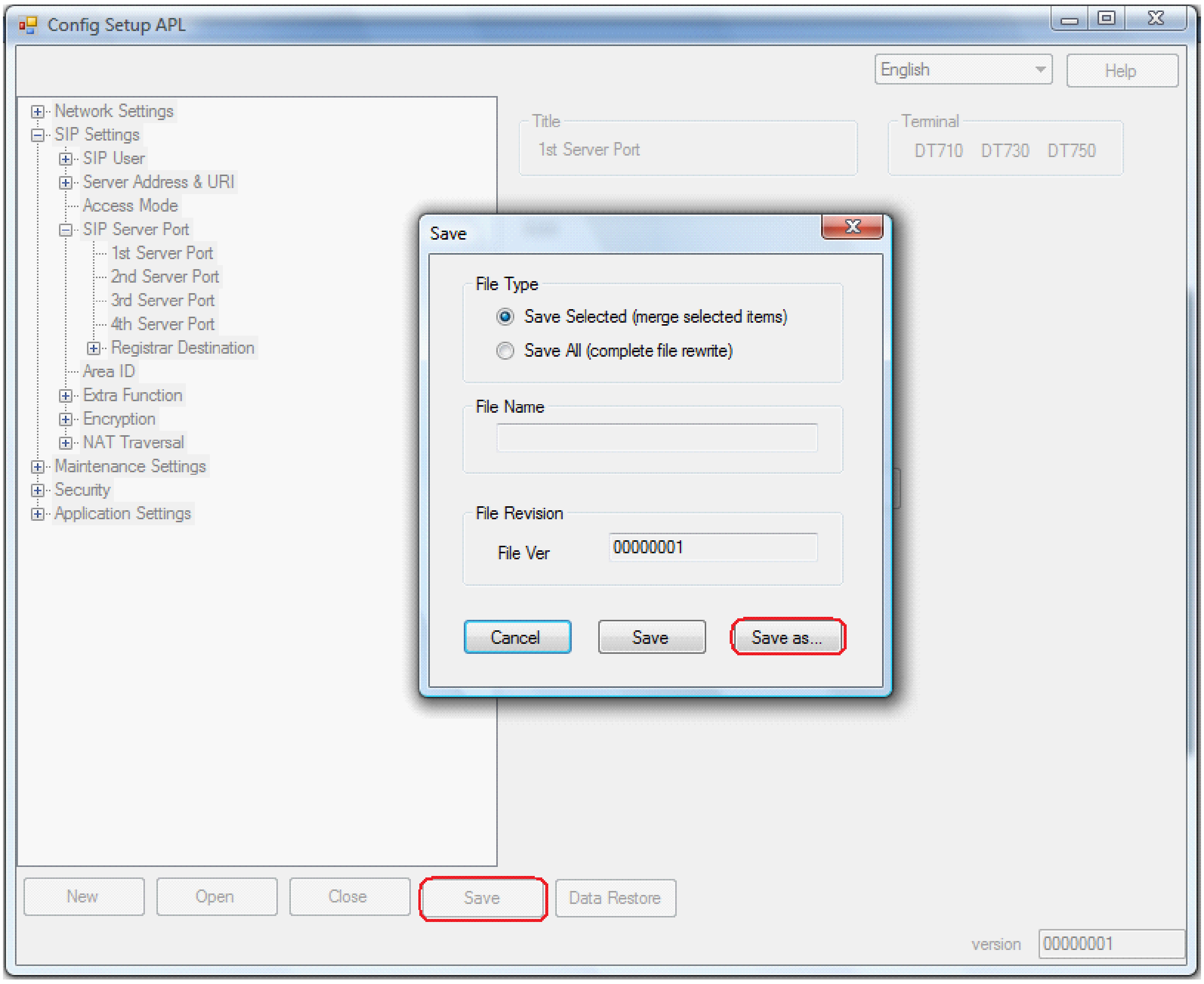
4. Click **1st Server Address**
5. Assign the 1st Server Address using the GPZ-IPLE IP Address, *Easy Edit* – *Advanced Items/VoIP/ General Settings/IP Addressing/CCPU IPL IP Network Setup (PRG10-12-09)*
6. Click **OK**



7. Click **1st Server Port**. Assign port 5080.
8. Click **OK**.

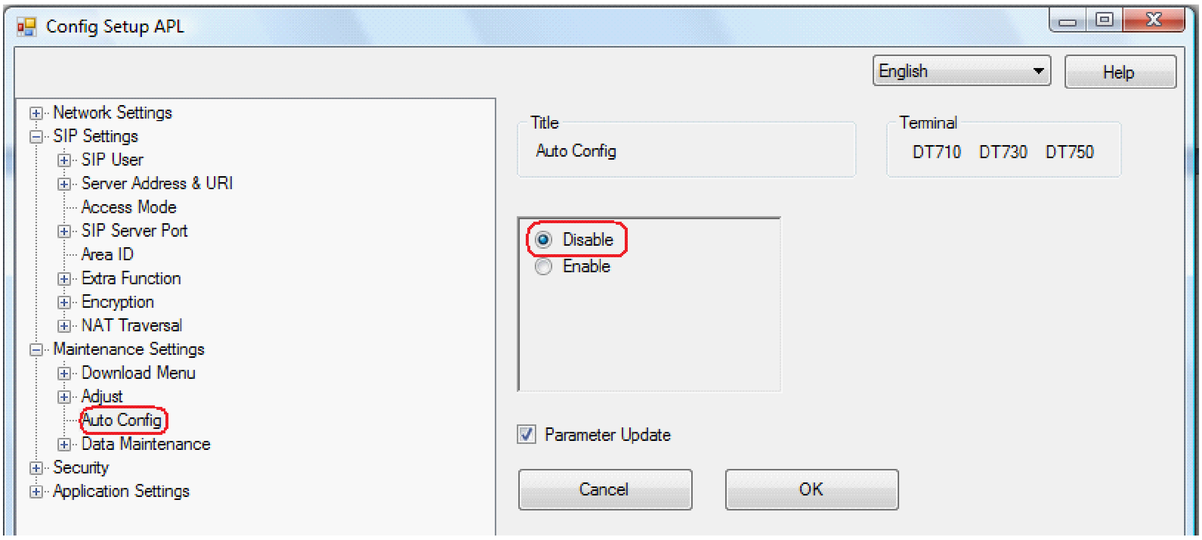


9. After the changes are made click **Save**.
10. When the Save window opens, click **Save as...**



11. In the Save as...window, name the file xxx.gz
    Example: To name the file test, enter **test.gz**
12. Place this file in the FTP Server

Note:
With the above config each handset will try and download the config every time it is reset which may be undesirable. To stop this from happening, set the **Auto Config** option to **Disable** in the Auto Config file.



Configuring an FTP Server

The file generated in the IP Phone Manager must be placed in an anonymous login folder. The FTP server must be configured with an anonymous login account.

The configuration of the FTP server will vary depending of the FTP server software. Refer to the manufactures instructions for further details.

DHCP Server Setup Windows 2003 Server

Defining Vendor Classes

1. In the DHCP server highlight the server machine on the left side. Right click on the server and select **Define Vendor Classes**.
2. Click **ADD**.
3. Display Name = NECDT700
4. Description = auto config
5. In the same window down below there is a section that shows ID, Binary, and ASCII. Click under ASCII.
6. Enter **NECDT700**. This should have also added 4E 45 43 44 54 37 30 30 under the binary section.
7. Click **OK** and close.

Setting Predefined Options

1. Highlight the server again. Then right click and select **Set Predefined Options**.
2. Change the option class to **NECDT700**.
3. Click **ADD,** and provide the following information:
   - Name = FTP Address
   - Data Type = IP address
   - Code = 141
4. Click **OK,** and start the process over again.
5. Click **ADD,** and provide the following information:
   - Name = Auto Config File Name
   - Data Type = String
   - Code = 151
6. Click **ADD,** and provide the following information:
   - Name = Auto Config File Name
   - Data Type = String
   - Code = 152

7. Click **ADD,** and provide the following information:
   - Name = Auto Config File Name
   - Data Type = String
   - Code = 153
8. Click on **ADD**, and give the following information:
   - Name = Download Protocol
   - Data Type = Byte
   - Code = 163
   - Click **OK**.

Option 151 is for DT700 Economy/Value/Sophisticated terminals (ITL-2E,ITL-6DE,ITL-8LDE,ITL-12PA,ITL-12D,ITL-24D,ITL-32D,ITL-320C)
Option 152 is for DT700 Gigabit Colour/Grayscale terminals (ITL-12CG,ITL-12DG)
Option 153 is for DT800 Value terminals (ITZ-8LDG,ITZ-12D,ITZ-24D,ITZ-12DG,ITZ-12CG))

Configuring Options

1. Highlight scope options on the left side. Then right click and choose **Configure Options**.
2. Click **Advanced** and change the vendor class to NECDT700.
3. Place a check mark next to 141 FTP Address. Down below assign the IP address of the FTP server. Then click **Apply**.
4. Place a check mark next to 151 auto config file name. Enter the name of the config file created using IP Phone Manager. Then click **Apply**.
5. Place a check mark next to 163 download protocol. Down below change the HEX address to be 0x1.
6. Click on **Apply** and **OK**.

2.5.1.7 SIP MLT Factory Default

SIP MLT Factory Default

SIP MLT handsets can be restored to factory default settings in several ways:

- Handset programming
- Web Programming
- IP Phone Manager

Be aware that a default SIP MLT terminal requires a DHCP server to obtain its network information.

As the ITL-2E terminal does not have a display it is not possible to use handset programming in the same way as the display terminals, there is a specific key press sequence which can be used to default this type of terminal.

Service Code Factory Default ITL-2E (2 Key DT700)

Under normal circumstances the ITL-2E SIP MLT handsets would be programmed using the web browser. If the IP address of the terminal is unknown and cannot be discovered by other means (i.e. system programming, Wireshark etc), the handset may required to be defaulted.
Be aware that a default SIP MLT terminal requires a DHCP server to obtain its network information.
Follow these steps to default the handset: -

Key Press	Function	Line Key 1	Line Key 2	MW Lamp
Hold Conf * *	Enter programming mode	Green	Green	Off

331#	Default terminal	Green	Flashing green	Off
Line key 1	Save settings	Red	Red	Off
	Result = Pass	Red	Red	Green after a delay
	Result = Fail	Red	Red	Red
Line key 1	Reset terminal*			

* If default was successful then the terminal is reset with default values. If default failed then the terminal is reset with existing settings.

Handset Programming Factory Default (ITZ-8, ITZ-12, ITZ-24, ITL-6, ITL-8, ITL-12, ITL-24, ITL-32, ITL-320C)

This must be performed on each handset: -

- Enter handset programming by pressing Menu 0
- Enter the correct User Name and Password
- 3. Maintenance Settings
- 3. Data Clear
- Factory Value
- OK
- Wait.....
- Exit
- Exit
- Save

Web Interface Factory Default (All Terminals)

This must be performed on each handset: -

- Browse to the IP address of the handset.
- Enter the correct User Name and Password
- Maintenance Settings
- Data Clear
- Factory Value
- OK
- OK
- Wait.....
- OK
- Save
- OK

IP Phone Manager Factory Default (All Terminals)

This can be used to control up to 8 handsets at a time.

- Use the Search, Import or Direct function to locate the handsets
- Tick the handsets that you wish to connect to and click ‘Connect’
- Click ‘Execute’
- Click ‘Yes’
- Click ‘OK’
- Click ‘Close’
- In the ‘Command’ box choose ‘DataReset’ and click ‘Execute’

- Click ‘Factory Default’ and click ‘Execute’
- Click ‘Yes’
- The selected terminals will now reboot with default settings.
- Close IP Phone Manager

2.5.2 Standard SIP Extensions

Standard SIP Extensions

Standard SIP (also referred to as 3rd Party SIP) is an industry standard protocol and therefore there are many manufacturers hardware and software based phones. As these phones are not developed by NEC, and are not designed specifically for use on the SV9100, they do not support majority of the features that you would find on an SV9100 Keytelephone. The features available to SIP extensions are detailed in the SIP Extension Compatibility Report for the relevant SIP terminal.

The SV9100 is compliant with the RFC3261 SIP standard.

To run Standard SIP extensions the SV9100 must have:

- GCD-CP10
- GPZ-IPLE
- Standard SIP License(s).

Various types of SIP phones are available, including:

- Standard SIP Softphone (not SP310) – Software application for PC's (usually used on laptop computers)
- Messaging software with integrated SIP capability (e.g. Windows Messenger)
- Hardware based telephone
- Analogue adapter - allows connection of analogue SLT telephone to SIP/H.323 network
- WiFi telephones – Portable WiFi devices with SIP clients (some GSM phones)
- DECT phone – IP DECT uses the SIP protocol to communicate with the SV9100

The SIP extension will register itself to the SV9100 system. The registration creates a map between the SIP phone and an extension port on the SV9100.
This means that any programming related to that extension port (for example, Class of Service) will apply to the SIP extension.

To allow registration of an SIP extension to a particular extension port it is necessary to assign an extension number to the port, this will be the extension number assigned to the SIP extension.

The SIP extension should be configured with a valid IP Address and should be connected to the same data network as the SV9100.
The procedure for configuring the SIP extension varies depending on the manufacturer - this guide does not cover the configuration of third party equipment.

Precaution
Correct programming of any system or application is, obviously, essential at any time, however. some support issues have shown the effects that incorrect programming can cause in the specific areas where an IP address is assigned to multiple devices.
It is essential that careful planning and deployment regarding IP addressing is performed to avoid the many problems caused when there are IP address conflicts.

- Please be aware that IP Duplication Groups should be programmed ***before*** the device(s) register to the switch, ***never*** afterwards.
- Please make sure that ***only*** the required SIP ports belong to IP Duplication Groups
- Especially please do ***not*** change SIP timers unless advised by NEC Technical Support Department.

For example, changing PRG 10-33-01 (Registration Expiry Time) on the SV9100 is currently not necessary or recommended for IP DECT as it is naturally set at the correct default for present purposes. Altering this and some associated commands such as in PRG 84-20 (SIP Extension Basic Set Up) has been shown in some cases to have serious consequences for customers IP DECT.

The defaults are;

- PRG 10-33-01 (Registration Expiry Time) 3600
- PRG 84-20-02/03/05/06 (SIP Extension Basic Set Up) 180

The correct methods of implementation for various systems and applications are covered in our relevant training courses.

SIP Extension Registration

Before attempting to register any SIP extensions to the SV9100 check whether the SIP device requires IP Duplication Allowed Mode set or not.
This is very important because if IP Duplication Allowed Mode is required it ***must*** be programmed ***before*** the SIP device registers to the SV9100.
Please refer to the SIP Extension Features page for more information about IP Duplication Allowed Mode.

Enter the extension number for the SIP extension in *Easy Edit– Advanced Items/VoIP/Extensions/SIP Extensions/SIP Terminal Settings (PRG11-02)* against an unused port with no associated hardware.

Program the SIP device to register to the GPZ-IPLE card on the SV9100. *Easy Edit– Advanced Items/VoIP/ Extensions/SIP Extensions/SIP Terminal Settings (PRG11-02)*

Program the SIP device with its "username" or "SIP ID" as the required extension number in *Easy Edit– Advanced Items/VoIP/Extensions/SIP Extensions/SIP Terminal Settings (PRG11-02)*

The actual terminology used by the third-party device varies depending on the manufacturer.

The SV9100 uses port UDP/5070 for SIP Extension registrations. Most SIP Extensions use port UDP/5060 by default so this needs to be changed on the SIP device.

SIP Extension Authentication

The SV9100 can be set so that a SIP device is required to authenticate itself using a password before the registration is complete. This option is Enabled by default.

Enable Authentication Mode by ticking the box in *Easy Edit– Advanced Items/VoIP/Extensions/SIP Extensions/SIP Device Setup (PRG10-33-02)*

It is also required to enter a password per SIP extension using the Authentication Password option in *Easy Edit– Advanced Items/VoIP/Extensions/SIP Extensions/SIP Terminal Settings (PRG15-05-16)*

A randomly generated password is created per port on the PBX to enhance the security of the system and minimise the risk or rogue SIP devices registering to the system. These passwords can be changed to make easier to configure and the password entered in system programming is then required to be entered in to the SIP device.

Note: If a password is not entered, per extension in the SV9100 system programming the SIP device will be able to register without a password even if Authentication Mode is enabled.
It is recommended to enter a password for every free extension number that, in theory, could have a SIP device registered to it. This gives additional security against unsolicited SIP registrations.
It is also recommended to check the Toll Restriction class assigned to each extension number, whether it has a registered device or not, to make sure is has the correct dialling permissions.

Delete SIP Extension Registration

Before attempting to delete the registration of a SIP extension, the SIP device must be unplugged or powered off.
Enter Program 90-23-01 (handset programming or Web Pro only), and enter the extension number of the SIP device. Press **1** and **Transfer** to delete the registration.

SIP Extension Codec Settings

SIP Extensions can use various CODECs. A CODEC is a standard for converting an analogue signal to digital. This conversion process is handled by the DSP (Digital Signal Processors) on the GPZ-IPLE card. Each CODEC has different voice quality and compression properties. The correct choice of CODEC will be based on the amount of bandwidth available, the amount of calls required and the voice quality required.

Available Codecs for SIP Extensions

- G.711 64Kbps codec MOS 4.4
- G.722 64Kbps codec MOS 4.4
- G.726 32Kbps codec MOS 4.2
- G.729 8Kbps codec MOS 4.0

The bandwidth values quoted for these codecs are for the digitized speech in one direction only. The actual bandwidth required for a call will depend on many other factors and will be much higher than these figures.

The above MOS values are quoted for ideal network conditions. The value could be lower depending upon the network performance.

The codec is programmed against a Type (profile). Only one Type (profile) can be set up. The extension is then assigned to 'Type 1'.

1) Program the codec for each Type using the 'Audio Capability Priority' option in *Easy Edit– Advanced Items/VoIP/Extensions/SIP Extensions/SIP Codec Settings(PRG84-19-28)*
2) Assign the Type number as '1' to the extension using the 'Codec Type' option in *Easy Edit– Advanced Items/Extensions/SIP Extensions/SIP Terminal Settings (PRG15-05-15)*

Please be aware that this codec selection is only a *preferred* setting. It is possible that a SIP extension will use one of the other available codecs depending on the destination of the conversation and also who was the originating party of the call.

License

The SV9100 requires licensing to allow the registration of Standard SIP handsets. One license is required for each registration to the SV9100. If no license is available, the SIP extension will fail to register. Other licenses may be required for certain Standard SIP features.
Up to 896 Standard SIP licenses can be added.
License Code: BE114054

2.5.2.1 SIP Extension Features

SIP Extension Features

The following is a list of features supported by the system when using SIP extension, any feature not listed here should be assumed to be not supported.

Outgoing

- Enblock sending
- Service Code (see 'Service Code List' below)
- Account Code
- Abbreviated Dial

Service code list

- Night Mode Switching (own group)
- Record/Erase VRS Message
- General Message Playback (VRS)
- Record and Erase General Message (VRS)
- Call Forward – Immediate/Busy/No Answer/Busy-No Answer/Dual Ring
- Dial Block
- Temporary Toll Restriction Override
- Walking Toll Restriction
- VRS/Off Premise Call Forward
- Transfer Dial setting for out of range
- DND/FWD Override (Bypass call)
- Conference
- Call Waiting (not receive)
- Barge In
- Last Number Redial
- Saved Number Dialling
- Clear LND
- Clear SND
- Specified Trunk Answer
- Call Park
- Group Hold
- Station Park Hold
- Common Cancelling Code
- Personal Speed Dial
- Call Own Mailbox (Inskin Voice Mail)
- Live Recording (Inskin Voice Mail)
- Tandem Trunking (Unsupervised Conference)

Incoming

- Extension
- Normal Trunk
- VRS/DISA
- DID

- DIL
- Leased Line (Tie Line)
- Door Phone (operation explained below)

Hold/Transfer

- Normal Hold
- Park Hold
- Group Hold
- Station Park Hold

Type of transfer service

- Call Forward – Immediate
- Call Forward – Both Ring
- Call Forward – No Answer
- Call Forward – Busy
- Call Forward – Busy/No Answer
- Follow Me
- Fixed Call Forward
- Fixed Call Forward Off Premise
- Call Forward to Device
- Automated Attendant

Transfer operation

- ISDN Normal Transfer
- ISDN Blind Transfer
- SLT Normal Transfer
- SLT Blind Transfer
- DSPDB VM Normal Transfer
- DSPDB VM Blind Transfer

CLI/Name Display

- CLIP Display
- Extension Name Display*[1]
- Nickname Display*[1]
- Extension Number Display*[1]
- SIP “Display Field” Display*[1]
- Abb Dial Name Display
- Door Phone Name Display
- Voicemail Name Display*[2]
- CLI Update after transfer (IP DECT)

*[1] One of these options can be displayed depending on system programming and the received SIP information.

*[2] Dependant on the type of Voicemail system in use.

Others

- Can belong to an Incoming Ring Group
- Can belong to Department Group, however all ring mode is not supported
- Peer to Peer Mode (allows RTP to be sent directly between SIP endpoints)
- Voice Mail Message Waiting
- Assign as Virtual Extension
- Conference Barge In/Monitor

- T.38 Fax Relay
- Video Support*3

*3 Please refer to the SIP Video section below.

Conditions
The above list of features are supported by the system for SIP extensions, however, this does not mean the device will work for all of these features.
The SIP extension certificate confirms which features are supported in Peer to Peer mode and non Peer to Peer mode for the specific device.

Operation
The operation for each feature is as described in each specific feature section.

Doorphone

To allow the SIP extension to operate the door lock PRG90-03-01 needs to be enabled. This command can only be accessed via handset programming.
A SIP extension can belong to a Doorphone ring group but the operation differs slightly from that of an SLT telephone. The operation has been tested using an NEC IP DECT handset:

- Doorphone call button is pressed
- IP DECT handset rings
- IP DECT user answers the Doorphone
- IP DECT user and the Doorphone user speak
- IP DECT user presses ‘R’ (green button) to operate the lock
- IP DECT user presses ‘R’ again to speak to the Doorphone user
- IP DECT user hangs up.
-

Note: If the IP DECT user does not press the ‘R’ button for the second time before hanging up the call, the Doorphone may recall back to the IP DECT user.

Peer to Peer

By default if two IP extensions are on an internal call together, the RTP will be sent directly between the two endpoints. This reduces the DSP consumption, reduces delay on the VoIP packets and increases voice quality on the call.

There may be instances where this operation is not supported. May be the SIP terminal does not support this operation or the customers network may not allow it. If this is the case it is possible to disable Peer to Peer for SIP extensions. Use the **Peer to Peer** option in *Easy Edit – Advanced Items/VoIP/Extensions/SIP Extensions/SIP Terminal Settings (PRG15-05-50)*

DTMF Relay (RFC2833)

By default any DTMF tones transmitted from a SIP extension will be sent as audio tones in the speech path. It is possible that these tones can be misinterpreted by the receiving device because of packet loss or errors on the IP network.
DTMF relay is a way of converting the DTMF tone into a signal then sending the signal across the IP network instead of the actual tone. To use this feature both devices (SV9100 and the SIP device) must support DTMF relay (RFC2833).
To enable this feature set the ‘DTMF Relay Mode’ option to ‘RFC2833’ in *Easy Edit – Advanced Items/VoIP/Extensions/SIP Extensions/SIP Terminal DTMF Settings (PRG84-34)*

T.38 Fax Relay

Standard SIP extensions now have the ability to communicate using the T.38 Fax Relay protocol.
By default any Fax tones transmitted to or from a Standard SIP extension will be sent as audio tones in the speech path. It is possible that these tones can be misinterpreted by the receiving device because of packet loss or errors due to the codec compression.
T.38 Fax Relay is a way of converting the Fax tones into a signal then sending the signal across the IP network where the signals are converted back to Fax tones.
The Standard SIP device must be compatible with T.38 for this to work.
Enable Fax Relay by using the 'Fax Relay Mode' option in *Easy Edit– Advanced Items/VoIP/SIP Terminal Options/SIP FoIP Settings (PRG84-33).*
The SIP extension must also be set as a 'Special' using the Terminal Type option in *Easy Edit– Advanced Items/VoIP/SIP Terminal Options/SIP Terminal Settings (PRG15-03-03).*
There are several other options to do with T.38 Fax relay that can also be found in *Easy Edit– Advanced Items/VoIP/SIP Terminal Options/SIP FoIP Settings (PRG84-33)*, these commands would usually be left at the default settings but may occasionally need altering depending on the SIP device, fax machine and network connection.

IP Duplication Allowed Mode

Easy Edit – Advanced Items/VoIP/SIP Terminal Options/SIP Terminal Settings (PRG15-05-18).

By default the SV9100 allows one SIP registration per IP address.

In certain circumstances multiple extension numbers may be required to be registered via the same IP address, e.g. Cisco ATA has two extension connections but only one IP address. With this scenario the second registration from the same IP address would overwrite the first registration. To overcome this limitation it is necessary to enable the SIP extensions for IP Duplication Allowed Mode. This allows multiple registrations from a single IP address and also allows the SIP registration to be overwritten by another IP address.

This command should be done ***before*** the SIP extensions are registered to the SV9100.

Automatic IP Duplication Allowed Group Assignment

This feature automatically assigns the IP Duplication Allowed Group when registering either IP DECT, UCB or BCT SIP extensions.
This means that the IP Duplication Allowed Group setting does not need to be programmed prior to registering the extensions to the SV9100.
The SV9100 detects that the registration request is from one of the above devices and assigns the SIP extensions to use **IP Duplication Allowed Mode** accordingly.

If the IP Duplication Group has been set manually prior to the registration request then the feature will not be activated for that SIP extension, it will keep its manual group assignment.
Be aware that this feature will only work for IP DECT, UCB and BCT. Other devices that require IP Duplication Allowed Mode will need assigning manually.

Peer to Peer SIP Video

It is possible to communicate directly between Standard SIP extensions using Video.
This is only possible if SIP Peer to Peer is enabled and SIP CTI is disabled, if any of these conditions are not met video communication will fail.
Check the SIP Peer to Peer and SIP CTI settings in *Easy Edit– Advanced Items/VoIP/Extensions/SIP*

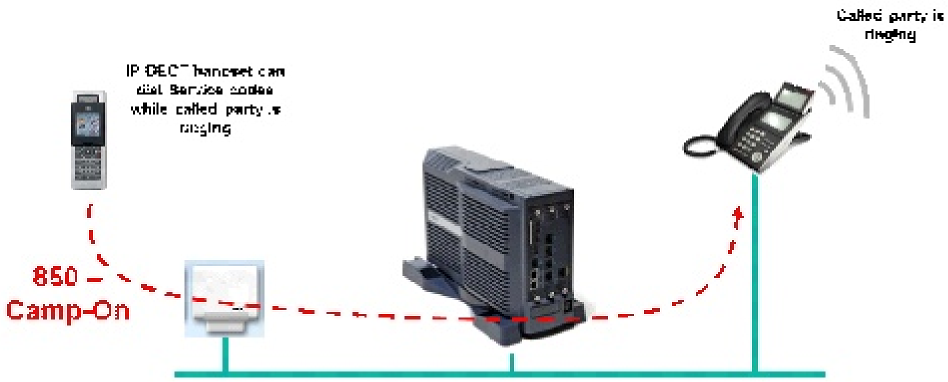
Extensions/SIP Terminal Settings
To enable SIP Video on a per extension basis, use the 'Video Mode' option in *Easy Edit– Advanced Items/ VoIP/Extensions/SIP Extensions/SIP Terminal Settings*

Conditions/Comments

- The video stream cannot pass through the GPZ-IPLE card, SIP Peer to Peer must be enabled.
- SIP CTI must be disabled.
- Video communication between a Standard SIP terminal and the UC Client Softphone is not possible.
- The SIP terminal must pass interoperability testing by NEC before it can be supported.
- The video codec is not supported by the GPZ-IPLE card. The video codec information from the received SDP message will be forwarded to the destination terminal.
- The communicating video terminals must support common audio and video codecs.
- SIP Video is not supported across AspireNet or K-CCIS as the communication between the SIP terminals is not Peer to Peer.
- Be aware of bandwidth requirements of video communication, this will be considerably higher than a voice call. Bandwidth is dependent on codec selection, frame rate and resolution. Check the manufacturer's data sheet for the relevant terminal for further details.

SIP INFO DTMF Support

This feature enables the SV9100 receive DTMF information in SIP INFO messages sent by standard SIP terminals so that the PBX can get the dial information before a RTP session between the GPZ-IPLE and the terminal is established. This allows the standard SIP terminals to initiate features during the ringing state such as CAMP ON and Message Waiting.



SIP INFO messages can be sent Out-of-band which allows SIP terminals to send the DTMF information without an active RTP session.
SIP INFO is described under RFC2976. There are two INFO formats which the main software will understand as DTMF information. Format 1 is the most widely used option and Format 2 is less-common but will be accepted to ensure maximum possible interoperability.

Format 1 is DTMF relay method and the body of the SIP message consists of signaling information and uses the content-type 'application/dtmf-relay'.

Format 1: Digit 5 with a duration of 160 msec

```
INFO sip:7007471000@example.com SIP/2.0
Via: SIP/2.0/UDP alice.uk.example.com:5060
From: <sip:7007471234@alice.uk.example.com>;tag=d3f423d
To: <sip:7007471000@example.com>;tag=8942
Call-ID: 312352@myphone
CSeq: 5 INFO
Content-Length: 24
Content-Type: application/dtmf-relay
Signal=5
Duration=160
```

Format 2 is DTMF trigger mechanism which uses the ‘application/dtmf’ mime-type. The body of the message consists only of the DTMF digit.

Format2: Digit 5

```
INFO sip:7007471000@example.com SIP/2.0
Via: SIP/2.0/UDP alice.uk.example.com:5060
From: <sip:7007471234@alice.uk.example.com>;tag=d3f423d
To: <sip:7007471000@example.com>;tag=8942
Call-ID: 312352@myphone
CSeq: 5 INFO
Content-Length: 1
Content-Type: application/dtmf
5
```

Easy Edit – Advanced Items/VoIP/Extensions/SIP Extensions/SIP Terminal Settings

Programming Command	Values	Command Description
15-05-49 Receiving SIP INFO	0=disabled 1= SIP INFO (DTMF) messages are accepted during call setup and conversation. 2= SIP INFO (DTMF) messages are accepted only during the call setup, they are ignored during conversation. (Default=0)	Enables and Disables SIP INFO (DTMF) support for standard SIP devices.

Call Waiting

SIP Call Waiting is designed for use with NEC IP DECT, the operation of this feature cannot be guaranteed with other Standard SIP Terminals. It allows a busy IP DECT user to receive a second call indication by a beep in the ear and some display information.
The IP DECT user has several options when they receive a second call indication:

- Ignore the second call and continue with the first.
- Hold the first call and answer the second (toggle between the callers is also possible).
- Hang up the first call and answer the second.

IP DECT Firmware

SIP Call Waiting is supported on any release of IP DECT handset firmware and any DAP firmware.

Conditions/Comments

- Call Waiting is not supported on the C124 IP DECT handset.
- M155 handset cannot hold the first call and answer the second or toggle between the calls.
- It is not possible to transfer a call to an IP DECT handset if it arrives at the IP DECT as the second

call.

- A Doorphone call cannot be answered as a second call. To answer the Doorphone the first call must be cleared then wait for the Doorphone call to ring the IP DECT handset and answer as normal.
- If there are no DSP's available when a user sends a second call to an IP DECT user Call Waiting is not possible and the caller will hear busy tone.
- When an IP DECT user is talking to the second call with the first call on hold, if the second call is cleared the first call will then recall to the IP DECT user as a new call.
- It is not possible to send Call Waiting indication to an IP DECT handset if the first call is either a Doorphone or Voicemail.

Programming

The Call Waiting feature needs to be allowed by Class of Service programming on a called extension basis.
To enable SIP Call Waiting on a per CoS basis, use the 'Call Waiting for standard SIP Terminal' option in *Easy Edit– Advanced Items/IP DECT/IP DECT Features/IP DECT COS Features.* (PRG20-13-54)
Apply the relevant CoS to each extension in *Easy Edit– Advanced Items/IP DECT/IP DECT Features/COS Per Mode.* (PRG20-06)
The calling extension also needs to be able to send a Call Waiting event to the IP DECT extensions. This is done by allowing 'Intercom Off-hook Signalling' or 'Automatic Off-hook Signalling' by Class of Service in *Easy Edit – COS.* (PRG20-13-05/06)
The CoS is applied to the extension in *Easy Edit- Extensions/Extension/Extension Properties/Class of Service Per Night Mode.* (PRG20-06)
If Automatic Off-hook Signalling is used then the calling party will not hear busy tone, Call Waiting is automatically sent.
If Intercom Off-hook Signalling is used then the calling party will hear busy tone and they will have to use the Override function (SC809 or Function Key 33) to send Call Waiting.
To allow Call Waiting from a trunk 'Call Queuing' or 'Second Call for DDI/DISA/DIL/E&M' may be required in *Easy Edit – COS.* (PRG20-09-01/07)

Programming of the IP DECT system is also required.
In the DAP Configurator go to the 'SIP Settings' tab and change the 'multiple_call_appearance' option to '=yes'.
It is also possible to alter what appears on the display of the IP DECT handset during a Call Waiting event. Chose the 'call_waiting_indication' option to the required text. Beware that if this text is too long the extension name that is waiting may not fit on the display at the same time. It is recommended to leave this setting at its default value of 'waiting'.

Operation

When a Call Waiting event is sent to an IP DECT handset the IP DECT user will hear a tone in the earpiece and some text on the display including the calling party information.

To hang up the first call and answer the Call Waiting:

1. Press the red 'Hang Up' key – this clears the first call
2. Wait for the second call to ring the handset
3. Answer the ringing second call by pressing the green 'Answer' button
4. Talk to the calling party

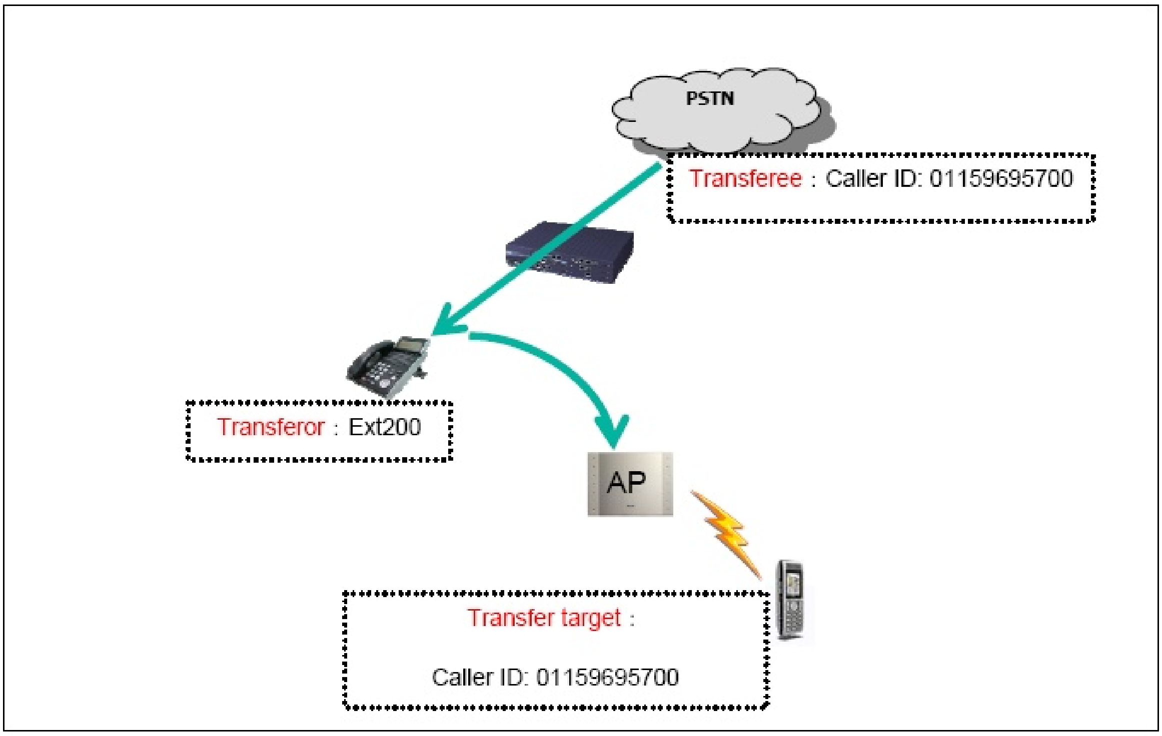
To hold the first call and answer the Call Waiting:

1. Press the * key – this holds the first and answers the second
2. Talk to the calling party
3. The first call will then indicate as a Call Waiting
4. Toggle between the callers by pressing the * key

If the IP DECT user doesn't answer the Call Waiting the tone will stop and the display will return to show the information of the first call.

Caller ID Update after Transfer

Caller ID Update after Transfer is designed for use with NEC IP DECT, the operation of this feature cannot be guaranteed with other Standard SIP Terminals.
It allows the CLI displayed on an IP DECT handset to be updated to show the transferred party's name or CLI after the call has been transferred.
Prior to this feature the IP DECT display would show the information from the transferor rather than the transferee.



IP DECT Firmware
Caller ID Update after Transfer is supported from DAP firmware V4910b510.dwl onwards and on any handset firmware.

Conditions/Comments

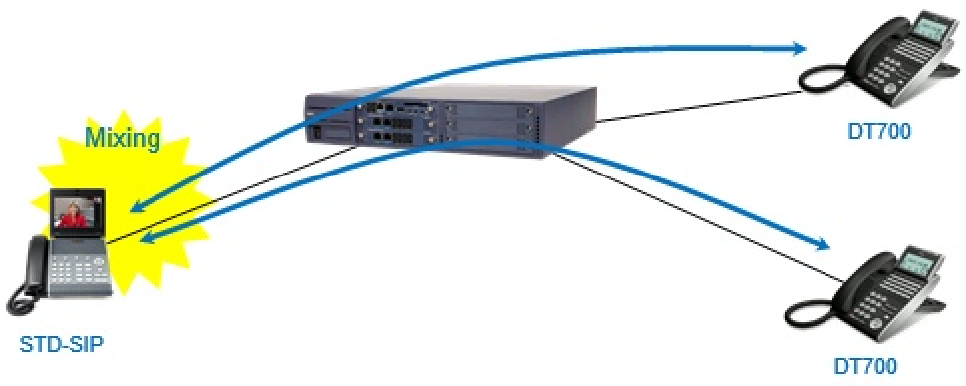
- Extension name or CLI to name conversion is not supported for this feature, only the extension number or CLI.
- If no CLI is available on the trunk call "Anonymous" is displayed on the IP DECT handset.

Programming
There is no programming required on the SV9100 or on the IP DECT system to activate this feature.

Conference Call by Standard SIP Phone

The SV9100 supports voice conference features of standard SIP extensions and does not use the conference resources on the system.
The target terminal of this feature is the POLYCOM VVX1500D. If a standard SIP terminal has the same conference sequence as the VVX1500D , then this may be able to be supported also using this feature.

The conference size supported is three party conference.



SV9100 Requirements

The following information provides the feature requirements.

Main Software

SV9100 R1.0 software or higher

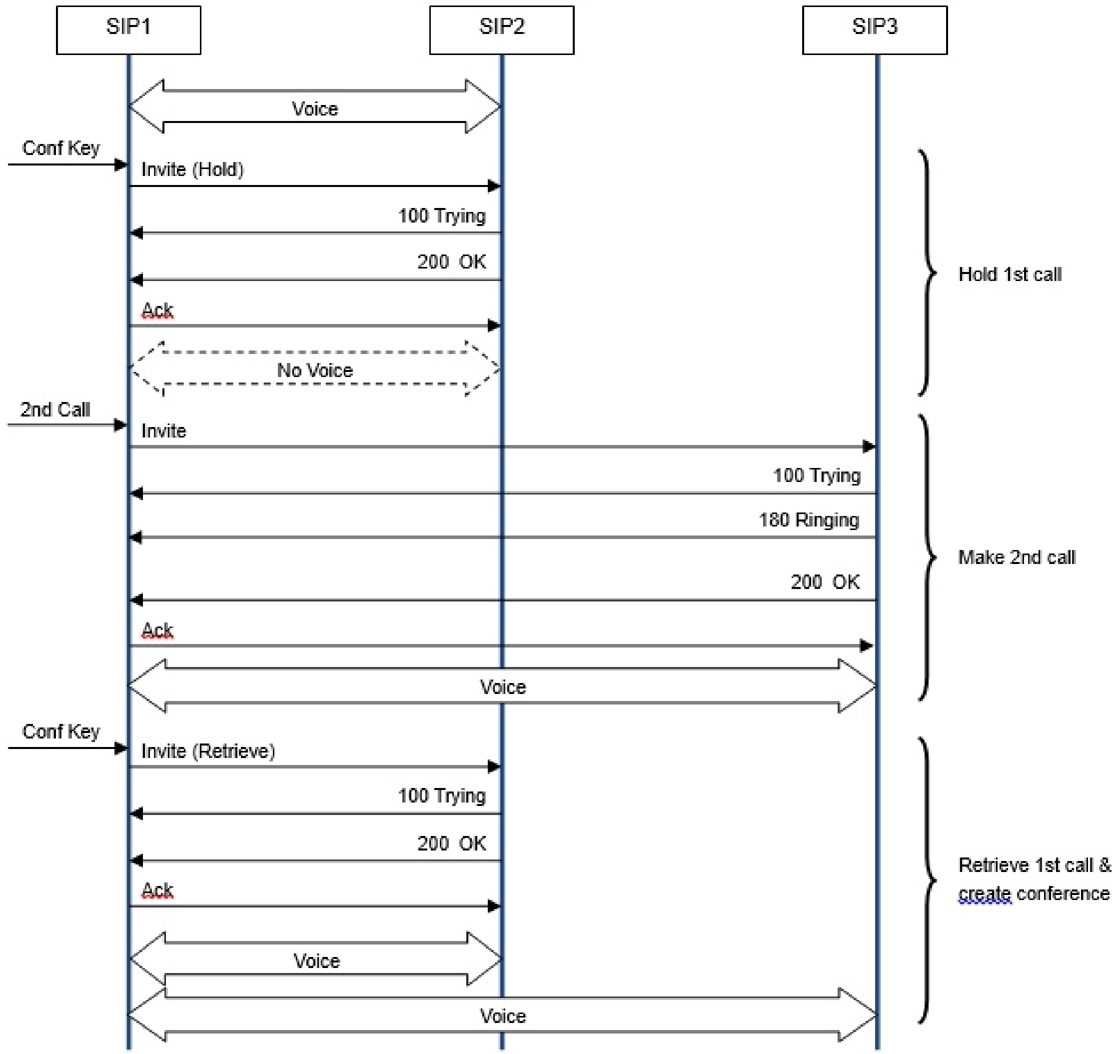
License

The system must be licensed for standard SIP terminals with a BE114054 (License 5111).

Service Condition

This feature does not use the conference resources on the system, the standard SIP extension operates the conference by combining two voices and sends it to the other conference member.

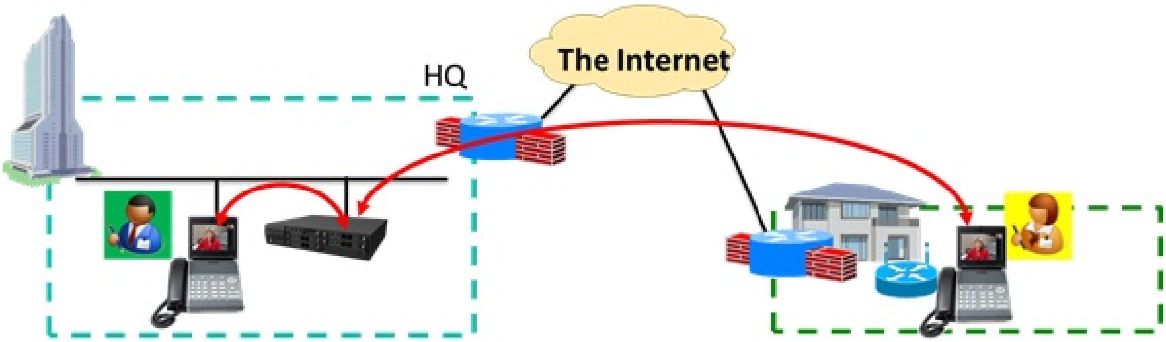
The sequence supported is below.



In this sequence, at first, SIP1 is talking with SIP2.
If SIP1 pushes the conference key during conversation, the call is held.
After that, SIP1 makes a call to another terminal (SIP3) that SIP1 wants to join the conference.
After SIP3 answers the call, SIP1 pushes the conference key again, and then the call between SIP1 and SIP2 is retrieved.
At this time, SIP1 combines together the SIP2 voice and SIP3 voice.
And SIP1 then sends the voice of SIP1 and SIP2 to SIP3, and the voice of SIP1 and SIP3 to SIP2.

NAT Mode for SIP Extensions

Previously standard SIP extensions could be registered as a device when located in the Intranet network to make outbound or receive inbound calls. This feature provides support for standard SIP extension registration when the phone is over the Internet at a remote location. In the case of a standard SIP extension with video, a video conversation can be made.



TCP Connection for SIP Extensions (Release 3)

When a SIP terminal application, such as a smartphone SIP client is used remotely through a Firewall, we need to have a keep-alive to check it's availability.

If a SIP terminal uses the UDP protocol, then the SIP terminal sends keep-alive. But if TCP protocol is used, then the system sends keep-alive, and the client application remains idle. This can increase the performance of the spartphone battery so it can be used for longer.

Whether TCP or UDP is used is determined by the SIP terminal when it sends a REGISTER request to the SV9100.

Easy Edit – Advanced Items/VoIP/Extensions/SIP Extensions/SIP Terminal Settings
Transport Protocol - This displays the transport protocol. used by the SIP terminal. *(PRG15-05-51)*

2.5.3 IP DECT

IP DECT

IP DECT is an NEC product that combines the functionality of traditional DECT with the flexibility of the Standard SIP protocol giving a robust and reliable wireless solution.
The handsets use the traditional DECT protocol to communicate with the DECT Access Points (DAPs) and the DAPs use the Standard SIP Protocol to communicate with the SV9100.

To run IP DECT extensions the SV9100 must have:

- GCD-CP10
- GPZ-IPLE
- IP DECT License(s).

General Information

- IP DECT handsets are seen as Standard SIP extensions by the SV9100 so the registration process is the same. See the **Standard SIP Extension** page for more details.
- The SV9100 can support up to 896 IP DECT handsets (license dependant).
- One DAP can support upto 25 IP DECT registrations so multiple DAPs may be required even if the coverage area does not warrant it.
- One DAP will support upto 12 simultaneous calls.

- The AP200s DAPs can be powered by PoE 802.3af or by local mains power supply.
- The AP300, AP300c, AP300e, AP400, AP400c, AP400e, AP400s can be only only be powered by 802.3af.
- IP DECT handsets can only use the G.711 codec.
- The supported IP DECT terminals are C124, G355, G955, i755, M155 G266, G566, G966, ML440.

IP DECT Configuration

All IP DECT configuration information is given on the IP DECT training course. No support can be provided if this course has not been followed by the installer.
The IP DECT manuals can be found on the SV9100 Tech USB stick.

License

The SV9100 requires licensing to allow the registration of IP DECT handsets. One license is required for each registration to the SV9100. If no license is available, the handset will fail to register.
Up to 896 IP DECT licenses can be added.
License Code: EU901001

2.6 Networking

Networking Overview

The following networking protocols are supported by the SV9100: -

- **NetLink** – Proprietary connection of several systems to make one large distributed system. Very feature rich. SV9100 only.
- **AspireNet** – Proprietary connection of several systems to make one large virtual system with a unified numbering plan. Feature rich. SV9100, SV8100 and Aspire can be connected.
- **System Feature Networking** – This is another name for AspireNet (see above) and will be referred to as AspireNet in this manual.
- **K-CCIS** – Proprietary connection of several systems to make one large virtual system with a unified numbering plan. Feature rich. SV9100, SV8100 only.
- **SIP Networking** – Standards based (RFC 3261) connection of any system that supports the SIP protocol (compatibility testing may be required)
- **H.323 Networking** – Standards based (ITU-T) connection of any system that supports the H.323 (version 3) protocol (compatibility testing may be required)

All the above networking protocols excluding SIP networking are only supported over a dedicated closed WAN IP connection or suitable VPN connection. SIP networking can be configured over a public connection with suitable Port Forwarding configuration.

2.6.1 NetLink

NetLink

NetLink provides a seamless connection, using an IP network, to join multiple SV9100 communication servers into what would appear to be a single communications server. With a unified numbering plan, users can access any extension in the network as if they were in the same location.
NetLink differs from other networking protocols because all slots, trunk ports and station ports belong to, and are controlled by, the Primary system. This makes the numbering plan and trunk routing much simpler.
NetLink allows the connection of up to 16 systems, each must have a unique Node ID. Each system in the network must have:

Only SV9100 systems can be Netlinked together.

- GCD-CP10
- GPZ-IPLE

Although 16 systems can be connected together, the maximum number of station and trunk ports is limited to the maximum for ***one*** system. This is due to the fact that ***all*** stations and trunks are allocated ports from the Primary system.

NetLink can control a maximum of 240 slots (including GCD-CP10's). This may reduce the maximum number of nodes in the network depending on the number of slots used per node.

From Release 3 software it is possible to register a SIP MLT to any node in a NetLink environment. Please refer to the SIP MLT section for further information.

NetLink Easy Edit Programming

Easy Edit – Advanced Items/VoIP/Networking/NetLink

NetLink Primary Settings

Easy Edit – Advanced Items/VoIP/Networking/NetLink/NetLink Primary Settings
IPL IP Address – This is the signalling address of the SV9100's own GPZ-IPLE card *(PRG10-12-09)*
IPL Subnet Mask – This is the subnet mask of the SV9100's own ILP card *(PRG10-12-10)*
Default Gateway – This is the IP address of the default gateway on the SV9100's own network *(PRG10-12-02)*
NetLink System ID - Used to assign all systems in the network with a unique node ID (1 – 50). *(PRG51-01-01)*
Primary Candidate Priority - Used to assign the Primary Candidate Priority. The number the system uses to elect the Primary System. (1 being the highest priority) *(PRG51-01-02)*
Primary System Selection Method - The method used for electing the Primary System. *(PRG51-01-03)*
Signal Transmit Method - Sets whether the system uses the nagle algorithm to buffer data and improve transfer efficiency through reduced network load. Benefits low bandwidth links. *(PRG51-01-04)*
Primary System IP Address – The IP address of the system which is nominated as the Primary when the Primary System Selection Method is set to Top Priority Primary System. *(PRG51-04-01)*
Automatic IP Address List Update – Controls whether to update the NetLink Systems list automatically or not. *(PRG51-13-01)*
Time Zone Method – Controls which features are adjusted to the correct time zone for a specific node. *(PRG51-13-02)*
MAC Address Authorization – If this is enabled, the system will check the MAC address of a system before allowing it to connect to the NetLink network. *(PRG51-13-03)*

AspireNet VoIP Resource IP Address Setup

Easy Edit – Advanced Items/VoIP/Networking/Netlink/Netlink IPL VoIP Resource IP Address (PRG84-26)
For an GPZ-IPLE card only one address is required regardless of the number of voip channels licensed.

For the RTP and RTCP ports enter the starting port number for each IP address. Each DSP requires one RTP port and one RTCP port. Under normal circumstances there is no need to change these settings from default.

NetLink Systems

Easy Edit – Advanced Items/VoIP/Networking/NetLink/NetLink Systems
IP Address – A list of IP addresses of each node in the network. *(PRG51-03)*
Name - Used to give a name to each node in the network. *(PRG51-02-01)*
Time Zone Hour - Used to set the time zone hour of where the particular node is located. *(PRG51-02-02)*
Time Zone Minute - Used to set the time zone minute of where the particular node is located. *(PRG51-02-03)*
MAC Address - Used to assign the MAC address of the node. Can be used to allow or deny connection to the network. *(PRG51-02-04)*

NetLink Replication

Easy Edit – Advanced Items/VoIP/Networking/NetLink/NetLink Replication
Automated Primary System Integration - Used to enable Automated Primary System Integration. When enabled, if the Primary System is available, it will take control of the NetLink network automatically. *(PRG51-06-01)*
System Package Reset Method - Used to control whether the system waits for all cards to be idle before resetting or anytime (even if calls are in progress) after automatic integration. *(PRG51-06-02)*
Enforced Primary System Integration - Used to allow or deny the ability to force Primary System Integration (by programming command). *(PRG51-07-01)*
System Package Reset Method - Used to control whether the system waits for all cards to be idle before resetting or anytime (even if calls are in progress) after enforced integration. *(PRG51-07-02)*
Replication Mode – This command controls whether Database Replication is done by time of day, by interval or disabled completely. *(PRG51-16-01)*
Replication Time – If the ***Replication Mode*** is set to ***Time Setting***, this command tells the system to replicate the database at this time every day. *(PRG51-16-02)*
Replication Interval – If the ***Replication Mode*** is set to ***Interval***, this command controls how often (in minutes) the database is replicated. *(PRG51-16-03)*
Replication Timestamp – This read only command displays the Date and Time of the last database replication event. *(PRG51-16-04)*
Replication Commencement Time – This tells the system how long to wait (in seconds) after a new NetLink node has joined the network before replicating the database to it (if enabled). *(PRG51-16-05)*
Node Replication Delay – If there are multiple Secondary Systems in the network, this is the delay (in seconds) between the replication from the Primary System to each Secondary System. *(PRG51-16-06)*
NetLink Fail-Over Limit – If this number of Fail-Over conditions is met within one hour the systems will not automatically re-integrate, they will stay as standalone systems until either forced integration is used or the systems are reset. If this command is set to 0 the systems will always try to re-integrate regardless of the number of Fail-Over conditions. This command should be set to the required value on each node before the first NetLink integration occurs. *(PRG51-18-01)*

NetLink Timers

Easy Edit – Advanced Items/VoIP/Networking/NetLink/NetLink Timers
This is a list of the timers used by NetLink.
The only timer that should be changed from default is ***KeepAlive Waiting Response Time.*** It is recommended to set this timer to 20 seconds. *(PRG51-05-02)*

NetLink Codec

Easy Edit – Advanced Items/VoIP/Networking/NetLink/NetLink CODEC Settings
NetLink can use various CODECs. A CODEC is a standard for converting an analogue signal to digital. This conversion process is handled by the DSP (Digital Signal Processors) on the GPZ-IPLE card.

Each CODEC has different voice quality and compression properties. The correct choice of CODEC will be based on the amount of bandwidth available, the amount of calls required and the voice quality required.

Available Codecs for NetLink

- G.711 64Kbps codec MOS 4.4
- G.722 64Kbps codec MOS 4.4
- G.726 32Kbps codec MOS 4.2
- G.729 8Kbps codec MOS 4.0

The bandwidth values quoted for these codecs are for the digitized speech in one direction only. The actual bandwidth required for a call will depend on many other factors and will be much higher than these figures.

The above MOS values are quoted for ideal network conditions. The value could be lower depending upon the network performance.

To change the codec in use in a NetLink network use the ***Audio Capability Priority*** setting in *Easy Edit – Advanced Items/VoIP/Networking/NetLink/NetLink Codec*

NetLink Information

Easy Edit – Advanced Items/VoIP/Networking/NetLink/NetLink Information
These are ‘read only’ commands where information about the NetLink network can be found.
Primary Information – Displays information about the Primary System. Node ID, IP address and MAC address etc. *(PRG51-12)*
NetLink Systems Information – Displays information about all nodes in the NetLink network. *(PRG51-11)*
NetLink Remaining Slots – Displays the number of remaining virtual slots. This number decreases every time a new card is installed from 240 down to Zero. When there are zero slots available no more cards can be installed.

NetLink TCP Ports

Easy Edit – Advanced Items/VoIP/Networking/NetLink/NetLink TCP Ports
This is a list of TCP ports used by the NetLink protocol. There is normally no need to change these, they are for information only. *(PRG51-09)*

NetLink DT800/DT700 Registrar Ports

Easy Edit – Advanced Items/VoIP/Networking/NetLink/NetLink DT700 Registrar Ports
This is a list of port numbers to define the Registrar and Session UDP port numbers on a per node basis. These are the port numbers that SIP MLT extensions use for registration and session communication. There is normally no need to change these from default. *(PRG51-17)*

Configuration Examples

Example 1

The example below shows the basic programming required for a three node NetLink network. Each system is on a separate network. They are configured using the Top Priority Primary System method with system A being the preferred Primary System. Automatic Primary Integration is enabled and the NetLink keep alive timer is set to the recommended 20 seconds.
No other advanced options are included here.

System A	System B	System C

10-12-01	192.168.0.10	10-12-01	192.168.0.10	10-12-01	192.168.0.10
10-12-02	255.255.0.0	10-12-02	255.255.0.0	10-12-02	255.255.0.0
10-12-03	172.16.0.1	10-12-03	172.17.0.1	10-12-03	172.18.0.1
10-12-09	172.16.0.10	10-12-09	172.17.0.10	10-12-09	172.18.0.10
10-12-10	255.255.0.0	10-12-10	255.255.0.0	10-12-10	255.255.0.0
51-01-01	1	51-01-01	2	51-01-01	3
51-01-03	1	51-01-03	1	51-01-03	1
51-04-01	172.16.0.10	51-04-01	172.16.0.10	51-04-01	172.16.0.10
51-05-02	20	51-05-02	20	51-05-02	20
51-06-01	1	51-06-01	1	51-06-01	1
84-26-01	172.16.0.20	84-26-01	172.17.0.20	84-26-01	172.18.0.20

With the above programming the systems will automatically integrate and the cards will be reset when they are idle. If the network is lost, the systems will revert to stand alone systems.

System A (172.16.0.10) will always be the Primary System when the network is up.

If Top Priority system is not available in the network, Primary System is elected by highest Primary Candidate Priority (lowest number). If this value is equal on all systems then the lowest Node ID will be elected as the Primary.

After programming NetLink, on exiting programming you will be asked if you wish to reset the system. *Always* choose yes otherwise the NetLink programming may be lost.

Example 2

With the programming below the first system to be powered on will be the Primary System. This is because the systems are ***not*** set to look for a specific IP address to be the Primary and when the first system is powered on there are no other systems available to be the Primary. When the other two systems are powered on they do a search and find there is already a Primary System so they accept that. If the network is lost, the systems will revert to stand alone systems. When the network comes back up, nothing will change automatically, NetLink will not be operational. Enforced Primary Integration can be used (if enabled), or the Secondary systems can be reset to bring NetLink back up again.

System A		System B		System C	
10-12-01	192.168.0.10	10-12-01	192.168.0.10	10-12-01	192.168.0.10
10-12-02	255.255.0.0	10-12-02	255.255.0.0	10-12-02	255.255.0.0
10-12-03	172.16.0.1	10-12-03	172.17.0.1	10-12-03	172.18.0.1
10-12-09	172.16.0.10	10-12-09	172.17.0.10	10-12-09	172.18.0.10
10-12-10	255.255.0.0	10-12-10	255.255.0.0	10-12-10	255.255.0.0
51-01-01	1	51-01-01	2	51-01-01	3
51-01-03	0	51-01-03	0	51-01-03	0
51-03-01	1 – 172.16.0.10 2 – 172.17.0.10	51-03-01	1 – 172.16.0.10 2 – 172.17.0.10	51-03-01	1 – 172.16.0.10 2 – 172.17.0.10

	3 – 172.18.0.10		3 – 172.18.0.10		3 – 172.18.0.10
51-05-02	20	51-05-02	20	51-05-02	20
51-06-01	0	51-06-01	0	51-06-01	0
84-26-01	172.16.0.20	84-26-01	172.17.0.20	84-26-01	172.18.0.20

Be aware that the above operation is not recommended as it is possible for the Primary System to move from one node to another if the Primary is reset.

Database Backup

Prior to setting up NetLink, a recovery database should be created for each system. This is used when you wish to remove a system from NetLink.
From handset programming:

- Create recovery database PRG90-57
- Restore recovery database PRG90-58
- Delete recovery database PRG90-59

All recovery databases on a particular GCD-CP10 will be lost if the system is defaulted.

Remove a NetLink Node

If it is required to remove a NetLink node from the network it should be deleted from the Primary System's database.
From handset programming:

- Delete system information PRG51-14

The system must be disconnected from the network before this command is executed.

Handset Information

Pressing **Feature 5** on a DT400/DT300 phone will show the following information about the system that the extension is connected to: -

- GPZ-IPLE IP Address
- System ID
- Primary or Secondary

Pressing **Feature 5** on a DT800/DT700 phone will show the information from the system that it is registered to.

Recommendations

- Use Top Priority Primary System rather than Dynamic for the **Primary System Selection Method**. *Easy Edit – Advanced Items/VoIP/Networking/NetLink/NetLink Primary Settings (PRG51-01-03)*
- Enable **Automated Primary System Integration**. *Easy Edit – Advanced Items/VoIP/Networking/NetLink/NetLink Replication (PRG51-06-01)*
- Set the **Keep Alive Response Waiting Time** to 20 seconds. *Easy Edit – Advanced Items/VoIP/Networking/NetLink/NetLink Timers (PRG51-05-02)*

These settings will allow the nominated Primary System to take control of the NetLink network whenever it (and the network) is available. It will also allow the Secondary Systems to select another Primary System or operate as a standalone system if the original Primary is not available.

Asynchronous Settings

The following programming commands are not sent from the Primary System to the Secondary Systems when Database Replication occurs:
PRG10-01, PRG10-02, PRG10-12, PRG10-13, PRG10-14, PRG10-15, PRG10-16, PRG10-45, PRG51-01, PRG90-01, PRG90-09.

SRAM Database

The information held in SRAM is not transferred to Secondary Systems. So if a Fail-Over situation occurs terminals may lose DND, Caller ID History, etc.

Considerations

Almost all features available at a single system are available via Net-Link.
All IP trunks must register from Primary system.
Centralised Voice Mail programming is not required because all extensions belong to the Primary system.
If there is a Voice Mail installed at the Primary system, this will service all nodes as a local Voice Mail.
InMail must be installed in the Primary system.
LAN/WAN connection – Is the IP connection between all systems suitable for NetLink.
QoS – NetLink signalling should have the highest priority possible followed by the speech data (RTP). The general data on the network should have the lowest priority or no priority.

Applications/Devices

Below is a list of applications or devices that would be affected if the Primary System changed to a different node, this is because the communication is between the device or application and the IP address of the Primary System or the hardware is installed in the Primary System: -

- InMail
- IP extensions registered to the Primary system
- All IP Trunks
- SMDR/P Event Applications (MyCalls)
- CTI Applications (TAPI/OAI)
- Desktop Applications
- AspireNet
- K-CCIS
- PMS

Licensing

All nodes in a NetLink network must be licensed except for the Primary System.
The licenses for all Secondary Systems are loaded onto the Primary System GCD-CP10.
E.g. If there is a ten node NetLink network, there must be a license for nine Secondary Systems loaded onto the Primary Systems GCD-CP10.
In the event of a Fail-Over situation, the licenses from the original Primary System will be copied to the new Primary System for a maximum of seven days. After the seven days have elapsed, the licenses will be removed from the new Primary System so it is imperative that the original Primary System is restored to this role.
License Code: BE114067

2.6.1.1 NetLink Advanced Features

Netlink Advanced Features

Fail-Over

An added feature of NetLink is the Fail-Over feature. If the Primary System is turned off or disconnected, without the Fail-Over feature, all communication servers would stop working. With Fail-Over, one of the Secondary Systems, depending on the SV9100 programming, will take over as the Primary System allowing the other linked nodes to continue functioning.

Enable Fail-Over by changing **KeepAlive Response Waiting Time** in *Easy Edit* – *Advanced Items/VoIP/ Networking/NetLink/NetLink Timers (PRG51-05-02)* to 20 seconds.

Automated Primary System Integration

This feature allows the Primary System to always take back control of the network automatically after it has been unavailable.
E.g. If the Primary System had a power failure, one of the Secondary Systems would take over as the Primary (if Fail-Over is enabled). Without this feature enabled, when the original Primary System comes back on line, it would continue to run as a Secondary. This operation may be undesireable, so, if Primary System Automatic Integration is enabled it would take over as the Primary System once it is back on line.
It is enabled using **Automated Primary System Integration** in *Easy Edit* – *Advanced items/VoIP/ Networking/NetLink/NetLink Replication. (PRG51-06-01)*
There is an option **System Package Reset Method** in *Easy Edit* – *Advanced items/VoIP/Networking/ NetLink/NetLink Replication (PRG51-06-02)* to wait until all cards are idle before the system resets or to do it immediately.

Fail-Over must be enabled for this feature to work.

Enforced Primary Integration

If Automated Primary System Integration is not used (see above), it is possible to manually select a new Primary System by entering the GPZ-IPLE IP address of the new Primary System into a programming command.
This feature must be enabled in *Easy Edit* – *Advanced items/VoIP/Networking/NetLink/NetLink Replication. (PRG51-07-01)*
Enforced Primary Integration should only be used when Primary Candidate Priority is in use or when the the Top Priority System is unavailable.
To change the Primary System, enter programming mode (handset only). Enter *PRG51-08-01*, type in the GPZ-IPLE IP address of the system you wish to be the Primary and press Transfer. The system will reset and the change will take place.

Database Replication

Once NetLink is operational, the database can be replicated from the Primary system to the Secondary system(s). This database will be used if a Fail Over condition occurs.
The database Replication can be done by time of day or by interval. This is controlled by the Replication options in *Easy Edit* – *Advanced items/VoIP/Networking/NetLink/NetLink Replication*
If Database Replication is not used and a Fail-Over condition occurs, the new Primary System will use the configuration that was stored in its own GCD-CP10 for the whole NetLink database. This means that the database is completely different from the original config.

DTMF Relay (RFC2833)

By default any DTMF tones transmitted across NetLink will be sent as audio tones in the speech path. It is possible that these tones can be misinterpreted by the receiving device because of packet loss or errors due to the codec compression.
DTMF relay is a way of converting the DTMF tone into a signal then sending the signal across the IP network instead of the actual tone.
To enable this feature set the **DTMF Relay Mode** option to **RFC2833** in *Easy Edit – Advanced Items/VoIP/Networking/NetLink/NetLink CODEC Settings (PRG84-34)*

Fax Relay (T.38)

By default any Fax tones transmitted across NetLink will be sent as audio tones in the speech path. It is possible that these tones can be misinterpreted by the receiving device because of packet loss or errors due to the codec compression.
Fax relay is a way of converting the Fax tones into a signal then sending the signal across the IP network instead of the actual tone.
To enable this feature set the **Fax Relay Mode** option to **Enabled** in *Easy Edit – Advanced Items/VoIP/Networking/NetLink/NetLink FoIP Settings. (PRG84-33)*

Time Zone Offset

This is used if one or more of the NetLink nodes are in a different time zone than the Primary System. Set the relavent Hours and minutes offset against each node in *Easy Edit – Advanced Items/VoIP/Networking/NetLink/NetLink Systems. (51-02-02/03)*
The following features can be adjusted to be in line with the Time Zone Offset: -

- Time Display
- Incoming/Outgoing Call History
- VRS Time Announcement
- Date and Time Setting by Service Code
- Alarm Clock

It is possible to select which features the Time Zone Offset is applied to. This is done using the **Time Zone Method** in *Easy Edit – Advanced Items/VoIP/Networking/NetLink/NetLink Primary Settings. (51-13-02)*

MAC Address Authorization

The Primary System is able to reject a NetLink connection request if the MAC address of the requesting system does not match the MAC address set in system programming.
Enable **MAC Address Authorization** in *Easy Edit – Advanced Items/VoIP/Networking/NetLink/NetLink Primary Settings. (51-13-03)*
Enter the MAC address to be authorised into the **MAC Address** item against the system number in *Easy Edit – Advanced Items/VoIP/Networking/NetLink/NetLink Systems. (51-02-04)*
The MAC address can be seen by pressing ‘Feature 3’ on a display telephone on the system that wants to join the NetLink network.

Netlink Improvement for Buffer Operation

The transmission of data packets via a NetLink connection can be set to Immediate or Buffered.

With Buffered operation the SV9100 will only send the data packets when one of the following conditions is met:

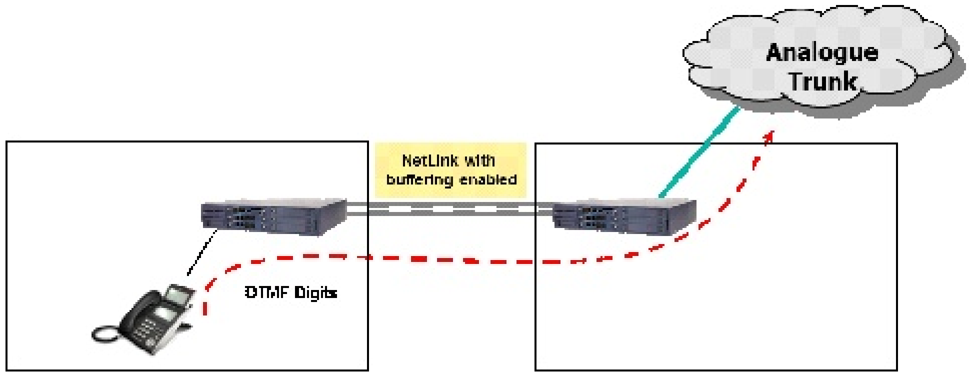
1. The previous packet has been acknowledged

2. The packet size exceeds the minimum size
3. 120mS after the previous packet was sent

Buffering operation can reduce the network load by grouping together smaller packets until the minimum size is exceeded, therefore sending a smaller quantity of larger packets.

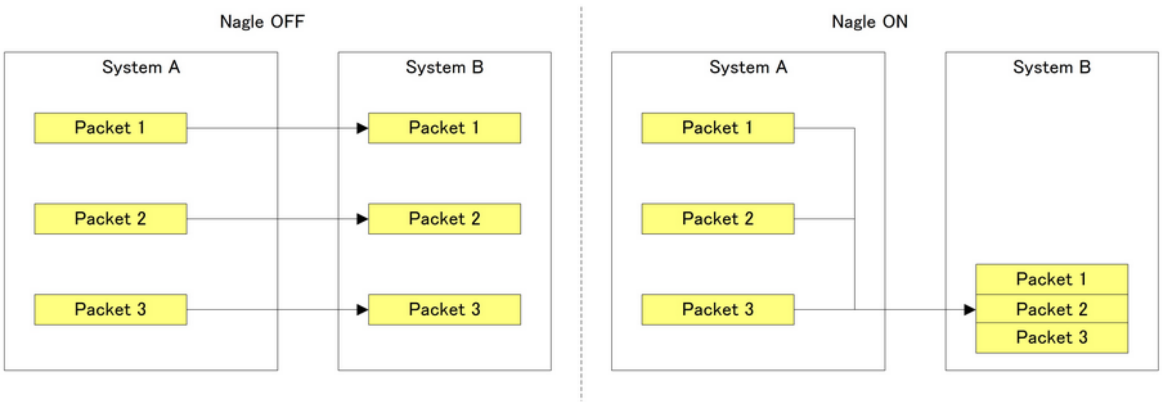
However implementing the Buffering operation can cause problems when sending DTMF digits via a NetLink connection. For example to a remote analogue trunk: DTMF digits must be sent immediately.

To ensure DTMF digits are sent immediately the SV9100 with R9 Main Software will ensure the data packet exceeds the minimum size.



Wizard – Advanced Items/VoIP/Networking/Netlink/Netlink Primary Settings/Signal Transmit Method (51-01-04) - (0=Immediate, 1=Buffered) default = Buffered

a) With Buffered operation the SV9100 will use the Nagle Algorithm to improve transmit efficiency and only send the data packets when one of the following conditions are met:
   1. The previous packet has been acknowledged
   2. The packet size exceeds the minimum size
      Packet size is larger than MSS (Maximum Segment Size)
   3. 120mS after the previous packet was sent



b) **CMD51-01-04 must be enabled at the Primary and Secondary systems as it can only process**

the transmitted data.

c) DTMF digits are always sent immediately by adding dummy data to ensure the packet size exceeds the MSS.

2.6.1.2 NetLink DSP Zones

Netlink DSP Zones

Description

A DSP provides format conversion from circuit switched networks (TDM) to packet switched networks (IP). Each voice channel from the circuit switched network is compressed and packetised for transmission over the packet network. In the reverse direction, each packet is buffered for de-jittering, decompressed, and sent to the circuit switched network. Each DSP converts a single speech channel from IP to TDM and vice versa.

- A DSP is used on the system GCD-CP10 which has the call. For instance, when a trunk on System ID 2 uses a receiver, a DSP on System ID 2 is used.
- The Primary System must control DSP resources on the Secondary Systems but it cannot control all of them.
- There are five zones to handle DSP resources in NetLink. The zone number depends on the System ID number.
- In the same Zone, the communication servers must share the DSP resource number.
- For instance, if a user in System ID 1 is using DSP resource 1, resource 1 becomes busy in Zone 1 (System ID 1, 6, 11, 16, 21, 26, 31, 36, 41 and 46).

Zone		**System ID**									
1		1	6	11	16	21	26	31	36	41	46
2		2	7	12	17	22	27	32	37	42	47
3		3	8	13	18	23	28	33	38	43	48
4		4	9	14	19	24	29	34	39	44	49
5		5	10	15	20	25	30	35	40	45	50

- All nodes in the NetLink network follow the DSP Setting in Program 10-19 of the Primary System.

2.6.2 AspireNet

AspireNet

The SV9100 uses the GPZ-IPLE card or PRI card to connect multiple systems together over a Data Communication IP Network (Intranet). AspireNet is used to provide telephony services between the SV9100 and other SV9100's, SV8100's or Aspire systems.

There can be up to 16 Nodes in an AspireNet Network.

The station and trunk ports are independantly allocated from the local CPU so extensions and trunks are dependant of the maximum capacities of each system.
Each system in the network must have:

- GCD-CP10
- GPZ-IPLE or PRI card
- Feature Networking (Aspirenet) license(s): BE114066

It is advisable to have compatible levels of system software installed on all systems within the Network.

Although the basic AspireNet will operate correctly there could be problems with features that are only available from a given level of software.

AspireNet Easy Edit Programming

AspireNet IP Setup

Easy Edit – Advanced Items/VoIP/Networking/AspireNet CVM/AspireNet Setup/AspireNet IP Setup
IPL IP Address – This is the signalling address of the SV9100's own GPZ-IPLE card *(PRG10-12-09)*
IPL Subnet Mask – This is the subnet mask of the SV9100's own IPL card *(PRG10-12-10)*
Default Gateway – This is the IP address of the default gateway on the SV9100's own network *(PRG10-12-02)*
Networking System – This is the TCP port that the SV9100 uses
Fast Start – This is a component of the H.323 protocol. This must be enabled for AspireNet

AspireNet address for Remote

Easy Edit – Advanced Items/VoIP/Networking/AspireNet CVM/AspireNet Setup/AspireNet address for Remote (PRG10-12-27)
Against the **Networking System ID** (1 – 50) enter the IP address of the remote systems GPZ-IPLE or VoIPDB.

AspireNet VoIP Resource IP Address Setup

Easy Edit – Advanced Items/VoIP/Networking/AspireNet CVM/AspireNet Setup/AspireNet IPL VoIP Resource IP Address (PRG84-26)
For an GPZ-IPLE card only one address is required regardless of the number of voip channels licensed. For the RTP and RTCP ports enter the starting port number for each IP address. Each DSP requires one RTP port and one RTCP port. Under normal circumstances there is no need to change these settings from default.

AspireNet ISDN setup

For configuration of the PRI card for AspireNet connection refer to the following Easy Edit page:

Easy Edit – Blade Configuration/ISDN Port Setup/PRT Port Setup

ISDN Line Mode - Set to one of the three available NW mode as follows:
3 - NW Mode (Leased Line)
4 - NW Mode (Interconnected Line) (generally used if the connected systems are directly connected via a fixed cable)
5 - NW Mode (Interconnected Line), (Fixed Layer 1 Forced NT Mode)

NW Mode (Leased Line)
The ISDN interface is Slave mode and must receive a clock signal from the network.
System connection diagram.

System 1 NW Leased Line Master side	--- Netw ork Termination Unit ---	BRI Leased Line	--- Netw ork Termination Unit ---	**System 2 NW Leased Line Slave side**

Clock signal diagram.

System 1 Slave	--- NTU (Clock signal generator) ---	BRI Leased Line	--- NTU (Clock signal generator) ---	**System 2 Slave**

NW Mode (Interconnected Line)
The ISDN interface is Slave mode at one end and Master mode at the other.
The maximum length of the interconnected cable should not exceed 200 metres for PRI using CAT5 cable.
System connection diagram.

System 1 NW Interconnected Line Master side	------	Interconnected Line	------	**System 2 NW Interconnected Line Slave side**

Clock signal diagram.

System 1 Master (Clock signal generator)	------	Interconnected Line	------	**System 2 Slave**

NW Mode (Interconnected Line, Layer 1=NT)
The ISDN interface is Slave mode at one end and Master mode at the other.
The Layer 1 of the ISDN interface is fixed at NT (Network Termination - Master mode).
System connection diagram.

System 1 NW Interconnected Line Master side	---Gatew ay---	Interconnected Line	---Gatew ay---	**System 2 NW Interconnected Line Slave side**

Clock signal diagram.

System 1 Clock signal generator	---Gatew ay (Slave)---	---Interconnected Line---	---Gatew ay (Slave)---	**System 2 Clock signal generator**

NW Mode Master/Slave System - set one side of the PRI link to Master and the other to Slave

NW Mode Networking System - The networking system ID number is used to select the access route for dialled digits. You can choose any number from 0 to 50. (0 equals no operation)

The commands below are to set up the local and remote extension number ranges for each system.
Easy Edit – Advanced Items/VoIP/Networking/AspireNet CVM/AspireNet Numbering Plan

System Numbering

Easy Edit – Advanced Items/VoIP/Networking/AspireNet CVM/AspireNet Numbering Plan/System Numbering (PRG11-01)

Set the relevant digits for the remote systems extension range to the correct length using **1st Dial Digit, 1st and 2nd Dial Digit and Dial Digit Length**. Set the **Type** to be **Networking System Access** and the **Networking ID** should match the **Networking System ID** in **AspireNet address for Remote**.

Extension Numbers

Easy Edit – Advanced Items/VoIP/Networking/AspireNet CVM/AspireNet Numbering Plan/Extension Numbers (PRG11-02)
Assign extension numbers to port numbers for the local system

F-Route

Easy Edit – Advanced Items/VoIP/Networking/AspireNet CVM/AspireNet Numbering Plan/F-Route (PRG44-XX)
Digits dialled by a user can be sent to the F-Route tables and specified as an AspireNet number by entering the Networked node ID (Trunk Group 101-150 correspond to Network ID's 1-50) as the target trunk group number, calls will be routed to the target system via the node ID specified. The dialled digits will then be analysed by the F-Route tables in the target system. At the target system the call will be analysed within F-Route for the following call types:

- Outgoing call to a trunk
- Extension access call (you must translate the dialled digits)
- Access to the other system via AspireNet
- No defined dial

Alternate route selection is not available when the primary network route is busy. When all channels are busy the call will return busy tone.

Compared With Single System Configuration

In a single system with F-Route used, the dialling is analysed when the call is initially dialled.

Operation

The operation is automatic once configured in F Route programming.

The commands below are to allow extensions on one system use the trunks on another system to dial out.
Easy Edit – Advanced Items/VoIP/Networking/AspireNet CVM/AspireNet Remote Trunk Access

Trunk Group Routing For Extensions

Easy Edit – Advanced Items/VoIP/Networking/AspireNet CVM/AspireNet Remote Trunk Access/Trunk Group Routing For Extensions (21-02)
Enter the Trunk Route Number (see below) per Night Service Mode against each extension.

Trunk Group Routing

Easy Edit – Advanced Items/VoIP/Networking/AspireNet CVM/AspireNet Remote Trunk Access/Trunk Group Routing (PRG14-06)
Against the relevant **Route Table** enter the Trunk Group Number for access to the relevant remote system (Trunk Group 101-150 correspond to Network ID's 1-50).

AspireNet Incoming Trunk Access Route

Easy Edit – Advanced Items/VoIP/Networking/AspireNet CVM/AspireNet Remote Trunk Access/AspireNet Incoming Trunk Access Route (PRG21-16)
This controls which local Trunk Route an incoming AspireNet call has access to for outgoing trunk calls. Set the Trunk Route on a per AspireNet Networking System ID.

AspireNet Busy Lamp Information

Easy Edit – Advanced Items/VoIP/Networking/AspireNet CVM/AspireNet Busy Lamp Information (PRG20-01-04)
This is a timer that controls the frequency of Busy Lamp updates between AspireNet nodes. Enter a value (in 100ms increments) of how often the local system should send out BLF updates to all other systems in the network. 1 = 100ms, 5 = 500ms etc.

AspireNet Park Hold Operation

Easy Edit – Advanced Items/VoIP/Networking/AspireNet CVM/AspireNet Park Hold Operation (PRG24-03)
Park Hold information is shared between all nodes in an AspireNet network so any user can pick up a Parked call from any system. In some circumstances this operation may be undesirable and each system may wish to see only its own Parked calls. To do this put all extensions from each system into its own Park Hold Group. E.g. put all extensions on System ID 1 into Park Group 1 and all extensions on System ID 2 into Park Group 2 etc.

Centralised Voicemail

Easy Edit – Advanced Items/VoIP/Networking/AspireNet CVM/Centralised Voicemail (PRG45-XX)
AspireNet will support the use of a single voicemail system for the entire network. A user may call into the voicemail from anywhere in the network and perform most functions as if the voicemail were located on their premises.

Please see the Centralised Voicemail page for further details.

AspireNet Codec

Easy Edit – Advanced Items/VoIP/Networking/AspireNet CVM/AspireNet Setup/AspireNet CODEC Settings
AspireNet can use various CODECs. A CODEC is a standard for converting an analogue signal to digital. This conversion process is handled by the DSP (Digital Signal Processors) on the GPZ-IPLE card.
Each CODEC has different voice quality and compression properties. The correct choice of CODEC will be based on the amount of bandwidth available, the amount of calls required and the voice quality required.

Available Codec's for AspireNet

- G.711 64Kbps codec MOS 4.4
- G.722 64Kbps codec MOS 4.4
- G.729 8Kbps codec MOS 4.0

The bandwidth values quoted for these codec's are for the digitized speech in one direction only. The actual bandwidth required for a call will depend on many other factors and will be much higher than these figures.

The above MOS values are quoted for ideal network conditions. The value could be lower depending upon the network performance.

To change the codec in use in an AspireNet network use the ***Audio Capability Priority*** setting in *Easy Edit – Advanced Items/VoIP/Networking/AspireNet CVM/AspireNet Setup/AspireNet CODEC Settings*

DTMF Relay (RFC2833)

By default any DTMF tones transmitted across K-CCIS will be sent as audio tones in the speech path. It is possible that these tones can be misinterpreted by the receiving device because of packet loss or errors due to the codec compression.
DTMF relay is a way of converting the DTMF tone into a signal then sending the signal across the IP network instead of the actual tone.
To enable this feature set the **DTMF Relay Mode** for **Networking** using **Profile 1** to **RFC2833** or **H.245** (all nodes should have the same setting) in *Easy Edit – Advanced Items/VoIP/General Settings/VoIP Configuration/IPL DTMF Settings/DTMF Setup (PRG84-34)*

Fax Relay

By default any Fax tones transmitted across AspireNet will be sent as audio tones in the speech path. It is possible that these tones can be misinterpreted by the receiving device because of packet loss or errors due to the codec compression.
Fax relay is a way of converting the Fax tones into a signal then sending the signal across the IP network instead of the actual tone.
To enable this feature set the **Fax Relay Mode** option to **Enabled** in *Easy Edit – Advanced Items/VoIP/Networking/AspireNet CVM/AspireNet Setup/AspireNet FoIP Settings (PRG84-33)*

Note:
The SV9100 uses T.38 for its Fax Relay protocol but the Aspire uses a proprietary protocol. This means that Fax Relay cannot be used between the two systems.

		Node 1	
		SV9100	**Aspire**
Node 2	**SV9100**	Pass	Fail
	Aspire	Fail	Pass

Configuration Example

The examples below shows the basic programming required for an SV9100 AspireNet network. Each system is on a separate network.
No other advanced options are included here.

Example A
This example shows the configuration necessary for an AspireNet over IP 3 node network.

System A		System B		System C	
10-12-01	192.168.0.10	10-12-01	192.168.0.10	10-12-01	192.168.0.10
10-12-02	255.255.0.0	10-12-02	255.255.0.0	10-12-02	255.255.0.0
10-12-03	172.16.0.1	10-12-03	172.17.0.1	10-12-03	172.18.0.1
10-12-09	172.16.0.10	10-12-09	172.17.0.10	10-12-09	172.18.0.10
10-12-10	255.255.0.0	10-12-10	255.255.0.0	10-12-10	255.255.0.0

10-27-01	ID 1 = 172.17.0.10 ID 2 = 172.18.0.10	10-27-01	ID 1 = 172.16.0.10 ID 2 = 172.18.0.10	10-27-01	ID 1 = 172.16.0.10 ID 2 = 172.17.0.10
11-01	1 = 3 Digit Type 2 2 = 3 Digit Type 8 ID 1 3 = 3 Digit Type 8 ID 2	11-01	1 = 3 Digit Type 8 ID 1 2 = 3 Digit Type 2 3 = 3 Digit Type 8 ID 2	11-01	1 = 3 Digit Type 8 ID 1 2 = 3 Digit Type 8 ID 2 3 = 3 Digit Type 2
11-02	1XX	11-02	2XX	11-02	3XX
84-26-01	172.16.0.20	84-26-01	172.17.0.20	84-26-01	172.18.0.20

Example B

Each system must have a dedicated ISDN circuit for each AspireNet over ISDN connection.
Therefore, for a system to connect to 2 different nodes via ISDN AspireNet 2 seperate PRI cards must be used.
The example below describes connection to a single node.

System A		System B	
10-03-01	4 = Network Mode Interconnected Line	10-03-01	4 = Network Mode Interconnected Line
10-03-10	1 = Master	10-03-10	0 = Slave
10-03-11	Network ID = 1	10-03-10	Network ID = 2
11-01	1 = 3 Digit Type 2 2 = 3 Digit Type 8 ID 1	11-01	1 = 3 Digit Type 8 ID 2 2 = 3 Digit Type 2
11-02	1XX	11-02	2XX

Licensing

Each SV9100 need to be licensed to use AspireNet. One license gives that system the ability to use one channel for AspireNet.
E.g. in the configuration example above, if each system needs the ability to have 4 concurrent conversations over AspireNet then each node must have four AspireNet licenses.
Licence Code: BE114066

2.6.2.1 AspireNet Centralised Voice mail

Centralised Voice Mail

AspireNet will support the use of a single voicemail system for the entire network. A user may call into the voicemail from anywhere in the network and perform most functions as if the voicemail were located on their premises.

Supported Configurations

If the AspireNet network consists of SV9100 or SV8100 systems then the Centralised Voicemail can be

provided by:
VM8000 InMail
UM8000
External Voicemail

If the AspireNet network has a mix of SV9100 systems and Aspire systems the Centralised Voicemail *must* be provided by one of the Aspire systems using:
AspireMail DMS
FMSU
VMSU
External Voicemail

Centralised Voice Mail Easy Edit Programming

Easy Edit – Advanced Items/VoIP/Networking/AspireNet CVM/Centralised Voicemail

Department Group Assignment
Easy Edit – Advanced Items/VoIP/Networking/AspireNet CVM/Centralised Voicemail/Department Group Assignment
Department Group – Set the Voice Mail ports into the relevant Department Group e.g.64 *(PRG16-02)*
Terminal Type – Set the Voice Mail ports to **Special** *(PRG15-03-03)*

Centralised Voicemail Setup
Voice Mail Department Group - This must be set to 0 otherwise the voice mail will not operate as a Centralised Voice Mail. *(PRG45-01-01)*
Centralised Voice Mail Pilot - Enter the Pilot Number that a user at any system within the network can dial to access to Centralised Voice Mail. Note - The pilot number must be within the network numbering plan. *(PRG45-01-07)*
This setting must be the same at all systems within the network.
Centralised Voice Mail Department group - Enter the Department group number that contains the InMail ports or SLIU ports connected to the voice mail system. (You should also ensure that this Department group does not have a pilot number assigned in Department Group Options).
This setting is not required at any system(s) within the network that do not have the Centralised Voice Mail installed. *(PRG45-01-08)*
Centralised Voice Mail Master Name - Give the Centralised Voice Mail a name that will be shown at the display keyphone while accessing the voice mail. *(PRG45-01-09)*
NSL Protocol - Required for softkey integration. *(PRG45-01-10)*
Centralised Voice Mail Type - Required to be set to 'enhanced' if InMail used for voicemail. *(PRG45-01-19)*

Configuration Example

Node 1 (VM Installed)		**Node 2**	
Department Group Assignment	Group 64	Department Group Assignment	None
Voice Mail Department Group	0	Voice Mail Department Group	None

Department Group Pilot Number	Group 64 = 0	Department Group Pilot Number	None
Centralised Voice Mail Pilot	600	Centralised Voice Mail Pilot	600
Centralised Voice Mail Department Group	64	Centralised Voice Mail Department Group	None
Numbering Plan	Dial 6XX = Extension	Numbering Plan	Dial 6XX = Networking System Access

2.6.2.2 AspireNet Features

AspireNet Features

The following system features are available between systems that are networked using AspireNet.

Features Available via AspireNet

- ARS/F-Route
- Barge In
- Busy Lamp Indication
- Call Forwarding Override
- Caller ID Display
- Call Forwarding: Immediately, Busy, No Answer, Both Ring
- Call Forwarding, Follow Me
- Call Forwarding, Off-Premise
- Call Waiting / Camp On
- Central Office Calls, Placing: Seizing a trunk in networked system
- Conference
- Department Calling
- Department Step Call
- Direct Dial In (DDI)
- Direct Inward Line (DIL)
- Direct Inward System Access (DISA)
- Hold
- DSS Console
- Intercom: Change Voice/Signal Ring
- Keep Alive Operation
- Last Number Redial
- Message Waiting
- Operator, Centralised
- Paging
- Park
- Ringdown Extension, Internal/External (Hotline)
- Selectable Display Messaging
- Toll Restriction

- Transfer
- Voice Mail, Centralised

ARS/F-Route

Digits dialled by a user can be sent to the F-Route tables and specified as a AspireNet number by entering the Networked node ID (Trunk Group 101-150 correspond to Network ID's 1-50) as the target trunk group number, calls will be routed to the target system via the node ID specified. The dialled digits will then be analysed by the F-Route tables in the target system. At the target system the call will be analysed within F-Route for the following call types:

- Outgoing call to a trunk
- Extension access call (you must translate the dialled digits)
- Access to the other system via AspireNet
- No defined dial

Alternate route selection is not available when the primary network route is busy. When all channels are busy the call will return busy tone.

Compared With Single System Configuration
In a single system with F-Route used, the dialling is analysed when the call is initially dialled.

Operation
The operation is automatic once configured in F-Route programming.

Barge In

Barge In is available in the Networking feature with the following options:

- Barge into a conversation between an extension's own system and a networked system
- Barge into a conversation between callers in a networked system
- Barge into a call between two networked systems
- Barge In can be used in either Monitor Mode (Silent Monitor) or Speech Mode depending on system programming

Barge In cannot barge into calls across the network in the following instances:

- Conference calls
- Off hook signalling a telephone in the other system

Operation
To Barge In after calling a busy extension:
(An analogue trunk call must be set up for 10 seconds before you can Barge In).
Listen for busy/ring or busy tone.
1. Dial Barge In service code 810
OR
2. Press Barge In key (SC 851: 34).

Call Forwarding

Call Forwarding Immediate / Busy / No Answer / Busy-No Answer / Both Ring options are available with the Networking feature.
With a networked system, when Call Forwarding enabled, there is a slight difference in the telephone's display. With a single system, the extension name is displayed on the extension which has Call Forwarding. With a networked system, the extension number is displayed.

Operation
To activate or cancel Call Forwarding:

1. Press Speaker (or lift handset) + Dial 888.
Also allowed are 848 (Call Forward Immediate), 843 (Call Forward Busy), 845 (Call Forward No Answer, 844 (Call Forward, Busy/No Answer, or 842 (Call Forward Both Ring).
OR
Press Call Forwarding key (SC 851: code 16).
2. Dial Call Forwarding condition:
1 = Personal Answering Machine Emulation (then skip to step 4 - refer also to "Voice Mail").
2 = Busy or not answered
4 = Immediate
6 = Not answered
7 = Immediate with simultaneous ringing (not for Voice Mail)
0 = Cancel
3. Dial destination extension, Voice Mail master number or press Voice Mail key.
4. Dial Call Forwarding type:
2 = All calls
3 = Outside calls only
4 = Intercom calls only
When you enable Call Forwarding, your Call Forwarding key flashes slowly. If you don't have a Call Forwarding key, DND flashes slowly.
OR
1. Press Call Forwarding key.
SC 851: code 10 for Forward All Calls Immediately
SC 851: code 11 for Forward when Busy
SC 851: code 12 for Forward when Unanswered
SC 851: code 13 for Forward Busy/No Answer
SC 851: code 14 for Forward with Both Ringing
SC 851: code 15 for Follow Me
SC 851: code 16 for Forward to Station (forward type is selected at the time the option is set by the user)
SC 851: code 17 for Forward to Device
2. Dial 1 plus extension to enable; dial 0 to disable.
Once you activate Call Forwarding, only your Call Forwarding destination can place an Intercom call to you.
3. Dial destination extension, Voice Mail master number or press Voice Mail key.
You'll hear stutter dial tone when placing a new call.

Call Forwarding / Do Not Disturb Override

The extension user may be able to call an extension which has Call Forwarding or Do Not Disturb set.

Operation
To override an extension's Call Forwarding or Do Not Disturb:
1. Call the forwarded or DND extension.
2. Dial Call Forward / DND Override service code 807
OR
3. Press Override key (SC 851: 37).

Call Forward, Off-Premise

Off-Premise Call Forwarding allows an extension user to forward their calls to an off-site location.
This feature works the same in a networked system as it does in a single system.
A call to an extension at a remote system will forward to the Abbreviated Dial bin using a trunk at the remote system.

Operation

To activate Call Forwarding Off-Premise
1. At system phone, press Speaker + Dial Call Forward Service Code (848, 843, 844, 845).
OR
Press Call Forward key (SC 851: 10, 11, 13 or 12)
OR
At an SLT, lift handset Dial 848, 843, 844 or 845.
2. Dial 1.
3. Dial the Abbreviated Dial Bin number (000 to 999) which your calls should be forwarded.
4. Press SPK (or hang up at SLT) to hang up.
Your DND and Call Forwarding Programmable Function Key flashes.

To cancel Call Forwarding Off-Premise
1. At system phone, press idle CALL key + Dial 848, 843, 844 or 845.
OR
Press Call Forward key (SC 851: 10, 11, 13 or 12)
OR
At an SLT, lift handset and dial 848, 843, 844 or 845.
2. Dial 0.
3. Press SPK (or hang up at SLT) to hang up.
Your DND or Call Forwarding Programmable Function Key stops flashing.

Call Forwarding with Follow Me

The extension user can program Call Forward Follow-Me to extension in a networked system. When the extension with the Follow Me setting receives an incoming call, both the original extension and the programmed destination extension starts ringing.
With a networked system, when Call Forward Follow-Me is enabled, there is a slight difference in the telephone’s display. With a single system, the destination extension displays the extension name for the phone with Follow-Me enabled. With a networked system, the extension number is displayed.

Operation

To activate Call Forward Follow Me:
1. At a system phone other than your own, press Speaker and dial 888.
OR
Press Call Forward (Station) key (SC 851: 15).
OR
At an SLT other than your own, lift handset and dial 888.
2. Dial 3 + Dial your own extension number (i.e., the source).
3. Dial Call Forwarding Type:
2 = All Calls
3 = Outside calls only
4 = Intercom calls only
4. SPK (or hang up at SLT) if you dialled 888 in step 1.
Your Call Forwarding (Station) Programmable Function Key flashes when Call Forwarding is activated.

To cancel Call Forward Follow Me:
1. At system phone, press Speaker and dial 888.
OR
Press Call Forward (Station) key (SC 851: 15).
OR
At an SLT, lift handset and dial 888.
2. Dial 0.

3. SPK (or hang up at SLT) if you dialled 888 in step 1.
Your Call Forwarding (Station) Programmable Function Key goes out.

Camp On

With Camp On, an extension user may call a busy extension and wait in line (Camp-On) without hanging up.
The call goes through when the busy extension becomes free. Camp On helps extension users to get through as soon as a busy extension becomes free. It also lets callers wait in line for a busy extension without being forgotten.
When you have set Camp-On you can choose to wait off hook or go on hook. If you go on hook your phone will ring when the extension becomes free.
With a networked system, camping on to an idle extension and Trunk Queuing/Camp On for a trunk port are not supported.
With a networked system, when Camp On is enabled, there is a slight difference in the telephone's display. With a single system, the target extension's name is displayed on the phone which has enabled Call Waiting. With a networked system, the extension number is displayed.

Operation

To Camp-On to a busy extension:
1. Call busy extension.
1. Dial Camp-On service code 850
OR
2. Press Camp-On key (SC 851: 35).
3. You can choose to hang up or not.

To cancel a Camp-On request:
1. Hang up.
2. At system phone, press Speaker and dial 870.
OR
At system phone, press Camp-On key (SC 851: 35).
OR
At single line set, lift handset and dial 870.

Caller ID Display

Caller ID information can be sent to the target extension in a networked system and show the Caller ID on the phone's display. The Abbreviated Dial Name is also shown on LCD by searching Abbreviated Dial Table at the target system.

Operation

A DDI call routed directly to a remote extension will send the Caller ID information to the remote system. The DDI name set in the system programming is also sent to the remote system.
At the remote system the Caller ID information will be displayed or, if the Caller ID number matches an Abbreviated Dial entry the Abbreviated Dial name will be displayed.
A trunk call that is first answered and then transferred to a remote extension will display the Caller ID number and the DDI name. The Abbreviated Dial name will NOT be displayed.

Central Office Calls, Placing: Seizing a trunk in a networked system

The system allows a user to seize a trunk in a networked system using the following methods:
Trunk Route Access (Dial trunk access code).
F-Route (F-Route seizes a trunk at another system).
The following are not available:
Specified Trunk Access (805 + trunk number).

Specified Trunk Group Access (804 + Trunk Group number).

Operation

The operation is automatic, the user dials the trunk access code in the normal way.
Abbreviated Dial numbers will follow the trunk routing if set to TRG 0. For AspireNet ensure that the VOIPU 'trunk' ports are in their own trunk group, do not create a trunk group with a mix of VOIP trunk ports and any other trunk port type.
VOIP trunk ports should not be seized directly via line keys or trunk access (SC 9, 805 or 804).

Conference

The user can create a Conference call to include a user in a networked system.

Operation

To establish a Conference:
Keyphone
1. Establish Intercom or trunk call.
2. Press CONF or Conference key (SC 851: 07) or press HOLD and dial 826.
3. Dial extension you want to add.
OR
Access outside call
OR
Retrieve call from Park orbit.
To get the outside call, you can either press a line key or dial a trunk/trunk group code.
You can optionally go back to step 2 to add more parties to your Conference.
4. When called party answers, press CONF or Conference key twice or HOLD key twice.
If you cannot add additional parties to your Conference, you have exceeded the system's Conference limit.
5. Repeat steps 2-4 to add more parties.

Single Line Telephone
1. Establish Intercom or trunk call.
2. Single Line Set
Hook flash and dial 826.
3. Dial extension you want to add.
OR
Access trunk call.
OR
Retrieve call from Park orbit.
4. Hook flash and repeat step 3 to add more parties.
OR
Hook flash twice to set up the Conference.
If you cannot add additional parties to your Conference, you have exceeded the system's Conference limit.

Department Calling

Department Group access is available via Networking. When the extension at System A tries to make a Department Call to System B, System A should have a numbering plan which defines the Department Access code at System B.

The following Department Calling options are supported with the Networking feature.

- Department Calling Cycle
- Department Routing When Busy

The following options are not available

- Hunting Mode No
- All Ring Mode When a call is transferred to a Department Group with All Ring, there is a difference

in operation. In a single system, an extension within the same system can transfer a call to a Department Group and the call will ring an extension within the Department Group once the transferring user hangs up. In a networked system, the transfer will not go through and the call will recall the extension performing the transfer.

- STG Withdraw Mode
- Call Recall Restriction for STG
- Maximum Queuing Number
- Enhanced Hunting Mode

Operation

1. When dialling the Department access code for the networked system, the call is dialled in the same way as normal.

Department Step Call

After calling a busy Department Calling Group member in a networked system, an extension user can have Department Step Calling Quickly call another member in the group.

Operation

To make a Step Call:
You step through Extensions within a Group.
1. Place call to busy Department Group member.
OR
Place call to Department Group pilot number.
2. Press Step Call key (SC 851: 36).
3. Repeat step 2 to call other Department Group members.

Direct Inward Dialling (DDI)

An incoming DDI call can be routed to an extension in a networked system.

Operation

For incoming DDI calls, the system uses DDI programming to determine how to route the call. If the extension number is determined to be in the networked system, the call will be routed to the appropriate system node.
It is possible to route to a Department Group Pilot number at a remote system.
It is not possible to route a DDI call to an IRG at the remote system.
The timer values are determined at the system for the incoming trunk.

Direct Inward Line (DIL)

A Direct Inward Line (DIL) is a trunk that rings an extension, virtual extension or Department Group directly. The DIL trunk can call an extension at a networked system, if the DIL trunk is set to route to an extension number at the other system.

Operation

1. An outside caller places a call to a DIL trunk.
2. The call will be routed to the networked system if the DIL target is defined as an extension at another system.

Direct Inward System Access (DISA)

Networking allows DISA callers to place a call to an extension in a networked system. Some system features can also be accessed from the networked system. The Class of Service is determined by the password entered by the DISA caller. The password table is referred to by the system on the incoming

trunk side.
The Networking feature allows the following DISA Class of Service Options.

- Trunk Route Access
- Operator access
- External Paging

The following are not available.

- Trunk Group Access
- Common Abbreviated dialling
- Internal Paging
- Specified trunk access
- Forced trunk disconnect
- Call Forward setting
- Break In

Operation

To place a DISA call into the system:
1. Dial the telephone number that rings the DISA trunk.
2. Wait for the DISA trunk to automatically answer with a unique dial tone.
3. Dial the optional 6-digit DISA password.
4. Wait for a second unique dial tone (if password was required).
5. Dial an extension number.

OR
Dial 9 for Trunk Group Routing or ARS.
OR
Dial Alternate Trunk Route Access Code (if enabled).
OR
Dial 805 + a trunk number (1-200) for an outside call.
OR
Dial 0 for the operator.
OR
Dial 803 + an External Paging Zone number (1-8 or 0 for All Call).
If the received digits are analysed as a networked extension number, the call is routed to the appropriate system within the network.

Hold

This feature is available with no changes in programming or operation.
The MOH tone is sourced at the local system where the caller is hearing the hold tone. For example a user at System A places a call to system B and puts the call on hold, the MOH source at system B will be heard by the held user.
Whilst the caller is on hold the network speech path will be reserved, waiting for the call to be taken off hold.

Direct Station Selection (DSS)

An extension user can have a DSS key to a networked extension. The DSS console keys can display the status lamp indication of an extension in a networked system.
The key will show the status for idle, busy, DND set and Call Forward Immediate set.
Lamp status may not be updated immediately. Status will be updated in the time interval specified in system programming, this setting should be consistent at all connected sites.
The status for ACD extensions or Virtual extensions will not be sent via AspireNet. It is still possible to have a DSS key for an ACD or Virtual extension but it will not show any BLF information, the key can only be used to call the extension.
The basic status for a Hotel extension is sent via AspireNet e.g. idle, busy, DND set, Call forward set. The Hotel room status is not sent e.g. check in/out, room status etc.

Operation

To Set a Function Key to your Hotline partner:
1. Press Speaker to go off hook.
2. Dial service code 851.
3. Press Hotline key + partner’s extension number + HOLD.
To place a call to your Hotline partner:
1. Press Hotline key
You can optionally lift handset after this step for privacy.

To transfer your outside call to your Hotline partner:
1. Press Hotline key.
2. Announce call and press the Transfer button.
OR
Press Transfer to have the call wait at your Hotline partner unannounced.
If unanswered, the call recalls like a regular transferred call.

To answer a call from your Hotline partner:
1. If you hear two beeps, speak toward phone.
OR
2. If your telephone rings, lift handset.
Calling an extension from your 110 button DSS Console:
1. Press EXT.1 or EXT.2 to select the range.
2. Press DSS Console key.
If the call voice-announces, you can make it ring by dialling 1.
If you don’t have Handsfree, you must lift handset to speak.

Intercom

An extension user can make an intercom call to a networked system if the networked extensions are defined in system programming.
A user can change the signalling type for the intercom call they place to either a voice announce or ringing call when calling an extension in a networked system.

Operation

To place an Intercom call:
1. At system phone, press Speaker.
OR
At single line telephone, lift handset.
2. Dial extension number (or 0 for your operator).
Your call may voice-announce or ring the called extension. Dial 1 to change the way your call alerts the called extension.
If the extension you call is busy or doesn’t answer, you can dial another extension without hanging up.

Keep Alive Operation

The Keep Alive operation will check that the distant end is available. A message is sent that the distant end must respond to, if no response is received the line will be taken out of service.

Operation

The response to the keep alive message is automatic.
The generation of the keep alive message is set in system programming. If the timer is set to 0 the keep alive generation is turned off.
The retry count for a keep alive message that is not responded to is also set at the originating system.
The line will be placed back in service when the line is active and a keep alive message is responded to.
The keep alive operation will only take place if the message is sent and not responded to by the distant

end, if the message is not sent (for example if the Ethernet cables are unplugged from the system) then the keep alive operation will not take place.
When the keep alive operation occurs the link will be taken out of service:

- Any calls that are in progress will be released.
- Park Hold orbits will be released.
- No further Park Hold information will be sent until the link is active.

Last Number Redial

Last Number Redial allows an extension user to quickly redial the last number dialled. When used with a networked system, the system can use the same trunk route on which the call was originally placed, even if the trunk is a trunk in another system.

Operation

To redial your last call:
1. Without lifting the handset, press Redial.
The last dialled number is displayed.
2. To redial the last number, press #.
OR
Search for the desired number from the Redial List by pressing the LND or VOLUME UP or VOLUME DOWN keys.
3. Lift the handset or press Speaker to place the call.
The system automatically selects a trunk from the same group as your original call and dials the last number dialled.
OR
1. At system phone, press idle line key (optional).
The system automatically selects a trunk from the same group as your original call.
2. Press Redial.
OR
1. At system phone, press Speaker.
OR
At single line telephone, lift handset.
2. Dial 816.
The system automatically selects a trunk from the same group as your original call and dials the last number dialled.

Message Waiting

This feature can be used when placing an intercom call to a networked extension and you receive either no answer or a busy tone.
With a networked system, when a Message Waiting has been left, there is a difference in the telephone’s display. With a single system, the extension’s name which left the message is displayed. With a networked system, the extension number is displayed.

Operation

To leave a Message Waiting:
1. Call busy or unanswered extension.
2. Dial the Message Waiting service code 841
OR
3. Press Message Waiting key (SC 851: 38)
4. Hang up. With keyphones, the MW LED lights.

To answer a Message Waiting:
At keyphones when you have a message your MW LED flashes fast.
1. At a keyphone, press Speaker and dial 841.
OR

Press Message Waiting key (SC 851: 38).
OR
At single line telephones, lift the handset and dial 841.
Normally, your MW LED goes out. If it continues to flash, you may have new messages in your “Voice Mail” mailbox or a new “General Message”.

Operator, Centralised

It is possible to have a centralised network operator extension that can be dialled with the operator access code (0).
Calls to the operator will be queued and answered in order. Up to 32 calls can be queued at the operator extension. The quantity of network calls that can queue at the operator may be limited by the quantity of networking channels available.

Operation

The network numbering plan must be set up to route the operator access code (0) to the system that has the operator extension.
The operator extension must be set in system programming.

If the operator’s extension is connected to system A the following settings are required:

- At System A the required extension must be set as the operator extension.
- At system A dial 0 must be set as Operator.
- At system B dial 0 must be set as Networking System Access and routed to the node ID of System A.
- Users at System A and B can access the operator by dialling 0.

Paging

An extension user can make internal or external pages to a networked system. Paging to a networked system can only be activated by dialling a service code and the target network’s system ID.

Operation

To Make an Internal Page
1. Dial 801.
2. Dial # and the system ID (01 to 50).
The system ID must be dialled as 2 digits (ex: #02).
3. Dial the Paging Zone number (00-64).
Dialling 00 calls All Call Internal Paging.
4. Make announcement to the networked system.
5. Press SPK to hang up.

To Make an External Page
1. Dial 803.
2. Dial # and the system ID.
The system ID must be dialled as 2 digits (ex: #02).
3. Dial the Paging Zone number (0-9).
Dialling 0 calls All Call External Paging.
4. Make announcement to the networked system.
5. Press SPK to hang up.

To Make a Combined Page
1. Dial 751.
2. Dial # and the system ID.
The system ID must be dialled as 2 digits (ex: #02).
3. Dial the Paging Zone number (0-9).
Dialling 0 calls All Call Combined Paging.

4. Make announcement to the networked system.
5. Press SPK to hang up.

Park

Park places a call in a waiting state (called a Park Orbit) so that an extension user may pick it up.
Any extension user who is in the same Park Group as the extension which placed the call in Park can answer the call.
This includes extension users in a networked system. For example, when an extension user in Park Group 3 within System A places a call in Park, the extension users in Park Group 3 at any connected system can retrieve the call by pressing the flashing park key or dialling a service code.
If you do not want the park hold orbits to be available to other users within the network then place the extension at each site in a different park hold group.

With a single system, when two users within the same Park Group try to place a call in the same park orbit at the same time, one user will get the orbit while the other user’s call will either ring back or it will remain an active call, depending on how the park orbit was accessed. With AspireNet, if both users try to access the same orbit, one user will get the orbit, while the other will hear ring back, at which time they can park the call in a different orbit.

Operation

To Park a call in a system orbit:
You can Park Intercom or trunk calls.
1. Press Park key (SC 852: *04 + orbit).
The Park key LED lights.
If you hear busy tone, the orbit is busy. Try another orbit.
2. Use Paging to announce call.
3. Press SPK to hang up.
If not picked up, the call will recall to you.
OR
1. At system phone or 2-Button telephone, press HOLD.
OR
At a SLT single line telephone, hook flash.
2. Dial 831 and the Park orbit (1-64).
If you hear busy tone, the orbit is busy. Try another orbit.
3. Use Paging to announce call.
4. Press SPK to hang up.
If not picked up, the call will recall to you.
Note: The parked call recalls after the Park Hold Timer.

To pick up a parked call:
1. Lift handset.
2. Press Park key (SC 852: *04 + orbit).
OR
1. At system phone or 2-Button telephone, press idle CALL key.
OR
At single line telephone, lift handset.
2. Dial 861 and the Park orbit (1-64).

Ringdown Extension, Internal/External (Hotline)

A networked system can have a phone defined as a Ringdown Extension to dial either an internal or external number.

Operation

To place a call if your extension has ringdown programmed:

1. Lift handset.
If you want to place a trunk call, press a line key before lifting the handset.
Depending on the setting of your ringdown timer, you may be able to dial an Intercom call before your ringdown goes through.
If the destination has Handsfree Answerback enabled, your call will voice announce.
If the destination has Forced Intercom Ringing enabled, your call will ring.

Selectable Display Messaging

An extension user can select a pre-programmed Selectable Display Message for their extension.
This message will be displayed on an incoming intercom caller's keyphone display when they call the extension in a networked system.

Operation

To select a message:
1. Press Speaker + dial 713.
OR
Press Call Forward (Device) key (SC 851: 17).
OR
Press Speaker + press Text Message key (SC 851: 18) + enter digits to append, if needed + Speaker to hang up. Skip the remaining steps.
2. Dial 3 + Message number (01-20).
Use VOL UP or VOL DOWN to scroll through the messages.
3. (Optional for messages 1-8 and 10)
Dial the digits you want to append to the message.
You can append messages 1-8 and 10 with digits (e.g., the time when you will be back).
You enter the time in 24-hour format, but it displays in 12-hour format.
4. Press Speaker to hang up.

To cancel a message:
1. Press Speaker + dial 713.
OR
Press Call Forward (Device) key (SC 851: 17).
OR
Press Speaker+ press Text Message key (SC 851: 18) + Speaker to hang up.
2. Dial 3.
3. Press Speaker to hang up.

Toll Restriction

Toll Restriction limits the numbers an extension user may dial. When accessing a trunk at another system the Toll Restriction Class of Service is defined by the calling extension's system, but the Toll Restriction tables will be used from the system which has the outgoing trunk. The Toll restriction class number is sent to the other system, the other system will use the class number to define the Toll Restriction tables to use. Since the restriction table is used for the system which has the outgoing trunk, the definition of the Class of Service may be different, unless all Toll Restriction Classes of Service and Toll Restriction Tables are defined the same between systems.

Operation

Example:
The extension user in System A, which has a Toll Restriction Class 2, dials an outside party after seizing a trunk from a networked system (System B). The dialled digits are compared to the Class 2 Restriction Table in System B. The call is then either allowed or rejected based on this table.

Transfer

The following types of Transfer are available with Networking:

- Screened Transfer
- Unscreened Transfer
- Transfer to busy extension

Operation

Transferring Trunk Calls

To Transfer a trunk call to a co-worker’s extension:
1. At system phone or 2-Button telephone, press HOLD.
OR
At a single line telephone, hook flash.
You hear Transfer dial tone.
2. Dial co-worker’s extension number.
If the extension is busy or doesn’t answer, you can dial another extension number or press the line key to return to the call.
SLT users can retrieve the call by pressing hook flash. If a call has been transferred and the SLT user has hung up the handset, the call be can retrieved by dialling 715 and the extension number to which it had been transferred.
3. Announce call and hang up.
If you don’t have Automatic On Hook Transfer, you must press CONF or your Transfer Programmable Function Key to Transfer the call.
If your co-worker doesn’t want the call, press the flashing line key to return to the call.
SLT users can retrieve the call by pressing hook flash. If a call has been transferred and the SLT user has hung up the handset, the call be can retrieved by dialling 815 and the extension number to which it had been transferred.
If you don’t want to screen the call, hang up without making an announcement.

Transferring to a busy extension

Will require the Transfer to Busy Extension option enabled in system programming at the originating system and the target system.
1. Dial the co-worker’s extension number.
Busy tone is heard.
2. Press the Transfer button.
3. The call will wait for the busy co-worker to become free and then will ring.

Transferring Intercom Calls

To Transfer your Intercom call:
1. At system phone, press HOLD.
OR
At single line telephone, hook flash.
2. Dial extension to receive your call.
If the extension is busy, doesn’t answer or does not want the call, you can dial another extension number or press the lit CALL key to return to the call. In addition, you may be able to transfer the call to the busy extension.
SLT users can retrieve the call by pressing hook flash. If a call has been transferred and the SLT user has hung up the handset, the call be can retrieved by dialling 715 and the extension number to which it had been transferred.
3. Announce your call and hang up.
With Automatic On Hook Transfer When you hang up, the call is automatically transferred.
Without Automatic On Hook Transfer You must press your Transfer Programmable Function Key to Transfer the call.
To Transfer the call unscreened, press your Transfer Programmable Function Key and hang up without making an announcement.

2.6.3 SIP Trunking

SIP Trunking

SIP (Session Initiation Protocol) is a protocol used for Voice over IP. It is defined by the IETF (Internet Engineering Task Force) in RFC3261. The SV9100 can use SIP to connect to another SV9100 system, an Aspire, an XN120 or a third party SIP enabled product.

SIP can also be used to provide external trunks to the SV9100 from ITSP's (Internet Telephony Service Providers).

The SV9100 must be 'certified' to connect to a particular ITSP or PBX, there is a list of certified carriers available, please refer to your support partner for more information.

From the SV9100's point of view there are two types of SIP Trunks, 'Networking Mode' and 'Carrier Mode'.

Each system in the network must have:

- GCD-CP10
- GPZ-IPLE
- IP Trunk License(s)

Networking Mode

This mode is *usually* used to connect to other NEC systems (SV9100, SV8100, Aspire, XN120) using SIP although some SIP Carriers use this mode to provide external SIP Trunks. The systems connect to each other using an internal routing table. The call is always attempted even if the remote end point is down. Each system does not know the state of the other because there is no registration procedure.

If this method is used to connect to an ITSP, the customer's public IP address will be used as a security measure.

Carrier Mode

This mode is *usually* used to connect the SV9100 to an ITSP to provide external SIP Trunks. The SV9100 uses the customer's internet connection to register to the ITSP's SIP server (although some ITSP's provide a dedicated circuit just for voice).

The SV9100 registers to the ITSP using a User ID and Password for security, this registration is constantly maintained. If the registration is lost the trunk ports will return busy tone allowing an overflow trunk group to be utilised.

Network Address Translation (NAT)

NAT will cause a problem for SIP Trunks if the SV9100 has been assigned private IP addresses. The problem is that the SV9100's IP address is embedded in the SIP signalling messages which cannot be manipulated by the NAT router. The NAT router can only change the IP header information.

When an outgoing packet arrives at a SIP server, the SIP server reads the SV9100 IP address from the SIP information which will be an internal private IP address. This address is not routable on the Internet resulting in communication problems.

This problem is resolved by entering the public IP address in the SIP signalling messages instead of the private IP address. This is done by enabling the **NAPT Router** option and entering the Public IP address of the router using **NAPT Router IP Address** on either of the pages below depending on the mode being used.

Networking Mode - *Easy Edit – Advanced Items/VoIP/SIP Networking/Profile x/SIP Profile x - Networking Mode/SIP Profile x - Server Setup (PRG10-12-07,10-29-21)*
Carrier Mode (IP Address) - *Easy Edit – Advanced Items/VoIP/SIP Networking/Profile x/SIP Profile x - Carrier Mode (IP Address)/SIP Profile x - Server Setup (PRG10-12-07,10-29-21)*
Carrier Mode (Domain Name) - *Easy Edit – Advanced Items/VoIP/SIP Networking/Profile x/SIP Profile x - Carrier Mode (Domain Name)/SIP Profile x - Server Setup (PRG10-12-07,10-29-21)*

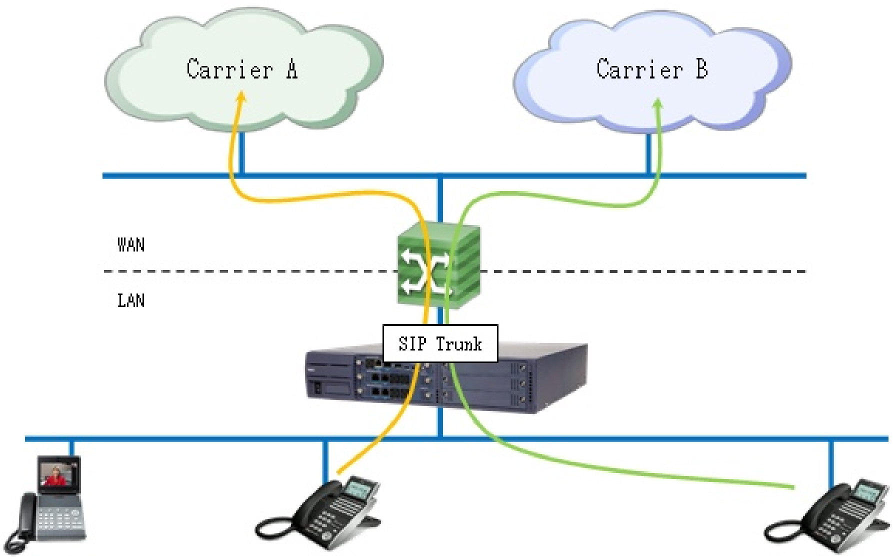
Port forwarding will also be required in the customer's router.
Forward the SIP Signalling port (default UDP/5060) to the GPZ-IPLE IP address. *(PRG10-12-09)*
Forward the RTP port range (default UDP/10020 -> 10275 (depending on GPZ-IPLE size)) to the VoIP Gateway IP addresses. *(PRG84-26)*

Port Forwarding Example (Default Settings)

Port Number (UDP)	Destination IP Address (GPZ-IPLE)	Description (GPZ-IPLE)
5060	172.16.0.10	GPZ-IPLE (Signalling)
10020 – 10532	172.16.0.20	VoIP Gateway (RTP)

SIP Multi Carrier Support

The SV9100 can now be configured with up to six SIP profiles so that a single system can be used to connect to both an external SIP carrier (ITSP), and at the same time use a System Interconnection to another SIP compatible PBX such as an SV8100 system. Alternatively a single system could be configured to connect to multiple external SIP carriers if required for redundancy.



Conditions

- SIP Multi Profiles must be configured with unique SIP Port numbers per profile. i.e. Profile 1 could use the default SIP port 5060 and Profile 2 could be configured to use 5061 etc.
- SIP Multi Profile carrier configurations must be reachable through the same IP gateway. i.e. the default gateway in PRG 10-12-03 must be able to route traffic to the carrier configured in Profile 1 and also be able to route traffic to the carrier configured in Profile 2.
- SIP Multi Profile carrier configurations must be reachable through the same DNS server settings.
- For SIP Multi Profile programming areas you will now require an index selection as to whether Profile 1 or Profile 2 is to be configured.

PRG	Name	Note
10-28	SIP System Information Setup	Index added. Select Profile 1-6.
10-29	SIP Server Information Setup	IIndex added. Select Profile 1-6.
10-36	SIP Trunk Registration Information	Index added. Select Profile 1-6.
15-16	SIP Register ID Setup for Extension	Index added. Select Profile 1-6.
21-19	IP Trunk (SIP) Calling Party Number Setup for Extensions	IIndex added. Select Profile 1-6.
84-13	SIP Trunk CODEC Information Setup	Index added. Select Profile 1-6.
84-14	SIP Trunk Information Basic Setup	Index added. Select Profile 1-6.
84-31	VoIPDB Echo Canceller Setup	Index added. Select Profile 1-6.
84-33	FAX over IP Setup	IIndex added. Select Profile 1-6.
84-34	VoIPDB DTMF Setup	Index added. Select Profile 1-6.
84-38	VoIPDB Network Side Echo Canceller	Index added. Select Profile 1-6.
84-39	SIP Trunk Message Customization	IIndex added. Select Profile 1-6.

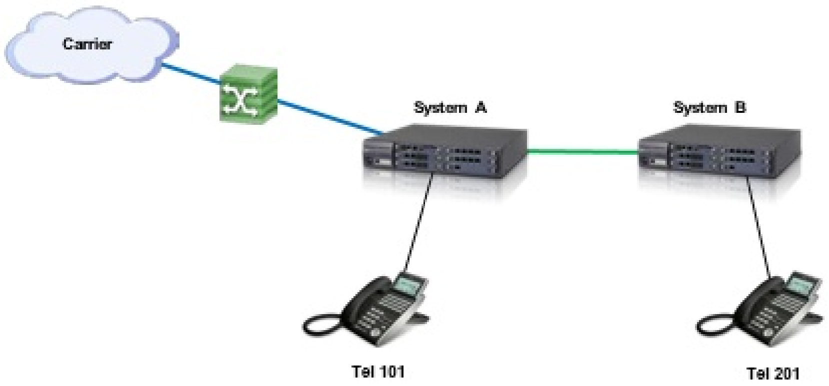
Licenses

- BE114065 SIP Trunk LIC, (5001). Port license

Example Usage

SIP Carrier and System Interconnection

SIP Trunks are assigned to System A. The number of ports available are 16 ports. Profile 1 is port 1-8. Profile 2 is port 9-16. Profile 1 is connected to a SIP carrier. Profile 2 is a SIP System Interconnection (System B).When the user in system A makes an outbound call, the ARS service will be used. When the user dials "050", the SIP carrier will be selected, and dials "2@@", SIP System Interconnection will be selected.



System A Configuration

IP Settings

PRG	Name	Data
10-12	CCPU Network Setup	Default Gateway = 172.16.10.254 NAT Route = 1(Yes) Default Gateway(WAN) = 10.1.1.254 IP Address (VoIP) = 172.16.10.10 Subnet Mask (VoIP) = 255.255.0.0
84-26	VoIPDB Basic Setup	Slot #1: IP Address = 172.16.10.20

System Numbering Plan

PRG	Name	Data
11-01	System Numbering	Dial 1: 3 digits, Extension Access Dial 0: 1 digits, Trunk Access
11-02	Extension Numbering	- Port 1-32: Extension Number = 101-132
11-09	Trunk Access Code	Trunk Access Code = 0
26-01	Automatic Route Selection Service	ARS Service = 1(Enable)
26-02	Dial Analysis Table for ARS/ LCR	- Table 1 Dial = 050 Service Type = 1(TRG) Additional Data = 3 - Table 2 Dial = 2 Service Type = 1(TRG) Additional Data = 5

IP Trunks

PRG	Name	Data
10-23	IP System Interconnection Setup	- System No: 1 System Interconnection = 1 IP Address = 172.16.20.10 Dial = 2
10-28	SIP System Information Setup	- SIP Profile 1 Domain Name = xxx.xxx.ne.jp Host Name = xxxxx Domain Assignment = 1(Domain) - SIP Profile 2 none

10-29	SIP Server Information Setup	- SIP Profile 1 Default Proxy = 1(On) Register Mode = 1(Manual) Domain Name = xxx.yyy.zzz.ne.jp Carrier Choices = 1(Carrier A) - SIP Profile 2 Default Proxy Port Number = 5062 Carrier Choices = 0(Standard)
10-36	SIP Registration Information Setup	- SIP Profile 1, Register ID 0 Registration = 1(On) User ID = v123456 Password = xxxxxxxxxx - SIP Profile 2, Register ID 0 Registration = 1(On) User ID = 100
10-40	IP Trunk Availability	- Index 1 Trunk Type = 1 (SIP) Start Port = 1 Number of Ports = 16
10-29	SIP Server Information Setup	- SIP Profile 1(Fixed) DNS Mode = 1(On) DNS IP Address = 172.16.10.254
14-05	Trunk Group	- Port: 1-8 Group = 3 - Port: 9-16 Group = 5
14-18-05	IP Trunk Data Setup	Port: 1-8 SIP Profile = 1(Profile 1) Port: 9-16 SIP Profile = 2(Profile 2)
22-02	Incoming Service Type Setup	Port: 1-8, Day/Night Mode: 1-8 Service Type = 3(DID) Port: 9-16, Day/Night Mode: 1-8 Service Type = 5(Tie Line)
84-14-06	SIP Trunk Basic Information Setup	- SIP Profile 1 SIP Trunk Port Number = 5060 - SIP Profile 2 SIP Trunk Port Number = 5062

System B Configuration

IP Settings

PRG	Name	Data
10-12	CCPU Network Setup	IP Address (VoIP) = 172.16.20.10 Subnet Mask (VoIP) = 255.255.0.0
84-26	VoIPDB Basic Setup	Slot #1: IP Address = 172.16.20.20

System Numbering Plan

PRG	Name	Data
11-01	System Numbering	Dial 2: 3 digits, Extension Access Dial 0: 1 digits, Trunk Access
11-02	Extension Numbering	- Port 1-32: Extension Number = 201-232
11-09	Trunk Access Code	Trunk Access Code = 0
26-01	Automatic Route Selection Service	ARS Service = 1(Enable)
26-02	Dial Analysis Table for ARS/LCR	- Table 1 Dial = 1 Service Type = 1(TRG) Additional Data = 5

IP Trunks

PRG	Name	Data
10-23	IP System Interconnection Setup	- System No: 1 System Interconnection = 1 IP Address = 172.16.10.10 Dial = 1
10-36	SIP Registration Information Setup	- SIP Profile 1, Register ID 0 Registration = 1(On) User ID = 200
10-29	SIP Server Information Setup	- SIP Profile 1 Default Proxy Port Number = 5062 Carrier Choices = 0(Standard)
10-40	IP Trunk Availability	- Index 1 Trunk Type = 1 (SIP) Start Port = 1 Number of Ports = 8
14-05	Trunk Group	- Port: 1-8 Group = 5
14-18-05	IP Trunk Data Setup	Port: 1-8 SIP Profile = 1(Profile 1)
22-02	Incoming Service Type Setup	Port: 1-8, Day/Night Mode: 1-8 Service Type = 5(Tie Line)
84-14-06	SIP Trunk Basic Information Setup	- SIP Profile 1 SIP Trunk Port Number = 5062

TEL 101 makes outbound call to SIP carrier

No.	Operation	LED	Tone	LCD 123456789012345678901234	Note
1	Off Hook		DT	Clock/Calendar Soft key	
2	Dial "0" + "050"	LK01(G)ON	NT	Line 001 050 Soft key	
3	Dial "12345678"	LK01(G)ON	RBT	Line 001 05012345678 Soft key	

TEL 101 makes outbound call to SIP carrier

No.	Operation	LED	Tone	LCD 123456789012345678901234	Note
1	Off Hook		NT	Clock/Calendar Soft key	
2	Dial "0" + "2"	LK09(G)ON	NT	Line 009 2 Soft key	
3	Dial "01"	LK09(G)ON	RBT	Line 009 201 Soft key	

SIP Trunk Codec

Easy Edit – Advanced Items/VoIP/SIP Networking/Profile x/SIP Profile x - Trunk General Settings

SIP Trunks can use various CODECs. A CODEC is a standard for converting an analogue signal to digital. This conversion process is handled by the DSP (Digital Signal Processors) on the GPZ-IPLE card.

Each CODEC has different voice quality and compression properties. The correct choice of CODEC will be based on the amount of bandwidth available, the amount of calls required and the voice quality required.

Available Codecs for SIP Trunks

- G.711 64Kbps codec MOS 4.4
- G.722 64Kbps codec MOS 4.4
- G.726 32Kbps codec MOS 4.2
- G.729 8Kbps codec MOS 4.0

The bandwidth values quoted for these codec's are for the digitized speech in one direction only. The actual bandwidth required for a call will depend on many other factors and will be much higher than these figures.

The above MOS values are quoted for ideal network conditions. The value could be lower depending upon the network performance.

To change the codec in use for SIP Trunks network use the ***Audio Capability Priority*** setting in *Easy Edit – Advanced Items/VoIP/SIP Networking/Profile x/SIP Profile x - Trunk General Settings/SIP Profile x - CODEC Settings (PRG84-13-28)*

DTMF Relay (RFC2833)

By default any DTMF tones transmitted across SIP Trunks will be sent as audio tones in the speech path. It is possible that these tones can be misinterpreted by the receiving device because of packet loss or errors due to the codec compression.

DTMF relay is a way of converting the DTMF tone into a signal then sending the signal across the IP network instead of the actual tone.

To enable this feature set the **DTMF Relay Mode** option to **RFC2833** in *Easy Edit – Advanced Items/VoIP/SIP Networking/Profile x/SIP Profile x - Trunk General Settings/SIP Profile x - DTMF Settings (PRG84-34-01)*

T.38 Fax Relay

SIP Trunks have the ability to communicate using the T.38 Fax Relay protocol.

By default any Fax tones transmitted to or from a SIP Trunk will be sent as audio tones in the speech path. It is possible that these tones can be misinterpreted by the receiving device because of packet loss or errors due to the codec compression.

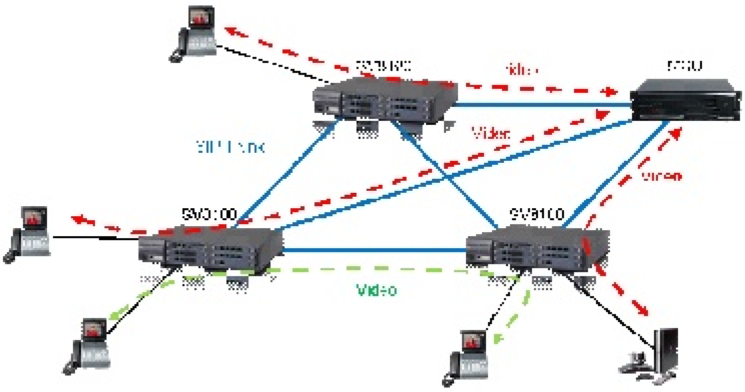
T.38 Fax Relay is a way of converting the Fax tones into a signal then sending the signal across the IP network where the signals are converted back to Fax tones.
The SIP Carrier or Server must support T.38 for this to work.

Enable Fax Relay by using the 'Fax Relay Mode' option in *Easy Edit – Advanced Items/VoIP/SIP Networking/Profile x/SIP Profile x - Trunk General Settings/SIP Profile x - FoIP Settings (PRG84-33-01).*

There are several other options to do with T.38 Fax relay that can also be found on the same page. These commands would usually be left at the default settings but may occasionally need altering depending on the SIP Carrier/Server, fax machine and network connection.

Peer to Peer Video Support over SIP Trunk

Peer to Peer video calls via SIP Trunk Interconnection are available for SIP video devices. Additionally, SIP trunk interconnection allows the SIP video device to access a Multi-Point Control Unit (MCU) to provide video conferencing over multiple SV9100 systems.



Benefits

Users can make video calls within their SV9100 wide area network.
Required Software and Hardware

- BE114065 SIP Trunk LIC, (5001). Port license
- BE114054 SIP Terminal LIC, (5111). Port license

The following example configuration is used to illustrate what is required to be configured to enable this feature.

Programming Commands	Values	Command Description
14-18-01 IP Trunk Type	0=None 1=SIP 2=H.323 3=CCIS (default=0)	This item is read only and will show the IP trunk type setup in CMD 10-03 Type 1=SIP is required for video support.
14-18-02 System ID (SIP Only)	(0-50) (default = 0)	This item is read only and will show the NetLink system ID when multi SIP trunk with NetLink is enabled.
14-18-03 P2P Mode (SIP Only)	0=disable 1=enable (default=0)	This item enables the Peer to Peer feature for SIP trunk.
14-18-04 Video Mode (SIP Only)	0=disable 1=enable (default = 0)	This item enables the Video feature for SIP trunk.
14-18-05 SIP Profile	0=Profile 1 1=Profile 2 2=Profile 3	This item assigns the IP trunk to specific SIP carrier profile

	3=Profile 4 4=Profile 5 5=Profile 6	
10-29-21 NAT Router	0=Not Used 1=Used (default = 0)	This item should be disabled.
15-05-50 Peer to Peer mode	0=Off 1=On (default = 0)	This item should be enabled.
10-26-05 SIP CTI mode	0=disable 1=enable (default = 0)	This item should be disabled.

a) The video call is Peer to Peer, no DSP resources are used during the video call.

b) Only SIP Trunk interconnection within an SV9100 network is available for SIP video calls.

c) When all of the following conditions are met the SIP terminal can make a P2P video call:

Peer to Peer Setup	
10-29-21	NAT mode = Off
14-08-03	SIP Trunk P2P mode = On
15-05-50	P2P mode = On
10-26-05	SIP CTI mode = Off
SIP Video setup	
14-08-04	SIP trunk video mode = On
15-05-43	SIP video mode = On

If these conditions are not met the following type of call can be made:

SIP Trunk	Standard SIP		
	P2P: Off 14-18-03=Off	Video P2P: Off 15-05-43=Off	Video P2P: On 15-05-43=On
P2P: Off 14-18-03=Off	Voice (Not P2P)	Voice (Not P2P)	Voice (Not P2P)
Video P2P: On 14-18-04=Off	Voice (Not P2P)	Voice (P2P)	Voice (P2P)
Video P2P : On 14-18-04=On	Voice (Not P2P)	Voice (P2P)	Voice & Video (P2P)

d) When Peer to Peer is enabled in 14-18-03.

- o The user cannot hold the call
- o The user cannot transfer a call to the SIP trunk
- o When the user makes a call to the SIP trunk from a non-standard SIP terminal the call will not be P2P, a DT400/DT300 terminal will use one DSP resource for the trunk, a DT800/DT700 terminal will use two DSP resources.

e) When the user makes a video call the following limitations occur.
- o Video capability is required in the initial invite message from the SIP video terminal
- o During the call the user cannot change from video to voice call or from voice to video.
- o Peer to Peer connection is required to make a video call. So the video feature is not available with CTI/OAI applications as these need non P2P connection.

Conditions/Comments

- o SIP Peer to Peer must be enabled.
- o SIP CTI must be disabled.
- o Video communication between a Standard SIP terminal and the UC Client Softphone is not possible.
- o The SIP terminal must pass interoperability testing by NEC before it can be supported.
- o The video codec is not supported by the GPZ-IPLE card. The video codec information from the received SDP message will be forwarded to the destination terminal.
- o The communicating video terminals must support common audio and video codecs.
- o SIP Video is not supported across AspireNet or K-CCIS as the communication between the SIP terminals is not Peer to Peer.
- o Be aware of bandwidth requirements for video communication, this will be considerably higher than a voice call. Bandwidth is dependent on codec selection, frame rate and resolution. Check the manufacturer's data sheet for the relevant terminal for further details.

Connection to a Multi-Point Control Unit (MCU)

a. 'Dial in' and 'Dial out' feature is supported.
b. When connecting the MCU into the SIP Network the Carrier Type setting in CMD 10-29-14 must be 0. No other carrier type is supported for SIP Video.
c. The user has to set the same video capability for the MCU as on their video device.
d. F-Route can be used to route specified dialled numbers to the SIP trunks connected to the MCU.

SIP Certificate of Compatibility

All of the required information and programming commands for a particular SIP carrier can be found on the relevant 'SIP Certificate of Compatibility', please refer to your support partner for access to these documents.

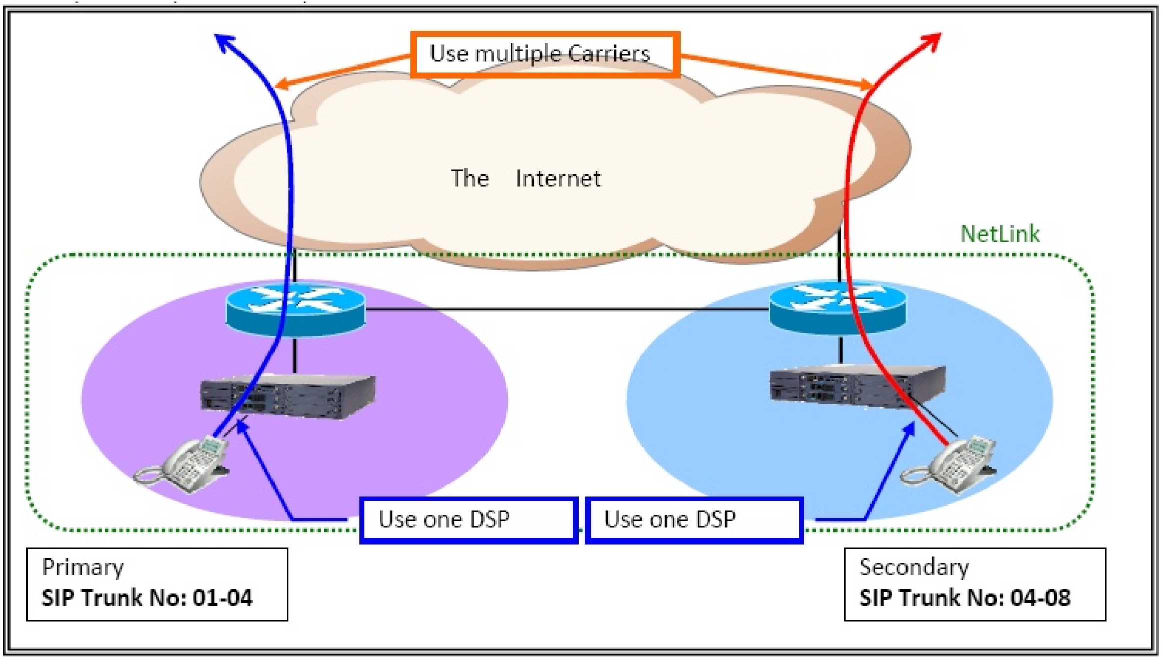
Licensing

Each SV9100 need to be licensed to use IP Trunks. One license gives that system the ability to use one IP Trunk.
Up to 256 IP Trunk licenses can be added.
Licence Code: BE114065

Netlink Multiple SIP Carriers

Description

This allows the systems to register or connect to several different SIP Carriers or SIP servers at different locations. This means that SIP trunks can be used in multiple locations.
This also means that the DSP consumption can be reduced when a SIP trunk is used by an extension on a Secondary system.
This feature can only be used when NetLink is deployed. If NetLink is not deployed only the 6 SIP carrier profiles of the single system can be configured.
The number of SIP carriers available depends on the number of NetLink nodes up to a maximum of 16. This can be a combination of Carrier Mode and Networking Mode. Each Netlink secondary node can only have one SIP Carrier configured.



Requirements

GPZ-IPLE
SIP Trunk License(s)

Capacity

Up to 400 SIP trunks can be configured across the NetLink network.

Configuration

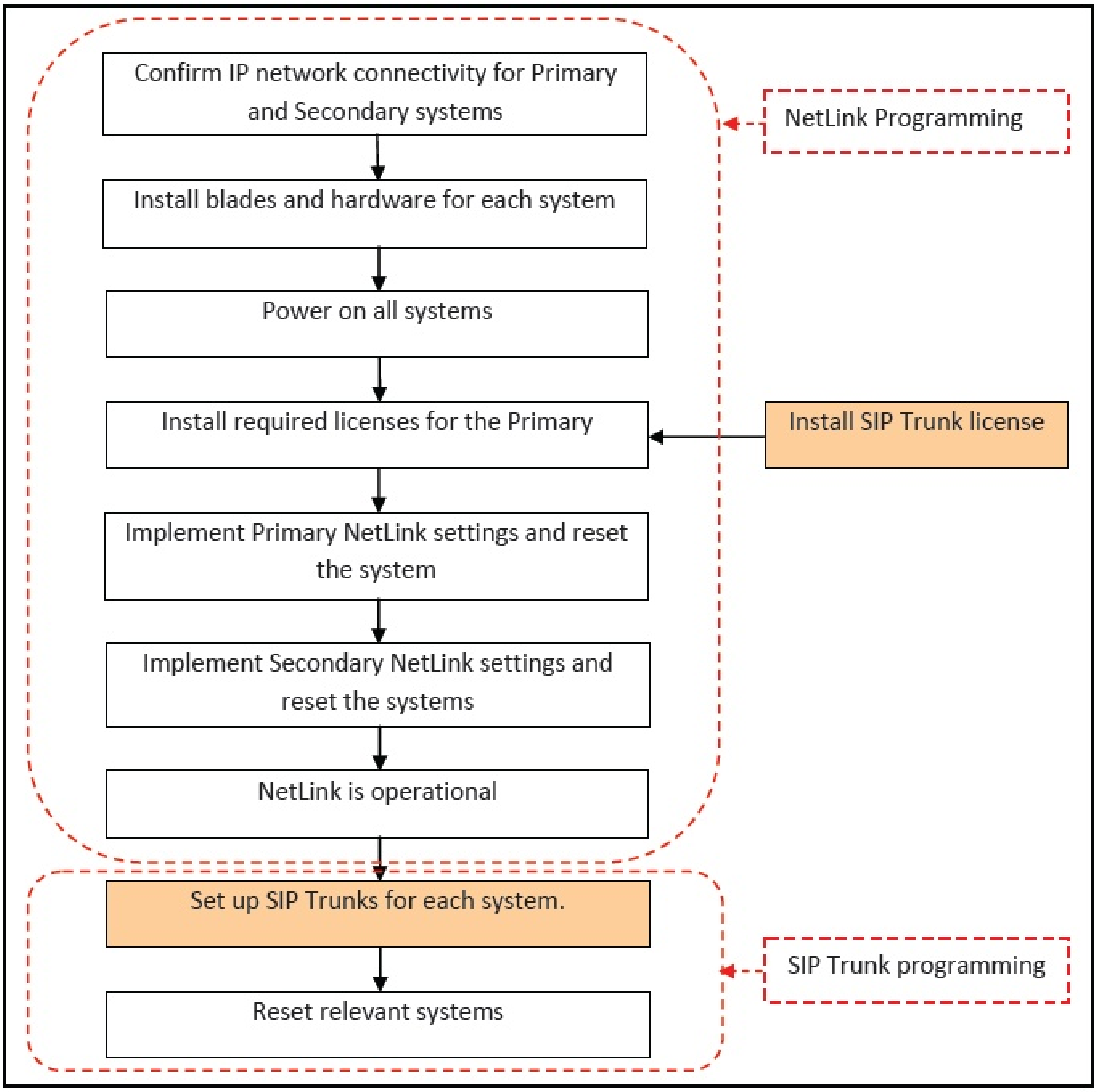
Certain commands must be programmed on the Primary system and some commands must be programmed on the relevant Secondary system.
The table below shows which commands should be programmed where.
To program a Secondary system PC Pro or Web Pro must be used by connecting directly to the specific GCD-CP10.

Programming Command	Program Primary Only	Program each Secondary	Replication (if enabled)

10-12		✓	X
10-19		✓	X
10-23		✓	X
10-26		✓	✓
10-28		✓	X
10-29		✓	X
10-36		✓	X
10-37		✓	X
10-68	✓	✓	X
14-12		✓	✓
14-18			X
15-16	✓		✓
21-17		✓	✓
21-19	✓		X
84-09		✓	✓
84-10		✓	✓
84-13		✓	X
84-14		✓	X
84-16		✓	✓
84-26		✓	X
84-27		✓	X
84-33		✓	X
84-34		✓	X
90-10	✓		✓

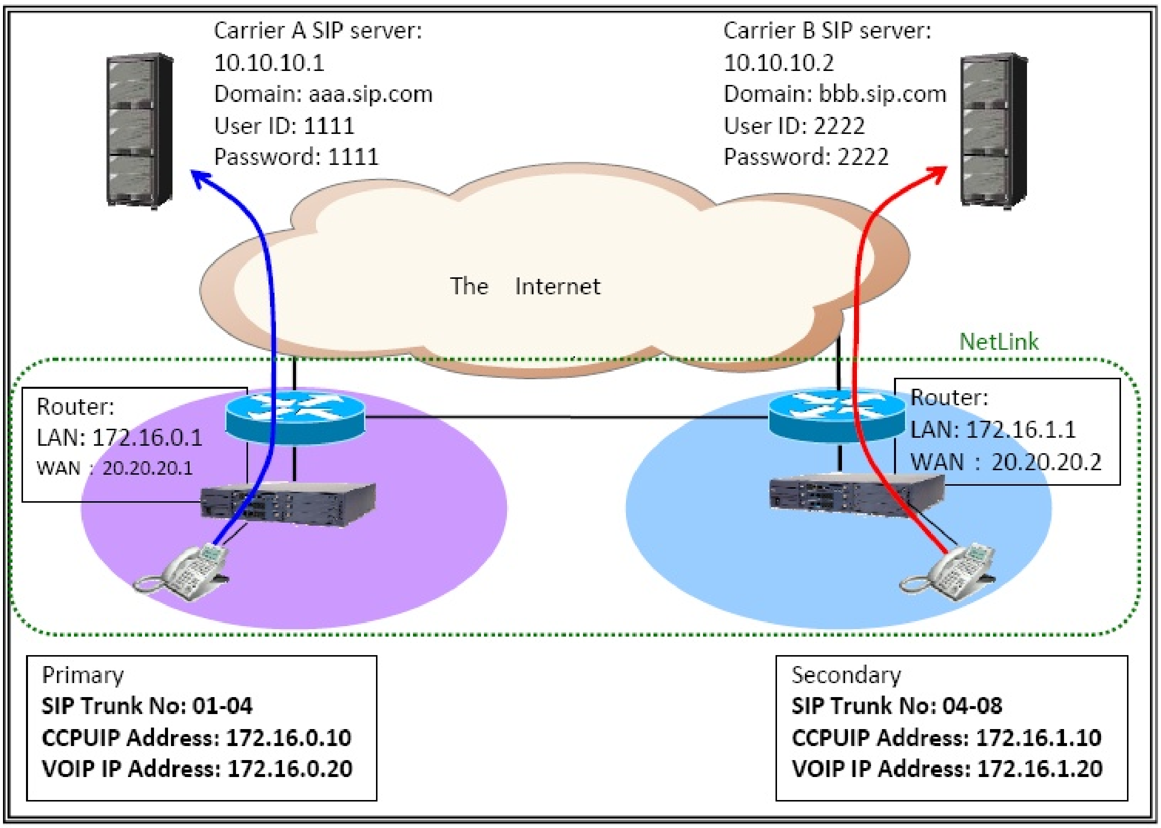
Note:
Certain command settings may be removed when NetLink is first configured if SIP trunks are already enabled. Be sure to check all SIP trunk programming after configuring NetLink.

The order of programming SIP trunks and NetLink are shown in the following table.



Example Configuration

The following programming details use the diagram below for SIP Trunk information (NetLink programming is not listed)



Primary System		Secondary System	
10-12-01	192.168.0.10	10-12-01	192.168.0.10
10-12-02	255.255.0.0	10-12-02	255.255.0.0
10-12-03	172.16.0.1	10-12-03	172.16.1.1
10-12-07	20.20.20.1	10-12-07	20.20.20.2
10-12-09	172.16.0.10	10-12-09	172.16.1.10
10-12-10	255.255.0.0	10-12-10	255.255.0.0
10-28-01	com	10-28-01	com
10-28-02	aaa.sip	10-28-02	bbb.sip
10-28-05	Domain name	10-28-05	Domain name
10-29-03	10.10.10.1	10-29-03	10.10.10.2
10-29-05	Manual	10-29-05	Manual
10-29-06	10.10.10.1	10-29-06	10.10.10.2
10-29-21	Enabled	10-29-21	Enabled
10-36-02	1111	10-36-02	2222
10-36-03	1111	10-36-03	2222
10-36-04	1111	10-36-04	2222

10-68-01	SIP	10-68-01	SIP
10-68-02	1	10-68-02	4
10-68-03	4	10-68-03	4
14-18-05	Profile 1	14-18-05	Profile 1
84-26-01	172.16.0.20	84-26-01	172.16.1.20

SIP Register ID

32 Register ID's can be programmed on each NetLink system that has SIP Trunks configured. Register ID 0 to 31 uses the User ID's programmed in PRG10-36.

Trunks

SIP Register ID's for trunks can only be applied to trunks that belong to the same system as the Register ID.

Stations

SIP Register ID's for Stations will only be applied when dialling out on a trunk from the Primary system. If a station dials out using a trunk on a Secondary system the Station Register ID is not applied.

Alarms

SIP Trunk problems can be indicated on the PC Pro alarm report and on the display of a handset (if configured).

The information below details the alarms from the DIM (alminfo), PC Pro will also show similar information:

```
LVL  NO   STAT   DATE     TIME      ITEM             UNIT      SYS  SLT  PRT  PARAMETER
----------------------------------------------------------------------------------------
MIN 0060 ERR  01/01/08 00:33 SIP Registration  Time Out   01       00
MIN 0060 ERR  01/01/08 00:33 SIP Registration  Time Out   02       00
MIN 0060 ERR  01/01/08 02:17 SIP Registration  Error      01       00  Code:400
MIN 0060 ERR  01/01/08 03:11 SIP Registration  Error      02       00  Code:400
MIN 0060 ERR  01/01/08 02:22 SIP Registration  Auth.      01       00  Code:406
MIN 0060 ERR  01/01/08 03:15 SIP Registration  Auth.      02       00  Code:406
```

The information below details the alarms shown on a display telephone (this may differ slightly depending on the size of the display):

Register Time Out Error

	Format	Key	Terminal LCD Example
NetLink Disabled	###:SIP(XX) REG REQ TIMEOUT	###:Alarm number(60) XX:Register ID(1-32) %%:System ID(1-16)	"60:SIP(05) REG REQ TIMEOUT "
NetLink Enabled	###:SIP(XX) REG TIMEOUT -%%		"60:SIP(05) REG TIMEOUT -02 "

Register Error

	Format	Key	Terminal LCD Example
NetLink Disabled	###:SIP(XX) REG FAILED($$$)	###:Alarm number (60) XX:Register ID (1-32) $$$:Err code (000-999) %%:System ID (1-16)	"60:SIP(07) REG FAILED(403) "
NetLink Enabled	###:SIP(XX) REG NG($$$) -%%		"60:SIP(07) REG NG(403) -02 "

Register Authentication Error

	Format	Key	Terminal LCD Example
NetLink Disabled	###:SIP(XX) AUTH FAILED($$$)	###:Alarm number (60) XX:Register ID (1-32) $$$:Error code (000-999) %%:System ID(1-16)	"60:SIP(20) AUTH FAILED(401)"
NetLink Enabled	###:SIP(XX) AUTH NG($$$) -%%		"60:SIP(20) AUTH NG(401) -02"

Comments

- It is not possible to program a Secondary system via handset programming when NetLink is operational.
- SIP trunk port numbers are assigned from the next available port number (the same as current operation).
- Previous assignments of SIP Trunk ports may be disabled when NetLink is first configured.
- The total number of SIP trunks assigned to all systems in the NetLink network must not exceed the number of licenses installed on the Primary system. If the number of trunk ports exceeds the number of licenses then the SIP trunks will fail to be assigned port numbers.
- Any node in NetLink can use the SIP trunks on its own node or on any other node (depending on system programming).

Incoming/Outgoing SIP Trunk for E.164

SIP Trunks now have the ability to communicate with an external SIP carrier using E.164 number formatting. When a user makes an outgoing call via SIP trunk from the system, it can be configured to add a '+' character and country code to the SIP Request-URI, To, From, P-Asserted Identity, and P-Preferred Identity header fields of the SIP message. This requirement may be necessary for connection to specific SIP carrier providers.

Enable Incoming/Outgoing SIP Trunk for E.164 by using the 'Incoming/Outgoing SIP Trunk for E.164' option in *Easy Edit* – *Advanced Items/VoIP/SIP Networking/Profile x/SIP Profile x - Trunk General Settings/SIP Profile x - E.164 Number Formatting/SIP Profile x - E.164 Number Format Settings*

When PRG84-14-13 is set to Enabled, then for any out bound call via SIP trunk a '+' and the Country Code in PRG10-02-01 (if configured in system programming) is added to the beginning of the Request-URI, To, and From header fields.

PRG 84-14-13 Incoming/Outgoing SIP Trunk for E.164	PRG 10-02-01 Country Code	Example Outgoing SIP Message (user dials "0356551700")
0	44	Request-URI: Invite sip:0356551700@172.16.18.100 SIP/2.0

		To header: To: sip:0356551700@172.16.18.100 From header: From: sip:0312345678@172.16.0.10
	No Setting	Request-URI: Invite sip:0356551700@172.16.18.100 SIP/2.0 To header: To: sip:0356551700@172.16.18.100 From header: From: sip:0312345678@172.16.0.10
1	44	Request-URI: Invite sip:+440356551700@172.16.18.100 SIP/2.0 To header: To: sip:+440356551700@172.16.18.100 From header: From: sip:+440312345678@172.16.0.10
	No Setting	Request-URI: Invite sip:+0356551700@172.16.18.100 SIP/2.0 To header: To: sip:+0356551700@172.16.18.100 From header: From: sip:+0312345678@172.16.0.10

When PRG84-14-13 is set to International Access Mode for any out bound call via SIP trunk if the leading digits of the Calling Party Number/Called Party Number are the same as the International Access Code assigned in PRG10-02-02 then delete the International Access Code and add '+' in the Request-URI, To, From, P-Asserted Identity, and P-Preferred Identity header fields.

Example Outgoing SIP Message Calling Party Number is ("00810312345678) Called Party Number is ("00810356551700) Country Code PRG10-02-02 configured as: 00
Request-URI: Invite sip:+810356551700@172.16.18.100 SIP/2.0 To header: To: sip:+810356551700@172.16.18.100 From header: From: sip:+810312345678@172.16.0.10 P-Asserted-Identity: P-Asserted-Identity:+810312345678@172.16.0.10 P-Preferred-Identity: P-Preferred-Identity:+810312345678@172.16.0.10

The SIP Carrier or Server must support E.164 numbering for this to work.

This feature is supported with all Carrier Choices configured through SIP Carrier Type PRG10-29-14.

With Netlink and multi-carrier support this feature will be applied across all SIP trunk configurations.

F-Route can be used to improve the user operation when using Incoming/Outgoing SIP Trunk for E.164 feature.

SIP Trunk SIP-URI E.164 Incoming Mode

This feature can work in conjunction to the Incoming/Outgoing SIP Trunk for E.164 feature. When an incoming call with a '+' and Country Code is received from an external SIP carrier it is recognised as an international call. The system can improve the operation of making an outbound call using the history of incoming calls by implementing this feature.

Enable SIP Trunk SIP-URI E.14 Incoming Mode by using the 'SIP Trunk SIP-URI E.14 Incoming Mode' option in *Easy Edit– Advanced Items/VoIP/SIP Networking/Profile x/SIP Profile x - Trunk General Settings/ SIP Profile x - E.164 Number Formatting/SIP Profile x - E.164 Number Format Settings*

PRG84-14-16 SIP Trunk SIP-URI E.14 Incoming Mode	**PRG84-14-13 Incoming/Outgoing SIP Trunk for E.164**	**Operation Description**

0:Off	0:Off	When '+' is used in the incoming call from an external SIP carrier, then delete '+' only.
0:Off	1:On	When a call comes in with a '+' and Country Code other than what is defined in PRG10-02-01 then delete '+' only. If a call comes in with a '+' and Country Code as assigned in PRG10-02-01 then delete the '+' and also the Country Code.
1:Mode 1	0:Off	When a call comes in with a '+' and Country Code other than what is defined in PRG10-02-01 then delete the '+' and add the International Access Code from PRG10-02-02. When a call comes in with a '+' and Country Code as assigned in PRG10-02-01 then delete the '+' and Country Code and do not add the International Access Code in PRG10-02-02.
2:Mode 2	0:Off	When a call comes in with a '+' and Country Code other than what is defined in PRG10-02-01 then delete the '+' and add the International Access Code from PRG10-02-02. When a call comes in with a '+' and Country Code as assigned in PRG10-02-01 then delete the '+' and Country Code and add the Caller ID Edit Code in PRG10-02-03.

Example usage operation from history of incoming calls

When '+' is used in the incoming call from an external SIP carrier, then delete '+' only.

Incoming number dialled: +4902131795770

PRG84-14-16 = 0

Resulting number displayed on terminal history of incoming calls

01:			4902131795770
*	3-5	11:17	
↑	↓	Store	DEL

When a call comes in with a '+' and Country Code other than what is defined in PRG10-02-01 then delete '+' only. If a call comes in with a '+' and Country Code as assigned in PRG10-02-01 then delete the '+' and also the Country Code.

Incoming number dialled: +4902131795770

PRG84-14-16 = 0

PRG84-14-13 =1

Resulting number displayed on terminal history of incoming calls

PRG10-02-01 = 0

01:			4902131795770
*	3-5	11:17	
↑	↓	Store	DEL

PRG10-02-01 = 49

01:			02131795770
*	3-5	11:17	
↑	↓	Store	DEL

When a call comes in with a '+' and Country Code other than what is defined in PRG10-02-01 then delete the '+' and add the International Access Code from PRG10-02-02. When a call comes in with a

'+' and Country Code as assigned in PRG10-02-01 then delete the '+' and Country Code and do not add the International Access Code in PRG10-02-02.

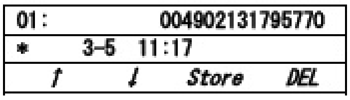
Incoming number dialled: +4902131795770

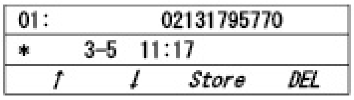
PRG84-14-16 = 1

PRG10-02-02 = 00

Resulting number displayed on terminal history of incoming calls

PRG10-02-01 = 0 PRG10-02-01 = 49





When a call comes in with a '+' and Country Code other than what is defined in PRG10-02-01 then delete the '+' and add the International Access Code from PRG10-02-02. When a call comes in with a '+' and Country Code as assigned in PRG10-02-01 then delete the '+' and Country Code and add the Caller ID Edit Code in PRG10-02-03.

Incoming number dialled: +4902131795770

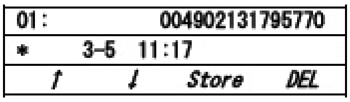
PRG84-14-16 = 2

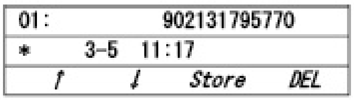
PRG10-02-02 = 00

PRG10-02-03 = 9

Resulting number displayed on terminal history of incoming calls

PRG10-02-01 = 0 PRG10-02-01 = 49





VAD Enhancement

RTP voice data is always transmitted during a VoIP call even if a user is not speaking. If VAD (Voice Activity Detection) is enabled in a system; the system can stop sending RTP voice data while a user is not speaking.

This enhancement improves the VAD determination method by using SIP negotiation (SDP).

Enable VAD Enhancement by using the 'VAD Negotiation on SDP' option in *Easy Edit - Advanced Items/ VoIP/SIP Networking/Profile x/SIP Profile x - Trunk General Settings/SIP Profile x - CODEC Settings (PRG84-13-65).*

VBD on SIP Trunk

Voice Band Data (VBD) is what is called modem over IP. This feature enables use of VBD (Voice Band Data) by System. If using VBD, the Analogue modem signal is converted into voice band data and can be submitted via SIP Trunk.

Enable VBD on SIP Trunk by using the ‘Voice Band Data (VBD)’ option in *Easy Edit - Advanced Items/VoIP/ SIP Networking/Profile x/SIP Profile x - Trunk General Settings/SIP Profile x - CODEC Settings (PRG84-13-66).*

For each VBD device connected to the system set the Terminal Type to SPECIAL using the ‘Terminal Type’ *(PRG15-03-03)* option and also the Device Type to MODEM using the ‘Select Special Terminal Type’ *(PRG15-03-18)* option in *Easy Edit– Extensions/Extension/Single Line Telephone SLT/SLT Basic Setup.*

2.6.3.1 SIP Trunks - Carrier Mode

SIP Trunks - Carrier Mode

All information about a specific SIP carrier can be found on the relevant ‘SIP Certificate of Compatibility’. The information below gives general information about programming SIP Trunks Carrier Mode.

Up to 6 SIP Carrier configurations can be configured on a single SV9100 system. SIP Profiles 1 - 6 contain identical programming pages. In the below Easy Edit references they are referred to as either Profile x or SIP Profile x to remain generic.

SIP Trunk Easy Edit Programming

Easy Edit – Advanced Items/VoIP/Networking/SIP Networking/

Easy Edit – Advanced Items/VoIP/Networking/SIP Networking/SIP IP Trunk Assignment
Trunk Type - Set to SIP *(PRG10-68-01)*
Start Port - Enable the logical starting port number *(PRG10-68-02)*
Number of Ports – Enter the required number of SIP trunk ports *(PRG10-68-03)*

Assign the **SIP Profile** used to the SIP trunks assigned in *Easy Edit – Advanced Items/VoIP/SIP Networking/ SIP Trunk Data Setup (PRG14-18)*
Set the trunk **Incoming Type** as required (usually **DID**) for each Trunk Port and Mode Number in *Easy Edit – Advanced Items/VoIP/SIP Networking/Profile x/SIP Profile x - General Settings/SIP Profile x - Trunk Incoming Type (PRG22-02)*

Carrier Mode IP Address

Easy Edit – Advanced Items/VoIP/SIP Networking/Profile x/SIP Profile x - Carrier Mode (IP Address)

Use this set of commands if the ITSP has provided you with an IP address for their SIP server rather than a Fully Qualified Domain Name.

System Information Setup

Easy Edit – Advanced Items/VoIP/SIP Networking/Profile x/SIP Profile x - Carrier Mode (IP Address)/ SIP Profile x - System Information Setup
Domain Assignment – This item tells the system whether an IP address or DNS address will be used to register to the SIPServer. Set to **IP Address**. *(PRG10-28-05)*

Server Setup

Easy Edit – Advanced Items/VoIP/SIP Networking/Profile x/SIP Profile x - Carrier Mode (IP Address)/ SIP Profile x - Server Setup
Outbound Default Proxy and **Inbound Default Proxy** – These items indicate whether a Proxy Server will be

used for the outgoing and incoming calls. Calls may be restricted only to/from the specified address. *(PRG10-29-01/02)*
Default Proxy Address – This is the IP address of the SIP Server where the outgoing calls will be routed to. *(PRG10-29-03)*
Default Proxy Port – This is the UDP port number that is used on the ITSP's SIP Server. *(PRG10-29-04)*
Register Mode – This switches the system between Networking Mode and Carrier Mode. For Carrier Mode use **Manual**. *(PRG10-29-05)*
Registrar IP Address – This is the IP address of the ITSP that the SV9100 will register to. This is *usually* the same as the **Default Proxy Address**. *(PRG10-29-06)*
Registrar Port – This is the UDP port number that is used on the ITSP's SIP Registrar. *(PRG10-29-07)*
SIP Carrier Choice – This defines the layout of the SIP messages, mainly for CLI purposes. *(PRG10-29-14)*

Register Sub Mode - Prevents an invalid INVITE message. If the register information that SV9100 send to SIP server and the Invite information that SV9100 receives are different, SV9100 sends "404 Not Found" Message. *(PRG10-29-16)*

Call Forward Moved Temporarily Support – When enabled a 302 Moved Temporarily response is sent to the configured SIP server for external call forward destinations. Requires support by the ITSP to be used. *(PRG84-14-17)*

Keep Alive By Option Message – This item will enable or disable the SIP OPTION keep alive function for checking a SIP server's availability. *(PRG10-29-19)*

Keep Alive By Option Interval Timer – This item sets the interval between receiving a 200 OK response of an OPTION message to sending the next OPTION message. Default value is 180 seconds (3 minutes). *PRG84-14-18)*

Keep Alive By Option Fail Limit – Failure Limit before PBX SIP trunks to destination server are unavailable (busy). (*PRG84-14-19)*

Option Keep Alive User ID – This parameter is set in request URI SIP URL of OPTION message.

For example sip:ping@xyzcustomer.com. *(PRG84-14-20)*

Primary Authentication Information

Easy Edit – Advanced Items/VoIP/SIP Networking/Profile x/SIP Profile x - Carrier Mode (IP Address)/ SIP Profile x - Primary Authentication Information
User ID– This is the Username (or User ID) that is supplied by the ITSP. It is part of the authentication details. This is usually the same as the **Username**. *(PRG10-36-02)*
Username – This is the Username (or User ID) that is supplied by the ITSP. It is part of the authentication details. *(PRG10-36-03)*
Password – This is the password that is supplied by the ITSP. It is part of the authentication details.It is part of the authentication details. Once entered the PBX will mask the entry to prevent it being seen by non-authorised parties *(PRG10-36-04)*

CODEC Settings

Easy Edit - Advanced Items/VoIP/SIP Networking/Profile x/SIP Profile x - Trunk General Settings/SIP Profile x - CODEC Settings
Audio Capability Priority – This is the preferred codec for the SIP Trunk call. It is possible that this codec is not used depending on the settings of the ITSP. *(PRG84-13-28)*

DTMF Settings

Easy Edit - Advanced Items/VoIP/SIP Networking/Profile x/SIP Profile x - Trunk General Settings/SIP Profile x - DTMF Settings
DTMF Payload Number – This value is used when **DTMF Relay** is enabled. The ITSP and the SV9100 must have equal values. If this is not the case, a common equal value will be negotiated. *(PRG84-34-02)*
DTMF Relay Mode – This item is to enable or disable DTMF Relay. To use DTMF Relay set to **RFC2833**. *(PRG84-34-01)*

E.164 Numbering

Easy Edit - Advanced Items/VoIP/SIP Networking/Profile x/SIP Profile x - Trunk General Settings/SIP Profile *x - E.164 Number Formatting/SIP Profile x - E.164 Number Format Settings*

Incoming/Outgoing SIP Trunk for E.164 - Defines the settings for support of E.164 number formatting when required for specified SIP carriers. *(PRG84-14-13)*

***Enabled** – When an outgoing call is made and the Country Code in 10-02-01 is empty. A + is added to the beginning of the Request-URI, To, and From header fields in SIP message. If 10-02-01 is configured with a Country Code then a + and also the Country Code are added to the beginning of the Request-URI, To, and From fields.*

***International Access Mode** - When an outgoing call is made and the digits from the beginning of the Calling Party Number/Called Party Number are the same as the International Access Code in 10-02-02 then deletes the International Access Code from 10-02-02 and replaces it with a +.*

SIP Trunk SIP - URI E.164 Incoming Mode - Defines the settings for additional SIP support of incoming E.164 number formatting when used in conjunction with incoming caller history. *(PRG84-14-16)*

***Disabled** - The system will delete the + only from the incoming call URI*

***Mode 1** – When an incoming call has a + and Country Code other than what is defined in 10-02-01 then deletes the + and adds the International Access Code in 10-02-02. If a call comes in with a + and the Country Code assigned in 10-02-01 then deletes the + and Country Code and does not add the International Access Code from 10-02-02.*

***Mode 2** - When an incoming call has a + and Country Code other than what is defined in 10-02-01 then deletes the + and adds the International Access Code in 10-02-02. If a call comes in with a + and the Country Code assigned in 10-02-01 then deletes the + and Country Code and adds the Caller ID Edit Code in 10-02-03.*

Carrier Mode DNS

Easy Edit – Advanced Items/VoIP/SIP Networking/Profile x/SIP Profile x - Carrier Mode (Domain Name)

Use this set of commands if the ITSP has provided you with a Fully Qualified Domain Name for their SIP server rather than an IP address.

System Information Setup

Easy Edit – Advanced Items/VoIP/SIP Networking/Profile x/SIP Profile x - Carrier Mode (Domain Name)/ SIP Profile x - System Information Setup

Domain Name – This is part of the SV9100's SIP ID which must be set to be able to communicate using SIP Trunks. This may be provided by the ITSP. *(PRG10-28-01)*

Host Name – This is part of the SV9100's SIP ID which must be set to be able to communicate using SIP Trunks. This may be provided by the ITSP. *(PRG10-28-02)*

Domain Assignment – This item tells the system whether an IP address or DNS address will be used to register to the SIP Server. Set to **Domain Name**. *(PRG10-28-05)*

Server Setup

Easy Edit – Advanced Items/VoIP/SIP Networking/Profile x/SIP Profile x - Carrier Mode (Domain Name)/ SIP Profile x - Server Setup

Outbound Default Proxy and **Inbound Default Proxy** – These items indicate whether a Proxy Server will be used for the outgoing and incoming calls. Calls may be restricted only to/from the specified address. *(PRG10-29-01/02)*

Default Proxy Port – This is the UDP port number that is used on the ITSP's SIP Server. *(PRG10-29-04)*

Register Mode – This switches the system between Networking Mode and Carrier Mode. For Carrier Mode use **Manual**. *(PRG10-29-05)*

Registrar Port – This is the UDP port number that is used on the ITSP's SIP Registrar. *(PRG10-29-07)*

DNS Mode – When using Carrier Mode DNS this item must be enabled. *(PRG10-29-08)*

DNS IP Address – Enter the IP address of the customer's (or ISP's) DNS server. *(PRG10-29-09)*

DNS Port – This is the port number used by the customer's (or ISP's) DNS server. *(PRG10-29-10)*

Registrar Domain Name – Enter the Fully Qualified Domain Name address of the ITSP's SIP registrar server. *(PRG10-29-11)*

Proxy Domain Name – Enter the Domain Name part of the ITSP's SIP server. *(PRG10-29-12)*

Proxy Host Name – Enter the Host Name part of the ITSP's SIP server. Together with the **Proxy Domain Name** will make up the Fully Qualified Domain Name address of the SIP server. *(PRG10-29-13)*

SIP Carrier Choice – This defines the layout of the SIP messages, mainly for CLI purposes. *(PRG10-29-14)*

DNS Source Port – This is the source port number of the customer's (or ISP's) DNS server. *(PRG10-29-17)*

Register Sub Mode - Prevents an invalid INVITE message. If the register information that SV9100 send to SIP server and the Invite information that SV9100 receives are different, SV9100 sends "404 Not Found" Message. *(PRG10-29-16)*

Call Forward Moved Temporarily Support – When enabled a 302 Moved Temporarily response is sent to the configured SIP server for external call forward destinations. Requires support by the ITSP to be used. *(PRG84-14-17)*

Keep Alive By Option Message – This item will enable or disable the SIP OPTION keep alive function for checking a SIP server's availability. *(PRG10-29-19)*

Keep Alive By Option Interval Timer – This item sets the interval between receiving a 200 OK response of an OPTION message to sending the next OPTION message. Default value is 180 seconds (3 minutes). *PRG84-14-18)*

Keep Alive By Option Fail Limit – Failure Limit before PBX SIP trunks to destination server are unavailable (busy). (*PRG84-14-19)*

Option Keep Alive User ID – This parameter is set in request URI SIP URL of OPTION message.
For example sip:ping@xyzcustomer.com. *(PRG84-14-20)*

Primary Authentication Information

Easy Edit – Advanced Items/VoIP/SIP Networking/Profile x/SIP Profile x - Carrier Mode (Domain Name)/ SIP Profile x - Primary Authentication Information

Registration – This command enabled registration of the user account details with the SIP server. This should be **Enabled** for each valid account. *(PRG10-36-01)*

User ID– This is the Username (or User ID) that is supplied by the ITSP. It is part of the authentication details. This is usually the same as the **Username**. *(PRG10-36-02)*

Username – This is the Username (or User ID) that is supplied by the ITSP. It is part of the authentication details. *(PRG10-36-03)*

Password – This is the password that is supplied by the ITSP. It is part of the authentication details. *(PRG10-36-04)*

CODEC Settings

Easy Edit - Advanced Items/VoIP/SIP Networking/Profile x/SIP Profile x - Trunk General Settings/SIP Profile x - CODEC Settings

Audio Capability Priority – This is the preferred codec for the SIP Trunk call. It is possible that this codec is not used depending on the settings of the ITSP. *(PRG84-13-28)*

DTMF Settings

Easy Edit - Advanced Items/VoIP/SIP Networking/Profile x/SIP Profile x - Trunk General Settings/SIP Profile x - DTMF Settings

DTMF Payload Number – This value is used when **DTMF Relay** is enabled. The ITSP and the SV9100 must have equal values. If this is not the case, a common equal value will be negotiated. *(PRG84-34-02)*

DTMF Relay Mode – This item is to enable or disable DTMF Relay. To use DTMF Relay set to **RFC2833**. *(PRG84-34-01)*

E.164 Numbering

Easy Edit - Advanced Items/VoIP/SIP Networking/Profile x/SIP Profile x - Trunk General Settings/SIP Profile x - E.164 Number Formatting/SIP Profile x - E.164 Number Format Settings

Incoming/Outgoing SIP Trunk for E.164 - Defines the settings for support of E.164 number formatting when required for specified SIP carriers. *(PRG84-14-13)*

Enabled *– When an outgoing call is made and the Country Code in 10-02-01 is empty. A + is added to the beginning of the Request-URI, To, and From header fields in SIP message. If 10-02-01 is configured with a Country Code then a + and also the Country Code are added to the beginning of the Request-URI, To, and From fields.*

International Access Mode *- When an outgoing call is made and the digits from the beginning of the Calling Party Number/Called Party Number are the same as the International Access Code in 10-02-02 then deletes the International Access Code from 10-02-02 and replaces it with a +.*

SIP Trunk SIP - URI E.164 Incoming Mode - Defines the settings for additional SIP support of incoming E.164 number formatting when used in conjunction with incoming caller history. *(PRG84-14-16)*

Disabled *- The system will delete the + only from the incoming call URI*

Mode 1 *– When an incoming call has a + and Country Code other than what is defined in 10-02-01 then deletes the + and adds the International Access Code in 10-02-02. If a call comes in with a + and the Country Code assigned in 10-02-01 then deletes the + and Country Code and does not add the International Access Code from 10-02-02.*

Mode 2 *- When an incoming call has a + and Country Code other than what is defined in 10-02-01 then deletes the + and adds the International Access Code in 10-02-02. If a call comes in with a + and the Country Code assigned in 10-02-01 then deletes the + and Country Code and adds the Caller ID Edit Code in 10-02-03.*

Note:
PRG10-29-16 Register Sub Mode if enabled might cause the SV9100 to reject incoming SIP Trunk calls depending on other settings. If problems are experienced with incoming calls being rejected turn this item off.

Configuration Examples

The examples below are for general information only, they will not work for all SIP carriers. Please refer to the relevant 'SIP Certificate of Compatibility' for specific information.

Carrier Mode IP Address

Command	Entry
10-12-01	192.168.0.10
10-12-02	255.255.0.0
10-12-03	172.16.0.1
10-12-07	<Public IP Address>
10-12-09	172.16.0.10
10-12-10	255.255.0.0
10-28-01	nec.co.uk
10-28-02	SV9100
10-28-05	IP Address
10-29-01	Enabled
10-29-02	Enabled
10-29-03	<ITSP IP Address>
10-29-05	Manual
10-29-06	<ITSP IP Address>
10-29-21	Used

10-36-01	Enabled
10-36-02	<User ID supplied by ITSP>
10-36-03	<User ID supplied by ITSP>
10-36-04	<Password supplied by ITSP>
10-68-01	SIP
10-68-02	1
10-68-03	4 ports
14-18-05	Profile 1
84-26	VoIP Gateway = 172.16.0.20

Carrier Mode DNS

Command	Entry
10-12-01	192.168.0.10
10-12-02	255.255.0.0
10-12-03	172.16.0.1
10-12-07	<Public IP Address>
10-12-09	172.16.0.10
10-12-10	255.255.0.0
10-28-01	NEC
10-28-02	SV9100
10-28-05	Domain Name
10-29-01	Enabled
10-29-02	Enabled
10-29-03	<ITSP IP Address>
10-29-05	Manual
10-29-08	Enabled

10-29-09	<DNS Server IP Address>
10-29-11	<ITSP FQDN Address>
10-29-12	<ITSP Domain Address>
10-29-13	<ITSP Host Address>
10-29-21	Used
10-36-01	Enabled
10-36-02	<User ID supplied by ITSP>
10-36-03	<User ID supplied by ITSP>
10-36-04	<Password supplied by ITSP>
10-68-01	SIP
10-68-02	1
10-68-03	4 ports
14-18-05	Profile 1
84-26	VoIP Gateway = 172.16.0.20

2.6.3.2 SIP Trunks - Networking Mode

SIP Trunks - Networking Mode

All information about a specific SIP carrier can be found on the relevant 'SIP Certificate of Compatibility'. The information below gives general information about programming SIP Trunks Networking Mode.

Up to 6 SIP Carrier configurations can be configured on a single SV9100 system. SIP Profiles 1 - 6 contain identical programming pages. In the below Easy Edit references they are referred to as either Profile x or SIP Profile x to remain generic.

SIP Trunk Easy Edit Programming

Easy Edit – Advanced Items/VoIP/Networking/SIP Networking/

Easy Edit – Advanced Items/VoIP/Networking/SIP Networking/SIP IP Trunk Assignment

Trunk Type - Set to SIP *(PRG10-68-01)*
Start Port - Enable the logical starting port number *(PRG10-68-02)*
Number of Ports – Enter the required number of SIP trunk ports *(PRG10-68-03)*

Assign the **SIP Profile** used to the SIP trunks assigned in *Easy Edit – Advanced Items/VoIP/SIP Networking/ SIP Trunk Data Setup (PRG14-18)*

Set the trunk **Incoming Type** as required (usually **DID**) for each Trunk Port and Mode Number in *Easy Edit – Advanced Items/VoIP/SIP Networking/Profile x/SIP Profile x - General Settings/SIP Profile x - Trunk Incoming Type (PRG22-02)*

For each remote system enable **System Interconnection**, enter the destination **IP Address** and the **Dial number** to reach the destination system and assign to the required **SIP Profile** in *Easy Edit – Advanced Items/VoIP/SIP Networking/Profile x/SIP Profile x - Networking Mode/SIP Profile x - Remote Destinations (PRG10-23)*

It is also required to set up the 'SIP ID' of the local system. Enter the **User ID** in *Easy Edit – Advanced Items/VoIP/SIP Networking/Profile x/SIP Profile x - Networking Mode/SIP Profile x - System Information Setup (PRG10-28)*.

There are some optional items that can be configured:

Set these as required for the specific configuration.

SIP Carrier Choice, Keep Alive for SIP, Keep Alive by OPTION Interval Timer, Keep Alive by OPTION Fail Limit, Option Keep Alive User ID available in *Easy Edit – Advanced Items/VoIP/SIP Networking/Profile x/ SIP Profile x - Networking Mode/SIP Profile x - Server Setup (PRG10-29, PRG84-14)*.

Audio Capability Priority available in *Easy Edit – Advanced Items/VoIP/SIP Networking/Profile x/SIP Profile x - Trunk General Settings/SIP Profile x - CODEC Settings (PRG84-13).*

DTMF Payload Number and DTMF Relay Mode available in *Easy Edit – Advanced Items/VoIP/SIP Networking/Profile x/SIP Profile x - Trunk General Settings/SIP Profile x - DTMF Settings (PRG84-34)*.

Incoming/Outgoing SIP Trunk for E.164, SIP Trunk SIP-URI E.164 Incoming Mode available in *Easy Edit – Advanced Items/VoIP/SIP Networking/Profile x/SIP Profile x - Trunk General Settings/SIP Profile x - E.164 Number Formatting/SIP Profile x - E.164 Number Format Settings (PRG84-14)*.

Some other general VoIP programming will also be required such as GPZ-IPLE IP Address, Subnet Mask, Default Gateway and VoIP Resource IP Address. These can be programmed in *Easy Edit – Advanced Items//VoIP/General Settings/IP Addressing (PRG10-12, PRG84-26)*

Configuration Example

The below configuration shows the programming required to connect three SV9100 systems together using SIP Trunks Networking Mode.
This programming allows desk to desk dialling to/from each system but without any extra functionality.
Each system is programming SIP Profile 1.

System A		System B		System C	
10-12-01	192.168.0.10	10-12-01	192.168.0.10	10-12-01	192.168.0.10
10-12-02	255.255.0.0	10-12-02	255.255.0.0	10-12-02	255.255.0.0

10-12-03	172.16.0.1	10-12-03	172.17.0.1	10-12-03	172.18.0.1
10-12-09	172.16.0.10	10-12-09	172.17.0.10	10-12-09	172.18.0.10
10-12-10	255.255.0.0	10-12-10	255.255.0.0	10-12-10	255.255.0.0
10-23-01	System 1 = Enabled System 2 = Enabled	10-23-01	System 1 = Enabled System 2 = Enabled	10-23-01	System 1 = Enabled System 2 = Enabled
10-23-02	System 1 = 172.17.0.10 System 2 = 172.18.0.10	10-23-02	System 1 = 172.16.0.10 System 2 = 172.18.0.10	10-23-02	System 1 = 172.16.0.10 System 2 = 172.17.0.10
10-23-04	System 1 = 2 System 2 = 3	10-23-04	System 1 = 1 System 2 = 3	10-23-04	System 1 = 1 System 2 = 2
10-23-06	System 1 = Profile 1 System 2 = Profile 1	10-23-06	System 1 = Profile 1 System 2 = Profile 1	10-23-06	System 1 = Profile 1 System 2 = Profile 1
10-28-05	IP Address	10-28-02	IP Address	10-28-02	IP Address
10-36-02	Profile 1, Registration ID 00 = 100	10-28-04	Profile 1, Registration ID 00 = 200	10-28-04	Profile 1, Registration ID 00 = 300
10-68-01	SIP	10-68-01	SIP	10-68-01	SIP
10-68-02	1	10-68-02	1	10-68-02	1
10-68-03	4 ports	10-68-03	4 ports	10-68-03	4 ports
11-01	1 = 3 Digit Type 2 2 = 3 Digit Type 6 3 = 3 Digit Type 6	11-01	1 = 3 Digit Type 6 2 = 3 Digit Type 2 3 = 3 Digit Type 6	11-01	1 = 3 Digit Type 6 2 = 3 Digit Type 6 3 = 3 Digit Type 2
11-02	1XX	11-02	2XX	11-02	3XX
14-05	SIP trunk Ports = Group 20	14-05	SIP trunk Ports = Group 20	14-05	SIP trunk Ports = Group 20
14-18-05	Trunks 1-4 = Profile 1	14-18-05	Trunks 1-4 = Profile 1	14-18-05	Trunks 1-4 = Profile 1
44-02-01	Table 1 – Dial = 2 Table 2 – Dial = 3	44-02-01	Table 1 – Dial = 1 Table 2 – Dial = 3	44-02-01	Table 1 – Dial = 1 Table 2 – Dial = 2
44-02-02	Table 1 = FRoute Table 2 = FRoute	44-02-02	Table 1 = FRoute Table 2 = FRoute	44-02-02	Table 1 = FRoute Table 2 = FRoute
44-02-03	Table 1 = 1 Table 2 = 2	44-02-03	Table 1 = 1 Table 2 = 2	44-02-03	Table 1 = 1 Table 2 = 2
44-05	Table 1 = TRK Group 20 Table 2 = TRK Group 20	44-05	Table 1 = TRK Group 20 Table 2 = TRK Group 20	44-05	Table 1 = TRK Group 20 Table 2 = TRK Group 20
84-26-	172.16.0.20	84-26-01	172.17.0.20	84-26-01	172.18.0.20

01					

The following extra programming allows the dialling extension to send its own extension number as CLI to the remote system.

System A		System B		System C	
10-29-14	Carrier B	10-29-14	Carrier B	10-29-14	Carrier B
21-19	Enter the extension number as the Calling Party Number against each extension.	21-19	Enter the extension number as the Calling Party Number against each extension.	21-19	Enter the extension number as the Calling Party Number against each extension.

The following extra programming allows the incoming CLI from a remote system to be converted to name which will be displayed on the called party's display.

System A		System B		System C	
13-04	Enter the remote extension numbers along with the remote users name	13-04	Enter the remote extension numbers along with the remote users name	13-04	Enter the remote extension numbers along with the remote users name

The following extra programming changes the Codec which is used between systems.

System A		System B		System C	
84-13-28	Choose from – G.711, G.722, G.726, G.729	84-13-28	Choose from – G.711, G.722, G.726, G.729	84-13-28	Choose from – G.711, G.722, G.726, G.729

The following extra programming enables DTMF Relay (RFC2833).

System A		System B		System C	
84-34-01	Profile 1, SIP Trunk = RFC2833	84-13-32	Profile 1, SIP Trunk = RFC2833	84-13-32	Profile 1, SIP Trunk = RFC2833

2.6.4 K-CCIS

K-CCIS

IP trunk connections over CCIS Networking via IP are used to connect multiple systems together over a Data Communication IP Network (Intranet). Key-Common Channel Interoffice Signalling (K-CCIS) is used to provide telephony services between the SV9100 and another SV9100 or SV8100.

The SV9100 uses the NEC proprietary CCIS Peer to Peer protocol over IP to communicate between systems.

An GPZ-IPLE daughter board is required for connections between IP terminals and IP trunks. A maximum of one GPZ-IPLE daughter board can be accommodated per system with a maximum of 128 DSP

Resources per system.

Each system in the network must have:

- GCD-CP10
- GPZ-IPLE
- Feature Networking (K-CCIS) license(s): BE114066

K-CCIS Easy Edit Programming

Easy Edit – Advanced Items/VoIP/Networking/K-CCIS

K-CCIS Setup

Easy Edit – Advanced Items/VoIP/Networking/K-CCIS/K-CCIS Setup/K-CCIS IP Trunk Assignment
Trunk Type - Set to CCIS *(PRG10-68-01)*
Start Port - Enable the logical starting port number *(PRG10-68-02)*
Number of Ports – Enter the required number of CCIS trunk ports *(PRG10-68-03)*

Easy Edit – Advanced Items/VoIP/Networking/K-CCIS/K-CCIS Setup/K-CCIS IP Setup
IPL IP Address – This is the signalling address of the SV9100's own GPZ-IPLE card *(PRG10-12-09)*
IPL Subnet Mask – This is the subnet mask of the SV9100's own ILP card *(PRG10-12-10)*
Default Gateway – This is the IP address of the default gateway on the SV9100's own network *(PRG10-12-02)*
CCIS Availability – Enable the availability of K-CCIS networking *(PRG50-01-01)*
Server TCP Port – This is the TCP port number used by the server side for K-CCIS *(PRG50-15-02)*
Client TCP Port – This is the TCP port number used by the client side for K-CCIS *(PRG50-15-03)*
Connection Method for DT800/DT700 – This enables peer to peer communication between DT800/DT700 extensions on different K-CCIS nodes *(PRG50-15-04)*

Easy Edit – Advanced Items/VoIP/Networking/K-CCIS/K-CCIS Setup/K-CCIS IPL VoIP Resource IP Address (PRG84-26)
For an GPZ-IPLE card only one address is required regardless of the number of voip channels licensed. For the RTP and RTCP ports enter the starting port number for each IP address. Each DSP requires one RTP port and one RTCP port. Under normal circumstances there is no need to change these settings from default.

Easy Edit – Advanced Items/VoIP/Networking/K-CCIS/K-CCIS Setup/K-CCIS Trunk Groups (PRG14-05)
Assign a unique trunk group to the K-CCIS trunk ports and set them as **Tie Line** for the relevant mode of service

Easy Edit – Advanced Items/VoIP/Networking/K-CCIS/K-CCIS Setup/K-CCIS Local ID (PRG50-02-03)
Assign the **Origination Point Code** for Route ID 9 for the local SV9100

Easy Edit – Advanced Items/VoIP/Networking/K-CCIS/K-CCIS Setup/K-CCIS Remote ID (PRG50-03)
Set the **Destination Point Code** and the **IP Address** of each remote node

Easy Edit – Advanced Items/VoIP/Networking/K-CCIS/K-CCIS Setup/K-CCIS Codec Setup (PRG84-21)
K-CCIS can use various CODECs. A CODEC is a standard for converting an analogue signal to digital. This conversion process is handled by the DSP (Digital Signal Processors) on the GPZ-IPLE card.
Each CODEC has different voice quality and compression properties. The correct choice of CODEC will be based on the amount of bandwidth available, the amount of calls required and the voice quality required.

Available Codec's for K-CCIS

- G.711 64Kbps codec MOS 4.4

- G.722 64Kbps codec MOS 4.4
- G.726 32Kbps codec MOS 4.2
- G.729 8Kbps codec MOS 4.0

The bandwidth values quoted for these codec's are for the digitized speech in one direction only. The actual bandwidth required for a call will depend on many other factors and will be much higher than these figures.
The above MOS values are quoted for ideal network conditions. The value could be lower depending upon the network performance.

It is possible to change the first and second priority codec in use in a K-CCIS network. Use the ***Audio Capability 1st Priority*** and ***Audio Capability 2nd Priority*** settings as required.

K-CCIS Numbering Plan

Easy Edit – Advanced Items/VoIP/Networking/K-CCIS/K-CCIS Numbering Plan/System Numbering (PRG11-01)
Assign local node digits as **Extension**
Assign the remote node digits as **F-Route**

Easy Edit – Advanced Items/VoIP/Networking/K-CCIS/K-CCIS Numbering Plan/Extension Numbers (PRG11-02)
Assign the ports on the local node with extension numbers as required

Easy Edit – Advanced Items/VoIP/Networking/K-CCIS/K-CCIS Numbering Plan/F-Route (PRG44-XX)
Use F-Route programming to route the required extension digits to the K-CCIS Trunk Group and to the relevant **Destination Point Code**. See the configuration example below.

K-CCIS Busy Lamp Field

K-CCIS can be programmed to send busy lamp field information to remote nodes.
Up to 120 extensions can be set to send their BLF status information to up to 8 different nodes.
The BLF updates can be sent at programmable intervals of 4, 8, 12 or 16 seconds.

K-CCIS BLF

Easy Edit – Advanced Items/VoIP/Networking/K-CCIS/K-CCIS BLF/K-CCIS BLF Destinations (PRG50-08)
Set the **Destination Point Code** per **Sending Group** of which node the BLF information will be sent to

Easy Edit – Advanced Items/VoIP/Networking/K-CCIS/K-CCIS BLF/K-CCIS BLF Extensions (PRG50-09)
Assign the extension numbers which wish to send their BLF status information and enable for the relevant **Sending Group**

Easy Edit – Advanced Items/VoIP/Networking/K-CCIS/K-CCIS BLF/K-CCIS BLF Timer (PRG50-10)
Set the interval for when the BLF updates will be sent out to the destination nodes

K-CCIS Night Mode Switching

It is possible to control the night mode switch of other nodes from a central location using K-CCIS.
All nodes that are controlled centrally must use the same mode number.
There can only be two modes when switching is controlled centrally.

Easy Edit – Advanced Items/VoIP/Networking/K-CCIS/K-CCIS Night Mode Switching/K-CCIS Night Mode

Destinations (PRG50-11)
Enter the **Destination Point code** of the system to be controlled. Up to sixteen destination point codes can be entered

Easy Edit – Advanced Items/VoIP/Networking/K-CCIS/K-CCIS Night Mode Switching/K-CCIS Night Switching Mode (PRG50-12)
Enter the required mode settings for **Day Mode** and **Night Mode**

K-CCIS Misc

Easy Edit – Advanced Items/VoIP/Networking/K-CCIS/K-CCIS Misc
Link Reconnect – This allows the system to drop redundant K-CCIS lines. E.g. If a K-CCIS call is transferred back to the originating system the K-CCIS links will be dropped. *(PRG50-06-01)*
Adding dial digits in front of the CPN - Digits entered here will be added as prefix to any called party number.
Centralized Day/Night Switching – This allows the system to receive a signal to change the mode of service. *(PRG50-06-02)*
CCIS Office Code – This is the systems access code when using an open numbering plan. *(PRG50-04-01)*
Maximum Hop Count – This is the maximum number of hops (tandem systems) a call that is forwarded (Call Forward All Calls) can make. If the destination is via a sixth hop it will not be forwarded and will ring on the last extension. *(PRG50-05-01)*
IAI Response Time – This is the amount of time (in seconds) the system will wait for a response to a K-CCIS request. *(PRG50-13-01)*

DTMF Relay (RFC2833)

By default any DTMF tones transmitted across K-CCIS will be sent as audio tones in the speech path. It is possible that these tones can be misinterpreted by the receiving device because of packet loss or errors due to the codec compression.
DTMF relay is a way of converting the DTMF tone into a signal then sending the signal across the IP network instead of the actual tone.
To enable this feature set the **DTMF Relay Mode** for **CCIS over IP** using **Profile 1** to **RFC2833** or **H.245** (all nodes should have the same setting) in *Easy Edit – Advanced Items/VoIP/General Settings/VoIP Configuration/IPL DTMF Settings/DTMF Setup (PRG84-34)*

Fax Relay (T.38)

By default any Fax tones transmitted across K-CCIS will be sent as audio tones in the speech path. It is possible that these tones can be misinterpreted by the receiving device because of packet loss or errors due to the codec compression.
Fax relay is a way of converting the Fax tones into a signal then sending the signal across the IP network instead of the actual tone.
To enable this feature set the **Fax Relay Mode** option to **Enabled** in *Easy Edit – Advanced Items/VoIP/Networking/K-CCIS/K-CCIS Setup/K-CCIS FoIP Settings (PRG84-33)*

Configuration Example

The example below shows the basic programming required for a three node SV9100 K-CCIS network with a closed numbering plan. Each system is on a separate network.
No other advanced options are included here.

System A		System B		System C	
10-12-01	192.168.0.10	10-12-01	192.168.0.10	10-12-01	192.168.0.10
10-12-02	255.255.0.0	10-12-02	255.255.0.0	10-12-02	255.255.0.0
10-12-03	172.16.0.1	10-12-03	172.17.0.1	10-12-03	172.18.0.1
10-12-09	172.16.0.10	10-12-09	172.17.0.10	10-12-09	172.18.0.10
10-12-10	255.255.0.0	10-12-10	255.255.0.0	10-12-10	255.255.0.0
10-40-01	Enable	10-40-01	Enable	10-40-01	Enable
10-40-04	4	10-40-04	4	10-40-04	4
11-01	1 = 3 Digit Type 2 2 = 3 Digit Type 6 3 = 3 Digit Type 6	11-01	1 = 3 Digit Type 6 2 = 3 Digit Type 2 3 = 3 Digit Type 6	11-01	1 = 3 Digit Type 6 2 = 3 Digit Type 6 3 = 3 Digit Type 2
11-02	1XX	11-02	2XX	11-02	3XX
14-05					
22-02	CCIS Trunk Ports = Tie Line	22-02	CCIS Trunk Ports = Tie Line	22-02	CCIS Trunk Ports = Tie Line
44-02	Dial 2 = FRoute, Data 1 Dial 3 = FRoute, Data 2	44-02	Dial 1 = FRoute, Data 1 Dial 3 = FRoute, Data 2	44-02	Dial 1 = FRoute, Data 1 Dial 2 = FRoute, Data 2
44-05-01	FRoute 1 = TRKGRP 20 FRoute 2 = TRKGRP 20	44-05-01	FRoute 1 = TRKGRP 20 FRoute 2 = TRKGRP 20	44-05-01	FRoute 1 = TRKGRP 20 FRoute 2 = TRKGRP 20
44-05-09	FRoute 1 = Digit 3 FRoute 2 = Digit 3	44-05-09	FRoute 1 = Digit 3 FRoute 2 = Digit 3	44-05-09	FRoute 1 = Digit 3 FRoute 2 = Digit 3
44-05-10	FRoute 1 = DPC 02 FRoute 2 = DPC 03	44-05-10	FRoute 1 = DPC 01 FRoute 2 = DPC 03	44-05-10	FRoute 1 = DPC 01 FRoute 2 = DPC 02
50-01-01	On	50-01-01	On	50-01-01	On
50-02-03	Route ID 9 = 01	50-02-03	Route ID 9 = 02	50-02-03	Route ID 9 = 02
50-03-01	System ID 1 = DPC 02 System ID 2 = DPC 03	50-03-01	System ID 1 = DPC 01 System ID 2 = DPC 03	50-03-01	System ID 1 = DPC 01 System ID 2 = DPC 02
50-03-03	System ID 1 = 172.17.0.10 System ID 2 = 172.18.0.10	50-03-03	System ID 1 = 172.16.0.10 System ID 2 = 172.18.0.10	50-03-03	System ID 1 = 172.16.0.10 System ID 2 = 172.17.0.10
84-26-01	172.16.0.20	84-26-01	172.17.0.20	84-26-01	172.18.0.20

Licensing

Each SV9100 needs to be licensed to use IP Trunks for K-CCIS. One license gives that system the ability to use one IP Trunk. Each K-CCIS node requires the relevant number of IP Trunk licenses.

K-CCIS IP Trunk Availability/Licensing Limitation

There is a limitation when configuring K-CCIS Trunk Availability that the correct number of system port licenses must be free and available on the SV9100.

For example a default system is configured without any additional port licenses. This means it can support up to 64 TDM ports.

If 60 TDM ports were in use on the SV9100 and you tried to assign 12 KCCIS over IP ports, the system reports Invalid Data and will not assign the K-CCIS IP trunks.

To resolve this you must either remove some used TDM ports from the system or enable the system free license (if available) and re-try assigning the K-CCIS IP trunks. In this scenario you can assign the ports ok.

Up to 200 IP Trunk licenses can be added. Licence Code: BE114066

2.6.4.1 K-CCIS Features

K-CCIS Features

The following system features are available between systems that are networked using K-CCIS.

Features Available via K-CCIS

- Automatic Recall
- Brokerage Hotline
- Call Back (R5)
- Call Forwarding – All Calls
- Call Forwarding – Busy/No Answer
- Call Park Retrieve
- Call Transfer – All Calls
- Calling Name Display
- Calling Number Display
- Calling Party Number Presentation from Station
- Centralised BLF
- Centralised Day/Night Mode Change
- Centralised E911
- Dial Access to Attendant
- Direct Inward Dialling

- Dual Hold
- Elapsed Time Display
- Flexible Numbering of Stations
- Handsfree Answerback
- Hot Line
- Link Reconnect
- Multiple Call Forwarding – All Calls
- Multiple Call Forwarding – Busy/No Answer
- Paging Access
- Quick Transfer to Voice Mail
- Station-to-Station Calling
- Uniform Numbering Plan
- Voice Call
- Voice Mail, Centralised

Automatic Recall – K-CCIS

Feature Description

This feature allows a call to be release transferred to another station in another office in the K-CCIS network and recall back to the originator of the transfer after a programmed time.

System Availability

Terminal Type:

All Terminals

Required Components

GPZ-IPLE

Operating Procedures

Using a multiline terminal with a call in progress (Closed Numbering Plan):

1. Press Transfer. Internal dial tone is heard. The call is placed on Common Hold.
2. Dial the distant K-CCIS station number where the call is to be transferred.
3. Wait for the ringback tone.
4. Hang up.

- OR -

1. When the party answers, announce the transfer.
2. Restore the handset (transfer is completed).

Using a multiline terminal with a call in progress (Open Numbering Plan):

1. Press Transfer, and receive internal dial tone. The call is placed on Common Hold.
2. Dial the trunk Access Code.
3. Dial the Office Code number.
4. Dial the distant K-CCIS station number where the call is to be transferred.
5. Wait for the ringback tone.
6. Hang up.

Service Conditions

- If PRG 34-07-05 is left at default (30) the transferred call recalls to the station that performed the transfer when not answered.
- A UNIVERGE SV9100 station can receive a K-CCIS transferred call as a camp-on call if allowed by Class of Service.

Restrictions:

- PRG 34-07-05 cannot be set based on a Timer Class of Service in PRG 20-31.

- Trunk-to-Trunk Transfer must be allowed in Program 14-01-13 (Trunk-to-Trunk Transfer Yes/No Selection).
- A blind transfer across a K-CCIS link cannot be completed until ringback tone is received at the transferring station.

Related Feature List

- Link Reconnect – K-CCIS
- Station-to-Station Calling – K-CCIS
- Uniform Numbering Plan – K-CCIS
- Call Transfer – All Calls – K-CCIS

Program/ Item No.	Description/Selection	Assigned Data	Comments
34-07-05	E&M Tie Line Timer – Trunk Answer Detect Timer for E&M	0 ~ 64800 seconds Default is 30	Determine the amount of time the call should ring a station in another office before recalling back to the originator of the transfer.

Brokerage Hotline – K-CCIS

Feature Description

This feature provides a ringdown connection between two stations, each using a multiline terminal, in different offices in the CCIS network.

System Availability

Terminal Type:

All Terminals

Required Components:

GPZ-IPLE

Operating Procedures

To use this feature at any terminal:

1. Lift the handset or press **Speaker**.
2. Press the line/feature key associated with the pre-assigned station.
3. The destination station is automatically dialled, ring back tone is heard and the destination station answers.
4. After completion of conversation, hang up or press **Speaker**. To make another Brokerage-Hot Line-CCIS call immediately, press another line/ feature key without going on hook and off hook.

Service Conditions

- Either multiline terminal in a Brokerage - Hot Line – (K-CCIS) pair may transfer a Hot Line call to another station in the K-CCIS network using the Call Transfer – All Calls - (K-CCIS) feature.

Restrictions:

None

Related Feature List

- Call Transfer – All Calls - K-CCIS
- Station-to-Station Calling – K-CCIS
- Uniform Numbering Plan – K-CCIS

Guide to Feature Programming

This guide provides a list of associated Programs that support this feature.

Program/ Item No.	Description/Selection	Assigned Data	Comments
15-07-01	Programmable Function Keys	01 = DSS / One-Touch	Assign a DSS/One Touch key of the station in the Distant Office.

Call Back – K-CCIS

Feature Description

This feature allows a station to set a Call Back after dialling across K-CCIS to a busy destination. The station that set the Call Back will receive a call as soon as the busy station becomes idle.

System Availability

Terminal Type:

All Multiline Terminals

Required Components

GPZ-IPLE

Operating Procedure

To set Call Back – K-CCIS from a multiline telephone (Closed Numbering Plan only):

1. Call destination extension number (across K-CCIS), busy tone is heard.
2. Calling party presses Camp On/Call Back Function Key.
3. Calling Party hangs up and waits for Call Back.

Service Conditions

Restrictions

- This feature can only be set or received by a Multiline Terminal.
- This feature is only supported using a closed numbering plan.
- This feature can only be set by pressing a programmable key, soft key or service code is not supported.
- This feature can only be set when the calling party hears busy tone from the called party.
- The calling party must hang up after setting the Call Back.
- K-CCIS Trunks must be available on both systems for the operation to be successful.
- One terminal can set one Call Back.
- One system can have a maximum of 50 Call Back/Camp On reservations at the same time.

- Any Call Back's that are set will be removed by a system reset.
- One extension can receive Call Back settings from multiple extensions. In this case the ring back will occur in the order they were set.
- If the Call Back destination has a Call Forward set the operation is as follows: -
    - If the Call Forward destination is an internal extension – Call Back will be established to the Call Forward destination.
    - If the Call Forward destination is another system or trunk – Call Back will not be established.

Related Feature List

- Station-to-Station Calling – K-CCIS
- Uniform Numbering Plan

Guide to Feature Programming

This guide provides a list of associated Programs that support this feature.

- PRG15-07 (Code: 35).
- PRG20-01-07 Camp On Extension Call Back Time.
- PRG20-01-09 Camp On Cancel Time.
- PRG20-13-35 Block Camp On.

Call Forwarding – All Calls – K-CCIS

Feature Description

This feature allows all calls destined for a particular station to be routed to another station or to an Attendant, in another office in the K-CCIS network, regardless of the status (busy or idle) of the called station. The activation and cancellation of this feature may be accomplished by either the station user or an Attendant position if allowed by Class of Service (COS). Attendant Positions can be used to cancel Call Forward – All Call system-wide.
For more details, refer to the UNIVERGE SV9100 Features and Specifications Manual.

System Availability

All multiline terminals

Required Components

GPZ-IPLE

Operating Procedures

To set Call Forward – All Calls – K-CCIS from a multiline telephone (Closed Numbering plan):

1. Press the Call Forward – All ON/OFF key.
2. Dial 1 to set, then enter the remote K-CCIS station number.
3. Press Speaker.

- OR -

1. Lift the handset or press Speaker.
2. Dial Access Code 848 (default), then 1 to set.
3. Dial the remote K-CCIS station number.

4. Restore handset or press Speaker.

To set Call Forward – All Calls – K-CCIS from a Multiline Telephone (Open Numbering Plan):

1. Press the Call Forward – All ON/OFF key.
2. Dial 1 to set.
3. Dial the trunk Access Code.
4. Dial the Office Code number.
5. Dial the distant K-CCIS station number.
6. Restore handset or press Speaker.

- OR -

1. Lift the handset or press Speaker.
2. Dial Access Code 848 (default), then 1 to set.
3. Dial the trunk Access Code.
4. Dial the Office Code number.
5. Dial the distant K-CCIS station number.
6. Restore handset or press Speaker.

To cancel Call Forward – All Calls – K-CCIS from a Multiline Telephone:

1. Press Call Forward – All ON/OFF key.
2. Dial 0 to cancel.
3. Press Speaker.

- OR -

1. Lift the handset or press Speaker.
2. Dial Access Code 848(default), then dial 0.
3. Restore the handset or press Speaker.

Service Conditions

General:

Any station or Call Arrival (CAR) key can be set for Call Forwarding – All Calls – K-CCIS.

Restrictions:

- Call Forward – Off-Premise must be allowed in PRG 20-11-12 (Class of Service External Call Forward) to set call forwarding to a remote K-CCIS station number.
- Trunk-to-Trunk Transfer must be allowed in PRG 14-01-13 (Trunk-to-Trunk Transfer Yes/No Selection).
- A Single Line Telephone user can transfer a trunk call to another internal station that is set for Call Forwarding – All Calls – K-CCIS, however, when the distant party answers the call, a conference cannot be established.
- The destination station in the distant system is the only station that can call a station with Call Forwarding – All Calls – K-CCIS set.
- Call Forwarding with Both Ringing (All Calls) is not supported.
- Call Forward Split Internal/External is not supported.
- Forwarding to Voice Mail is not included in the Maximum Hop Count.
- Call Forward continues to operate to a *MLT* that has been removed.

Related Feature List

- Call Forwarding – Busy/No Answer – K-CCIS
- Multiple Call Forwarding – All Calls – K-CCIS
- Multiple Call Forwarding – Busy/No Answer – K-CCIS
- Link Reconnect – K-CCIS
- Uniform Numbering Plan – K-CCIS

Guide to Feature Programming

This guide provides a list of associated Programs that support this feature.

Program/ Item No.	Description/ Selection	Assigned Data	Comments
20-11-12	Class of Service Options – Call Forwarding Off-Premise (External Call Forwarding)	0 = Off (default) 1 = On Default is 0	Enable per class of service.
20-06-01	Class of Service for Extensions	0~15	Default: Class 1
20-09-07	Class of Service Options (Incoming Call Service) – Call Queuing	0 = Off 1 = On Default is 1	Must be Off for Call Forward – Busy to operate.
20-13-06	Class of Service Options (Supplementary Service) – Automatic Off Hook Signaling (Automatic Override)	0 = Off 1 = On Default is 1	Must be Off for Call Forward – Busy to operate.
15-07-01	Programmable Function Keys	10 = Call Forward – Immediate 11 = Call Forward – Busy 12 = Call Forward – No Answer 13 = Call Forward – Busy No Answer	Service Codes: 848 843 845 844
14-01-13	Basic Trunk Data Setup – Trunk-to-Trunk Transfer Loop Supervision	0 = Disable 1 = Enable Default is 1	Must enable for Trunk-to-Trunk Transfer, Call Forward – Off-Premise, and tandem trunking.
50-06-01	CCIS Feature Availability – Link Reconnect	0 = Not Available 1 = Available Default is 1	Enable/Disable Link Reconnect.
50-05-01	CCIS Maximum Call Forwarding Hop Counter	0~7 Hops Default is 5	Set Maximum Hops allowed in a CCIS network.

Call Forwarding – Busy/No Answer – K-CCIS

Feature Description

This feature permits a call to a Busy or unanswered station to be forwarded to another station or an Attendant, in another office in the K-CCIS network. The activation and cancellation of this feature may be accomplished by either the station user or an Attendant position, if allowed by Class of Service (COS). For more details, refer to the UNIVERGE SV9100 Features and Specifications Manual.

System Availability

Terminal Type:

All multiline terminals

Required Components:
GPZ-IPLE

Operating Procedures
To set Call Forward – Busy/No Answer – K-CCIS from a Multiline Telephone (Closed Numbering Plan):
1. Press the Call Forward – Busy/No Answer ON/OFF key.
2. Dial 1 to set.
3. Dial the remote K-CCIS station number.
4. Press Speaker.

- OR -
1. Lift the handset or press Speaker.
2. Dial Access Code 844 (default), then 1 to set.
3. Dial the remote K-CCIS station number.
4. Restore handset or press Speaker.

To set Call Forward – Busy/No Answer - K-CCIS from a Multiline Telephone (Open Numbering Plan):
1. Press the Call Forward – Busy/No Answer ON/OFF key.
2. Dial 1 to set
3. Dial the trunk Access Code.
4. Dial the Office Code number.
5. Dial the distant K-CCIS station number.
6. Press Speaker.

- OR -
1. Lift the handset or press Speaker.
2. Dial Access Code 844 (default), then Dial 1 to set.
3. Dial the trunk Access Code.
4. Dial the Office Code number.
5. Dial the distant K-CCIS station number.
6. Restore handset or press Speaker.

To cancel Call Forward – Busy/No Answer – K-CCIS from a Multiline Telephone:
1. Press Call Forward – Busy/No Answer On/Off key.
2. Dial 0 to cancel.
3. Press Speaker.

- OR -
1. Lift the handset or press Speaker.
2. Dial Access Code 844 (default), then Dial 0 to cancel.
3. Restore handset or press Speaker.

Service Conditions

General:
Any station or Call Arrival (CAR) key can be set for Call Forwarding – Busy/No Answer – K-CCIS.

Restrictions:
- Call Forward – Off-Premise must be allowed in Class of Service (PRG 20-11-12) External Call forward to set call forwarding to a remote K-CCIS station number.
- Trunk-to-Trunk Transfer must be allowed in PRG 14-01-13 for each trunk (Trunk-to-Trunk Transfer Yes/No Selection).
- A Single Line Telephone user can transfer a trunk call to another internal station that is set for Call Forwarding – All Calls - K-CCIS, however, when the distant party answers the call, a conference cannot be established.
- The destination station in the distant systems is the only station that can call a station with Call Forwarding – All Calls – K-CCIS set.
- Call Forwarding with Both Ringing (All Calls) is not supported.

- Call Forward Split Internal/External is not supported.
- Forwarding to Voice Mail is not included in the Maximum Hop Count.
- Call Forward continues to operate to a *MLT* that has been removed.

Related Feature List

- Call Forwarding – Busy/No Answer – K-CCIS
- Multiple Call Forwarding – All Calls – K-CCIS
- Multiple Call Forwarding – Busy/No Answer – K-CCIS
- Link Reconnect – K-CCIS
- Uniform Numbering Plan – K-CCIS

Guide to Feature Programming

This guide provides a list of associated Programs that support this feature.

Program/ Item No.	Description/ Selection	Assigned Data	Comments
20-11-12	Class of Service Options – Call Forwarding Off-Premise (External Call Forwarding)	0 = Off (default) 1 = On Default is 0	Enable per class of service.
20-06-01	Class of Service for Extensions	0~15	Default: Class 1
20-09-07	Class of Service Options (Incoming Call Service) – Call Queuing	0 = Off 1 = On Default is 1	Must be Off for Call Forward – Busy to operate.
20-13-06	Class of Service Options (Supplementary Service) – Automatic Off Hook Signaling (Automatic Override)	0 = Off 1 = On Default is 1	Must be Off for Call Forward – Busy to operate.
15-07-01	Programmable Function Keys	10 = Call Forward – Immediate 11 = Call Forward – Busy 12 = Call Forward – No Answer 13 = Call Forward – Busy No Answer	Service Codes: 848 843 845 844
14-01-13	Basic Trunk Data Setup – Trunk-to-Trunk Transfer Loop Supervision	0 = Disable 1 = Enable Default is 1	Must enable for Trunk-to-Trunk Transfer, Call Forward – Off-Premise, and tandem trunking.
50-06-01	CCIS Feature Availability – Link Reconnect	0 = Not Available 1 = Available Default is 1	Enable/Disable Link Reconnect.
50-05-01	CCIS Maximum Call Forwarding Hop Counter	0~7 Hops Default is 5	Set Maximum Hops allowed in a CCIS network.

Call Park Retrieve – K-CCIS

Feature Description

This feature allows a station user to retrieve Parked Calls at remote sites across K-CCIS. Locally parked calls can be retrieved from a remote system, connected via K-CCIS, by dialling the Call Park Hold Group Number, plus the park orbit location.

System Availability

Terminal Type:

All Terminals

Required Components:

GPZ-IPLE

Operating Procedures

Retrieve Park Call at remote location:

1. Go off-hook, and wait for internal dial tone.
2. Dial the Call Park Retrieve Access Code 861 (default) + Park Hold Group Number (1~64) + Park Orbit Number (1~64) of the call to be retrieved. Call

(Park Retrieve access codes cannot be the same at all locations in the K-CCIS Network.)

3. Talk with party.

Service Conditions

General:

- A different Call Park Retrieve Access Code must be programmed for each system in the K-CCIS network.
- The Park Group Number and Park Orbit Number must be dialled immediately following the Park Retrieve Service Code.
- When two or more stations attempt to retrieve the parked call, only one station can retrieve the call.
- A station connected to a PBX can retrieve a parked call in an UNIVERGE SV9100, but the station connected to the UNIVERGE SV9100 system cannot retrieve a parked call in a PBX.
- A Park Hold key cannot be used to retrieve a parked call from a distant system.
- F-Routes are required to route Call Park Retrieve Access Code to proper system in the K-CCIS network.
- When a remote location retrieves a call from another location, the call is treated as if it were transferred from the distant location.
- SMDR reports the retrieved call from the distant location as if it were a transferred call.
- When a call that has Caller ID Information is retrieved at the distant location the Caller ID information is treated as if it were a transferred call.
- Link Reconnect operates when the trunk is retrieved back to the origination system.

Restrictions:

- A Call cannot be placed into remote systems Call Park Location.
- Call Park Retrieve – K-CCIS is only a Key System-to-Key System supported feature.
- The digit (# or *) cannot be used in conjunction with IP K-CCIS.
- When the UNIVERGE SV9100 is connected to the Electra Elite IPK II, the maximum digits assignment in the UNIVERGE SV9100 is determined by Program 44-05-09.
- Call Park Searching is supported in the local system only.

Related Feature List

- Call Park – System

Guide to Feature Programming

This guide provides a list of associated Programs that support this feature.

Park Originate System

Program/ Item No.	Description/ Selection	Assigned Data	Comments
11-12-32	Answer for Park	861 (default)	This varies based on the K-CCIS network configuration and PRG 11-01-01.
20-14-12	Class of Service for DISA/ E&M – Retrieve Park Hold	0 = Off (default) 1 = On	Enable Retrieve Park Hold feature per Class of Service.
24-03-01	Park Group	01~64 1 = Default	Assigns an extension to a Park Group.

Remote System (Call Park Retrieve)

Program/ Item No.	Description/ Selection	Assigned Data	Comments
11-01-01	System Numbering		
11-12-32	Service Code Setup (for Service Access) – Answer for Park Hold	Default is 861	
20-14-12	Class of Service Options for DISA/E&M – Retrieve Park Hold	0 = Off 1 = On Default is 1	Enable Retrieve Park Hold feature per Class of Service.
24-03-01	Park Group	01~64 Default is 1	Assigns an extension to a Park Group.
44-02-01	Dial Analysis Table for ARS/F-Route Access – Dial	Analysis Table 1 = 861 Default is No Setting	Assigns access code used to retrieve the parked call.

Program/ Item No.	Description/ Selection	Assigned Data	Comments
44-02-02	Dial Analysis Table for ARS/F-Route Access – Service Type	0 = No setting (None) 1 = Extension Call (Own) 2 = ARS/F-Route Table (F-Route) 3 = Dial Extension. Analyze Table (Option) Default is 2	To assign the service type used.
44-02-03	Dial Analysis Table for ARS/F-Route Access – Additional Data	0 = No setting 1 = Delete Digits = 0~255 (255 = delete all digits) 2 = 0~500 3 = Dial Extension Analyze Table Number = 0~4 Default is 0	Enter additional data required for the Service Type selected in PRG 44-02-02.
44-05-01	ARS/F-Route Table – Trunk Group Number	Trunk Groups (1~254)	Select trunk group number used for outgoing ARS calls. Setting of 255 = Internal Extension Call.
44-05-02	ARS/F-Route Table – Delete digits	0 = No setting 1~254 255 = Delete all Digits Default is 0	Enter number of digits to delete from the dialed number.
44-05-03	ARS/F-Route Table – Additional Dial Number Table	0 = No setting 1~1000 Default is 0	Enter table number (defined in 44-06) for additional digits to be dialed.
44-05-09	ARS/F-Route Table – Max Digit	0 = No Max 1~24 Default is 0	Assign Max digits for the Call Park Retrieve Access Code.

Call Transfer – All Calls – K-CCIS

Feature Description

This feature allows a station user to transfer incoming or outgoing Central Office, intraoffice and interoffice calls to another station in the K-CCIS network without Attendant assistance. For more details, refer to the UNIVERGE SV9100 Features and Specifications Manual.

System Availability

Terminal Type:

All multiline terminals

Required Components:

GPZ-IPLE

Operating Procedures

Using a Multiline Terminal with a call in progress (Closed Numbering Plan):

1. Press Transfer, and internal dial tone is heard. The call is placed on Common Hold.
2. Dial the distant K-CCIS station number where the call is to be transferred.
3. Wait for the ringback tone.
4. Hang up.

- OR -

1. When the party answers, announce the transfer.
2. Restore the handset (transfer is completed).

1. Using a Multiline Terminal with a call in progress (Open Numbering Plan):
2. Press Transfer, and receive internal dial tone. The call is placed on Common Hold.
3. Dial the trunk Access Code.
4. Dial the Office Code number.
5. Dial the distant K-CCIS station number where the call is to be transferred.
6. Wait for the ringback tone.
7. Hang up.

- OR -

1. When the party answers, announce the transfer.
2. Restore the handset (transfer is completed).

Service Conditions

General:

- A UNIVERGE SV9100 station can receive a K-CCIS transferred call as a camp-on call if allowed by Class of Service.

Restrictions:

- Trunk-to-Trunk Transfer must be allowed in Program 14-01-13 (Trunk-to-Trunk Transfer Yes/No Selection).
- A blind transfer across a K-CCIS link cannot be completed until ringback tone is received at the transferring station.

Related Feature List

- Link Reconnect – K-CCIS
- Station-to-Station Calling – K-CCIS
- Uniform Numbering Plan – K-CCIS

Guide to Feature Programming

This guide provides a list of associated Programs that support this feature.

Program/ Item No.	Description/ Selection	Assigned Data	Comments
20-09-07	Class of Service Options (Incoming Call Service) – Call Queuing	0 = Off 1 = On Default is 1	To enable receiving Call Queuing.
20-06-01	Class of Service for Extensions	0~ 15	Default: Class 1
20-09-01	Class of Service Options (Incoming Call Service) – Second Call for DID/DISA/ DIL/E&M Override	0 = Off 1 = On Default is 1	Turn Off or On the extension ability to receive the second call.
20-13-06	Class of Service Options (Supplementary Service) – Automatic Off Hook Signaling (Automatic Override)	0 = Manually 1 = Automatically Default is 1	Allow a busy extension user to manually or automatically receive off-hook signals.
14-01-13	Basic Trunk Date setup – Trunk-to-Trunk Transfer Loop Supervision	0 = Disable 1 = Enable Default is 1	Must enable for Trunk-to-Trunk Transfer, Call-Forward – Off-Premise, or tandem trunking.
50-06-01	CCIS Feature Availability – Link Reconnect	0 = Not Available 1 = Enable Default is 1	Enable Link Reconnect.

Calling Name Display – K-CCIS

Feature Description

This feature permits the station name of a calling or called party at another switching office to be displayed on a multiline terminal, through the K-CCIS network. For more details, refer to the UNIVERGE SV9100 Features and Specifications Manual.

System Availability

Terminal Type:

All multiline terminals

Required Components:

GPZ-IPLE

Operating Procedures

Normal call handling procedures apply.

Service Conditions

General:

- Both the caller/calling station name and number can be displayed on an UNIVERGE SV9100 station if allowed by Class of Service.

- For incoming or outgoing K-CCIS calls, the Calling/Called Name and Number are displayed for the entire length of the call including the Elapsed Call Time.

RESTRICTIONS:

In the UNIVERGE SV9100 system, only 12 digits/characters can be entered for each station name.

Related Feature List

- Calling Number Display – K-CCIS
- Station-to-Station Calling – K-CCIS
- Uniform Numbering Plan – K-CCIS

Guide to Feature Programming

This guide provides a list of associated Programs that support this feature.

Program/ Item No.	Description/ Selection	Assigned Data	Comments
14-02-10	Analog Trunk Date Setup – Caller ID	0 = No 1 = Yes Default is 0	Enable/Disable a trunk ability to receive Caller ID.
20-09-02	Class of Service Options (Incoming Call Service) – Caller ID Display	0 = Off 1 = On Default is 0	Control the Caller ID Display at an extension.
20-09-08	Class of Service Options (Incoming Call Service) – Calling Party Information	0 = Off 1 = On Default is 1	Enable receiving Calling Party Information from K-CCIS.
20-06-01	Class of Service for Extensions	0~15	Default: Class 1
50-02-05	Connecting System Settings – Calling Name Indication (T1)	0 = Disable 1 = Enable Default is 1	Enable receiving Calling Name indication from K-CCIS.
15-01-01	Basic Extension Data Setup – Extension Name	Up to 12 Characters Default: 200 = EXT 200 201 = EXT 201 etc.	Set the extension/Virtual extension name.

Calling Number Display – K-CCIS

Feature Description

This feature permits the number of a calling or called party at another switching office, to be displayed on a multiline terminal through the K-CCIS network. For more details, refer to the UNIVERGE SV9100 Features and Specifications Manual.

System Availability

Terminal Type:

All multiline terminals

Required Components:
GPZ-IPLE

Operating Procedures
Normal call handling procedures apply.

Service Conditions

General:
- Both the caller/calling station number and name can be displayed on an UNIVERGE SV9100 station if allowed by Class of Service.
- For incoming or outgoing K-CCIS calls, the Calling/Called Name and Number are displayed for the entire length of the call including the Elapsed Call Time.
- For an open numbering plan the Office Code number and station number are displayed for caller/ calling station number.

Restrictions:
- The UNIVERGE SV9100 supports 2 to 8-Digit station numbers.
- When calling over a K-CCIS tandem connection, the calling party number (CPN) is transferred to the ISDN network.

Related Feature List
- Calling Name Display – K-CCIS
- Station-to-Station Calling – K-CCIS
- Uniform Numbering Plan – K-CCIS

Guide to Feature Programming
This guide provides a list of associated Programs that support this feature.

Program/ Item No.	Description/ Selection	Assigned Data	Comments
14-02-10	Analog Trunk Date Setup – Caller ID	0 = Disable (No) 1 = Enable (Yes) Default is 0	Enable/Disable a trunk ability to receive Caller ID.
20-09-02	Class of Service Options (Incoming Call Service) – Caller ID Display	0 = Off 1 = On Default is 0	Control the Caller ID Display at an extension.
20-09-08	Class of Service Options (Incoming Call Service) – Calling Party Information	0 = Off 1 = On Default is 1	Enable receiving Calling Party Information from K-CCIS.
20-06-01	Class of Service for Extensions	0~15	Default: Class 1
50-02-05	Connecting System Settings – Calling Name Indication (T1)	0 = Disable 1 = Enable Default is 1	Enable receiving Calling Name indication from K-CCIS.
15-01-01	Basic Extension Data Setup – Extension Name	Up to 12 Characters Default: 200 = EXT 200 201 = EXT 201 etc.	Set the extension/Virtual extension name.

Calling Party Number (CPN) Presentation from Station – K-CCIS

Feature Description

Calling Party Number (CPN) Presentation from Station K-CCIS feature allows each station of the remote systems a unique 10-digit number (the DID number of the originating station) to be sent out over the PRI circuit of the main system.

System Availability

Terminal Type:

All Terminals

Required Components:

GPZ-IPLE

Operating Procedures

Placing a call with CPN:

- Lift the handset or press Speaker.
- Dial 9 + the number.
- Converse with caller.
- Hang up the handset.

Service Conditions

Restrictions:

- A maximum of 16 digits can be assigned as the Calling Party Number (CPN) in Program 21-12-01 and Program 21-13-01.
- The PRI provider must provision for the CPN used for E911. The CPN must be within the allowable range. For more information please contact your local ISDN provider regarding allowable ranges.
- The Calling Party Number (CPN) is sent only to the network when the calling party from the remote system dials a trunk access code of **9** when making an outbound call.
- The Calling Party Number (CPN) is not sent to the network when the originating station of the remote system calls a station in the main system that is call forwarded off site.

Related Feature List

- ISDN Compatibility
- Automatic Route Selection
- Central Office Calls, Placing

Guide to Feature Programming

This guide provides a list of associated Programs that support this feature.

Program/ Item No.	Description/ Selection	Assigned Data	Comments
14-01-24	Basic Trunk Data Setup – Trunk-to-Trunk Outgoing Caller ID through Mode	0 = Off 1 = On Default is 0	Enable Outgoing Caller ID through Mode for each CCIS trunk to enable CPN information to pass through the Tandem Office. Tandem System Only
20-08-13	Class of Service Options (Outgoing Call Service) – ISDN CLIP	0 = Off 1 = On Default is 0	Determine if the ISDN calling line identity presentation and screening indicators are to be allowed.
21-12-01	ISDN Calling Party Number Setup for Trunks	Up to 16 digits max. Default is No Setting	Assign each trunk a Calling Party Number. When a call is made by an extension which does not have an Extension Calling Number assigned (Program 21-13), the system sends the calling number for the ISDN trunk defined in 21-12.
21-13-01	ISDN Calling Party Number Setup for Extensions	Up to 16 digits max. Default is No Setting	Assign each extension a Calling Party Number.

Centralised BLF (K-CCIS)

Feature Description

This feature provides a busy indication for another station across the K-CCIS network on programmed Direct Station Selection/Busy Lamp Field (DSS/BLF) keys. The busy indication is a red LED associated with a Feature Access or One-Touch key programmed for Centralised BLF (K-CCIS). Pressing the Centralised DSS/BLF key allows direct access to the station through the K-CCIS network. Do Not Disturb and Voice Mail Message Waiting on Line key indications are also supported. For more details, refer to the UNIVERGE SV9100 Features and Specifications Manual.

System Availability

Terminal Type:

All multiline terminals
Attendant Add-On Console

Required Components:

GPZ-IPLE

Operating Procedures

To program a Feature Access or One-Touch key for Centralised DSS/BLF:

1. Press Speaker.
2. Dial 851.
3. Press the key to be programmed.
4. Dial 01 to assign a DSS/One Touch Key.
5. Dial the station number.

6. Press Hold.

Using a Feature Access or a One-Touch key programmed for Centralised DSS/BLF:

1. Press the programmed Feature Access or One-Touch key. Hear ringback tone.
2. When the called party answers, lift the handset or talk using handsfree if allowed.

Service Conditions

General:

- Voice Mail Message Waiting on Line Key indication is supported for Centralised DSS/BLF keys if PRG 20-13-41 [Class of Service Options (Supplementary Service)] – VM Message Indication on DSS/BLF key (VMS Message Indication) is allowed.
- If Voice Mail Message Waiting on Line Key indication is allowed and a VM Message Waiting indication is provided (a new message is stored), pressing the Centralised DSS/BLF key performs the following;
    - At system with Voice Mail installed, the user is logged into the owner mail box.
    - At remote systems, the station is called.

BLF Sending Service Conditions:

- The maximum number of destination offices for sending BLF messages is eight per system.
- Up to 120 Extension Numbers (entries into the table) can be assigned for sending BLF messages. With each assigned Extension Number, up to eight destination offices can be selected until a maximum of 240 total sending Extension Numbers are assigned.
- A maximum of 240 total sending Extension Numbers (BLF messages) can be assigned. If 30 Extension Numbers (entries into the table) are assigned with each set for all eight groups (systems), the 240 limit is reached and no more Extension Numbers can be entered.
- The BLF messages are sent in a four-second cycle (at default), so some delay occurs to change the indication in the destination office. In the network configured with two systems, it can take about four to five seconds (at default) to change the BLF indication in the destination office.
- This feature is provided with DSS/One-Touch Keys on multiline terminals and with an Attendant Add-On Console.
- When the button on the Attendant Add-On Console has a Mail Box button of a remote user programmed and the button is pressed the call is placed to the station on the remote side.

BLF Receiving Service Conditions:

- BLF information can be received for up to 120 remote extensions per system.
- All multiline terminals in the system can assign Centralised DSS/BLF keys for the supported remote extensions.
- The LED indication of the DSS/BLF button on a multiline terminal is as follows:
- Idle – No lamp indication
- Busy – Steady red lamp
- Do Not Disturb – Flashing red lamp
- VM Message Waiting – Fast flashing red lamp
- The LED indication of the DSS/BLF button on the Attendant Add-on Console is as follows:
    - Idle No lamp indication
    - Busy Steady red lamp
    - Do Not Disturb Flashing red lamp
    - VM Message Waiting Fast flashing red lamp
- The BLF Information expels when data cannot be sent because of link disconnect. Status changes of BLF information while the system could not send data are not indicated on restoration.
- The Voice Mail MSG Waiting has priority over any other state of the flashing line key or One-Touch key.

Restrictions:

- This feature is not supported between UNIVERGE SV9100 and NEAX PBXs.
- This feature is supported with a Closed Numbering Plan only (not available with an Open Numbering plan).

- The same extension line from a remote site can be assigned to multiple DSS/One Touch keys.
- The BLF information is expelled when data cannot be sent if the K-CCIS link is down. The UNIVERGE SV9100 does not send BLF information again when the K-CCIS link is restored.
- BLF messages can be forwarded up to eight times in the network. When designing the K-CCIS network, this should be a consideration.
- When a Centralised DSS/BLF key is first programmed on a Feature Access or One Touch key, the BLF status does not change (update) until new BLF information is received from the remote system.

Related Feature List

- Do Not Disturb (DND)
- Feature Access – User Programmable
- Voice Mail Message Indication on Line Keys

Guide to Feature Programming (FOR MAIN SYSTEM)

This guide provides a list of associated Programs that support this feature.

(For Sending System)

Program/ Item No.	Description/ Selection	Assigned Data	Comments
30-01-01	DSS Console Operating Mode	0 = Business Mode 1 = Hotel Mode 2 = ACD Monitor Mode 3 = Business/ACD Mode	
30-02-01	DSS Console Extension Assignment	Up to eight digits Default is No Setting.	Identify extensions with DSS Consoles attached.
30-03-01	DSS Console Key assignment	Keys No. 001~114 00~99 = General Functional Level *00~*99 = Appearance Functional Level Default = extensions. 101~160	Customize key assignments for DSS Consoles 1~32.
50-08-01	CCIS Centralized BLF Sending Group Assignment – Destination Point Code	0~16367 1~8+Destination Point Code Default is 0	Define the Point Code of Billing Center Office.

Program/ Item No.	Description/ Selection	Assigned Data	Comments
50-08-02	CCIS Centralized BLF Sending Group Assignment – CCIS Route ID	0~8 Default is 0	Define the CCIS Route ID to send Billing Center Office. ✎ Not used with IP K-CCIS.
50-09-01	CCIS Centralized BLF Sending Extension Number Assignment – Extension number	Up to eight digits Default is No setting.	BLF message is indicated when the status of the specified extension number is changed.
50-09-02	CCIS Centralized BLF Sending Extension Number Assignment – Send to Sending Group 1	Select Tables 1~ 120 0 = Disable 1 = Enable Default is 0	Enable sending BLF to Send Group 1 assigned in PRG 50-08-XX.
50-10-01	CCIS Centralized BLF Interval Time Assignment – Type of Interval Time	0 = 4 seconds 1 = 8 seconds 2 = 12 seconds 3 = 16 seconds Default is 0	Assign BLF sending interval to each sending system.

(For Receiving System)

Program/ Item No.	Description/ Selection	Assigned Data	Comments
20-13-41	Class of Service Options (Supplementary Service) – Voice Mail Message Indication on DSS key	0 = Off 1 = On Default is 0	Allow the DSS/BLF to indicate when the extension has a new message waiting in VM.
15-07-01	Programmable Function keys	LK01 = ✱01(Trunk Line Key)	Enter extension number up to eight digits.
20-06-01	Class of Service for Extensions	0~15	Extension 101 is in Class 15 by default. All other extensions are in Class 1.
30-03-01	DSS Console Key Assignment	1~114	0~99 (General Functional) ✱00~✱99 (Appearance Functional Level) 95 = Page Switching

Centralised Day/Night Mode Change – K-CCIS

Feature Description

This feature switches the Day/Night mode of a remote office that is linked to a main office using K-CCIS, in accordance with the Day/Night mode switching from an Attendant Position at the main office. When a UNIVERGE SV9100 system is connected to another UNIVERGE SV9100 system, the main office *can* control remote offices. For more details, refer to the UNIVERGE SV9100 Features and Specifications Manual.

System Availability

Terminal Type:
All multiline terminals

Required Components
GPZ-IPLE

Operating Procedures
To set or cancel Night Transfer system-wide from an Attendant Position:

Main Office:
1. Press Speaker.
2. Dial Access Code 818.
3. Dial the Night service Code:
   1. Day 1 mode
   2. Night 1 mode
   3. Midnight 1 mode

   4. Rest 1 mode
   5. Day 2 mode
   6. Night 2 mode
   7. Midnight 2 mode
   8. Rest 2 mode
4. Press Speaker or hang up.

- OR -

1. Press the Night Transfer key on the Attendant Add-On Console.

Remote Office:
No manual operation is required.

Service Conditions

General:
- A maximum of 16 remote offices can be controlled by one main office.
- If Automatic Day/Night Mode Switching is assigned in the main office, all remote offices change the mode, if assigned.
- If the remote office is to be restricted from overriding the Day/Night Mode setting, the following Programming Commands should be assigned:
- 12-01-01 Night Mode Function Setup – Manual Night Service enable
- 20-07-01 Class of Service Options (Administrator Level) – Manual Night Service enable
- When the remote office is in Night Mode (as assigned in the Centralised Day/Night Mode - K-CCIS feature), normal Night Mode indications are provided.
- The Night Mode indication is the first word (Night) on the second row of the multiline terminal LCD. The LED for any Feature Access key assigned for Night Mode transfer and the Night Mode key on the Attendant console are On.
- If the K-CCIS link is not available due to network trouble, the UNIVERGE SV9100 main office resends the K-CCIS Day/Night Mode switch command every 16 minutes.

Restrictions:
- Centralised Day/Night Mode switching from a main office can send a system-wide K-CCIS Day/Night mode switch command only. Individual Night Service Groups Mode switching is not supported.
- When an UNIVERGE SV9100 receives the K-CCIS Day/Night Mode switch command from a main office, the remote office changes all Night Service Groups to the requested mode.

- Program 50-03-01 (Destination Point Code Transfer Assignment) must be set for all offices for the Centralised Day/Night Mode feature.

Related Feature List

- Assigned Night Answer (ANA)
- Authorisation Code
- Automatic Day/Night Mode Switching
- Centralised Billing – K-CCIS
- Code Restriction
- Dial Access to Attendant – K-CCIS
- Direct Inward Termination (DIT)
- Flexible Ringing Assignment
- Night Call Pickup
- Night Chime
- Night Transfer
- Voice Mail Integration – K-CCIS

Guide to Feature Programming

This guide provides a list of associated Programs that support this feature.

Centralised Day/Night Mode Change

Program/ Item No.	Description/ Selection	Assigned Data	Comments
50-01-01	CCIS System Setting – CCIS Availability	0 = Disable 1 = Enable Default is 0	All CCIS settings lose functionality when this setting is 0.
50-03-01	CCIS Destination System Settings – Destination Point Code	0~16367 Default is 0	Enable for all offices for Centralized Day/Night mode change.
50-06-02	CCIS Feature Availability – Centralized Day/Night Switching (for message receiver side)	0 = Disable 1 = Enable Default is 1	If this data is set to 0, Link Reconnect does not run.
50-11-01	CCIS Centralized Day/ Night Switching Sending Group Assignment – Destination Point Code	Send Group (1~16) Point Code (1~16367) 0 = No Setting Default is 0	Select the Remote Office to send Day/Night Switching control message.
50-11-02	CCIS Centralized Day/ Night Switching Sending Group Assignment – CCIS Route ID	Send Group (1~16) CCIS Route ID (0~8) 0 = No Setting Default is 0	Select the Remote Office to send Day/Night Switching control message.
50-12-01	CCIS Centralized Day/ Night Mode to System Mode Assignment – Switching Synchronized Day/Night Mode Group	Day Mode = Mode 1~8 Default is 1 Night Mode = Mode 1~8 Default is 2	Set the mode for Day/Night Switching Synchronized Day/Night Group.

For Night Transfer Feature

Program/ Item No.	Description/ Selection	Assigned Data	Comments
12-01-01	Night Mode Function Setup – Manual Night Mode Switching	0 = Off 1 = On Default is 1	Allow user to activate Night Service by dialing a service code.
12-02-01	Automatic Night Service Patterns	Night Mode Group (1~32) Time Pattern Number (01~10) Set Time Number (01~20) Default = All Groups, All patterns: 00:00~00.00 for Mode 1	Set to define the daily pattern for the auto night mode switch setting.
12-03-01	Weekly Night Service Switching	Night Mode Service Group Number = 01~32 Default: 01 Sunday = Pattern 2 02 Monday = Pattern 1 03 Tuesday = Pattern 1 04 Wednesday = Pattern 1 05 Thursday = Pattern 1 06 Friday = Pattern 1 07 Saturday = Pattern 2	Set to define a weekly schedule of night switch settings.
12-04-01	Holiday Night Service Switching	Night Mode Service Group Number = 1~32 Default is No Setting	Set to define a yearly schedule for holiday.
30-03-01	DSS Console Key Assignment	Key Number (001~114) 00~99 = General Functional Level *00~*99 = Appearance Functional level Default is extensions. 101~160	Customize key assignments for DSS Consoles 1~32.
20-07-01	Class of Service Options (Administrator Level) – Manual Night Service Enabled	0 = Off 1 = On Default is 1 for COS 15, 0 for COS 1~14	
15-07-01	Programmable Function Keys	09 = Day/Night Mode Switch	Enter 0 to toggle night mode.
20-06-01	Class of Service for Extensions	0~15	Extension 101 is in Class 15 by default. All other extensions are in Class 1.

Centralised E911 – K-CCIS

Feature Description

This feature allows a remote system to transmit a Calling Party Number to the 911 Emergency System over a K-CCIS direct or tandem connection.

System Availability

Terminal Type:

All Stations

Required Components

GPZ-IPLE

Operating Procedures

To use this feature at any terminal:

1. Lift the handset, and wait for internal dial tone.
2. Dial 911.

- OR -

1. Dial 9 911.

Service Conditions

General:

- If you want to send your phone number via CCIS, please refer to Calling Party Number (CPN) Presentation from Station – K-CCIS
- The Calling Party Number (CPN) is sent only to the network when the remote system accesses an ISDN – PRI trunk in the distant system and the ISDN – PRI trunk has Calling Party Number (CPN) Presentation and Screening service enabled from the network.
- If Program 21-01-10 is programmed with an entry other than 0, a call does not have a talk path unless the user dials at least the number of digits entered in this option when placing an outgoing call. This means that an entry of 4 or higher in this program causes a problem when dialling 911. Since it is only a 3-digit number, the call does not have a talk path preventing the emergency dispatcher from hearing the caller. It is recommended that this option be kept at its default setting of 0 to prevent any problems with dialling 911.
- The attendant receives a notification each time a co-worker dials an emergency 911 call. This notification is the co-worker name and number display optionally accompanied by an audible alarm. Notification occurs regardless of whether the attendant is idle or busy on a call. You can optionally extend this ability to other supervisory extensions as well.
- The PRI provider must provision for the CPN used for E911. The CPN must be within the allowable range. For more information please contact your local ISDN provider regarding allowable ranges.
- Virtual Extensions notify the attendant with the stations name and number when an emergency 911 call is originated from the Virtual Extension.

Restrictions:

- Centralised E911 (outgoing with CES-ID) is not supported.
- A maximum of 16 digits can be assigned as the Calling party Number (CPN) in Program 21-13-01.
- If Virtual Extensions are used to make E911 calls, they provide the information for the VE key.

Related Feature List

- ISDN Compatibility
- Calling Party Number (CPN) Presentation from Station K-CCIS
- E911 Compatibility
- Automatic Route Selection

Guide to Feature Programming

This guide provides a list of associated Programs that support this feature.

Program/ Item No.	Description/ Selection	Assigned Data	Comments
20-08-13	Class of Service Options (Outgoing Call Service) – ISDN CLIP	0=Off 1=On Default is 0	Determine if the ISDN calling line identity presentation and screening indicators are to be allowed.
21-12-01	ISDN Calling Party Number Setup for Trunks	Up to 16 digits max. Default is No Setting	Assign each trunk a Calling Party Number. When a call is made by an extension which does not have an Extension Calling Number assigned (Program 21-13), the system sends the calling number for the ISDN trunk defined in 21-12.
21-13-01	ISDN Calling Party Number Setup for Extensions	Up to 16 digits max. Default is No Setting	Assign each extension a Calling Party Number.
14-01-24	Basic Trunk Data Setup – Trunk-to-Trunk Outgoing Caller ID Through Mode	0 = Disable (Off) 1 = Enable (On) Default is 0	Enable CPN information to pass through the Tandem Office.

Dial Access to Attendant – K-CCIS

Feature Description

This feature allows a station user to call an Attendant by dialling a call code through the K-CCIS network. For more details, refer to the UNIVERGE SV9100 Features and Specifications Manual.

System Availability

Terminal Type:

All multiline terminals

Required Components:

GPZ-IPLE

Operating Procedures

To call an Attendant Position:

1. Lift the handset or press Speaker.
2. Dial 0 or the operator call code if it is different from 0.

Service Conditions
General:

- The operator call code must be for an individual Attendant Access Code number.
- When calling to a UNIVERGE SV9100 Attendant Position, the SV9100 sends Operator to the call originator as the name.
- Shows Office Code if using Open Numbering Plan.
- If using an Open Numbering Plan and a call is made to an UNIVERGE SV9100 Attendant Position, the operator office code is included with the name.
- When making a call from a UNIVERGE SV9100 Attendant Position across a K-CCIS network, the Caller ID Name and Number display is the same as for a station-to-station call.
- In a Closed Numbering Plan network, a station can call an Attendant in the K-CCIS network by dialling 0.
- In an Open Numbering Plan network, a station user can call an Attendant within the K-CCIS network by dialling: Access Code + Office Code + 0.

Restrictions:

- Operator Calling, PRG 20-14-05, does not keep a Tie Line caller from dialling 0 for the operator.

Related Feature List

- Attendant Positions
- Calling Name Display – K-CCIS
- Calling Number Display – K-CCIS
- Centralised Day/Night Mode Change – K-CCIS
- Voice Calls – K-CCIS

Guide to Feature Programming

This guide provides a list of associated Programs that support this feature.

For Main System

Program/ Item No.	Description/ Selection	Assigned Data	Comments
11-01-01	System Numbering	Default is 0 = 1 digit Intercom	Refer to UNIVERGE SV8100 Programming Manual for all options and default settings.
20-17-01	Operator Extension – Operator Extension Number	Up to eight digits Default is not assigned	Define extension numbers that are used as operators. Assign only in KTS-to-KTS network.

For Remote System

Program/ Item No.	Description/ Selection	Assigned Data	Comments
11-01-01	System Numbering	Default is 0 = 1 digit; F-Route	Refer to UNIVERGE SV8100 Programming Manual for all options and default settings.
44-02-01	Dial analysis Table for ARS/F-Route Access – Dial	Analysis Table 1 = 0 Default is No Setting.	Assign access code (up to eight digits) to dial the Attendant.
44-02-02	Dial analysis Table for ARS/F-Route Access – Service Type	0 = No Setting (None) 1 = Extension Call (Own) 2 = ARS/F-Route Table (F-Route) 3 = Dial Extension Analyze Table (Option) Default is 0	Assign the service type to be used.
44-02-03	Dial analysis Table for ARS/F-Route Access – Additional Data	0 = No Setting 1 = Delete Digit = 0~255 (255: Delete all digits) 2 = 0~500 3 = Dial Extension Analyze Table Number (0~4) Default is 0	Enter additional data for Service Type selected in PRG 44-02-02.
44-05-01	ARS/F-Route Table – Trunk Group Number	0~100, 255 0 = No Setting 255 = Extension Call Default is 0	Select trunk group number for outgoing calls.
44-05-02	ARS/F-Route Table – Delete Digits	0 = No Setting 0~255 (255 = Delete all digits) Default is 0	Enter number of digits to delete from the dialed number.
44-05-03	ARS/F-Route Table – Additional Dial Number Table	0~1000 Default is 0	Enter Table Number defined in PRG 44-06.
44-05-09	ARS/F-Route Table – Maximum Digit	0~24 Default is 0	Assign Max. digits for Call Park Retrieve Access Code.
44-05-10	ARS/F-Route Table – CCIS over IP Destination Point Code	0~16367 Default is 0	Assign remote IP Destination Point Code.

Direct Inward Dialling – K-CCIS

Feature Description

This feature allows an incoming DID call (centralised DID) to be routed directly across a K-CCIS link to reach a station in the remote system without Attendant assistance. For more details, refer to the UNIVERGE SV9100 Features and Specifications Manual.

System Availability

Terminal Type:

All Stations

Required Components:

GPZ-IPLE

Operating Procedures

Normal call handling procedures apply.

Service Conditions

General:

- Call billing to the outside party starts when the incoming call connects to the K-CCIS trunk.
- When an incoming DID call from the CD-PRTA card with Caller ID information is transferred to the station in K-CCIS network, the Caller ID Name and Number follow across the K-CCIS network to the distant system.
- This feature is supported when a Closed Numbering Plan or Open Numbering is used.
- The UNIVERGE SV9100 system supports DID Digit Conversion when using station numbers with 2 to 8 digits.
- An extension on a remote system can be the destination for the DID Received Vacant Number Operation Assignment (Program 22-09-02).

Restrictions:

- Program 20-02-15 (Caller ID Display Mode) must be set to 0 to display the DID Name on incoming DID calls.
- Refer to the Key-Common Channel Interoffice Signalling (K-CCIS) feature for more details related to Single Line Telephone and IP (K-CCIS) support.

Related Feature List

- Key-Common Channel Interoffice Signalling (K-CCIS)
- Flexible Numbering of Stations – K-CCIS
- Uniform Numbering Plan – K-CCIS

Guide to Feature Programming

This guide provides a list of associated Programs that support this feature.

Program/ Item No.	Description/ Selection	Assigned Data	Comments
22-09-01	DID Basic data Setup – Expected Number of Digits	1~8 Default is 4	Assign number of digits the Table expects to receive from Telco. Use this program to make the system compatible with three- and four- digit DID service.
22-10-01	DID Translation Table Setup – Conversion Table Area Number	0 = No setting 1~2000 Default is 0	Program the Translation Table size.
22-11-01	DID Translation Number Conversion – Received Number	Maximum eight digits Default is No Setting	Assign the received number to the Conversion Table number.
22-11-02	DID Translation Number Conversion – Target Number	Maximum 24 digits Default is No Setting.	Assign the destination extension based on the digits received.
22-11-03	DID Translation Number Conversion – DID Name	Maximum 12 digits Default is No Setting	Assign the DID Name based on the digits received.

Dual Hold – K-CCIS

Feature Description

This feature allows two connected Multiline Telephones to be placed on hold simultaneously over the K-CCIS link. This enables the held parties to answer or originate a call from a secondary line or intercom path. For more details, refer to the UNIVERGE SV9100 Features and Specifications Manual.

System Availability

Terminal Type:

All multiline terminals

Required Components:

GPZ-IPLE

Operating Procedures

Normal call handling procedures apply.

Service Conditions

General:

- This feature is available for interoffice calls through K-CCIS.
- Both Common Hold and Exclusive Hold can be used for Dual Hold – K-CCIS.
- The K-CCIS call is held on a Call Appearance key.

Restrictions:

None

Related Feature List

- Station-to-Station Calling – K-CCIS

Guide to Feature Programming

This guide provides a list of associated Programs that support this feature.

Program/ Item No.	Description/ Selection	Assigned Data	Comments
24-01-01	System Options for Hold – Hold Recall Time	0~64800 seconds Default is 90	A call on Hold recalls to the extension that placed the call on hold after this time expires.
24-01-03	System Options for Hold – Exclusive Hold Recall Time	0~64800 seconds Default is 90	A call left on Exclusive Hold recalls to the extension that placed it on hold after this time expires.
20-29-01	Timer Class for Extensions – Day/Night Mode 1~8, Class Number	0~15 0 = Not Assigned Default is 0	Assign Timer Class (0~16) to each extension for night mode. Virtual extension numbers are included.
20-30-01	Timer Class for Trunks – Day/Night Mode 1~8, Class Number	0~15, #, ✱ 0 = Not Assigned Default is 0	Assign Timer Class (0~16) to each trunk for night mode.
20-31-01~23	Timer Class Timer Assignment	Refer to Flexible Timeouts in the UNIVERGE SV8100 Features and Specifications Manual for more Flexible Time details.	Assign times. These timers are referred when a class is set to any number from 1 to 16 in PRG 20-29-01/20-30-01.

Elapsed Time Display – K-CCIS

Feature Description

This feature provides an Elapsed Call Time on the LCD which shows the duration of time that a multiline terminal is connected to any call through the K-CCIS network. For more details, refer to the UNIVERGE SV9100 Features and Specifications Manual.

System Availability

Terminal Type:

All Display multiline terminals

Required Components:

GPZ-IPLE

Operating Procedures

No manual operation is required.

Service Conditions

General:

- When a call is retrieved from Exclusive Hold and/or Common Hold from the same station, the elapsed call timer begins at 0.
- When a call is transferred, the elapsed time of the party receiving the transfer begins at zero.

Restrictions:

For calls across a K-CCIS link, the Elapsed Call timer begins only after receiving answer supervision from the distant system.
For Voice Calls across the K-CCIS link, the Elapsed Call timer does not begin until the distant station answers.
For conference calls established across a K-CCIS link, the elapsed call timer does not start during an active conference call.

Related Feature List

- Station-to-Station Calling – K-CCIS

Guide to Feature Programming

This guide provides a list of associated Programs that support this feature.

Program/ Item No.	Description/ Selection	Assigned Data	Comments
20-13-36	Class of Service Options (Supplementary Service) – Call Duration Timer Display	0 = Off 1 = On Default is 1	Turn off the extension Call Timer. The system waits for the interdigit time (21-01-01) before this time begins.
20-09-06	Class of Service Options (Incoming Call Service) – Incoming Time Display	0 = Off 1 = On Default is 0	Turn on the Incoming Time and Date display on the LCD while the Telephone is ringing.

Flexible Numbering of Stations – K-CCIS

Station numbers can be assigned by the 10's group for 4-digit station numbers, 100's group for 5-digit, 1,000's group for 6-digit station numbers, and 10,000's group for 7-digit station numbers.

Example:

Station Numbering Plan	Site A	Site B	Site C
4-digit station numbers	1000 ~ 1009	1010 ~ 1019	1020 ~ 1029
5-digit station numbers	10000 ~ 10009	10010 ~ 10019	10020 ~ 10029
6-digit station numbers	100000 ~ 100009	100010 ~ 100019	100020 ~ 100029
7-digit station numbers	1000000 ~ 1000009	1000010 ~ 1000019	1000020 ~ 1000029
8-digit station numbers	10000000 ~ 10000009	10000010 ~ 10000019	10000020 ~ 10000029

Feature Description

This feature allows telephone numbers to be assigned to any stations in the K-CCIS network, based solely upon numbering plan limitations. For more details, refer to the UNIVERGE SV9100 Features and Specifications Manual.

System Availability

Terminal Type:
All Stations

Required Components:
GPZ-IPLE

Operating Procedures
Normal call handling procedures apply.

Service Conditions

General:
- Give careful consideration to the network numbering plan to avoid needless loss of Access Codes or duplication of telephone numbers.
- The first digit or first two digits of a telephone number distinguishes one system from another system.
- Station Numbering Plan can have 2 to 8 digits.

Restrictions:
- Tenant service is not provided, i.e., numbers cannot be duplicated for different tenants.
- Extension numbers should not start with 0, 9, * or #.
- For non-K-CCIS feature support, refer to the UNIVERGE SV9100 Features and Specifications Manual, Flexible Numbering Plan feature.

Related Feature List
- Key-Common Channel Interoffice Signalling (K-CCIS)
- Station-to-Station Calling – K-CCIS
- Uniform Numbering Plan – K-CCIS

Guide to Feature Programming
This guide provides a list of associated Programs that support this feature.

Program/ Item No.	Description/ Selection	Assigned Data	Comments
11-11-01	System Numbering	Default is 1 = 3-digit; Intercom	Refer to the UNIVERGE SV8100 Programming Manual for all options and default settings.
11-02-01	Extension Numbering – Dial (up to eight digits)	Default : 200 - 499 5000 - 5211	Assign up to eight digits for Extension Numbers.
11-20-01	Dial Extension Analyze Table – Dial (up to eight digits) Use tables 01~128 to assign the digits to be dialed using the Dial Extension Analyze Tables. These tables are used when Program 11-01-01 is set to option 9 = Dial Extension Analyze. (Up to eight digits can be assigned with valid entries: 0, 1~9, #, ✱).	Valid entries: 0, 1~9, #, ✱ Default is not assigned.	
11-20-02	Dial Extension Analyze Table – Type of Dials Assign the type of dial for the Dial Extension Analyze Table from Program 11-20-01. (Svc Code, Intercom, operator, or F-Route)	0 = Not used 1 = Service Code 2 = Intercom 5 = Operator 6 = F-Route Default is Not Set.	

Handsfree Answerback – K-CCIS

Feature Description

This feature allows Multiline Telephone station users to respond to voice calls through a K-CCIS network without lifting the handset. For more details, refer to the UNIVERGE SV9100 Features and Specifications Manual.

System Availability

Terminal Type:

All multiline terminals

Required Components:

GPZ-IPLE

Operating Procedures

To turn the microphone On/Off:

1. Press Feature.
2. Dial 1.

- OR -
Press the programmable line key assigned as the MIC On/Off key.

Service Conditions

Restrictions

Handsfree Answerback – (K-CCIS) can be used only when responding to Voice Calls – (K-CCIS) from a remote user.
After a user changes ring back tone to voice call, it cannot be changed back to ringing.
Voice Call cannot be set as the initial call across K-CCIS. The initial call must be a ringing call.

Related Feature List

- Voice Calls – K-CCIS

Guide to Feature Programming

This guide provides a list of associated Programs that support this feature.

Program/ Item No.	Description/ Selection	Assigned Data	Comments
11-16-03	Single Digit Service code Setup – Switching of Voice/Signal Call	Default is 1	Customize the one-digit Service Code used when a busy or ring back signal is heard.
11-12-06	Service Code Setup (for Service Access) – Switching of Voice Call and Signal Call	Default is 812	Toggle an ICM call between Handsfree Answerback or Forced Intercom Ringing for outgoing Intercom Calls.
20-08-10	Class of Service Options (Outgoing Call service) – Signal/Voice Call	0 = Off 1 = On Default is 1	Turn Off or On the ability to force Handsfree Answerback or Forced Intercom Ringing for outgoing Intercom Call on/off.
20-08-11	Class of Service Options (Outgoing Call service) – Protect for the Call Mode Switching from Caller (Internal Call)	0 = Off 1 = On Default is 0	When extension is set for ICM calls, enable this option to prevent callers from changing to voice announce mode.

Hot Line – K-CCIS

Feature Description

This feature allows two stations at different nodes in the K-CCIS network to be mutually associated on automatic ringdown through the K-CCIS network. For more details, refer to the UNIVERGE SV9100 Features and Specifications Manual.

System Availability

Terminal Type:

All multiline terminals

Required Components:

GPZ-IPLE

Operating Procedures

To execute at any station programmed for Hot Line:

1. Lift the handset or press Speaker.
2. The remote K-CCIS station is called.

Service Conditions

General:

Any multiline terminal (a maximum number of 512 stations) can be assigned for Hot Line – (K-CCIS). Either multiline terminal in a Hot Line – (K-CCIS) pair may transfer a Hot Line call to another station in the K-CCIS network using the Call Transfer – All Calls - (K-CCIS) feature.

Restrictions:

None

Related Feature List

- Call Transfer – All Calls - K-CCIS
- Station-to-Station Calling – K-CCIS
- Uniform Numbering Plan – K-CCIS

Guide to Feature Programming

This guide provides a list of associated Programs that support this feature.

Program/ Item No.	Description/ Selection	Assigned Data	Comments
15-01-02	Basic Extension Data Setup – Outgoing Trunk Line Preference	0 = Off 1 = On Default is 0	If enabled, the extension user gets trunk dial tone when the handset is lifted.
20-06-01	Class of Service for Extensions	1 ~ 15 Default: Class 1	Assign a Class of Service to an extension
20-08-09	Class of Service Options (Outgoing Call Service) – Hotline/ Extension Ringdown	0 = Off 1 = On Default is 0	Turn Off or On Ringdown Extension for extensions with this COS.
20-08-19	Class of Service Options (Outgoing Call Service) – Hotline for SPK	0 = Off 1 = On Default is 0	When Hotline is programmed and 20-08-19 is turned ON (1), the user can press the speaker button and the Hotline destination is dialed.
21-01-09	System Options for Outgoing Calls – Ringdown Extension Timer (Hotline Start)	0~64800 seconds Default is 5	A Ringdown extension automatically calls its programmed destination after this time.
21-11-01	Extension Ringdown (Hotline) Assignment – Hotline Destination Number	Maximum 24 digits (0~9, ✱, #, Pause, Hook Flash, and @(code to wait for answer supervision) Default is No Setting	Define the Hotline Destination number for each extension number.

Link Reconnect – K-CCIS

Feature Description

This feature provides the system that is connected to a K-CCIS network with the ability to release the redundant K-CCIS link connections and reconnect the link with the system for efficient usage of the K-CCIS trunks.

System Availability

Terminal Type:

All multiline terminals

Required Components

GPZ-IPLE

Operating Procedures

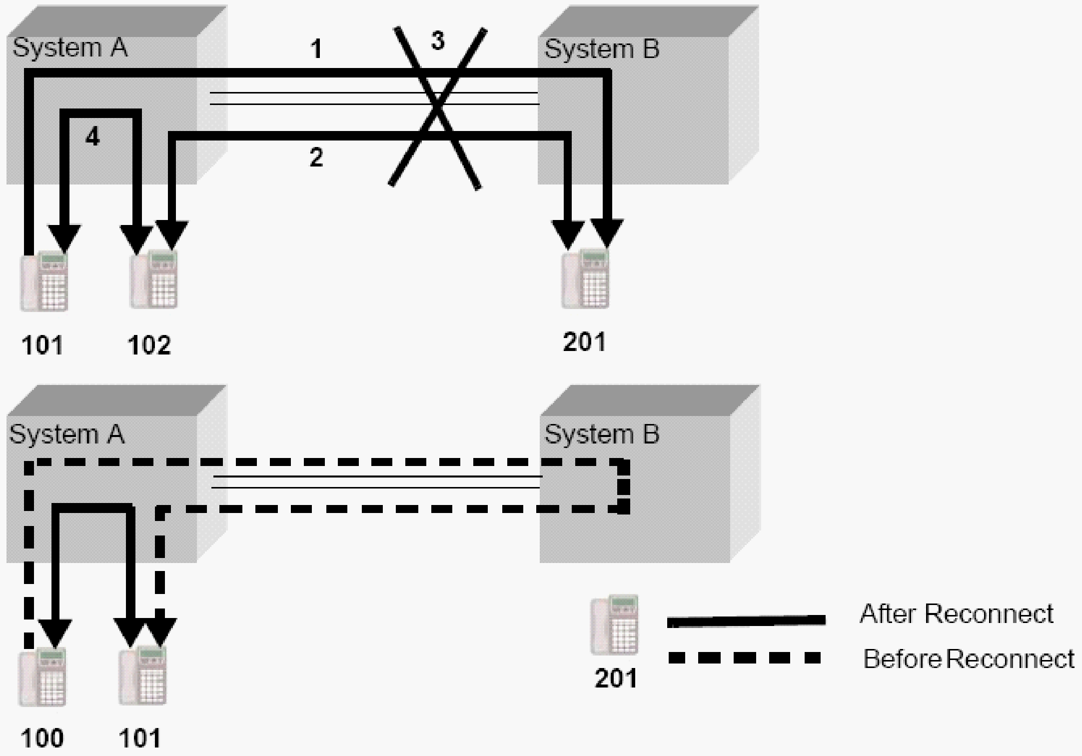
Normal call handling procedures apply.

Service Conditions

General:

The link reconnect ability is provided for a station call over K-CCIS that is transferred or forwarded to another station or trunk in the same office as the call originating station.

Example:

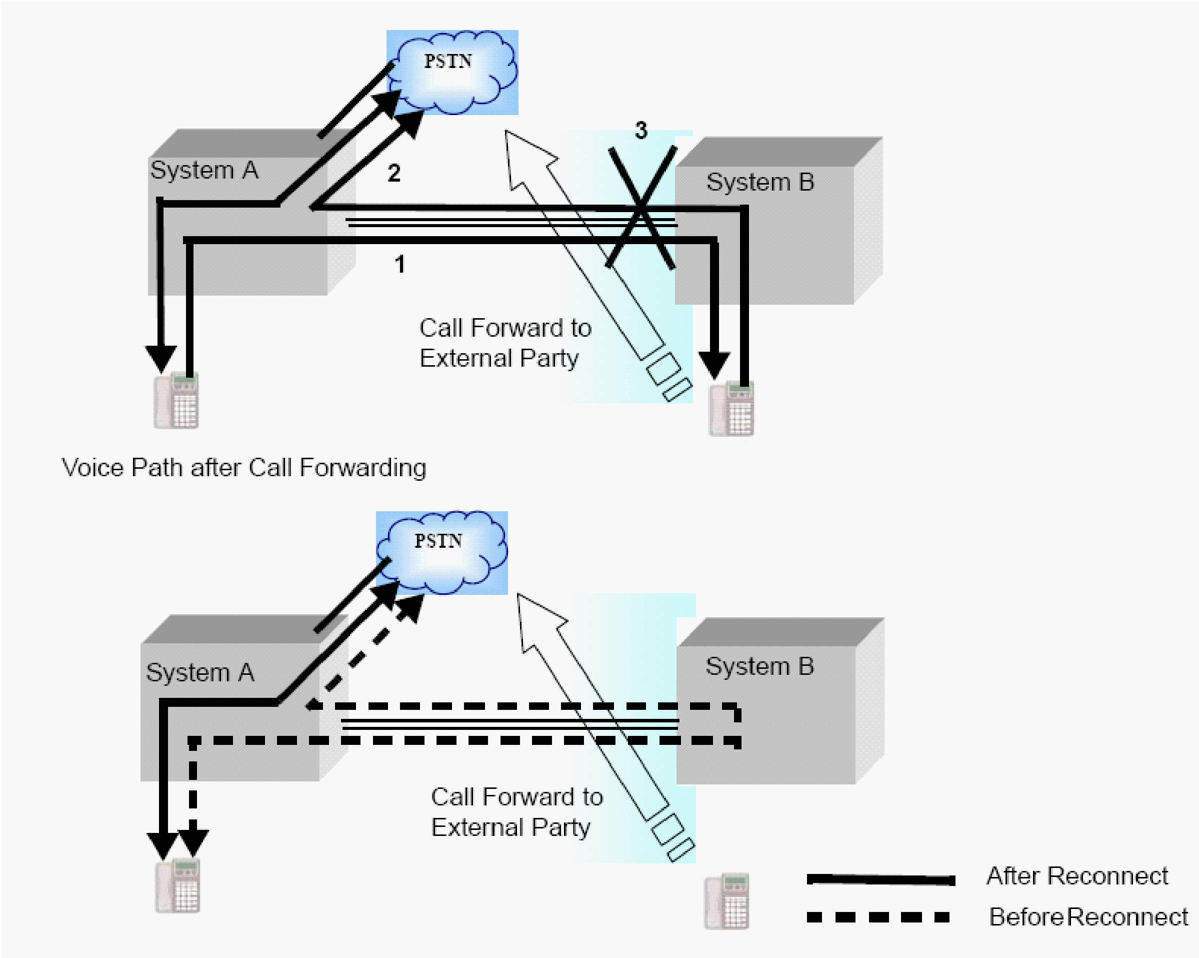


Stations 101, 102, and 201 must be multiline terminals.

When Station A holds the call or is in the conference, Link Reconnect is not provided.

- A trunk call (CO/PBX/TIE/DID/K-CCIS) over a K-CCIS network is transferred or forwarded to another station or trunk within the same office as the original incoming trunk.

Call Forward to Trunk Line



- Link reconnect occurs after answering a transferred or forwarded K-CCIS call.

Restrictions:

- Answer supervision is required for Link Reconnect to occur. For outgoing calls on analogue trunks, Answer supervision is based on the Elapsed Call Time - Program 21-01-03 (Trunk Interdigit Time).
- When a call is on hold, or in a conference, and is transferred back across the K-CCIS link, Link Reconnect is not provided.

Related Feature List

- Call Forwarding – All Calls – K-CCIS
- Call Forwarding – Busy/No Answer – K-CCIS
- Call Transfer – All Calls – K-CCIS
- Multiple Call Forwarding – All Calls – K-CCIS
- Multiple Call Forwarding – Busy/No Answer – K-CCIS
- Station-to-Station Calling – K-CCIS
- Uniform Numbering Plan – K-CCIS

Guide to Feature Programming

This guide provides a list of associated Programs that support this feature.

Program/ Item No.	Description/ Selection	Assigned Data	Comments
50-06-01	CCIS Feature Availability – Link Reconnect	0 = Not Available 1 = Available Default is 1	Enable Link Reconnect.
21-01-03	System Options for Outgoing Calls – Trunk Interdigit Time (External)	0 = Disabled 1~64800 seconds Default is 5	The system waits for this time to expire before placing the call (Call time starts after this time expires).

Multiple Call Forwarding – All Calls – K-CCIS

Feature Description

This feature allows a Multiple Call Forwarding – All Calls sequence to be forwarded over a K-CCIS network to a station in another office. For more details, refer to the UNIVERGE SV9100 Features and Specifications Manual.

System Availability

Terminal Type:

All multiline terminals

Required Components:

GPZ-IPLE

Operating Procedures

To set Call Forward – All Calls – K-CCIS from a Multiline Telephone (Closed Numbering Plan):

1. Press the Call Forward – All ON/OFF key.
2. Dial 1 to set. Then enter the K-CCIS station number.
3. Press Speaker.

- OR -

1. Lift the handset or press Speaker.
2. Dial Access Code 741 (set as default). Then Dial 1 to set.
3. Dial the remote K-CCIS station number.
4. Restore handset or press Speaker.

To set Call Forward – All Calls – K-CCIS from a Multiline Telephone (Open Numbering Plan):

1. Press the Call Forward – All Call ON/OFF key, and Dial 1 to set.
2. Dial the trunk Access Code (normally 8).
3. Dial the Office Code number.
4. Dial the distant K-CCIS station number.
5. Press Speaker.

- OR -

1. Lift the handset or press Speaker.
2. Dial Access Code 741 (set as default), and Dial 1 to set.
3. Dial the trunk Access Code (normally 8).
4. Dial the Office Code number.
5. Dial the distant K-CCIS station number.
6. Restore handset or press Speaker.

To cancel Call Forward – All Calls – K-CCIS from a Multiline Telephone:

1. Press Call Forward – All Call On/Off key.

2. Dial 0 to cancel.
3. Press Speaker.

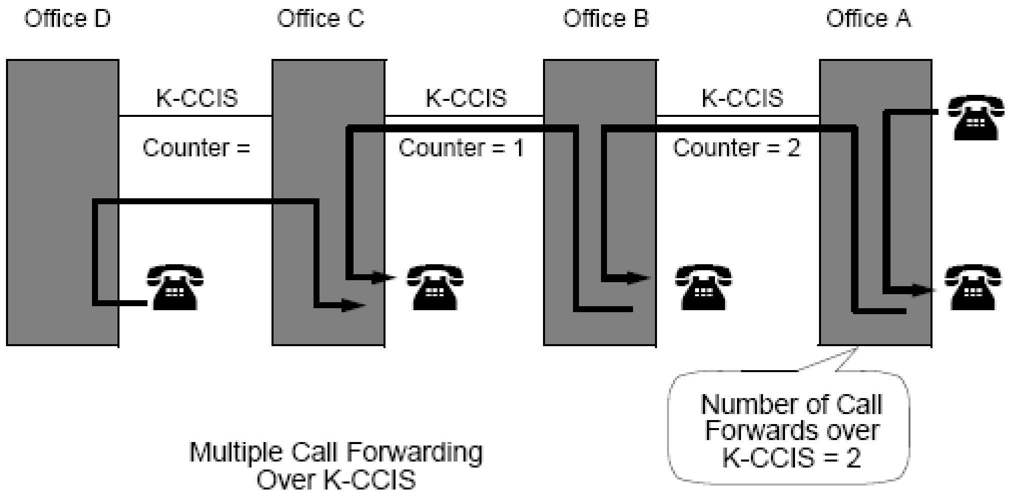
- OR -

1. Lift the handset or press Speaker.
2. Dial Access Code 741 (set as default), and Dial 0 to cancel.
3. Restore handset or press Speaker.

Service Conditions

General:

- Multiple Call Forwarding – All Calls – K-CCIS can forward a call up to seven times across K-CCIS links (up to seven hops) depending on system data.
- Multiple Call Forwarding over a K-CCIS link is combined with Multiple Call Forwarding – All Calls/ Busy/No Answer.
- If the calling station is set as the destination in a multiple hop scenario, Multiple Call Forwarding – All Calls – K-CCIS is not performed (*i.e.*, an infinite loop does not occur).
- For multiple Call Forwarding – All Calls/Busy (Immediate) calls, the display on the calling party Multiline Telephone displays the terminating station user name and the station number for the first station of a distant system in the Multiple Call Forwarding group. For the terminating station, the telephone display indicates the name and the number of the calling party and the trunk number of the incoming call.
- When a calling station has been Call Forwarding – All Calls – K-CCIS to the maximum times assigned in Program 50-05-01 (K-CCIS Maximum Call Forwarding Hop Assignment) and encounters another Call Forwarding – All Calls – K-CCIS condition, the calling station is not forwarded and rings at the
- last destination.
- If the destination station in a Multiple Call Forwarding – All Calls – K-CCIS situation is busy and has not set Call Forwarding – Busy and has Call Alert Notification disabled, the calling party receives busy tone.
- When combining Call Forwarding – Busy and Call Forwarding – All Calls – K-CCIS, if the destination station is busy and has Call Alert Notification disabled, the calling party hears busy tone after the maximum hops assigned in Program 50-05-01 (K-CCIS Maximum Call Forwarding Hop Assignment).
- Multiple Call Forwarding – All Calls -K-CCIS and Call Forwarding – Busy – K-CCIS may be mixed; up to seven combined multiple forwardings may occur.
- An example of Multiple Call Forwarding over a K-CCIS link is shown below



	Multiple Call Forwarding Over K-CCIS
Office A	Allowed
Office B	Allowed
Office C	Allowed
Office D	Allowed

✎ The counter is reduced by one with each hop (tandem connection).

Related Feature List

- Call Transfer – All Calls – K-CCIS
- Call Forwarding – All Calls – K-CCIS
- Call Forwarding – Busy/No Answer – K-CCIS
- Multiple Call Forwarding – Busy/No Answer – K-CCIS
- Link Reconnect – K-CCIS
- Uniform Numbering Plan – K-CCIS

Guide to Feature Programming

This guide provides a list of associated Programs that support this feature.

Program/ Item No.	Description/ Selection	Assigned Data	Comments
20-06-01	Class of Service for Extensions	0~15	Default: Extension 101 is in Class 15. All other extensions are in Class 1.
20-09-07	Class of Service Options (Incoming Call Service) – Call Queuing	0 = Off 1 = On Default is 1	Must be Off for Class of Service for Call Forward Busy to operate.
20-11-12	Class of Service Options (Hold/Transfer Service) – Call Forwarding Off Premise (External Call Forwarding	0 = Off 1 = On Default is 0	Enable Call Forward – Off-Premise per Class of Service.
20-13-06	Class of Service Options (Supplementary Service) – Automatic Off Hook Signaling (Automatic Override)	0 = Off 1 = On Default is 1	Must be Off for Call Forward – Busy to operate.
15-07-01	Programmable Function Keys	10 = Call Forward – Immediate 11 Call Forward – Busy 12 Call Forward – No Answer 13 Call Forward – B/NA	Service Codes: 848 843 845 844
14-01-13	Basic Trunk Data Setup – Trunk-to-Trunk Transfer Loop Supervision	0 = Disable 1 = Enable Default is 1	Must be enabled for Trunk-to-Trunk Transfer; Call Forward – Off- Premise, or Tandem Trunking.
50-06-01	CCIS Feature Availability – Link Reconnect	0 = Not Available 1 = Available Default is 1	Enable Link Reconnect.
50-05-01	CCIS Maximum Call Forwarding Hop Counter	0~7 Hops Default is 5	Set Maximum Hops.

Multiple Call Forwarding – Busy/No Answer - K-CCIS

Feature Description

This feature allows a Multiple Call Forwarding – Busy/No Answer sequence to be forwarded over a K-CCIS network to a station in another office. For more details, refer to the UNIVERGE SV9100 Features and Specifications Manual.

System Availability

Terminal Type:

All multiline terminals

Required Components:

GPZ-IPLE

Operating Procedures

To set Call Forward – Busy/No Answer - K-CCIS from a Multiline Telephone (Closed Numbering Plan):

1. Press the Call Forward – Busy/No Answer ON/OFF key.
2. Dial 1 to set.
3. Dial the remote K-CCIS station number.
4. Press Speaker.

- OR -

1. Lift the handset or press Speaker.
2. Dial Access Code 844 (default), then 1 to set.
3. Dial the remote K-CCIS station number.
4. Restore handset or press Speaker.

To set Call Forward – Busy/No Answer - K-CCIS from a Multiline Telephone (Open Numbering Plan):

1. Press the Call Forward – Busy/No Answer ON/OFF key.
2. Dial 1 to set.
3. Dial the trunk Access Code.
4. Dial the Office Code number.
5. Dial the distant K-CCIS station number.
6. Press Speaker.

- OR -

1. Lift the handset or press Speaker.
2. Dial Access Code 844 (default), then dial 1 to set.
3. Dial the trunk Access Code.
4. Dial the Office Code number.
5. Dial the distant K-CCIS station number.
6. Restore handset or press Speaker.

To cancel Call Forward – Busy/No Answer – K-CCIS from a Multiline Telephone:

1. Press Call Forward – Busy/No Answer On/Off key.
2. Dial 0 to cancel.
3. Press Speaker.

- OR -

1. Lift the handset or press Speaker.
2. Dial Access Code 844 (default), then Dial 0 to cancel.
3. Restore handset or press Speaker.

To set for any station for Attendant Positions only (Closed Numbering Plan):

1. Lift the handset or press Speaker.
2. Dial the Call Forward Busy/No Answer for any Extension to Destination
3. Service Code (default: 793).
4. Dial 1 (Set).
5. Dial the extension number to be forwarded and then the destination number.
6. Press Speaker or hang up.

To cancel for any station for Attendant Positions only:

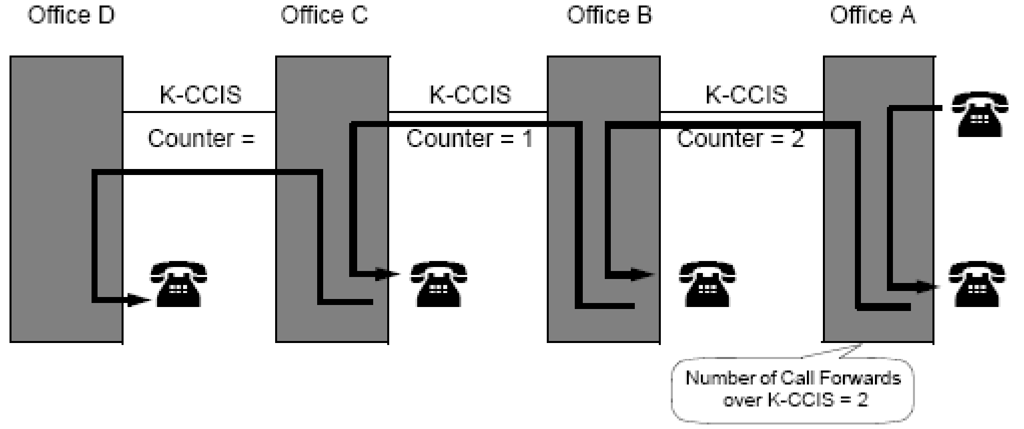
1. Pick up the handset or press Speaker.
2. Dial the Call Forward Busy/No Answer for any Extension to Destination
3. Service Code (default: 793).
4. Dial 0 (Cancel).
5. Dial the station number, which is forwarded.
6. Press Speaker or hang up.

Service Conditions

General:

- Multiple Call Forwarding – Busy/No Answer Calls - K-CCIS can forward a call up to five times across K-CCIS links (up to five hops) depending on systems data.
- Multiple Call Forwarding over a K-CCIS link is combined with Multiple Call Forwarding – All Calls/ Busy/No Answer.
- If the calling station is set as the destination in a multiple hop scenario, Multiple Call Forwarding – Busy/No Answer Calls - K-CCIS are not performed, i.e., an infinite loop does not occur.
- For multiple Call Forwarding – All/Busy (Immediate) calls, the display on the calling party's Multiline Telephone indicates the terminating station user's name and the station number for the first station of a distant system in the Multiple Call Forwarding group. For the terminating station, the telephone display indicates the name and the number of the calling party and the trunk number of the incoming call.

- For multiple Call Forwarding – No Answer/Busy (Delay) calls, the display on the calling party's Multiline Telephone indicates the name and number of the first station of a distant system in the Multiple Call Forwarding group. For the terminating station, the telephone display indicates the name and the number of the calling party and the trunk number of the incoming call.
- When a calling station has been Call Forwarding – Busy/No Answer Calls – K-CCIS to the maximum times assigned in Program 50-05-01 (K-CCIS Maximum Call Forwarding Hop Assignment) and encounters another Call Forwarding – Busy/No Answer Calls – K-CCIS condition, the calling station is not forwarded and rings at the last destination.
- When the destination station in a Multiple Call Forwarding – Busy/No Answer Calls – K-CCIS situation is busy and has not set Call Forwarding – Busy and has Call Alert Notification disabled, the calling party receives busy tone.
- When combining Call Forwarding – Busy and Call Forwarding – All Calls – K-CCIS and the destination station is busy and has Call Alert Notification disabled, the calling party hears a busy tone after the maximum hops assigned in Program 50-05-01 (K-CCIS Maximum Call Forwarding Hop Assignment).
- Multiple Call Forwarding – All Calls – K-CCIS can forward a call a maximum of five times across K-CCIS link (maximum of five hops) depending on system data assignments.
- An example of Multiple Call Forwarding over a K-CCIS link as shown



Multiple Call Forwarding Over K-CCIS

Office A	Allowed
Office B	Allowed
Office C	Allowed
Office D	Allowed

✎ Note: The counter is reduced by one with each hop (tandem connection).

Restrictions:

- Trunk-to-Trunk Transfer must be allowed in Program 20-11-14 [Class of Service Options (Hold/ Transfer Service) Trunk-to-Trunk Transfer Restriction].

Related Feature List

- Call Forwarding – All Calls – K-CCIS
- Call Forwarding – Busy/No Answer – K-CCIS
- Multiple Call Forwarding – All Calls – K-CCIS
- Link Reconnect – K-CCIS
- Uniform Numbering Plan – K-CCIS

Guide to Feature Programming

This guide provides a list of associated Programs that support this feature.

Program/ Item No.	Description/ Selection	Assigned Data	Comments
20-06-01	Class of Service for Extensions	0~15	Default: Extension 101 is in Class 15, All other extensions are in Class 1.
20-09-07	Class of Service Options (Incoming Call Service) – Call Queuing	0 = Off 1 = On Default is 1	Must be Off for Class of Service for Call Forward Busy to operate.
20-11-12	Class of Service Options (Incoming Call Service) – Call Forwarding Off Premise (External Call Forwarding)	0 = Off 1 = On Default is 0	Enable Call Forward – Off-Premise per Class of Service.
20-11-14	Class of Service Options (Incoming Call Service) – Trunk-to-Trunk Transfer Restriction	0 = Off 1 = On Default is 0	Turn Off or On the Trunk-to-Trunk Transfer Restriction. If enabled (turned on), Trunk-to-Trunk Transfer is not possible.
20-13-06	Class of Service Options (Supplementary Service) –Automatic Off Hook Signaling (Automatic Override)	0 = Off 1 = On Default is 1	Must be Off for Call Forward – Busy to operate.
15-07-01	Programmable Function Keys	10 = Call Forward – Immediate 11 = Call Forward – Busy 12 = Call Forward – No Answer 13 = Call Forward – B/NA	Service Codes: 741 742 743 744
14-01-13	Basic Trunk Data Setup – Trunk-to- Trunk Transfer Loop Supervision	0 = Disable (No) 1 = Enable (Yes) Default is 1	Must be enabled for Trunk-to-Trunk Transfer; Call Forward – Off- Premise, or Tandem Trunking.
50-06-01	CCIS Feature Availability – Link Reconnect	0 = Not Available 1 = Available Default is 1	Enable Link Reconnect.
50-05-01	CCIS Maximum Call Forwarding Hop Counter	0~7 Hops Default is 5	Set Maximum Hops.

Paging Access – K-CCIS

Feature Description

This feature allows users to access internal or external paging from remote sites across the K-CCIS network. Local stations where the external paging equipment is installed can use the Meet-Me Answer feature to answer the page and establish a station-to-station K-CCIS call. For more details, refer to the UNIVERGE SV9100 Features and Specifications Manual.

System Availability

Terminal Type:
All multiline terminals

Required Components:
GPZ-IPLE

Operating Procedures
To access internal or external paging across a K-CCIS network:

1. Lift the handset or press Speaker.
2. Dial the Access Code for the required zone, or press the programmed Feature Access or One-Touch key.

Service Conditions

General:
- The single external paging zone output built into the basic B64-U20 KSU can be used for Paging Access – (K-CCIS).
- Program 31-01-02 (Paging Announcement Duration) applies to Paging Access – (K-CCIS).
- If a user dials during Paging Access – (K-CCIS), DTMF tones are heard from the external paging equipment at the remote site.
- Program 31-02-01 (Internal Paging Group Number) applies to Paging Access – (K-CCIS).
- Program 31-02-02 (Internal All Call Paging Receiving) applies to Paging Access – (K-CCIS).

Restrictions:
- Amplifiers and speakers must be locally provided.
- Combined Paging is not supported over K-CCIS.
- Internal Paging across K-CCIS is supported only between UNIVERGE SV9100 and UNIVERGE SV9100.

Related Feature List
- Background Music Over External Speakers
- External Zone Paging (Meet-Me)
- Internal Zone Paging (Meet-Me)

Guide to Feature Programming
This guide provides a list of associated Programs that support this feature.

For Paging Installation

Program/ Item No.	Description/ Selection	Assigned Data	Comments
10-03-01	ETU Setup – Terminal Type (B1)	0 = Not Set 1 = Multiline Terminal 2 = SLT Adapter 3 = Bluetooth Cordless Handset 6 = PGD (Paging) 7 = PGD (Tone Ringer) 8 = PGD (Door Box) 9 = PGD (ACI) 10 = DSS Console 11 = ---Not Used---	Assign ESI port for External Paging.
11-01-01	System Numbering	Default is 51 = 2 digit: F-Route.	This Service Code must be assigned also in PRG 11-12-20.
11-12-20	Service Code Setup (for Service Access) – External Paging	Default is 803	Setting 703 should be changed based on the K-CCIS network configuration.
11-12-22	Service Code Setup (Service Access) – Meet Me Answer to External Paging	Default is 865	The Service Code assigned in this Program is used for Meet Me Answer to External Paging.
15-07-01	Programmable Function Keys	19 = External. Group Paging 1~8 20 = External. All Call Paging 21 = Internal. Group Paging 1~64 22 = Internal. All Call Paging	Set the functions of programmable extension Function Keys.
20-10-06	Class of Service Options (Answer Service) – Meet Me Conference and Paging	0 = Off 1 = On Default is 1	Enable Meet Me Conferencing and Paging.
20-14-07	Class of Service Options for DISA/E&M – External Paging	0 = Off 1 = On Default is 1	Allow DISA or Tie Line Trunk user to use External Paging.

Program/ Item No.	Description/ Selection	Assigned Data	Comments
31-01-01	System Options for Internal/External Paging – All Call Paging Zone Name	Up to 12 Characters Default is Group All	Assign a name to each All Call Internal Paging Zone. The name is displayed to make the announcement.
31-01-02	System Options for Internal/External Paging – Page Announcement Duration	0~64800 seconds Default is 1200	Set the length of Paging Announcements.
31-01-04	System Options for Internal/External Paging – Privacy Release Time	0~64800 seconds Default is 90	After user initiates a Meet Me or Voice Call conference, the system waits this time for the Paged Party to answer the call.
31-04-01	External Paging Zone Group	0 = No Setting Default: Speaker 1 = Group 1 Speaker 2 = Group 2 Speaker 3 = Group 3 Speaker 4 = Group 4 Speaker 5 = Group 5 Speaker 6 = Group 6 Speaker 7 = Group 7 Speaker 8 = Group 8 Speaker 9 = CPU Group 1	Assign each External Paging Zone to an External Paging Group.
31-06-01	External Speaker Control – Broadcast Splash Tone before Paging (Paging Start Tone)	0 = No Tone 1 = Splash Tone 2 = Chime Tone Default is 2	Enable Splash Tone before paging.
31-06-02	External Speaker Control – Broadcast Splash Tone After Paging (Paging End Time	0 = No Tone 1 = Splash Tone 2 = Chime Tone Default is 2	Enable Splash Tone after paging.
31-06-03	External Speaker Control – Speech Path	0 = Both Ways (Duplex) 1 = One Way PGD → SPK (Simplex) Default is 1	Establish whether or not the external speaker is used for talkback. (Not Available on CPU page port 9)

For Remote System

Program/ Item No.	Description/ Selection	Assigned Data	Comments
11-01-01	System Numbering	Default is 151 = 2 digit: F-Route	Assign also in PRG 11-12-20.
11-12-20	Service Code Setup (for Service Access) – External Paging	Default is 803	Change703 Setting based on the K-CCIS network configuration.
44-02-01	Dial Analysis Table for ARS/F-Route Access) – Dial	Analysis Table 1 = 511 Default is No Setting	Assign the access code used to page. Up to eight digits can be assigned.
44-02-02	Dial Analysis Table (ARS/ F-Route Access) – Service Type	0= No Setting (None) 1 = Extension Call (Own) 2 = ARS/F-Route Table (F-Route) 3 = Dial Extension Analyze Table (Option) Default is 0	Assign Service Type.
44-02-03	Dial Analysis Table (ARS/ F-Route Access) – Additional data	0= No Setting 1 = Delete Digits 0~255 (255: Delete All Digits) 2 = 0~500) 3 = Dial Extension Analyze Table Number (0~4) Default is 0	For the Service Type selected in 44-02-02, enter the additional data required.
44-05-01	ARS/F-Route Table – Trunk Group Number	0~ 100, 255 0 = No Setting	Select trunk group number used for outgoing ARS calls. Setting 255 = Internal Extension Call.
44-05-02	ARS/F-Route Table – Delete digits	0 = No setting 0~255 255 = Delete All Digits Default is 0	Enter number of digits to delete from the dialed number.
44-05-03	ARS/F-Route Table – Additional Dial Number Table	0= No Setting 0~1000 Default is 0	Enter Table Number (defined in PRG 44-06) for additional digits to dial.
44-05-09	ARS/F-Route Table – Maximum Digit	0 = No Maximum 0~24 Default is 0	Assign max digits for the Paging Access Code.

Quick Transfer to Voice Mail – K-CCIS

Feature Description

A station user transferring a call can force the call to be transferred to the called party voice mail box after the transferred call recalls, after an internal station number is dialled while performing a screened transfer, or during intercom calls.

System Availability

Terminal Type:

All multiline terminals allow either operation.
Single line telephones may perform the Quick Transfer only during screened transfer operations. They may not perform Quick Transfer after recall.

Required Components

GPZ-IPLE

Operating Procedures

Quick Transfer Across K-CCIS:

To Quick Transfer a call while talking with an outside or internal party:

1. Press Transfer, and wait for an internal dial tone.
2. Enter a station number, and wait for a ring back tone.
3. Dial the Quick Transfer Access Code. The outside party is transferred to the station user Voice Mail box.
4. Hang up.
5. The Voice Mail answers.

To leave a message using Quick Transfer to voice mail during an intercom call:

1. Make the intercom call.
2. Dial the Quick Transfer Access Code.
3. Leave a voice mail message.
4. Hang up.

Service Conditions

General:

- The Quick Transfer to Voice Mail feature is allowed when:
    - Listening to the ring back tone (RBT)
    - Listening to the call waiting tone (CWT)
    - In Handsfree Answerback Mode
    - In Voice Over Mode
- This feature is allowed from a single line telephone (SLT) until the PBR times out (default: 10 sec).
- An SLT may perform the Quick Transfer only during screened transfer operations.
- VM8000 InMail is supported in a KTS to KTS network for K-CCIS.

Related Feature List

- Digital Voice Mail

Guide to Feature Programming

This guide provides a list of associated Programs that support this feature.

Program/ Item No.	Description/ Selection	Assigned Data	Comments
11-16-09	Single Digit Service Code Setup – Access to Voice Mail	Default is not assigned	Assign access code for Quick Transfer to Voice Mail.
11-07-01	Department Group Pilot Numbers	Tel Groups 1~64 Dial up to eight digits. Default is No Setting	Assign pilot number to each Department Group set up in PRG 16-02. Extension numbers are assigned in PRGs 11-02, 11-04, 11-06, and 11-08.
15-03-01	Single Line Telephone Basic Data Setup – SLT Signaling Type	0 = DP 1 = DTMF Default is 1	Tell the system which dialing is used by the connected telephone users. For each Voice Mail extension this option must be 0.
15-03-03	Single Line Telephone Basic Data Setup – Terminal Type	0 = Normal 1 = Special Default is 0	Enter 1 to allow a single line port to receive DTMF tones after the initial call setup.
45-01-01	Voice Mail Integration Options – Voice Mail Department Group Number	0 = No Voice Mail 0~64 Groups Default is 0	Assign Department Group Number as the Voice Mail Group.
45-01-14	Voice Mail Integration Options – CCIS Centralized Voice Mail Number	Up to eight digits Default not assigned. Default is No Setting	Assign the CCIS Centralized Voice Mail Pilot Number for Remote Sites.

Station-to-Station Calling – K-CCIS

Feature Description

This feature permits any multiline terminal user to dial another multiline terminal directly through a K-CCIS network. For more details, refer to the UNIVERGE SV9100 Features and Specifications Manual.

System Availability

Terminal Type:

All multiline terminals

Required Components:

GPZ-IPLE

Operating Procedures

Normal call handling procedures apply.

Service Conditions

General:

- If the called station is off-hook and has Call Queuing disabled, the originating station receives a busy tone. If the called station is idle, the called station rings and the caller hears ringback tone.
- If the called station is off-hook on a call and has Call Queuing enabled, the originating station receives ringback tone and the called station receives call alert tone.
- Station-to-Station Calling between tenants in the K-CCIS network is not restricted.
- The release process is First Party Release.

Restrictions:

- The same telephone numbers cannot be duplicated in the same system.

Related Feature List

- Call Transfer – All Calls - K-CCIS
- Calling Name Display – K-CCIS
- Calling Number Display – K-CCIS
- Dual Hold – K-CCIS
- Elapsed Time Display – K-CCIS
- Flexible Numbering of Stations – K-CCIS
- Hands-Free Answerback – K-CCIS
- Key-Common Channel Interoffice Signalling (K-CCIS)
- Uniform Numbering Plan – K-CCIS

Guide to Feature Programming

This guide provides a list of associated Memory Blocks that support this feature.

Program/ Item No.	Description/ Selection	Assigned Data	Comments
11-01-01	System Numbering – Extension Number	1X = 3 Digit; Intercom	Assign the system internal (intercom) numbering plan.
11-02-01	Extension Numbering	Default: 200 - 499 5000 - 5211	Assign the Extension Numbers.

Uniform Numbering Plan – K-CCIS

Feature Description

In a K-CCIS network, a Uniform Numbering Plan enables a multiline terminal user to call any other multiline terminal in the network. Two types of numbering plans are provided. In the first plan, the station user dials any telephone number from two to eight digits. The location of the office is identified by the first digit or first two digits of the telephone number. In the second plan, the station user dials a one-, two- or three-digit office code and a telephone number from two to eight digits.
For more details, refer to the UNIVERGE SV9100 Features and Specifications Manual.

System Availability

Terminal Type:

All multiline terminals

Required Components:

GPZ-IPLE

Operating Procedures

To call a station at another office using Numbering Plan 1 (Closed Numbering Plan):

1. Lift the handset or press Speaker.
2. Dial the remote K-CCIS station number.

To call a station at another office using Numbering Plan 2 (Open Numbering Plan):
1. Lift the handset or press Speaker.
2. Dial the trunk Access Code.
3. Dial the Office Code number.
4. Dial the remote K-CCIS station number.

Service Conditions

General:
- In a closed numbering plan, the location of the office can be identified by the first digit or first two digits of the telephone number.
- In an open numbering plan, each office in the K-CCIS network is assigned a one-, two- or three-digit office code and each station in the office is assigned telephone numbers from two to eight digits.
- In the same office, a station-to-station call is made by dialling the telephone number of the desired station.

Restrictions:
- For a Closed Numbering Plan network, a maximum of 255 systems can be connected per K-CCIS Network.
- When a Closed Numbering plan is used the extensions in the network cannot have the same prefix number.
- For an Open Numbering Plan network, the Automatic Route Selection (ARS)/ Flexible Routing (F-Route) feature must be used to place Station-to-Station calls over K-CCIS.
- When an Open Numbering plan is used, the extensions in the network can have the same prefix number, however the office location number cannot be the same.

Related Feature List
- Call Transfer – All Calls – K-CCIS
- Flexible Numbering of Stations – K-CCIS
- Key-Common Channel Interoffice Signalling (K-CCIS)
- Station-to-Station Calling – K-CCIS

Guide to Feature Programming
Refer to Flexible Numbering of Stations feature

Voice Call – K -CCIS

Feature Description
This feature provides a voice path, through the K-CCIS network, between a *MLT* in one office and a *MLT* in another office. This path is established from the *calling* party to the *called* party built-in speaker. If the called party MIC is on, the called party can converse hands-free.

System Availability

Terminal Type:
All multiline terminals

Required Components:
GPZ-IPLE

Operating Procedures

From one *MLT* to another *MLT*:

- The originating *MLT* user dials the desired station number in a different office and receives ring back tone.
- Calling party dials 1. A signal tone is transmitted over the K-CCIS network to the called party speaker.
- The called party can press MIC, or press FEATURE and dial 1 (if the MIC LED is not on) to allow two-way conversation with the calling party.

Service Conditions

General:

- The UNIVERGE SV9100 can assign a Feature Access/One Touch Button as a Voice Call key. This performs the same operation as pressing 1.
- Any station in the same system can use Directed Call Pick Up to retrieve the Voice Call over K-CCIS.
- When a Voice Call is sent to a station that is unable to receive voice announcement, RST is displayed on the originator display.
- During Voice Call, the ICM Key is flashing (Red).

Restrictions:

- The calling party must wait for at least one ring back before Voice Call is attempted.
- After the calling party changes ring back to Voice Call, it cannot be changed back to tone.
- Voice Call cannot be set as the initial call across K-CCIS.
- Group Call Pick Up is not allowed to retrieve voice calls over K-CCIS.
- Single Line terminals can be used to originate a Voice Call Over K-CCIS. However, they are not allowed to receive a voice call.

Related Feature List

- Station-to-Station Calling – K-CCIS
- Handsfree Answerback – K-CCIS

Guide to Feature Programming

This guide provides a list of associated Programs that support this feature.

Program/ Item No.	Description/ Selection	Assigned Data	Comments
11-12-06	Service Code Setup (for Service Access) – Switching Voice Call and Signal Call	Default is 812	Assigns the access code used to toggle ICM call between Handsfree Answerback and Forced Intercom Ringing for Outgoing Intercom calls.

Voice Mail Integration – K-CCIS

Feature Description

This feature allows any station user in the K-CCIS network to use the Voice Mail System (VMS) in another office in the K-CCIS network.

VM8000 In-Mail voice mail is supported for centralised voice mail in a KTS to KTS network for K-CCIS.

VM8000 In-Mail voice mail is supported for centralised voice mail in a Netlink network.

For more details, refer to the UNIVERGE SV9100 Features and Specifications Manual.

System Availability

Terminal Type:

All Stations

REQUIRED COMPONENTS:

VM8000 InMail
GPZ-IPLE

Operating Procedures

To access voice mail from a Multiline Telephone in the Main system:

1. Lift the handset or press Speaker.
2. Dial pilot number for voice mail.
3. When voice mail answers use soft keys to navigate.

- OR -

4. Wait for soft keys to time out and listen to voice prompts to navigate.
5. When finished hang up.

To access voice mail from a Multiline Telephone in the Remote system:

1. Lift the handset or press Speaker.
2. Dial extension number for voice mail.
3. When voice mail answers listen to voice prompts to navigate.
4. When finished hang up.

To program a One-Touch/Feature Access key for easy message access:

1. Press Speaker.
2. Dial 851.
3. Press One-Touch/Feature Access key.
4. Dial 77 followed by Mailbox number.
5. Press Hold.

Service Conditions

General:

- Any station or Call Arrival (CAR) key can be set for Call Forwarding – Busy/No Answer to voice mail.
- The following features **are** supported for voice mail users in remote systems:
    - Message Waiting Indication
    - Automated Attendant
    - Auto Login center
    - Call Forward – Busy/No Answer to voice mail
    - Call Forward – All Call to voice mail
  - A voice mail with at least eight ports should be used in any K-CCIS system with a shared voice mail.
  - InMail is supported for centralised voice mail in a NetLink and KTS to KTS CCIS network.
  - A maximum of 16 VM8000 InMail ports are supported.
  - When InMail is used as centralised voice mail in a KTS to KTS CCIS system, remote mailbox users cannot access End User Web Pro for telephone and InMail configuration.

Restrictions:

  - In the voice mail, only release transfer type is supported for mail boxes of stations in Remote systems.
  - In a KTS to KTS Network, only digital voice mails are supported for K-CCIS.
  - In a KTS to KTS network, Centralised Voice Mail is supported only via closed numbering plan and only up to 7-digit station numbers.

- In a PBX to KTS network, Centralised Voice Mail is supported only via closed numbering plan.
- In a PBX to KTS network, Centralised Voice Mail is supported using the PBX voice mail.
- Extension numbers of remote extensions must be cleared from command 11-02.
- Single Line Telephones (SLTs) connected to the AP(A)-R Unit/AP(R)-R Unit or APA-U Unit/APR-U Unit cannot be used to transfer a Trunk call across the K-CCIS Network to another station or Voice Mail.
- When a call is forwarded to voice mail by multiple call forwarding, the message is left in the mailbox of the first forwarded station.
- Call Forward – Off-Premise must be allowed in Class of Service Feature Selection to set call forwarding to main K-CCIS voice mail.
- Trunk-to-Trunk Transfer must be allowed in Program 14-01-13 (Trunk-to-Trunk Transfer Yes/No Selection).
- A remote system can have only Message Waiting LED on Line key for extensions in the remote system. Remote system users cannot press a flashing Line key to route to voice mail or the message box of an extension on Message Waiting LED on the Line key.
- The following features are **not** supported for voice mail users in remote systems:
  - Live Record
  - Live Monitoring
  - Caller ID Display
  - Soft keys
  - Await Answer transfer from voice mail
  - Call Holding
  - Constant Message Count Indication
  - Call Back to VM
  - Live Transfer (Caller ID Return Call)
- The Dial Access Code for Single Line Telephone Hook flash is supported for trunk calls into the main system only.
- The voice mail must be installed in the PBX (NEAX system) when 5-, 6-, or 7-digit station numbers are used.
- Centralised Voice Mail and Local Voice Mail cannot be mixed in a K-CCIS network.

Related Feature List

- Key-Common Channel Interoffice Signalling (K-CCIS)
- Call Forwarding – All Calls - K-CCIS
- Call Forwarding – Busy/No Answer - K-CCIS
- Multiple Call Forwarding – All Calls - K-CCIS
- Multiple Call Forwarding – Busy/No Answer - K-CCIS

Guide to Feature Programming

This guide provides a list of associated Memory Blocks that support this feature.

Program/ Item No.	Description/ Selection	Assigned Data	Comments
10-03-01	ETU Setup – Logical Port Number	VMS Unit Default is 0	The CPU automatically defines each PCB during installation.
11-01-01	System Numbering	1 = Service Code 2 = Extension Number 3 = Trunk Access 4 = Special Trunk access 5 = Operator Access 6 = Flexible Routing	Defaults for 1X, 2X, and 3X = 2 Extension Number.
11-02-01	Extension Numbering	Assign Station Numbers to Port Numbers	Defaults for Ports 1~512: 200 - 499 5000 - 5211
16-01-02	Department Group Basic Data Setup – Department Calling Cycle	0 = Normal Routing (Priority) 1 = Easy – UCD Routing (Circular) Default is 0	Set the call routing for Department Calling.
16-01-03	Department Group Basic Data Setup – Department Routing When busy	0 = Normal (Intercom caller to busy department member hears busy) 1 = Circular (Intercom callers to busy department member route to idle member) Default is 0	Assign how the system routes an Intercom Call to a busy Department Group member.
16-01-04	Department Group Basic Data Setup – Hunting Mode	0 = Last extension is called and hunting is stopped 1 = Circular Default is 0	Assign the action taken when a call reaches the last extension in the Department Group.
16-02-01	Department Group Assignment for Extensions	Groups 1~64 Priority 1~999 Default = 1-XXX	Assign the Department Groups. The initial priority value becomes the numerical port order assigned in PRG 11-02 and 11-04 (Ports 1~256).
11-11-01	Service Code Setup (for Setup/Entry Operation) – Call Forward – All Call	Default is 848	Assign the Call Forward – All Call service Set /Cancel Service Code.
11-11-02	Service Code Setup (for Setup/Entry Operation) – Call Forward – Busy	Default is 843	Assign the Call Forward – Busy Set/ Cancel Service Code.

Program/ Item No.	Description/ Selection	Assigned Data	Comments
11-11-03	Service Code Setup (for Setup/Entry Operation) – Call Forward – No Answer	Default is 845	Assign the Call Forward – No Answer Set/ Cancel Service Code.
11-11-04	Service Code Setup (for Setup/Entry Operation) – Call Forward – Busy/No Answer	Default is 844	Assign the Call Forward – Busy/No Answer Set/Cancel Service Code.
11-07-01	Department Group Pilot Numbers – Dial	UP to eight digits can be assigned. Default is No Setting.	Assign pilot numbers to each Department Group set up in PGM 16-02.
11-16-09	Single Digit Service Code Setup – Access to Voice Mail	Default is No Setting.	Assign single digit access code for Quick Transfer to Voice Mail.
20-06-01	Class of Service for Extensions	0~15	Default is Extension 101 is in Class 15. All other extensions are in Class 1.
20-09-02	Class of Service Options (Incoming Call Service) – Caller ID Display	0 = Off 1 = On Default is 0	Enable the Caller ID display at an extension.
20-11-01	Class of Service Options (Hold/Transfer Service) – Call Forward All	0 = Off 1 = On Default is 1	Disable Call Forward – All Call at an extension.
20-11-02	Class of Service Options (Hold/Transfer Service) – Call Forward When Busy	0 = Off 1 = On Default is 1	Disable Call Forward – Busy at an extension.
20-11-03	Class of Service Options (Hold/Transfer Service) – Call Forwarding When Unanswered	0 = Off 1 = On Default is 1	Disable Call Forward – No Answer at an extension.
20-11-12	Class of Service Options (Hold/Transfer Service) – Call Forwarding Off Premise (External Call Forwarding)	0 = Off 1 = On Default is 0	Enable Call Forward – Off-Premise at an extension.
20-11-13	Class of Service Options (Hold/Transfer Service) – Operator Transfer After Hold Callback	0 = Off 1 = On Default is 0	Turn Off or On an extension user ability to have a call which recalls from hold transfer to the operator.

Program/ Item No.	Description/ Selection	Assigned Data	Comments
20-11-14	Class of Service Options (Hold/Transfer Service) – Trunk-to-trunk Transfer Restriction	0 = Off 1 = On Default is 0	Enable Trunk-to-Trunk Transfer Restriction at an extension.
15-07-01	Programmable Function Keys	10 = Call Forward – Immediate 11 = Call Forward – Busy 12 = Call Forward – No Answer 13 = Call Forward – Busy/No Answer	Service Codes: 848 845 843 844
14-01-13	Basic Trunk Data Setup – Trunk-to-Trunk Transfer Loop Supervision	0 = Disable (No) 1 = Enable (Yes) Default is 1	Must be enabled for Trunk-to-Trunk Transfer, Call Forward – Off-Premise, and Tandem Trunking.
14-01-22	Basic Trunk Data Setup – Caller ID to Voice Mail	0 = Disable (No) 1 = Enable (Yes Default is 0	Enable the system to send Caller ID Digits to Voice Mail.
22-02-01	Incoming Call Trunk Setup	0 = Normal 1 = VRS (second dial tone if no VRS installed) 2 = DISA 3 = DID 4 = DIL 5 = E&M Tie Line 6 = Delayed VRS 7 = ANI/DNIS 8 = DID(DDI) Mode Switching Default is 0	Set the feature for the trunk being programmed.
22-07-01	DIL Assignment	Extension Number/ Pilot Number (eight digits maximum) Default is No Setting	Assign destination extension or Department Group pilot number programmed in PRG 11-07.
30-03-01	DSS Console Key Assignment	Key Numbers 001~114 00~99 = General Functional Level *00~*99 = Appearance Function Level Default is Extensions. 101~160	Customize Key Assignments for DSS Consoles 1~32.
45-01-01	Voice Mail Integration Options – Voice Mail Department Group Number	0 = No Voice Mail 0~64 Groups Default is 0	Assign an Extension Department Group as the Voice Mail Group.

Program/ Item No.	Description/ Selection	Assigned Data	Comments
45-01-14	Voice Mail Integration Options – CCIS Centralized Voice Mail Number	Up to eight digits Default is No Setting.	Assign the CCIS Centralized Voice Mail Pilot number for remote sites.

2.6.5 Networking DSP Usage

Networking GPZ-IPLE DSP Usage

NetLink GPZ-IPLE DSP Usage

Peer to Peer is enabled where possible

		Primary System						Secondary System 1			Secondary System 2		
		DT700/ DT800	DTermIP	STD SIP	TDM Ext	SIP Trunk	TDM Trunk	DT700/ DT800	TDM Ext	TDM Trunk	DT700/ DT800	TDM Ext	TDM Trunk
Primary System	DT700/ DT800	0	P=2	0	P=1	P=2	P=1	0	S1=1	S1=1	0	S2=1	S2=1
	DTermIP	P=2	0	P=2	P=1	P=2	P=1	P=2	S1=1	S1=1	P=2	S2=1	S2=1
	STD SIP	0	P=2	0	P=1	P=2	P=1	0	S1=1	S1=1	0	S2=1	S2=1
	TDM Ext	P=1	P=1	P=1	0	P=1	0	P=1	P=1 S1=1	P=1 S1=1	P=1	P=1 S2=1	P=1 S2=1
	SIP Trunk	P=2	P=2	P=2	P=1	P=2	P=1	P=2	P=2 S1=1	P=2 S1=1	P=2	P=2 S2=1	P=2 S2=1
	TDM Trunk	P=1	P=1	P=1	0	P=1	0	P=1	P=1 S1=1	P=1 S1=1	P=1	P=1 S2=1	P=1 S2=1

Secondary System 1	DT700/ DT800	0	S1=2	0	P=1	P=2	P=1	0	S1=1	S1=1	0	S2=1	S2=1
	TDM Ext	P=1	S1=1	S1=1	P=1 S1=1	P=2 S1=1	P=1 S1=1	P=1	0	0	P=1	S1=1 S2=1	S1=1 S2=1
	TDM Trunk	S1=1	S1=1	S1=1	P=1 S1=1	P=2 S1=1	P=1 S1=1	S1=1	0	0	S1=1	S1=1 S2=1	S1=1 S2=1
Secondary System 2	DT700/ DT800	0	S2=2	0	P=1	P=2	P=1	0	S1=1	S1=1	0	S2=1	S2=1
	TDM Ext	S2=1	S2=1	S2=1	P=1 S2=1	P=2 S2=1	P=1 S2=1	S2=1	S1=1 S2=1	S1=1 S2=1	S2=1	0	0
	TDM Trunk	S2=1	S2=1	S2=1	P=1 S2=1	P=2 S2=1	P=1 S2=1	S2=1	S1=1 S2=1	S2=1 S2=1	S2=1	0	0

P = Number of DSP's in use on the Primary System
S1 = Number of DSP's in use on Secondary System 1
S2 = Number of DSP's in use on Secondary System 2

AspireNet GPZ-IPLE DSP Usage

Peer to Peer is enabled where possible

		Node 1				Node 2				Node 3			
		DT700/ DT800	**TDM**	**SIP Trunk**	**TDM Trunk**	**DT700/ DT800**	**TDM**	**SIP Trunk**	**TDM Trunk**	**DT700/ DT800**	**TDM**	**SIP Trunk**	**TDM Trunk**
Node 1	**DT700/ DT800**	0	N1=1	N1=2	N1=1	N1=2 N2=2	N1=2 N2=1	N1=2 N2=2	N1=2 N2=1	N1=2 N3=2	N1=2 N3=1	N1=2 N3=2	N1=2 N3=1
	TDM	N1=1	0	N1=1	0	N1=1 N2=2	N1=1 N2=1	N1=1 N2=2	N1=1 N2=1	N1=1 N3=2	N1=1 N3=1	N1=1 N3=2	N1=1 N3=1
	SIP Trunk	N1=2	N1=1	N1=2	N1=1	N1=2 N2=	N1=2 N2	N1=2 N2=2	N1=2 N2=1	N1=2 N3=	N1=2 N3	N1=2 N3=2	N1=2 N3=1

						2	=1			2	=1		
	TDM Trunk	N1=1	0	N1=1	0	N1=1 N2=2	N1=1 N2=1	N1=1 N2=2	N1=1 N2=1	N1=1 N3=2	N1=1 N3=1	N1=2 N3=1	N1=1 N3=1
Node 2	**DT700/ DT800**	N2=2 N1=2	N2=2 N1=1	N2=2 N1=2	N2=2 N1=1	0	N2=1	N2=2	N2=1	N2=2 N3=2	N2=2 N3=1	N2=2 N3=2	N2=2 N3=1
	TDM	N2=1 N1=2	N2=1 N1=1	N2=1 N1=2	N2=1 N1=1	N2=1	0	N2=1	0	N2=1 N3=2	N2=1 N3=1	N2=1 N3=2	N2=1 N3=1
	SIP Trunk	N2=2 N1=2	N2=2 N1=1	N2=2 N1=2	N2=2 N1=1	N2=2	N2=1	N2=2	N2=1	N2=2 N3=2	N2=2 N3=1	N2=2 N3=2	N2=2 N3=1
	TDM Trunk	N2=1 N1=2	N2=1 N1=1	N2=1 N1=2	N2=1 N1=1	N2=1	0	N2=1	0	N2=1 N3=2	N2=1 N3=1	N2=1 N3=2	N2=1 N3=1
Node 3	**DT700/ DT800**	N3=2 N1=2	N3=2 N1=1	N3=2 N1=2	N3=2 N1=1	N3=2 N2=2	N3=2 N2=1	N3=2 N2=2	N3=2 N2=1	0	N3=1	N3=2	N3=1
	TDM	N3=1 N1=2	N3=1 N1=1	N3=1 N1=2	N3=1 N1=1	N3=1 N2=2	N3=1 N2=1	N3=1 N2=2	N3=1 N2=1	N3=1	0	N3=1	0
	SIP Trunk	N3=2 N1=2	N3=2 N1=1	N3=2 N1=2	N3=2 N1=1	N3=2 N2=2	N3=2 N2=1	N3=2 N2=2	N3=2 N2=1	N3=2	N3=1	N3=2	N3=1
	TDM Trunk	N3=1 N1=2	N3=1 N1=1	N3=1 N1=2	N3=1 N1=1	N3=1 N2=2	N3=1 N2=1	N3=1 N2=2	N3=1 N2=1	N3=1	0	N3=1	0

N1 = Number of DSP's in use on Node 1
N2 = Number of DSP's in use on Node 2
N3 = Number of DSP's in use on Node 3

K-CCIS GPZ-IPLE DSP Usage

Peer to Peer is enabled where possible

		Node 1				Node 2				Node 3			
		DT700/DT800	TDM	SIP Trunk	TDM Trunk	DT700/DT800	TDM	SIP Trunk	TDM Trunk	DT700/DT800	TDM	SIP Trunk	TDM Trunk
Node 1	DT700/DT800	0	N1=1	N1=2	N1=1	0	N2=1	N2=2	N2=1	0	N3=1	N3=2	N3=1
	TDM	N1=1	0	N1=1	0	N1=1	N1=1 N2=1	N1=1 N2=2	N1=1 N2=1	N1=1	N1=1 N3=1	N1=1 N3=2	N1=1 N3=1
	SIP Trunk	N1=2	N1=1	N1=2	N1=1	N1=2	N1=2 N2=1	N1=2 N2=2	N1=2 N2=1	N1=2	N1=2 N3=1	N1=2 N3=2	N1=2 N3=1
	TDM Trunk	N1=1	0	N1=1	0	N1=1	N1=1 N2=1	N1=1 N2=2	N1=1 N2=1	N1=1	N1=1 N3=1	N1=2 N3=1	N1=1 N3=1
Node 2	DT700/DT800	0	N1=1	N1=2	N1=1	0	N2=1	N2=2	N2=1	0	N3=1	N3=2	N3=1
	TDM	N2=1	N2=1 N1=1	N2=1 N1=2	N2=1 N1=1	N2=1	0	N2=1	0	N2=1	N2=1 N3=1	N2=1 N3=2	N2=1 N3=1
	SIP Trunk	N2=2	N2=2 N1=1	N2=2 N1=2	N2=2 N1=1	N2=2	N2=1	N2=2	N2=1	N2=2	N2=2 N3=1	N2=2 N3=2	N2=2 N3=1
	TDM Trunk	N2=1	N2=1 N1=1	N2=1 N1=2	N2=1 N1=1	N2=1	0	N2=1	0	N2=1	N2=1 N3=1	N2=1 N3=2	N2=1 N3=1
Node 3	DT700/DT800	0	N1=1	N3=2 N1=2	N1=1	0	N3=2 N2	N3=2 N2=2	N3=2 N2=1	0	N3=1	N3=2	N3=1

							=1						
	TDM	N3=1	N3=1 N1=1	N3=1 N1=2	N3=1 N1=1	N3=1 N2=2	N3=1 N2=1	N3=1 N2=2	N3=1 N2=1	N3=1	0	N3=1	0
	SIP Trunk	N3=2 N1=2	N3=2 N1=1	N3=2 N1=2	N3=2 N1=1	N3=2 N2=2	N3=2 N2=1	N3=2 N2=2	N3=2 N2=1	N3=2	N3=1	N3=2	N3=1
	TDM Trunk	N3=1	N3=1 N1=1	N3=1 N1=2	N3=1 N1=1	N3=1	N3=1 N2=1	N3=1 N2=2	N3=1 N2=1	N3=1	0	N3=1	0

N1 = Number of DSP's in use on Node 1
N2 = Number of DSP's in use on Node 2
N3 = Number of DSP's in use on Node 3

2.7 VoIP Troubleshooting

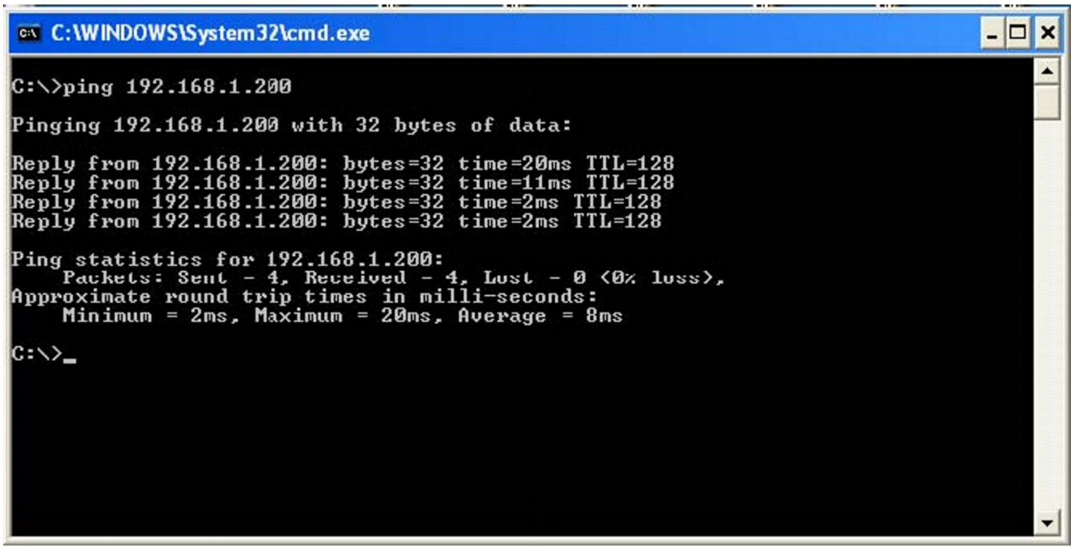
Enter topic text here.

2.7.1 Testing the SV9100 Network Connection

To test the UNIVERGE SV9100 network connections, it is possible to use the ICMP (Internet Control Message Protocol) Ping command. This basically sends a small amount of data from one device to another and then waits for a reply. This test confirms that the IP addressing and physical connection are good. To perform this test, from a Windows PC:

1. Click **Start**.
2. Click **Run...** .
3. In the Open dialogue box, enter **cmd**
4. Click **OK**. A Command prompt window opens.
5. Type **ping 192.168.1.200**.

The below screen shot shows that the UNIVERGE SV9100 system has replied to the Ping request – this indicates that the UNIVERGE SV9100
system is correctly connected to the network.



```
C:\WINDOWS\System32\cmd.exe

C:\>ping 192.168.1.200

Pinging 192.168.1.200 with 32 bytes of data:

Reply from 192.168.1.200: bytes=32 time=20ms TTL=128
Reply from 192.168.1.200: bytes=32 time=11ms TTL=128
Reply from 192.168.1.200: bytes=32 time=2ms TTL=128
Reply from 192.168.1.200: bytes=32 time=2ms TTL=128

Ping statistics for 192.168.1.200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 20ms, Average = 8ms

C:\>_
```

Depending on whether you have connected the GCD-CP10 or GPZ-IPLE to the network the following IP addresses can be checked.

Description	PRG Command	Default Value
GCD-CP10 IP address	10-12-01	192.168.0.10
GPZ-IPLE IP address	10-12-09	172.16.0.10
VoIP Media Gateway IP Address	84-26-01	172.16.0.20

2.8 Appendix A: TCP_UDP Port Numbers

Appendix A: TCP_UDP Port Numbers

Application	Type	Port
NetLink Primary to Secondary Signalling	TCP	58000
NetLink Secondary to Secondary Signalling	TCP	58001
NetLink Replication	TCP	58002
AspireNet Signalling	TCP	1730
AspireNet Keep Alive	TCP	30000

K-CCIS Server Signalling	TCP	57000
K-CCIS Client Signalling	TCP	59000
DHCP Server	TCP	67
DIM	TCP	5964
H.323 H.245	TCP	5600
H.323 Trunk RAS	TCP	20001
H.323 Trunk Signalling	TCP	1720
SIP MLT Signalling (handset)	UDP	5060
SIP MLT RTP (handset)	UDP	3462
GPZ-IPLE RTP	UDP	10020 (increment by two per call)
GPZ-IPLE RTCP	UDP	10021 (increment by two per call)
Standard SIP Extension Signalling (system)	UDP	5070
SIP MLT Extension Signalling (system)	UDP	5080
SIP MLT Extension Session (system)	UDP	5081
SIP Trunk Signalling	UDP	5060
WebPro	TCP	80
PC Pro	TCP	8000
GPZ-IPLE Voip Channel Range	**Type**	**Port Range**
GPZ-IPLE VoIP Channels (RTP/RTCP)	UDP	10020 – 10532

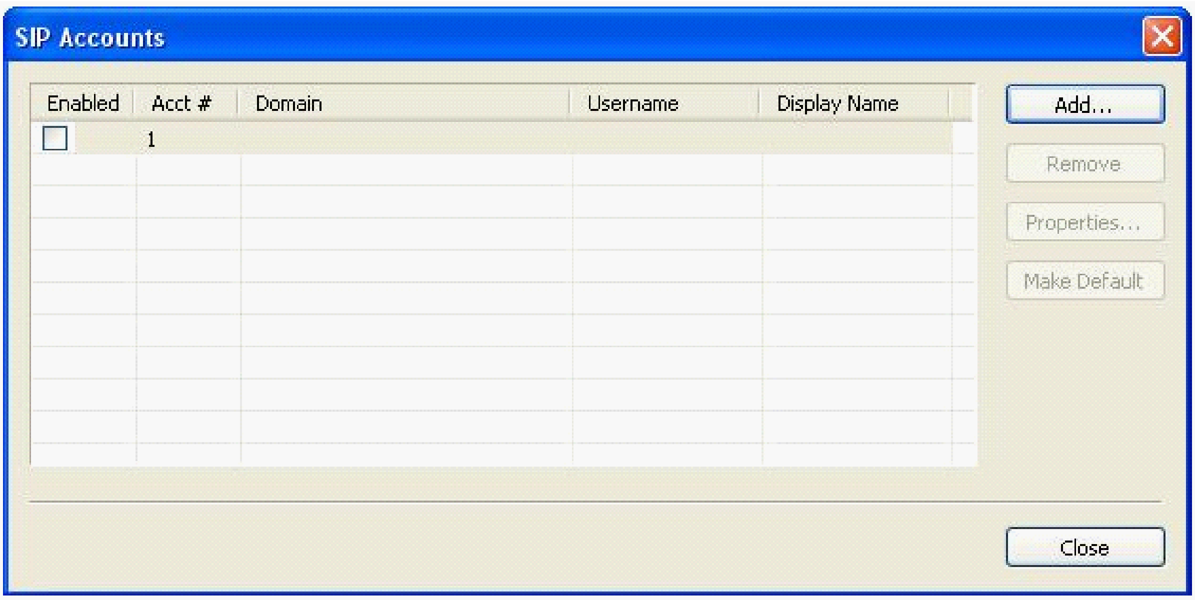
2.9 Appendix B: SIP Configuration Example

Appendix B: SIP Configuration Example

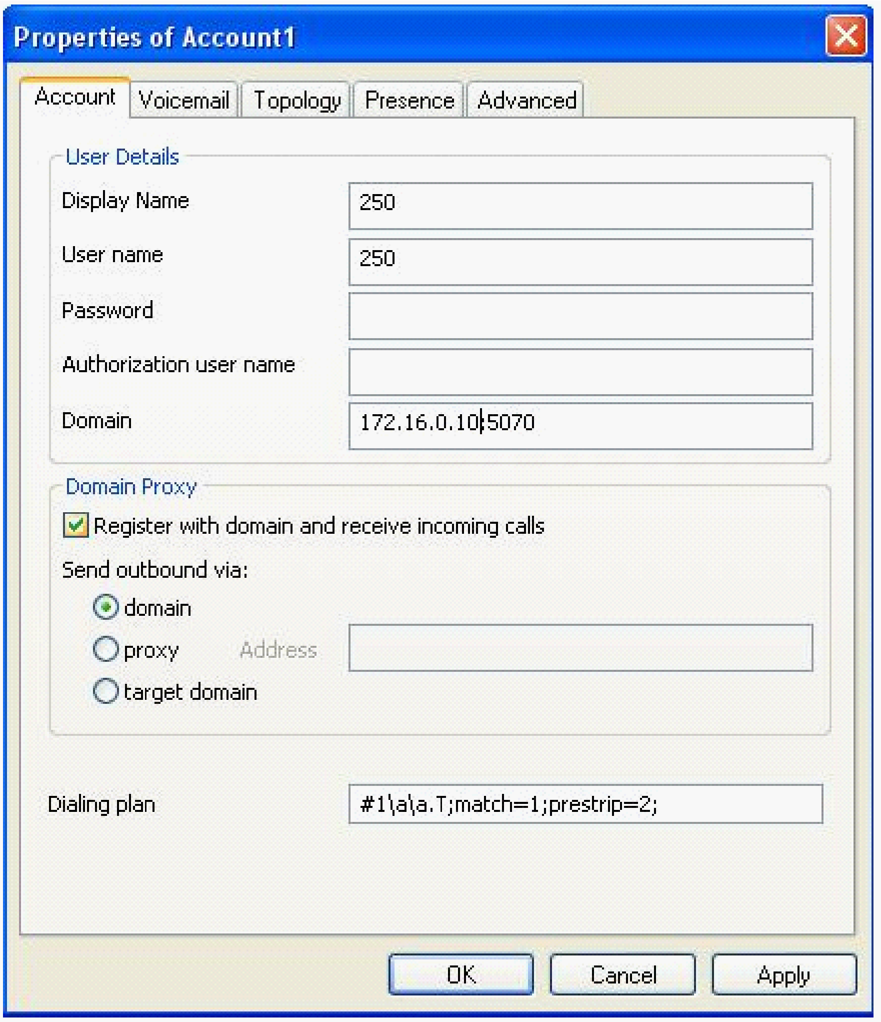
SIP Softphone Configuration (CounterPath, X-Lite)

X-Lite is a software based SIP phone, available from CounterPath Corporation. The software is freely available from their website. X-Lite is a reduced feature version of their commercial software, eyeBeam. If G.729 CODEC is required it is necessary to use the eyeBeam software.

1. Install the application using the Installation Easy Edit.
2. The SIP Accounts dialog will open. Click the Add button.

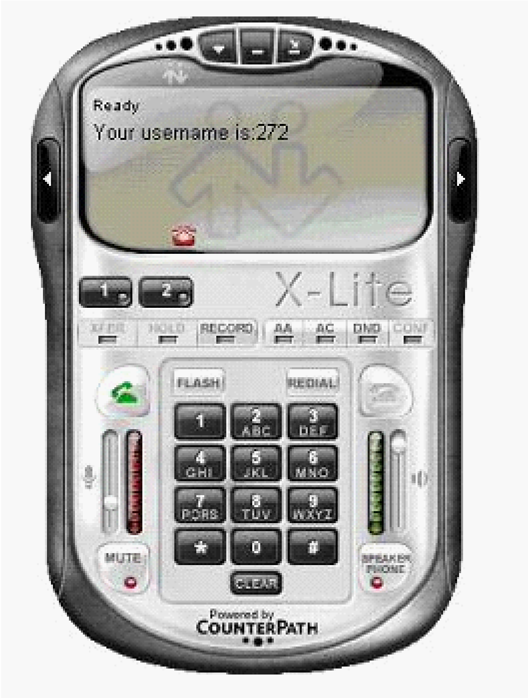


3. Configure the Account Properties as per the example below:



Display Name: The name that will appear on the softphone display.
User name: The extension number assigned to the extension port
Password: The password assigned in **Authentication Password** in *Easy Edit – Advanced Items/IP SIP/ SIP Terminal Options/SIP Terminal Setup. (PRG15-05-16)*
Authorization User name: Same as User name
Domain: The IPLE card IP address and port number. *i.e. 172.16.0.10:5070*

4. Click on OK and Close to exit the configuration dialog
5. The softphone should register to the telephone system



Please refer to http://www.counterpath.com/ for further information on this product

2.10 Appendix C: ToS Field Values

Appendix C: ToS Field Values

Description (*1)	Layer 3 QoS (*2)	IP Ext QoS (*3)	ToS Field Bit Pattern (*4)
Best Effort / Class Selector 0	0	0	00000000
Class Selector 1 (CS1)	8	20	00100000
Assured Forwarding 11 (AF11)	10	28	00101000
Assured Forwarding 12 (AF12)	12	30	00110000
Assured Forwarding 13 (AF13)	14	38	00111000
Class Selector 2 (CS2)	18	48	01001000
Assured Forwarding 21 (AF21)	18	48	01001000
Assured Forwarding 22 (AF22)	20	50	01010000
Assured Forwarding 23 (AF23)	22	58	01011000
Class Selector 3	24	60	01100000
Assured Forwarding 31 (AF31)	26	68	01101000
Assured Forwarding 32 (AF32)	28	70	01110000
Assured Forwarding 33 (AF33)	30	78	01111000
Class Selector 4 (CS4)	32	80	10000000
Assured Forwarding 41 (AF41)	34	88	10001000
Assured Forwarding 42 (AF42)	36	90	10010000
Class Selector 5 (CS5)	40	A0	10100000
Expedited Forwarding (EF)	46	B8	10111000
Class Selector 6 (CS6)	48	C0	11000000
Class Selector 7 (CS7)	56	E0	11100000

2.11 Appendix D: Configuration of External DHCP Server

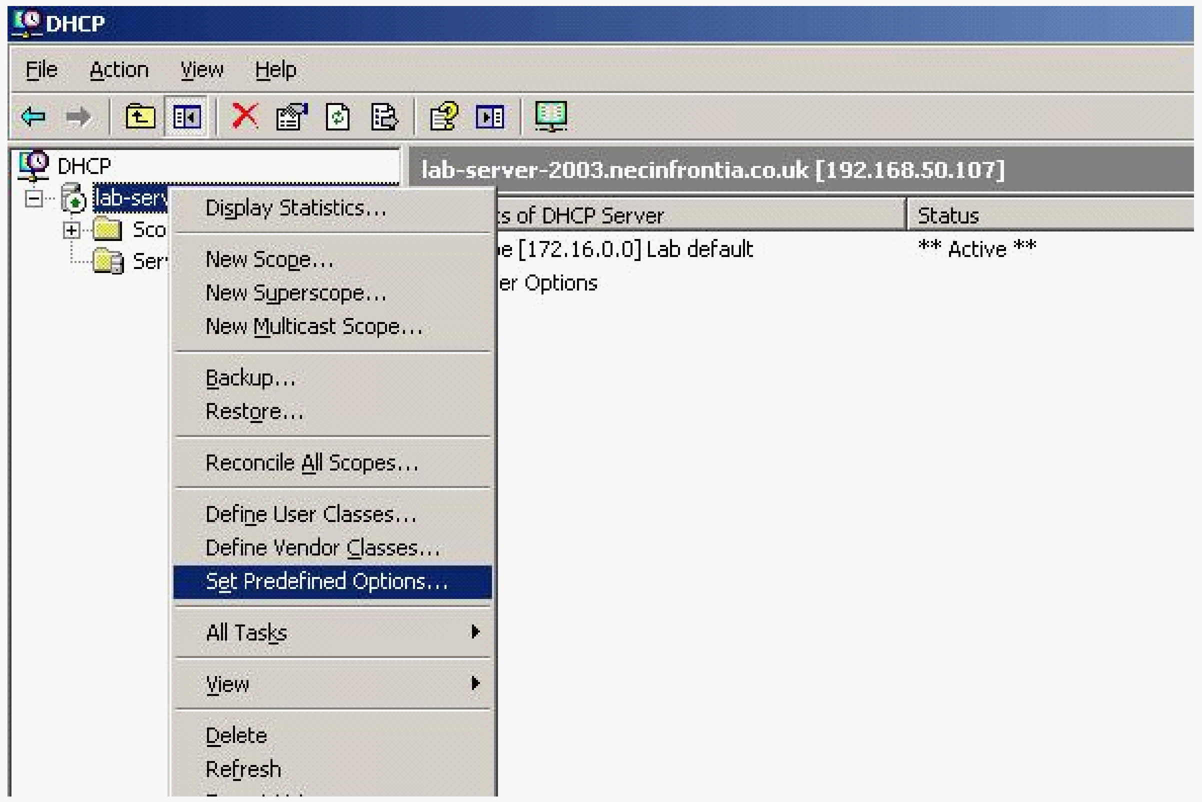
Configuration of External DHCP Server

Note: - Although the SV9100 supports DHCP Server functionality, it is only designed for demonstration or test purposes. Please be aware that no support can be offered if the DHCP Server is used on a customer's site.
It is possible to use either an external DHCP server (e.g. Windows 2003 Server) or the SV9100 internal DHCP server, to provide IP details to the DT800/DT700 IP phones.

If you are using an external DHCP server, it is necessary to add a new Option Code to the DHCP scope for the SIP Server. The method for adding this service varies dependent on the DHCP server used.

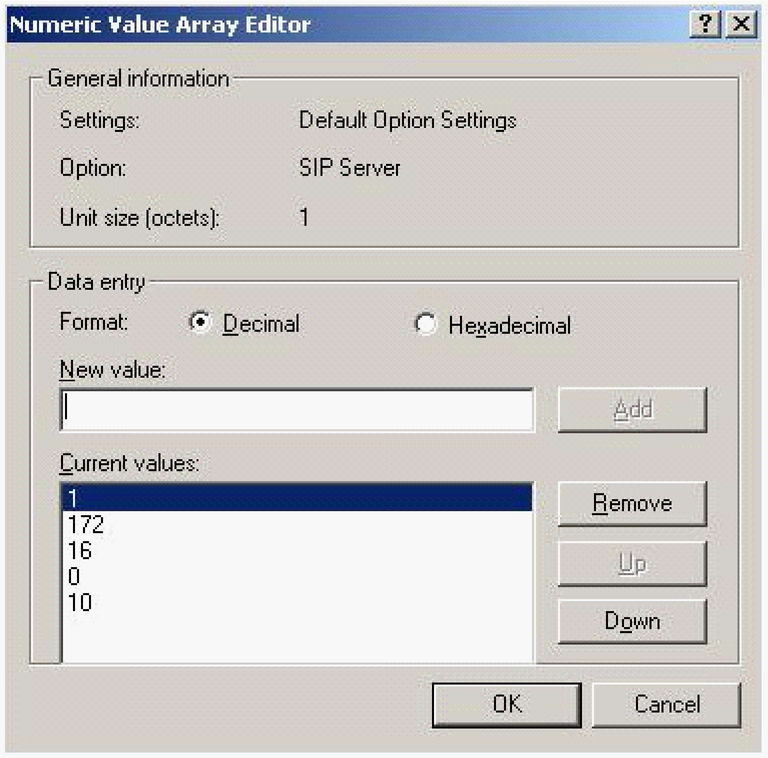
<u>The example below shows the necessary steps to add Option 120 (SIP Server) to a Windows 2003 Server.</u>

1. Enter DHCP via Administrative Tools.
2. Right click on the relevant DHCP server and click on "Set Predefined Options".

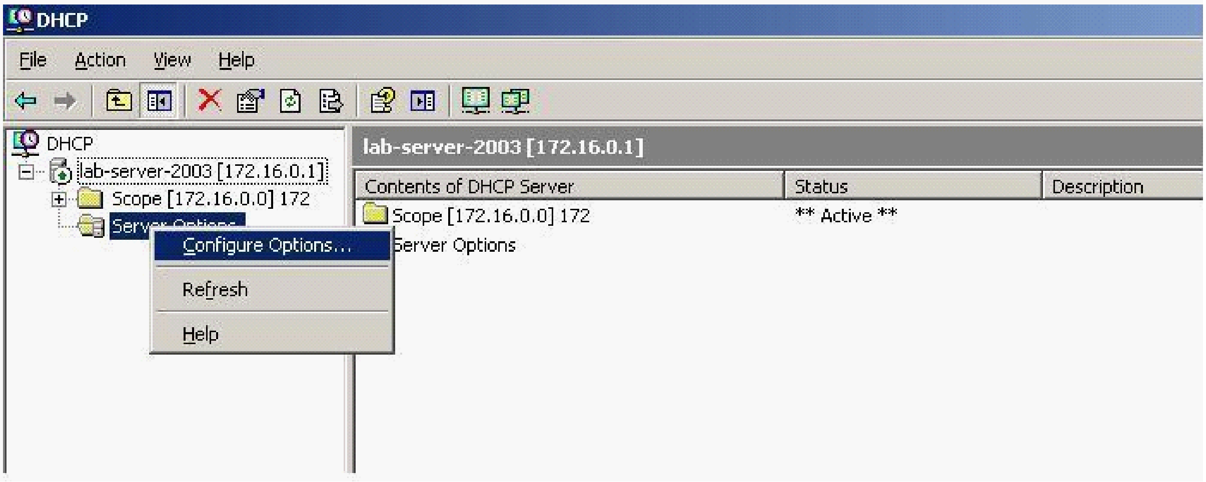


3. When the "Predefined Options and Values" dialogue box opens, click on **Add**.
4. Enter the information below in to the **Option Type** dialogue box.

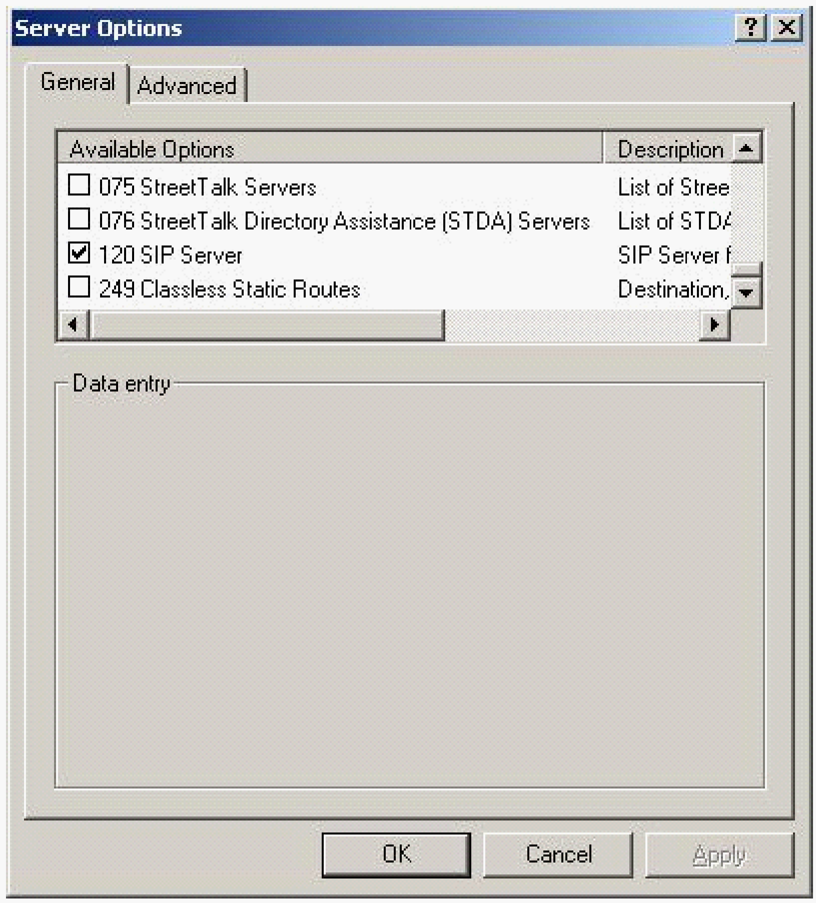
5. Click **OK** and this will create a new Option type for the DHCP server.



6. Enter each octet of the SV9100 IPLE card IP address, click **Add** after each octet. The digit 1 **must** always precede the IP Address as shown above.
7. Reorder the octets into the correct sequence using the up and down buttons. Click **OK** when complete.
8. Right click on **Server Options** in the left hand pane and choose **Configure Options**.



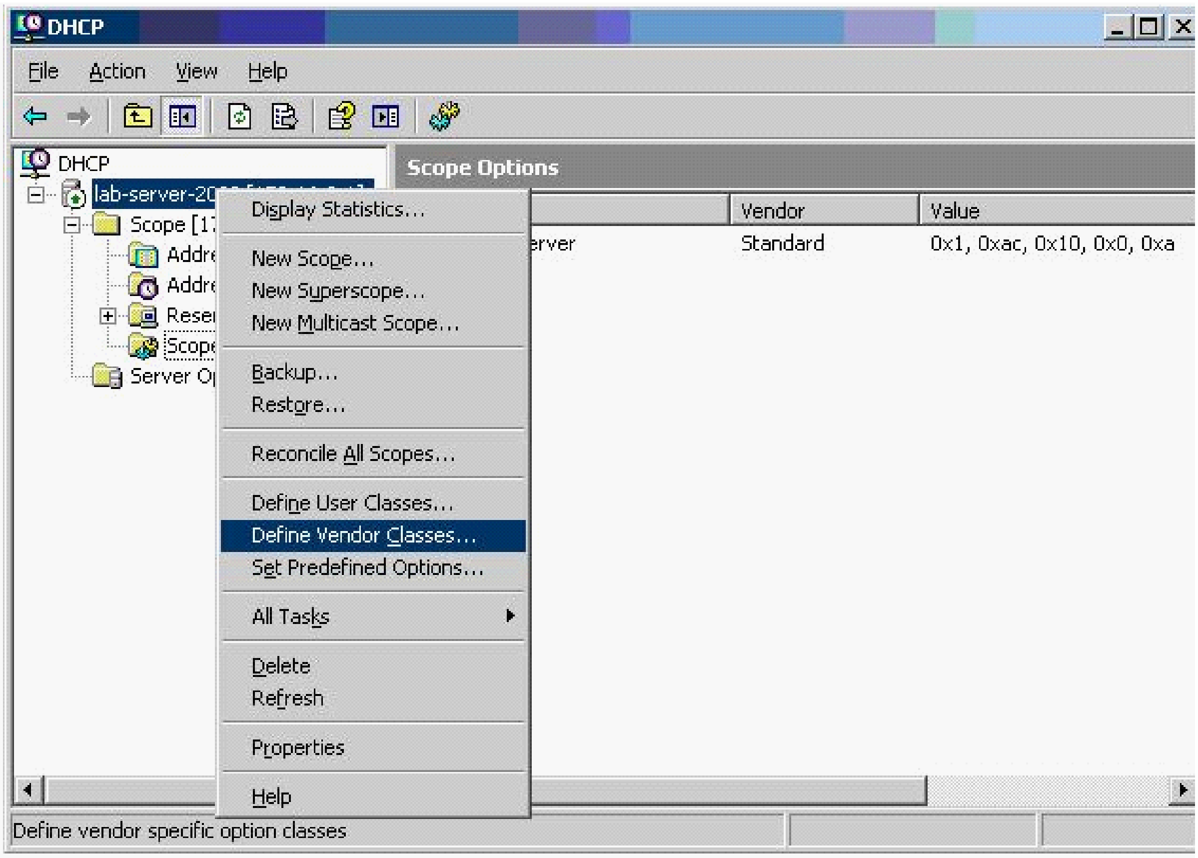
9. Scroll down the Available Options list and tick **120 SIP Server**, click **OK**.



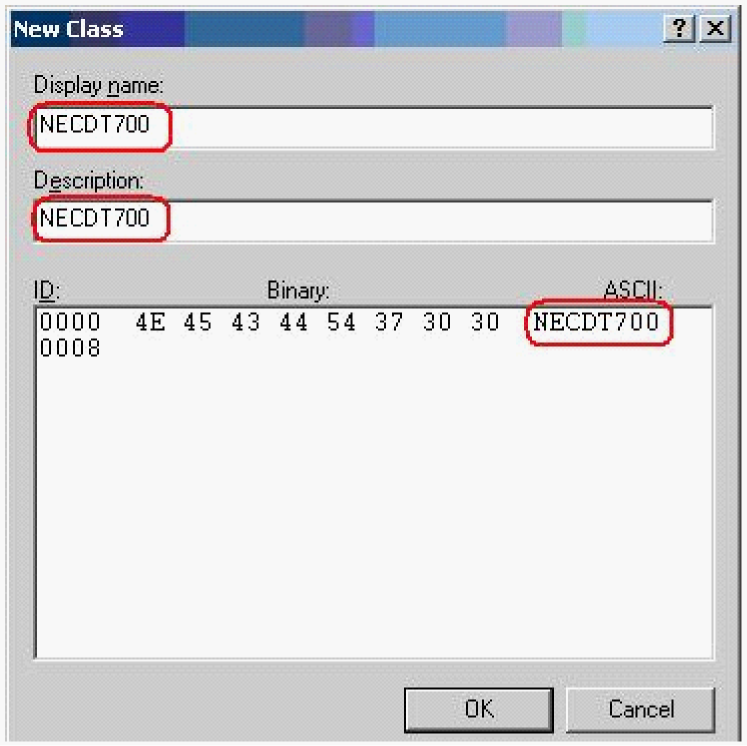
10.The DHCP server is now ready to provide DT800/DT700 phones with the SIP Server address.

The example below shows the necessary steps to add Option 168 (SIP Server Port) to a Windows 2003 Server.

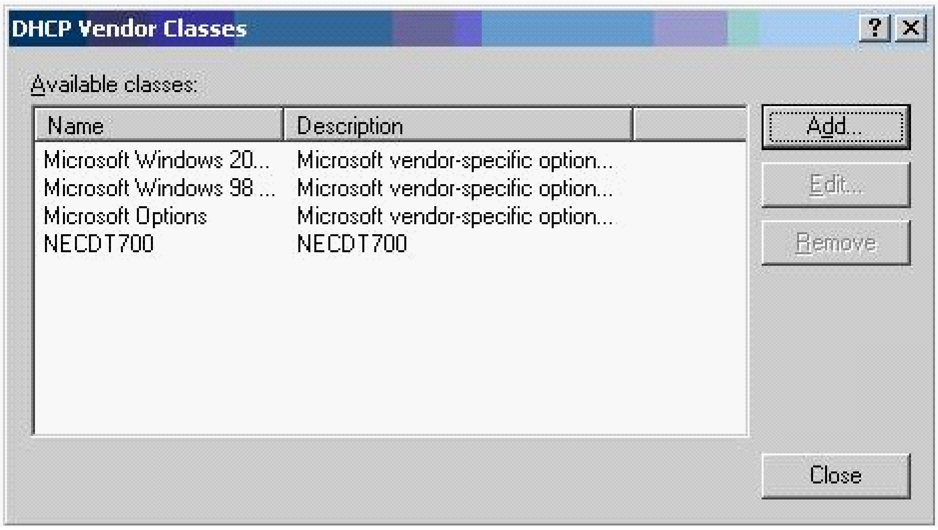
1. In the DHCP server, highlight the server machine on the left hand side. Right click on the server and select Define Vendor Classes.



2. Click **Add** and enter the information show below. The ID and Binary information is entered automatically when you enter the Display name, Description and ASCII value.



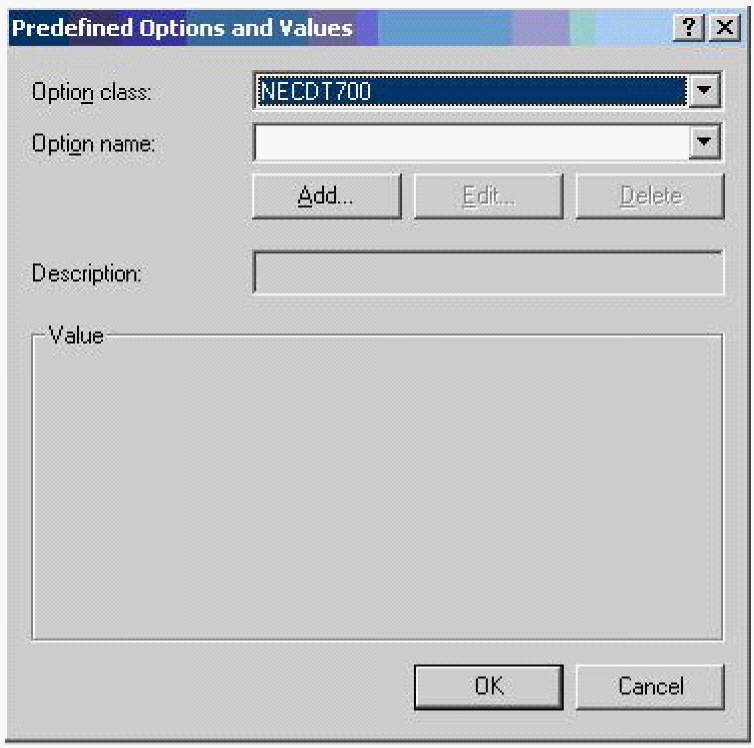
3. Click **OK**.



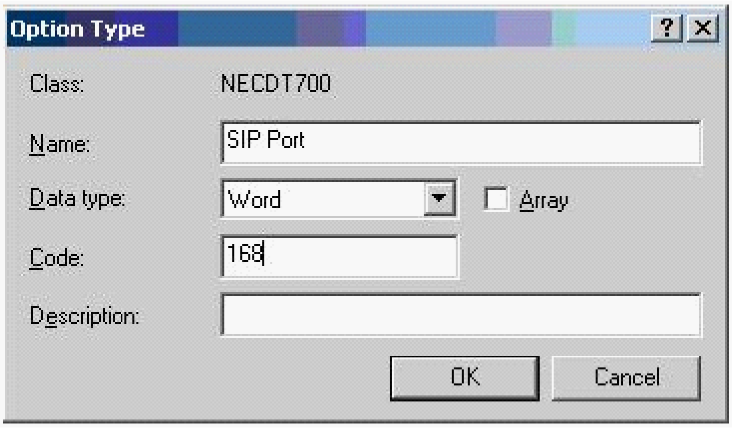
4. Click **Close**.

5. Highlight the server again, then right click and select **Set Predefined Options**.

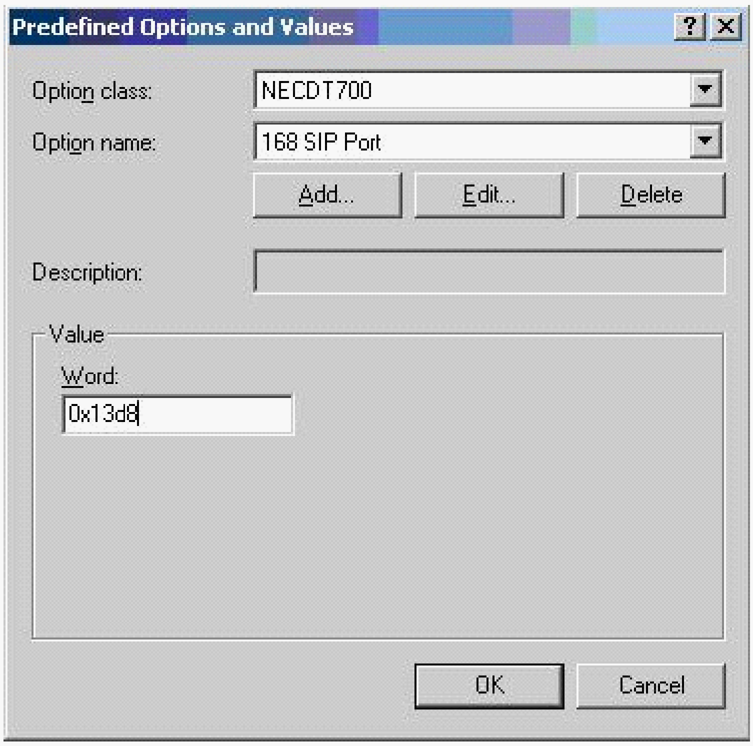
6. Change the Option class to **NECDT700**.



7. Click **Add** and enter the information show below.



8. Click **OK**.
9. In the Word box, enter **0x13d8** as shown below.

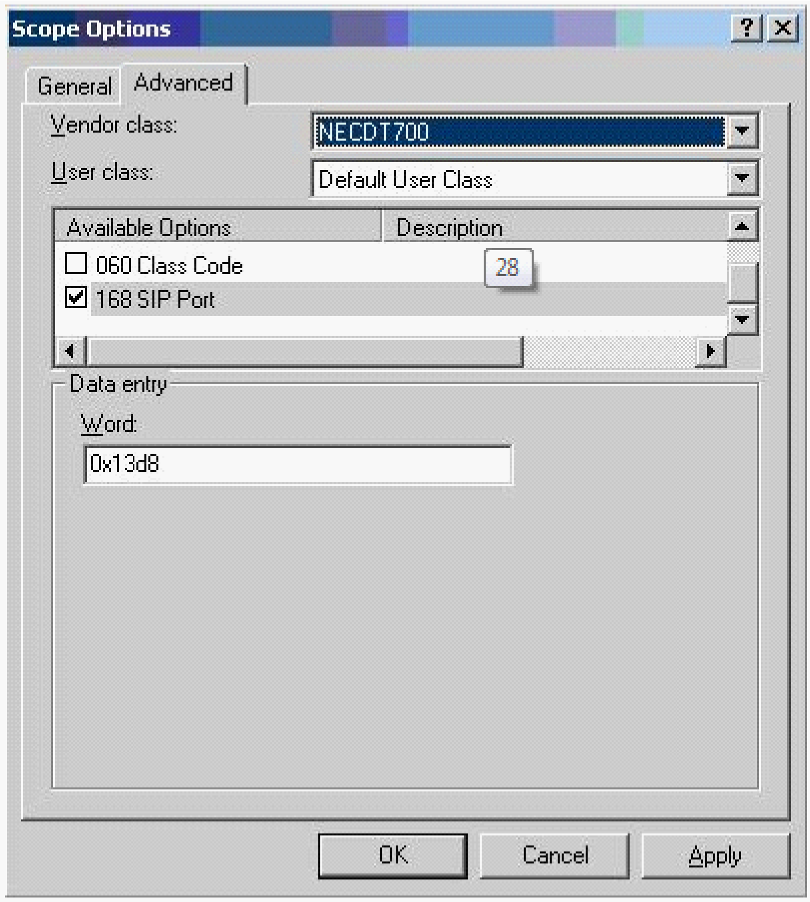


10.Click **OK**.

11.Highlight scope options on the left hand side. Then right click and choose Configure Options.

12.Click **Advanced** and change the vendor class to **NECDT700**.

13.Place a check mark next to **168 SIP Port**, check that **0x13d8** is in the Word box.



14.Click **OK**.

The DHCP server is now ready to provide IP Phones with the SV9100 SIP Port 5080.

2.12 Appendix E: SV9100 RFC Support

Appendix E: SV9100 RFC Support

RFC Number	Title	SV9100 Support			Comments
		Std. Station	Trunk	System	
768	User Datagram Protocol (UDP)	Y	Y	Y	
783	THE TFTP PROTOCOL (REVISION 2)	N/A	N/A	N	

791	INTERNET PROTOCOL	Y	Y	Y	
792	INTERNET CONTROL MESSAGE PROTOCOL	N	N	Y	
793	TRANSMISSION CONTROL PROTOCOL (TCP)	Y	Y	Y	
826	An Ethernet Address Resolution Protocol (ARP)	Y	Y	Y	
854	TELNET PROTOCOL	N/A	N/A	N	
959	FILE TRANSFER PROTOCOL (FTP)	N/A	N/A	Y	
1034	DOMAIN NAMES - CONCEPTS AND FACILITIES (DNS)	Y	Y	Y	Resolve only supported
1035	DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION (DNS)	Y	Y	Y	
1157	A Simple Network Management Protocol (SNMP)	N/A	N/A	Y	
1305	Network Time Protocol (Version 3) (NTP)	N/A	N/A	Y	
1350	The TFTP Protocol (Revision 2)	N/A	N/A	N	
1889	A Transport Protocol for Real-Time Applications (RTP)	Y	Y	Y	
2131	Dynamic Host Configuration Protocol (DHCP)	N/A	N/A	Y	
2132	DHCP Options and BOOTP Vendor Extensions	N/A	N/A	Y	Partial System support
2247	Using Domains in LDAP/X.500 Distinguished Names (LDAP)	N/A	N/A	N	
2251	Lightweight Directory Access Protocol (v3)	N/A	N/A	N	

2252	Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions	N/A	N/A	N	
2253	Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names	N/A	N/A	N	
2254	The String Representation of LDAP Search Filters	N/A	N/A	N	
2255	The LDAP URL Format	N/A	N/A	N	
2256	A Summary of the X.500(96) User Schema for use with LDAPv3	N/A	N/A	N	
2327	SDP: Session Description Protocol	Y	Y	N/A	
2401	Security Architecture for the Internet Protocol (IPSEC)	N/A	N/A	Y	
2460	Internet Protocol, Version 6 (IPv6)	N	N	N	
2616	Hypertext Transfer Protocol -- HTTP/1.1	N/A	N/A	Y	
2617	HTTP Authentication: Basic and Digest Access Authentication	Y	Y	Y	
2806	URLs for telephone calls	Y	Y	N/A	
2833	RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals	Y	Y	N/A	
2854	The 'text/html' Media Type	N	N	N	
2865	Remote Authentication Dial In User Service (RADIUS)	N	N	N	
2976	The SIP INFO Method	Y	N	N/A	
3261	SIP: Session Initiation Protocol	Y	Y	N/A	

3262	Reliability of Provisional Responses in the Session Initiation Protocol	Y	Y	N/A	
3263	Session Initiation Protocol (SIP): Locating SIP Servers	Y	Y	N/A	
3264	An Offer/Answer Model with the Session Description Protocol (SDP)	Y	Y	N/A	
3265	Session Initiation Protocol (SIP)-Specific Event Notification	Y	Y	N/A	
3311	The Session Initiation Protocol (SIP) UPDATE Method	Y	Y	N/A	
3323	A Privacy Mechanism for the Session Initiation Protocol (SIP)	Y	Y	N/A	
3325	Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks	Y	Y	N/A	
3326	The Reason Header Field for the Session Initiation Protocol (SIP)	Y	Y	N/A	Receive only supported
3362	Real–time Facsimile (T.38) – image/t38 MINE Sub-type Registration	Y	Y	N/A	Note: This RFC specification is not supported since FAX over IP from SV7000 is handled on own VoIP protocol.
3407	Session Description Protocol (SDP) Simple Capability Declaration	N	N	N/A	Note: This RFC specification is not supported, since we have not seen any third party SIP telephone set compatible with this standard.
3411	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks	N/A	N/A	N	
3428	Session Initiation Protocol (SIP) Extension for Instant Messaging	N	N	N/A	

3489	STUN – Simple Traversal of User Datagram Protocol (UDP) Through NAT	N	N	N/A	Note: This RFC specification is not supported and no requirement from market yet.
3515	The Session Initiation Protocol (SIP) Refer Method	Y	N	N/A	
3550	RTP: A Transport Protocol for Real-Time Applications	Y	Y	N/A	
3555	MIME Type Registration of RTP Payload Formats	Y	Y	N/A	
3578	Mapping of Integrated Services Digital Network (ISDN) User Part Overlap Signaling to SIP	N	N	N/A	Note: This RFC specification is not supported. The ISUP (ISDN User Part) is not required these days.
3581	An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing	N	N	N/A	
3711	The Secure Real-time Transport Protocol (SRTP)	N	N	Y	Note: This RFC specification is not supported, since "the common standard way to pass encryption key to the terminal" is not defined by the industry yet.
3842	A Message Summary and Message Waiting Indication Event Package for SIP	Y	N	N/A	
3891	The Session Initiation Protocol (SIP) "Replaces" Header	Y	N	N/A	
3892	The Session Initiation Protocol (SIP) Referred-By Mechanism	Y	N	N/A	
3920	Extensible Messaging and Presence Protocol (XMPP):	N	N	N/A	
3959	The Early Session Disposition Type for the Session Initiation Protocol (SIP)	Y	Y	N/A	

3966	The tel URI for Telephone Numbers	N	Y	N/A	
3977	Network News Transfer Protocol (NNTP)	N	N	N/A	
4028	Session Timers in the Session Initiation Protocol (SIP)	Y	Y	N/A	
4250	The Secure Shell (SSH) Protocol Assigned Numbers	N	N	N	
4346	The Transport Layer Security (TLS) Protocol	N	N	N	MA4000/OW5000 can use HTTPS using TLS

SV8100 Voice Over IP Manual