MITEL

SX-200 IP Communications Platform

Engineering Guidelines
Release 5.0 UR1

NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

Mitel SX-200 ICP Engineering Guidelines
Release 5.0 UR1
October 2009

About this Document

Overview

These guidelines provide an overview of the SX-200® IP Communications Platform (ICP), including available features, applications, and services. Major call management facilities, peripheral devices that can be connected to the system, and hardware configurations are outlined to allow you to tailor the system to your needs.

The topics covered in these guidelines are:

- Overview of SX-200 ICP, its hardware, embedded applications and features
- Supporting applications
- Maintenance

Audience

This guide is intended for:

- Customers
- Sales executives
- Consultants
- Industry analysts
- Media analysts
- Sales engineers
- System engineers

About the SX-200 ICP documentation

The following guides provide information about the Mitel SX-200 ICP:

- SX-200 ICP Technician’s Handbook provides instructions to install, upgrade, maintain, and troubleshoot the Mitel SX-200 ICP.
- SX-200 ICP Technical Documentation in Folio (NFO)
- SX-200 Safety Instructions.

SX-200 ICP System Architecture

The SX-200 ICP is built upon Mitel Data Integrated Voice Applications™ architecture delivering sophisticated call management, applications and desktop solutions to businesses. Mitel delivers a highly scalable, robust call control that fully utilizes the power of IP while fully supporting the traditional TDM-based telephony for legacy devices and PSTN connectivity.

Mitel architecture uses the IP network to connect IP telephony devices and provides a supplementary TDM (Time Division Multiplexing) subsystem to switch calls between traditional telephone devices (Figure 1). The SX-200 ICP has the advantage of being able to optimally switch all types of traffic, IP or TDM. The SX-200 ICP provides native call setup, tear down, and signaling between Ethernet IP-connected telephones. For traditional telephony, such as POTS and PSTN trunks, call handling is also handled natively by the SX-200 ICP through a conventional TDM circuit-switched subsystem.

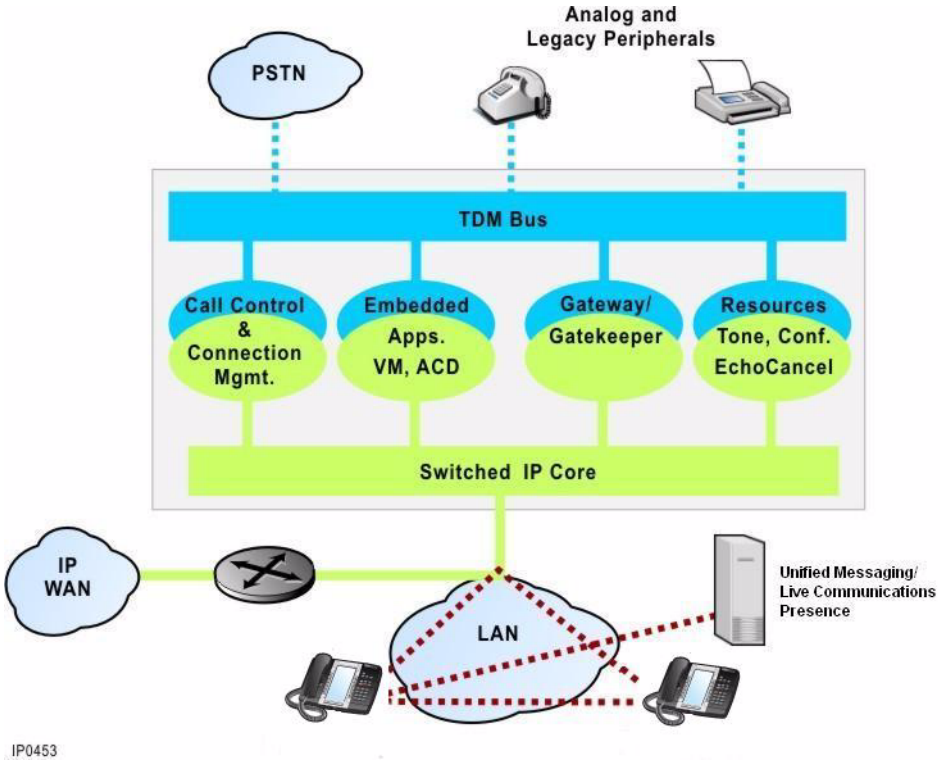


Figure 1: SX-200 ICP system architecture

This ability to use two different switching techniques simultaneously means that:

- All traffic is switched with minimum conversion between packet and traditional telephony to provide optimum voice quality in all call scenarios.
- Embedded gateway functionality is required only between the IP and non-IP networks optimizing the use of system resources.
- Migration from traditional PBX to IP telephony is seamless and efficient.

Supported countries

The SX-200 ICP range of products includes support for North America. Language support for set display is included.

Typical Configurations

The SX-200 ICP product line includes a number of platforms, IP phones, and a range of applications. Each platform is designed for a different business segment and size, but each contains a number of common components. The main difference between the units is the quantity of components contained in each system.

System configurations

The units are flexible and can be used in a number of different configurations, for example:

- IP-PBX with phones, Voice Mail, and PSTN gateway
- Standalone controller, in conjunction with other units
- Standalone wireless gateway
- Standalone IP network gateway
- Standalone Teleworker gateway
- TDM controller for legacy interfaces

The use of the LAN infrastructure and IP networking allows the units to be installed and used in a number of different configurations. It also allows for a more distributed architecture and dispersal of equipment compared to a more traditional central TDM PBX system. With the history of the product being influenced by the more traditional SX-200, it can also be easily integrated with an existing installation.

Business models

There are a number of potential business models that require different network configurations. The following examples illustrate how the business model affects the overall network and unit configurations.

In the descriptions below, a unit is considered a SX-200 ICP with a particular configuration and is part of the overall telephony system.

Multiple units

In a multiple unit configuration, a number of units are clustered together, but each unit functions independently. The units connect to each other through the network, using IP trunks, or TDM trunks. In the event of a unit failure, some of the overall system will fail. In the event of a network failure, the units still maintain PSTN access. In a small- or medium-sized office, a number of units could be installed together to make a larger system. Another scenario could be a small- or medium-sized business with a number of branch offices (for example, an automobile dealership), where local access is needed, but intershop traffic is also a requirement.

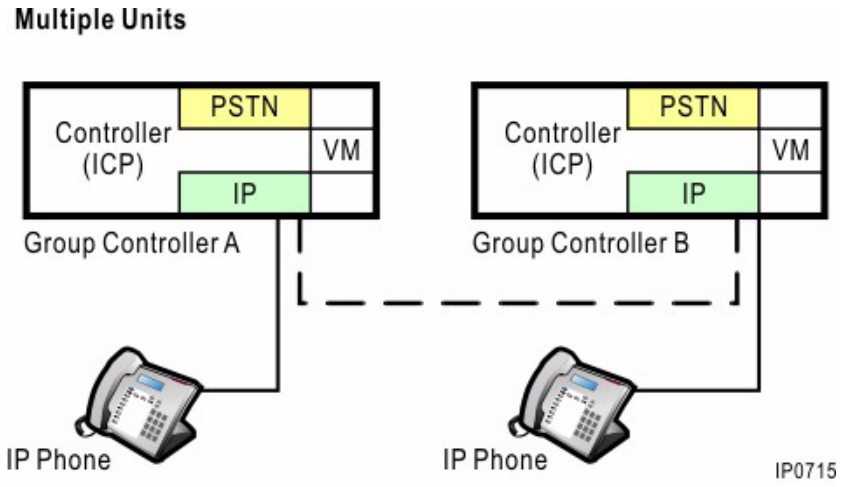


Figure 2: Example of a Multiple Units Configuration

Distributed system

In a distributed system, different telephony system functions are dedicated to individual units. These are then distributed to different parts of the network, or business as required. This is potentially a larger and possibly geographically dispersed enterprise. For example, a number of units could act purely as TDM gateways, providing central access, with other units acting as central voice mail and others acting as the group controllers (a group controller is a SX-200 ICP to which a group of IP phones have been registered). An example is a university campus where each building possesses the group controller and local phones, but the PSTN access is in a separate secure building. A different scenario is a large enterprise with corporate headquarters in different cities. Each would have distributed trunk units and could be considered multiple copies of the campus scenario.

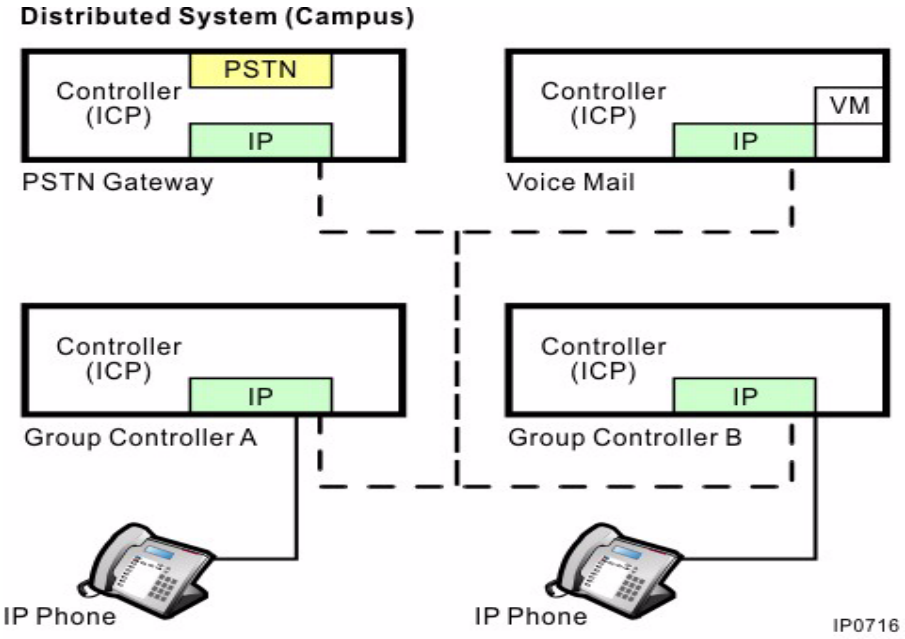


Figure 3: Example of a Campus Environment Configuration

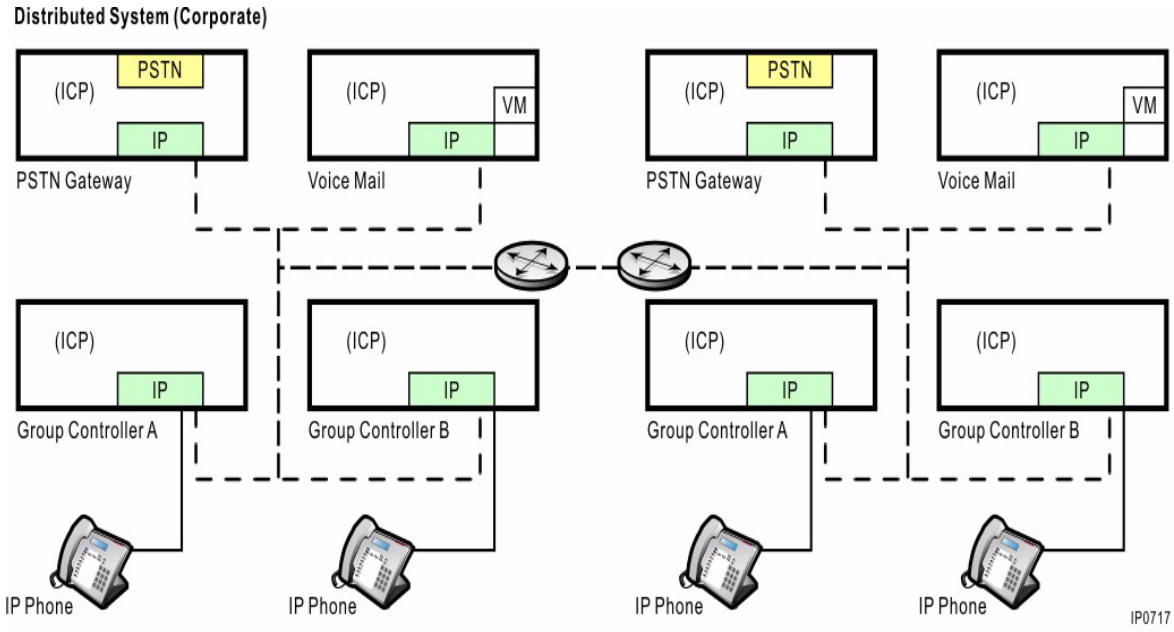


Figure 4: Example of a Corporate Configuration with Multiple HQs

Hybrid system

A Hybrid system combines both of the previous scenarios and involves a distributed system for a headquarters and combined units for remote branch offices. The branch office has access to corporate PSTN access as well as local access through the local group controller. In the event the WAN link is lost, the separate sites can still operate as independent units.

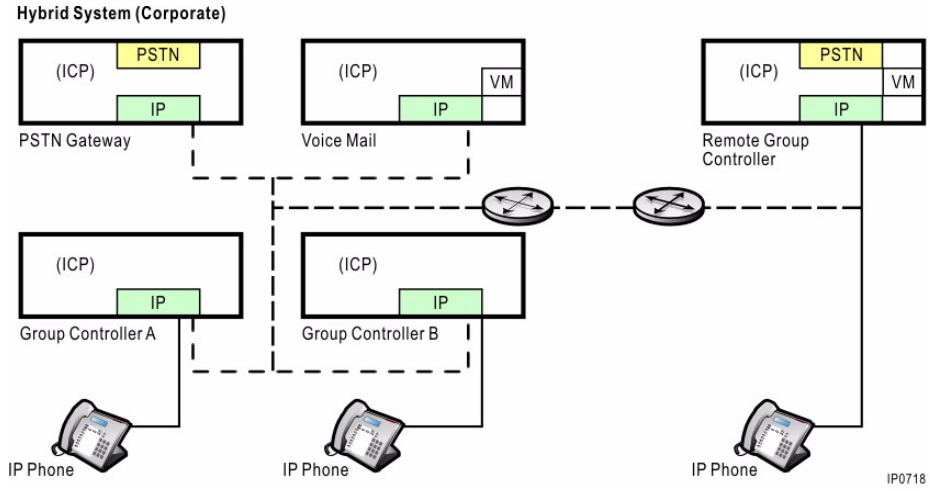


Figure 5: Example of a Hybrid Configuration

Using the ICP as a centralized voice mail server

There are two similar situations where this configuration needs to be considered. One is where the ICP is used as a dedicated voice mail server without additional end devices attached; the other is where it might be used as a central mail server, but still with devices attached.

When used as a dedicated voice mail server, the ICP provides up to 24 channels for continuous use. Voice mail cannot be stored using compression (for example, the incoming call may be compressed, but it will not be stored in compressed form).

Note: Using voice mail ports to support auto attendant functions reduces the overall VM capacity, and may not be suitable for this application. When determining network bandwidth, consider voice mail sessions as being active 100% of the time.

Voice mail is a particularly heavy user of system resources. Where the unit is used as a centralized voice mail server, consider the number of other functions provided on the box. Typically, as more voice mail sessions are activated, the number of IP phones that can be handled decreases. The System Engineering tool should be used to determine, with accuracy, the exact numbers of VM sessions, IP phones, and TDM phones the system can support. Typically, 24 VM sessions and more than 200 users are in direct opposition. For numbers outside this range, multiple units should be considered.

Slot numbering conventions

The SX-200 ICP MX Controller has four locations for MMC modules (Slots 1 through 4). Figure 6 is a top view of the SX-200 ICP MX Controller, showing the MMC slot numbering convention for this platform. The diagram also indicates the type of MMC module that can be used in a particular slot. All four MMC slots are front-accessible.

<table>
<tr><td>Power
Supply</td><td colspan="2">Analog Main Board
Analog Option Board
(optional, installed on AMB)</td><td>Compact Flash
or
Hard Drive</td></tr>
<tr><td></td><td colspan="2">Clock Module</td><td>SysID</td></tr>
<tr><td>Slot 1
FIM, T1/E1, or quad CIM</td><td>Slot 2
DSP, T1/E1, quad CIM</td><td>Slot 3
DSP</td><td>Slot 4
Compact Flash</td></tr>
</table>

Figure 6: MX Controller, MMC/A Slot Numbering and Usage

The SX-200 ICP CX/CXi platform has three locations for MMC modules (Slots 1 through 3). Figure 7 is a top view of the SX-200 CX/CXi system, showing the MMC slot numbering convention for this platform. The diagram also indicates the type of MMC module that can be used in a particular slot. Of the three MMC slots available, only the first two are front-accessible.

Hard Drive (optional)	**Power Supply**		**Analog Main Board** **Analog Option Board** (optional, installed on AMB)
Compact Flash	Clock Module		SysID (iButton)
Slot 1 T1/E1 Combo Quad CIM	**Slot 2** T1/E1 Combo Quad CIM	**Slot 3** DSP	**Powered Ethernet Module (CXi only)**

Figure 7: CX/CXi Controller, MMC/A Slot Numbering and Usage

The SX-200 ICP AX platform has two locations for MMC modules (Slots 1 and 2). Figure 7 is a top view of the SX-200 AX system, showing the MMC slot numbering convention for this platform. The diagram also indicates the type of MMC module that can be used in a particular slot. Of the two MMC slots available, only MMC Slot 1 is front-accessible.

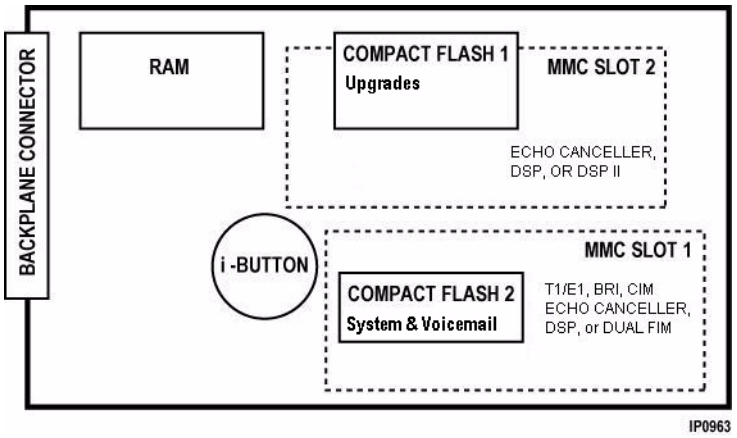


Figure 8: AX Controller, MMC Slot Numbering and Usage

Configuration table

This table shows the maximum values for each feature or resource in each type of controller. You cannot configure a system to support all maximum values at the same time.

Feature/ Resource	CX/CXi	MX	AX
IP users	100	248	248
TDM users (see note 1)	100	576	288
Total users	150	768	536
ACD agents	50 IP	100 (IP + TDM)	40 IP
Echo channels/IP gateway (E2T)	12/64 (default) 42/64 (maximum)	64/64 (default and maximum)	40/64
Conference channels (see note 2)	30	64	64
Voice Mail ports (see note 3)	16	24	20
Record-a-Call (see note 4)	8	12	4**
Compression channels (see note 5)	16	24	24
CIM ports (including Quad CIM)	3	10	0
ASU/ASU II supported (see note 6)	3 external	6 external	0
LS trunks (in ASU)	12 internal 36 external	12 internal 36 external	48
IP trunks	16	30	30
MMC modules (installed slots)	Dual or Quad DSP (3) T1/E1 Combo (1, 2) Quad CIM (1, 2)	Dual or Quad DSP (2,3) Dual T1 (1, 2) Dual FIM (1, 2) Quad CIM (1, 2)	Dual or Quad DSP (2) T1/E1 Combo (1) Dual T1/E1 (1)
Digital links (T1) (see note 7)	1	8	2
Peripheral cabinets	0	7	0
NSU cabinets	0	4	0
DTMF generators	as required	as required	as required
Note: ** Record-a-Call is limited on the AX because of the flash-based system.			

Note:

1. Together, both IP and TDM devices can make up the overall system capacity, and individually, the limits are as shown. The system capacity is not the sum of the maximum IP and TDM users, simultaneously. The CX can support a combined total of 180 users. For the MX, at the maximum number of IP users, the number of TDM users is limited to 384. At the maximum number of TDM users, the number of IP users is limited to 96, and traffic capacity is also reduced. Verify any installations that go beyond the nominal configuration with Customer Engineering Services (or by using the System Engineering Tool). On the MX, TDM supports DNIC and ONS devices. On the AX and CX, TDM supports ONS devices only.
2. Conference channels are a fixed allocation at system start-up, based on the available DSP resources in a given configuration, and may be well below the maximum shown. They can be used in any combination of 3-party to 5-party conferences up to the maximum number of available channels.
3. The Voice Mail capacity on a base unit is lower, but may be expanded to the maximum shown. As with conferences, VM ports are assigned at start-up, based on the available DSP resources.
4. Every Record-A-Call session uses a conference resource and a Voice Mail session.
5. Compression is not a standard offering on base systems. Additional DSP resources are needed to achieve the values shown. For CX controllers, the practical limit under most conditions is 8 compression channels, although up to 16 can be configured. For MX controllers, it is as shown.
6. The Analog Main Board and Option Board together may be considered to be an internal ASU. External ASU cabinets (24 port ONS) or ASU II cabinets (with both ONS and ONS/LS cards) may be connected to the embedded CIM ports and Quad CIM module(s).
7. Digital trunks may be embedded T1/E1 modules, PRI cards or T1/E1 modules in digital bays, or external NSUs.
8. It is not possible to install the maximum number of ASU, NSU and peripheral bays at the same time because they all use a limited number of FIM/CIM links. The maximum number of external connections is 10.

Provisioning system resources

The internal hardware of the 200 ICP CX/CXi, MX and AX controllers is significantly different. Available features and resources are based on the option package purchased and the installed DSP resources. These are summarized in other customer documentation, but the following tables will give more detail, showing the capacity of a system in its factory default configuration, and with additional MMC modules installed.

Note: It is not possible to configure all of the parameters or features to the maximum limit at the same time.

Table 1: SX-200 ICP MX Configurations

Option Package	Feature/ Resource	1 Dual DSP (default)	2 Dual DSP or 1 Quad DSP	2 Dual DSP + 1 Quad DSP	2 Quad DSP
Business Option 1	Total IP users	48	96	96	192
	Total ONS/DNIC	6	6	96	192
	ACD users IP/DNIC	8	25	50	100
	G.729 Compression	8	8	16	24
	3-party Conference	3	8	12	12
	Voice Mail ports	4	12	18	24
	CIM/FIM ports	2	2	3	4
	External ASU ONS	0	0	48	48
	Digital bays	0	0	1	2
	T1 (or PRI) trunks	0	24	48	96
	Embedded T1/E1 MMC	0	1	1	1
	NSU bays	0	1	1	2
Business Option 2	Total IP users	48	96	96	192
	Total ONS/DNIC	6	6	96	288
	ACD users IP/DNIC	8	25	50	100
	G.729 Compression	0	0	8	16
	3-party Conference	8	12	18	21
	Voice Mail ports	8	18	24	24
	CIM/FIM ports	0	1	3	4
	External ASU ONS	0	0	48	48
	Digital bays	0	0	1	3
	T1 (or PRI) trunks	0	24	48	96
	Embedded T1/E1 MMC	0	1	1	1
	NSU bays	0	1	1	2
Hospitality Option	Total IP users	0	48	96	248
	Total ONS/DNIC	96	96	192	384
	ACD users IP/DNIC	0	0	0	0
	G.729 Compression	0	8	16	16
	3-party Conference	8	8	12	12
	Voice Mail ports	8	12	18	24
	CIM/FIM ports	3	4	5	6

Table 1: SX-200 ICP MX Configurations (continued)

Option Package	Feature/ Resource	1 Dual DSP (default)	2 Dual DSP or 1 Quad DSP	2 Dual DSP + 1 Quad DSP	2 Quad DSP
	External ASU ONS	48	48	48	48
	Digital bays	1	1	2	4
	T1 (or PRI) trunks	0	0	48	96
	Embedded T1/E1 MMC	0	1	1	2
	NSU bays	0	1	1	2
Analog Option 1	Total IP users	24	48	96	192
	Total ONS/DNIC	288	288	288	384
	ACD users IP/DNIC	0	0	0	0
	G.729 Compression	0	0	0	0
	3-party Conference	2	8	12	21
	Voice Mail ports	6	18	24	24
	CIM/FIM ports	4	5	5	6
	External ASU ONS	0	0	48	48
	Digital bays	3	3	3	4
	T1 (or PRI) trunks	48	72	72	96
	Embedded T1/E1 MMC	1	2	2	2
	NSU bays	1	2	2	2
Analog Option 2	Total IP users	24	48	48	96
	Total ONS/DNIC	384	384	480	480
	ACD users IP/DNIC	0	0	0	0
	G.729 Compression	0	0	0	0
	3-party Conference	2	10	12	21
	Voice Mail ports	4	12	16	24
	CIM/FIM ports	6	6	6	6
	External ASU ONS	0	0	48	48
	Digital bays	4	4	5	5
	T1 (or PRI) trunks	48	48	48	48
	Embedded T1/E1 MMC	1	1	1	1
	NSU bays	1	1	1	1

Table 1: SX-200 ICP MX Configurations (continued)

Option Package	Feature/ Resource	1 Dual DSP (default)	2 Dual DSP or 1 Quad DSP	2 Dual DSP + 1 Quad DSP	2 Quad DSP
Analog Option 3	Total IP users		96		
	Total ONS/DNIC		576		
	ACD users IP/DNIC		0		
	G.729 Compression		0		
	3-party Conference		8		
	Voice Mail ports		12		
	CIM/FIM ports		10		
	External ASU ONS		48		
	Digital bays		6		
	T1 (or PRI) trunks		96		
	Embedded T1/E1 MMC		2		
	NSU bays		4		
					Page 3 of 3

Note:

1. IP users include all types of IP phones and applications (such as YA and YA-Pro).
2. ACD users indicates the number of active agents. One ACD agent is equivalent to 3 or 4 normal users in terms of traffic and performance load, so the total number of users must be reduced accordingly when ACD agents are active.
3. Compression channels are assigned in blocks of 8 at system initialization. If the number of compression channels selected in CDE is less than the available number in the table, then more voice mail and conference channels will be assigned for the given option and DSP hardware configuration.
4. For debugging purposes, one DSP can be assigned to echo cancellation by enabling System Option 82 (Use DSP Echo Canceller). If this is done, the number of devices available for other compression and telecom functions is reduced, and the number of voice mail and conference channels will be reduced.
5. The MX can always have both the Analog Main Board and the Analog Option Board installed (such as the internal ASU fully populated with 2 DNIC + 4 ONS + 12 LS ports). Extra DSP resources are not needed if the AOB is installed to a base system.
6. Migration from an EL system can usually use any of the above options, but if there are more than 6 bays in use, then the only possibility is Analog Option 3. In this configuration, there are two quad CIM cards installed (or one quad CIM and one dual FIM), providing up to 10 external connections (7 digital bays + 3 NSU cabinets or PRI cards). In this size range, the system can support an average of 4CCS per port, but that is no different than the SX-200 EL supported in its maximum configuration.
7. With Analog Option 2, the traffic will always be limited by trunk availability to 4CCS per port or less. With all other options, the system can always support heavy office traffic of 6CCS per port.
8. In all options, the number of digital trunk links can be increased, but there may not be enough resources to operate these additional trunks at full capacity. The nominal limit on digital links is always 8, but this may be reduced depending on available physical connectivity, performance, and DSP resources.

Table 2: SX-200 ICP CX/CXi Configurations

Business Option 1						
Feature/ Resource	Base	Base + T1/E1 Combo	Base + Dual DSP	Base + Dual DSP + T1/E1 Combo	**Base + Quad DSP**	**Base + T1/E1 Combo + Quad DSP**
Number of DSPs	**2**	**3**	**4**	**5**	**6**	**7**
Total IP users	24	64	40	80	80	100
Total ONS	8	24	40	150	150	150
ACD users IP	6	10	6	10	6	10
G.729 Compression	0	0	0	0	0	0
3-party Conference	3	10	10	10	10	10
Voice Mail ports	4	16	16	16	16	16
CIM ports	0	0	2	3	3	3
External ASU	0	0	2	3	3	3
Digital bays	0	0	0	0	0	0
LS/CLASS Trunks	12	12	16	12	36	16
T1 trunks	0	24	0	24	0	24
Embedded T1/E1 combo	0	1	0	1	0	1
NSU bays	0	0	0	0	0	0
Alternative combination with compression enabled:						
Total IP users	--	--	40	80	80	100
Total ONS	--	--	8	100	56	130
ACD users IP	--	--	6	10	6	10
G.729 Compression	--	--	8	8	8	16
3-party Conference	--	--	3	10	10	10
Voice Mail ports	--	--	4	16	16	16
CIM ports	--	--	0	0	3	3
External ASU	--	--	0	0	3	3
Digital bays	--	--	0	0	0	0
LS/CLASS Trunks	--	--	12	12	36	16
T1 trunks	--	--	0	24	0	24
Embedded T1/E1 combo	--	--	0	1	0	1
NSU bays	--	--	0	0	0	0

Note: Not all maximum values for lines and trunks can be realized at the same time.

Notes:

1. The number of ACD agents is limited in this system by the available E2T (echo cancellation) channels. Again, the total number of users must be reduced accordingly when ACD agents are active.
2. The CX/CXi can always have both the Analog Main Board and the Analog Option Board installed (for example, the internal ASU fully populated with 8 ONS + 12 LS ports). Extra DSP resources are not needed if the AOB is installed to a base system.
3. Again, because of E2T and echo limitations, the total number of active trunks cannot exceed 24, although it is possible that up to 12 LS and 24 T1 might be connected.

Table 3: SX-200 ICP AX Configurations

Business Option 1				
Feature/Resource	**Base**	**Base + Dual T1/E1**	**Base + T1/E1 Combo**	**Base + Dual T1/E1 + Quad DSP**
Number of DSPs	**4**	**4**	**5**	**8**
Total IP users	200	248	248	248
Total ONS	192	288	288	288
ACD IP Users	40	40	40	40
G.729 Compression	0	0	8	24
3-party Conference	21	21	10	21
Voice Mail Ports	20	20	20	20
LS/CLASS Trunks	48	48	24	48
T1 Trunks	0	48 T1 or 46 PRI	24 T1 or 23 PRI	48 T1 or 46 PRI
Embedded Dual T1/E1	0	1	1	1

Note: G.729 Compression requires that additional DSP resources must be installed, either a T1/E1 Combo card or a Dual or Quad DSP card.

Paging limits

Group paging to IP sets (including All Sets Page) is limited to the maximum number of available E2T channels. On a busy system, this may be less than the physically provisioned limit of channels. Paging groups should be configured with this limit in mind. PA paging is not generally affected by the number of E2T channels available.

Paging Source	Paging Destination	E2T Channels Required	E2T Channels Limit
TDM set (ONS, DNIC)	TDM and/or IP set(s). May be single directed page, group page, or All Sets page.	Number of IP sets paged.	Available E2T channels
	PA Zone(s)	none	not applicable
IP set	TDM and/or IP set(s).	1 + number of IP sets paged	Available E2T channels
	PA Zone(s)	1	Available E2T channels
Note: The available E2T channels is the number of free channels at the time the page is made, not the total number on the system (i.e. maximum E2T channels minus those already in use).			

Maximum limits

Most of the system maximum limits are documented in the *General Information Guide*. The following section highlights some relevant system limits.

Note: All maximum limits cannot be achieved at the same time.

- The maximum number of MiTAI™ sockets supported on the SX-200 ICP is 150.
- The maximum number of Your Assistant (YA) is 75. YA softphone is supported to the same limits.
- The absolute limit for compression channels in the AX or MX system is 24, and on the CX/CXi is 16, but this can only be reached under some unusual configurations, such as an IP trunking gateway with no local Voice Mail. A typical system will never reach the limit on compression channels without running out of DSP resources for other features and applications.
- There is only one compression zone for a controller. Each IP phone or trunk can be selected to be normal or compressed through a COS option.

Maximum Ringing and Wake-up Calls

Maximum ringing and wake-up calls per system are dependent on the installed hardware.In all systems, presence of any active message waiting lamps will reduce the maximum number of ringing circuits by 25%,

SX-200 AX Controller

There is a hardware maximum of 12 simultaneously ringing ONS ports per 24 port ONSP card. The AX also has a system-wide ringing limit of 96 ONS ports, lower than the limit of 12 ports per card.

The same limit applies to wake-up calls on ONS ports. Maximum simultaneous wake-up calls is 12 per 24-port ONSP card and a maximum system capacity of 96 wake-up calls.

SX-200 MX Controller with Peripheral Nodes

There is a hardware maximum of 20 simultaneously ringing ONS ports per Peripheral Node.

The same limit applies to wake-up calls on ONS ports. The maximum simultaneous wake-up calls is 20 per Peripheral Node.

SX-200 ICP with ASU II Bays

There is a hardware maximum of 12 simultaneously ringing ONS ports per 24 port ONSP card. Maximum ASU II capacity is 24 (12 ringing ports x 2 ONSP cards).

The same limit applies to wake-up calls on ONS ports. The maximum simultaneous wake-up calls is 24.

Provisioning for traffic

All SX-200 ICP controllers contain an internal TDM switching fabric. Calls that go between TDM sets, or from TDM sets to trunks, will stay within this TDM switch. Calls between IP phones stream their voice packets directly over the data network, without going into the TDM domain in the SX-200 ICP controller, but calls between IP sets and TDM devices (including both lines and trunks) must go from the IP domain to the TDM switch fabric through the TDM gateway (E2T processor). All of these calls require bandwidth or channels within the various domains, and may require specific resources (DSP tone generators and detectors, echo cancellation, etc.) within the controller. The provisioning of these resources is done using the standard type of traffic analysis.

Under most ordinary conditions, the “rules based” provisioning suggested in previous sections gives a good estimate of the resources required for the number of lines (users) and trunks in a system. For systems which are approaching the limits of the system, more detailed calculations may be required through Customer Engineering Services or the System Engineering Tool.

Note: For custom settings and more accurate results based on AT&T traffic tables, refer to the System Engineering Tool.

- There are 36 CCS in an hour, and 1e (erlang) in an hour.
- Call rates (CPH) and duration may vary from business to business. It may be necessary to monitor a business to get more accurate values.
- Typical phone calls are 100 seconds in duration.
- Typically, a normal office phone is busy 16% of the time, or 0.16 e, or 6 CCS (this is 6 CPH @ 100 seconds, for example, 600 call seconds or 6 centum call seconds).
- Typically, a hotel phone is busy 6% of the time, or 0.06 e, or 2 CCS.
- Typically, a busy office phone, such as one handling dispatch orders, can be busy 33% of the time, or 0.33 e, or 12 CCS.
- Typically, ACD workers are busy 75% to 100% of the time. Typically one ACD agent requires one resource, such as one E2T channel, one echo channel, one DSP channel (compression), and one trunk.
- Typically, calls are split in thirds, with 33% incoming from trunks, 33% outgoing to trunks and 33% handling internal calls (of which 50% is making calls and 50% receiving calls).
- Typically, in a given ACD group, all calls are either incoming or outgoing trunks, rarely mixed.
- For normal users, typically one voice mail session is needed for 20 users. More or less traffic per user modifies this number accordingly.
- Erlang adds a statistical blocking factor and is always higher than the straight calculation. Add a further 10% to 20% as a rough estimation, and round up.
- Operators or attendants can typically handle up to100 calls per hour (as long as transfer is handled quickly and number lookup is sufficiently quick). Most incoming trunk calls arrive at the operator station.

Hardware Modules and Platforms

The SX-200 ICP Controller provides the voice, signaling, central processing, and communications resources for the system. Controllers are available in the following configurations:

- CX/CXi (100 users. The CXi includes an internal L2 switch. The CX does not.)
- AX and MX (200+ users)

Refer to the *General Information Guide* and the *Technician's Handbook* for further details on the systems.

There are a number of resources that are provided in each SX-200 unit. These can be used in conjunction with other units to provide a large network, or be used in a combined unit for a smaller installation.

Internally, there are sufficient switching paths, both IP and TDM, to provide a non-blocking scenario. However, a shortage of internal resources can produce the same effect as blocking within the switching fabric. In addition, some legacy devices provide concentration before connection to the controller, and some blocking can occur there.

Blocking is a situation that could occur during a call that might stop the call from completing. For instance, lack of a speech path will stop the call from being completed. These conditions usually occur where there is limited resource, or shared resources, such as DTMF detectors. A non-blocking scenario is one where there are sufficient resources such that limitations due to number of users cannot occur.

Processor modules

The processor in the system is used for two distinct applications: Real Time Controller call control (RTC) and TDM Gateway (E2T).

In MX, AX, and CX systems, one single processor, installed directly on the main board, is shared between the functions.

Real Time Controller

The Real Time Controller contains the Call Control software and also controls functions in the platform.

TDM Gateway

The TDM Gateway is also known as the E2T (Ethernet to TDM). It provides the voice gateway conversion between IP packet voice streams and TDM voice connections.

Compact Flash Cards

Some MX and CX systems are configured with two compact flash cards. The external (front panel accessible) card is used to store the files for installation and upgrades, and may be removed during normal operation. The internal compact flash stores the operating system, database and configuration data over a power failure, and at installation. It also stores data for voice mail.

The AX Main Controller card has two sites for Flash memory:

- The Flash in site 1 is used for upgrading/installing the software and performs basically the same functionality as the front Flash on the CX/CXi/MX controllers. The Main Controller card for the AX is shipped without a Flash Card in site 1. You can use a 256 MB Flash Card to upgrade the software.
- The Flash in site 2 hosts the system files, partitions and voice mail storage. The Main Controller is shipped with a 4 GB Flash Card in site 2.

Hard drive

Newer MX and CX systems are shipped with an internal hard drive. Systems with internal CompactFlash cards can be upgraded to an internal hard drive (Mitel hard drive only) for more storage capacity. All AX systems use Compact Flash cards only, and cannot be upgraded to hard drives.

System ID module

The system ID module contains a unique serial number which identifies the system for the purposes of installing options. The module can be moved to a new controller along with the internal compact flash or hard drive (which contains the matching software key) during hardware upgrades or maintenance activities.

In the MX controller, this is a small circuit card, and in the CX/CXi and AX controllers, it is an i-Button.

Clock module

Each ICP controller has a default clock source which will handle IP sets, IP trunks, and all analog lines and trunks, but digital trunks need a more tightly controlled clock. The MX controller comes with a Stratum 3 clock module installed, allowing it to serve either as an end node or an intermediate node in a digital trunk network. In the CX/CXi controller, the T1/E1 Combo module has a Stratum 4 clock on it, allowing the system to operate under normal conditions as an end node in a digital trunk network. If for any reason a tighter tolerance is required on the clock source, the Stratum 3 clock module can also be installed in the CX/CXi. The AX system has a Stratum 3 clock module embedded on the controller card.

Embedded analog card

Both the MX and CX/CXi controllers come with an Analog Main Board installed, and each can be optionally configured with an Analog Option Board. Installing these boards is functionally similar to installing an external Analog Services Unit.

For the MX controller:

- The Analog Main Board (MX) supports two ONS ports, six LS trunks, two DNIC ports, one MOH port (3mm stereo), and one paging port (RJ45).
- The Analog Option Board can be installed on top of this to add another two ONS ports and six LS trunks.
- The PFT function is associated with ONS1/LS1 and ONS2/LS2 pair on the main board.
- Connectivity for both boards is through a common Amphenol (RJ77) connector for the ONS, LS, and DNIC ports.

For the CX/CXi controller:

- The Analog Main Board provides 6 LS, 4 ONS, with 2 PFT ports, a MOH port (3mm stereo), a Paging port (RJ45), and 2 generic relays.
- The Analog Option Board provides an additional 6 LS, 4 ONS, and 2 PFT ports. The LS Trunk and ONS ports on the AOB have the same interface characteristics as the ports on the AMB.
- The PFT function is associated with ONS1/LS1 and ONS2/LS2 pair on each board.
- Connectivity for both boards is through independent RJ11 connectors for the ONS and LS ports.

Identifying versions for AMB/AOB

When adding or replacing these boards, they must always be compatible (i.e. the AOB V2 will only work with the AMB V2). It they are mismatched, there will most likely be problems with the loss plan for the LS trunks. See Table 4 for compatibility.

Table 4: AMB/AOB Compatibility

AMB Version	must use AOB Version:
1	1
2	2
3	2

On the Maintenance Terminal, use the access sequence SYSTEM, SHOW, DEVICE, ASU INFO. The marketing and engineering numbers of the analog main and option boards will be displayed under the CIM3 PROM heading. The part numbers you might see are:

- 50004403 - Analog Main Board (CX) version 1
- 50004870 - Analog Main Board (CX) version 2

- 56008157 - Analog Main Board (CX) version 3*
- 50004401 - Analog Option Board (CX) version 1
- 50004871 - Analog Option Board (CX) version 2
- 50003724 - Analog Main Board (MX)
- 50003725 - Analog Option Board (MX)

*AMB version 3 has an extra connector on the back of the board. Ignore this connector when connection AMB v3 to the controller.

DSP modules

Each unit contains a number of Digital Signal Processors (DSPs), provisioned in modules with two or four DSP devices each. Each DSP device may be used for either telecom, compression or echo cancellation applications. The function of each device is assigned by the RTC at system initialization time based on the device availability and the database requirements.

DSP devices for telecom applications

Telecom applications include tone generation and detection, and conferencing. A block of DSP resource is allocated for conferencing at startup, but tone generation and detection are allocated as required by traffic conditions, on a per-call basis.

Voice Mail ports use these same telecom functions, and also provide the ability to record and play PCM data (to/from the hard disk). Like the conference function, devices are allocated to Voice Mail at startup, depending on the number of devices available and the echo and/or compression programmed in the customer database.

DSP devices for compression applications

All E2T compression (G.729, used for IP networking and wireless phones) requires the use of DSP modules. Compression channels are considered bidirectional (each two-party conversation requires one compression channel). Each DSP device provides eight (8) bidirectional channels of compression, so that a quad DSP module can provide 32 compression channels. DSP devices are allocated to compression at initialization, before telecom applications are configured.

Echo cancellation

Each IP (Ethernet) to TDM session (E2T) is considered bidirectional, and requires one Echo Canceller channel (also bidirectional). The Echo Canceller function (EC) may be provided by DSP devices or by dedicated hardware devices. The MX systems have built-in 64-channel EC, and do not normally require any additional resources. A block of 12 DSP Echo Cancellers (one device) may be enabled for special applications, using a system option. The CX/CXi and AX systems use DSP resources for Echo Cancellation in the minimum (default) configuration, but add hardware resources in the T1/E1combo module for expansion.

Dual FIM modules

Dual FIM modules are used to connect to Peripheral bays and NSU cabinets in any combination. Each module can support two independent connections, of either Peripheral Cabinets or NSU cabinets. The types of FIM and the cabinets they support are shown in the following table.

Table 5: Dual FIM Applications

FIM type	Fiber run length (see Note 1)	Fiber optic cable type	Use
820 nm multi-mode	1km (0.62 miles)	62/125 or 50/125 um multi-mode	Peripheral bays NSU cabinets
1300 nm multi-mode	3km (1.9 miles)	62/125 or 50/125 um multi-mode	Peripheral bays
1300 nm single-mode	14km (8.7 miles) (see Note 2)	9/125 nm single-mode	Peripheral bays

Note:

1. The run length is the one-way length of fiber optic cable between nodes.
2. Frame synchronization errors occur if the loop length of fiber optic cable - from control node to peripheral cabinet or DSU node and back - is between 10.0 km and 10.6 km (6.2 miles and 6.6 miles). Nodes are typically connected by two-strand or “paired” fiber optic cable. For paired cable, a loop length of 10.0 km to 10.6 km equals a 5.0 km to 5.3 km cable run length.

Dual T1/E1 modules

Each module can support two independent connections to the PSTN over digital trunks, and each link can run a different protocol. Because of the significant processing overhead involved in running these modules, only a limited number can be installed in any given system, and installation of the embedded digital trunks may reduce or eliminate the capacity to run other applications on the controller.

Table 6: Dual T1/E1 Protocol Support

PRI (ISDN primary rate)	Supported since Release 3.0 Does not support min/max, NFAS, and D-channel backup
QSIG	Not supported on module.
T1/D4	Supported since Release 2.0
Note: The dual trunk modules are NOT supported on the CX/CXi controller.	

T1/E1 Combo modules

Each module can support one connections to the PSTN over digital trunks, and also contains the necessary DSP and echo cancellation resources for the number of trunk channels available.

Table 7: T1/E1 Combo Protocol Support

PRI (ISDN primary rate)	Supported since Release 3.0 Does not support min/max, NFAS, and D-channel backup
QSIG	Not supported on module.
T1/D4	Supported since Release 2.0
Note: The T1/E1 Combo trunk modules are ONLY supported on the CX/CXi and AX controller, not the MX.	

External TDM interfaces

The systems can support three different types of external TDM interfaces:

- Network Service Units (NSU) connect using the Dual FIM or CIM ports.
- Peripheral bays connect using the Dual FIM or a CIM port.
- For lower-density peripheral support, Analog Service Units can be connected by copper interface (CIM). These modules provide 24 ONS lines (standard ONS ASU) or a combination of ONS and LS trunks (ASU II).

Network Services Unit (NSU)

Network Services Units are used to provide digital trunk connectivity from the SX-200 ICP to the PSTN.

The NSU provides T1 connectivity and supports up to two T1 links per unit.

T1 interfaces support the following protocols: T1 Primary Rate ISDN (4ESS, 5ESS, DMS 100, DMS 250, NI-2, NI-3, NI-2-5ESS, NI-2-GTD5), and QSIG. The NSU also supports min/max, NFAS, and D-channel backup.

Note: Both interfaces on each NSU must run the same protocol.

The NSU connects to a SX-200 ICP Controller through a fiber cable or via the Copper Interface Module (CIM) connection on the front of the NSU using a Category 5 crossover cable.

Peripheral Cabinet

The SX-200 ICP is able to connect to up to seven SX-200 Peripheral Cabinets (Bays) depending on the number of FIMs and/or CIMs installed in the SX-200 ICP. One Bay Control Card (BCC2 or BCC3) is installed in slot 9 of each peripheral cabinet. The Bay Control Card provides control for all peripheral interface cards. The BCC2 connects to the SX-200 ICP controller through a FIM or CIM port on a carrier card in slot 12. The BCC3 can connect in the same manner, but it can also connect directly from a FIM or CIM mounted directly on it.

Each peripheral cabinet holds up to eight peripheral interface cards and provides up to 96 ONS or DNI ports.

The following peripheral interface cards are available:

- DID trunk card
- DNI line card
- LS/GS trunk card
- LS/CLASS trunk card
- ONS CLASS line card
- ONS line card
- OPS line card
- Universal card

Note: For a list of cards and devices that are supported or not supported, refer to the *Mitel SX-200 ICP General Information Guide*.

Analog Services Units (ASU, ASU II)

Analog phones and trunks are also supported on the SX-200 ICP with Analog Services Units, each of which has 24 analog lines (ONS). The ASU connects to one of the embedded CIM ports on the SX-200 MX controller using a category 5 crossover cable.

The ASU II is connected to the CX/CXi controller via Quad CIM module and supplies one or two cards of 16 ONS ports or 24 ONS ports each. An optional combo card supplies 12 ONS and 4 LS ports. Up to three ASU II units can be connected to the CX/CXi controller and up to six ASU II units can be connected to the MX controller.

Phones

The SX-200 ICP supports the following IP phones:

- 5540 IP Console
- 5304 IP Phone
- 5312 IP Phone
- 5324 IP Phone
- 5330 IP phone
- 5340 IP phone
- TeleMatrix 3000IP phone
- 52xx range (5201, 5207, 5212, 5215, 5220, 5224)
- 50xx range (5010, 5020)

Note: The AX controller only supports the following IP phones: 5304, 5312, 5324, 5330, 5340, and 5540 IP Phones.

The number of sets that can be connected to a system is determined by the nominal size of the system (analog and digital sets) and by the number of IP user and IP device licenses (IP sets).

- The number of IP user and IP device licenses determines the absolute maximum number of IP sets that can be installed.
- The system size (100, 200) is an indicator of the approximate number of IP sets that could be supported with no other applications installed.

Voice or telephony applications outside of call control use some CPU or DSP resource, and therefore, reduce the number of lines which can be supported. The quantity of each type of set, as well as both analog and digital trunks, can be set in the System Engineering Tool. The tool flags any performance or capacity problems based on the limits of the system size and configuration.

The voice or telephony applications generally add to the number of “sets” on the system because they emulate IP sets. Each pseudo IP set counts the same as a real set for purposes of system limits, so it is possible to reach the system limit without having that number of real sets installed, if there are a large number of applications. The quantity of real + emulated sets can never exceed the number of IP device licenses on the system. Applications also use other internal resources, such as DSP and E2T functions.

Go to http://edocs.mitel.com, the documentation pages of Mitel OnLine, for easy access to the applications documentation. You require a Mitel OnLine username and password to access this site.

Note: PDF versions of end user documents (such as telephone user guides) can be viewed and downloaded without a Mitel OnLine account.

All IP sets and applications use up a combination of IP sockets for MiNET, MiTAI and voice sockets, which have a finite limit. A detailed analysis of the socket usage on a system is included in the calculations done as part of the System Engineering Tool.

LIM Module

The Line Interface Module provides users of 5220, 5224 and 5324 IP Phones with the ability to make and receive calls on an analog line in either of the following modes:

- Line Interface Module (LIM) Mode: user can access the analog line at any time by pressing the programmed LIM key.
- Fail-over Mode: user can access the analog line when the IP connection has failed.

Users can place Emergency Calls to the Local Emergency Number using the analog line in either mode.

For information about LIM configuration refer to the LIM Installation Guide. For information about programming these IP Phones with a LIM, refer to the appropriate User Guide.

Phone Stands

Release 4.0 supports the Gigabit Ethernet phone stand and the Wireless LAN (WLAN) phone stand. These phone stands can be installed in place of the regular phone stand on 5200/5300 series IP phones.

Table 8 indicates which phones support the Gigabit Ethernet and Wireless LAN Stand.

Table 8: Phone Stand Support

Device	GigE Stand Support	WLAN Stand Support
5201	No	No
5207	No	No
5010	No	No
5020	No	No
5212	Yes	Yes
5215	No	No
5215 dual mode	Yes	Yes
5220	No	No
5220 dual mode	Yes	Yes
5224	Yes	Yes
5304	Yes	Yes
5312	Yes	Yes
5324	Yes	Yes
5330	Yes	Yes

Table 8: Phone Stand Support

Device	GigE Stand Support	WLAN Stand Support
5340	Yes	Yes
5540	No	No
Navigator	No	No
TeleMatrix 3000IP	No	No
5485 Paging Unit	No	No

Gigabit Ethernet Phone Stand

The Gigabit Ethernet Phone Stand allows a 5200/5300 series IP phone to be interfaced to a Gigabit Ethernet LAN. Details on the Gigabit Ethernet Phone Stand can be found in "*Gigabit Ethernet Stand Installation Guide*" in and "*Mitel Wireless LAN Stand Configuration and Engineering Guidelines"* on Mitel Online.

1000 Base-T or Gigabit Ethernet can be run on Category 5 or better cabling plant. It is recommended that the cabling plant be tested/certified for Gigabit Ethernet operation. This is particularly important in cases where Gigabit Ethernet equipment is being deployed onto an existing 100 Base-T Category 5 network.

Category 3 cabling plant cannot be used for Gigabit Ethernet.

IEEE 802.11 b/g Wireless LAN Phone Stand

The WLAN Phone Stand can operate as an IEEE 802.11b/g Wi-Fi client when used with 5200/5300 series IP phones. The stand connects to the IP phone via a wired 10/100 Base-connection. The stand provides a Wi-Fi LAN interface to a Wi-Fi LAN.

The WLAN Phone Stand can also operate as an IEEE 802.11b/g Wi-Fi access point by bridging from the Wi-Fi interface to a wired 10/100 Base-T interface.

Details on the WLAN Phone Stand can be found in "*Wireless LAN Stand Installation Guide*" and in "*Mitel Wireless LAN Stand Configuration and Engineering Guidelines"* on Mitel Online.

Power

Installation practices

Data signals on an Ethernet, or similar, connection are low power. It is important to correctly install the data equipment and interconnections in a controlled manner to minimize interference onto and from the equipment and also loss of these signals.

Follow the relevant safety and building installation codes for the location. See the *SX-200 ICP Technical Documentation* under Cabling Characteristics and Guidelines for recommended wiring practices and equipment grounding.

Controller power input

The controllers have flexible power input operating over a wide range to allow global connectivity. The units operate with standard supplies of 60/50 Hz and 110/230 VAC input, and are auto-sensing. NSU cabinets also have universal (auto-sensing) power inputs. SX-200 peripheral cabinets have bay power supplies which are unique to either 120 VAC/60 Hz or 230 VAC/50 Hz.

More details on platform power consumption and settings can be found in the *SX-200 ICP Technical Documentation*.

Mitel IP Phone Power

Mitel IP Phones are IEEE 802.3af power over Ethernet (PoE) compliant. Power can be provided to the phones either locally by an AC power adapter or remotely by a network device that supports power over ethernet (PoE). PoE is a method of providing power to the phones over the existing Ethernet wiring that the phones use for connecting to the LAN.

Controllers Supporting PoE

The SX-200 ICP CXi controller is a network device that is capable of providing IEEE 802.3af PoE to 16 phones. The SX-200 ICP CXi controller uses the LAN signal cable pairs (phantom) to deliver power to the phones.

Note: The SX-200-ICP MX, AX and CX controllers do not provide an integrated IEEE 802.3af PoE. For details on this capability, please refer to the *SX-200 ICP Technical Documentation*.

Local phone powering

Phones can be powered locally with the following methods (depending on the model):

- With an AC power adapter that converts mains voltage into the 24VDC required by the phone.

- With a special in-line Ethernet power adapter that provides a local power feed to the Mitel 5000 and 5200 series of IP phones. This adapter converts mains voltage into -48 VDC and supplies power to the phone over the Ethernet cable.

Remote phone powering

Phones can use one of three different communication standards to advertise their power requirements to a powered Ethernet switch. In all cases, both the phone and the powered Ethernet switch must comply with the same standard. The three standards are:

1. IEEE 802.3af Power Over Ethernet Standard (PoE)
2. IEEE 802.3ab Link layer Discovery Protocol (LLDP)
3. Cisco Discovery Protocol (CDP)

To determine which standard(s) a particular phone supports, refer to Table 9, “IP Phone Power Options,” on page 45.

Phones can be powered remotely with the following methods:

- If the phone supports the IEEE 802.3af power over Ethernet standard, remote power to the phone can be supplied by an IEEE 802.3af compliant Ethernet switch. Alternately, if the phone and the powered ethernet switch both support LLDP, then the phone can advertise it's power requirements to IEEE 802.3ab compliant switch.
- In the case where the phone supports the IEEE 802.3af power over ethernet standard, but the ethernet switch does not support the IEEE 802.3af power standard, a midspan IEEE 802.3af power hub can be used to remotely supply power to the phone over the ethernet cabling. The mid-span power hub resides between the ethernet switch (which in this case does not support IEEE 802.3af) and the phone.
- Certain older Cisco Ethernet switches are capable of providing power over Ethernet cables but are not fully IEEE 802.3af compliant. In this instance, a separate 3300 Power Dongle (Cisco-compliant) can be used to allow the phone to be powered over the Ethernet cable by the Cisco switch.
- Cisco Discovery Protocol (CDP) is a protocol that allows Cisco switches to learn information about devices on the LAN. CDP compliant LAN devices, such as IP phones, can advertise their power requirements to the L2 switch and the L2 switch can then deliver the required power to the connected device. This exchange of information via CDP is independent of the 802.3af protocol.

Important Note: The CXi only supports the IEEE 802.3.af communication standard. Because alternate PoE standards are not relevant to the CXi the installer must reference Table 12 when planning PoE installations that use the CXi to determine what the phones will advertise as their power requirements.

Recommended phone powering

Power over Ethernet from a central location is recommended whenever possible, resulting in the following benefits:

- Reliable and redundant power backup, especially for emergency 911 operation
- Lower installation cost (existing cabling can be used)
- International standard
- Remote reset and power-off capability.

Options for IP phone powering

The following Table indicates the powering options that are supported for the various phones.

Note: To ensure proper operation, avoid connecting the IP phone to both local and remote power sources simultaneously. An IP phone that is locally powered, either through an AC or an Ethernet power adapter, should have its remote power feed disabled.

Table 9: IP Phone Power Options

Phones	In-Line Ethernet AC Power Adapter (48 VDC LAN)	AC Power Adapter (24 VDC)	Power Dongle (Cisco-Compliant)	802.3af Mid-Span Power Hub	802.3af Spare Pair Power	802.3af Signal (Phantom) Pair Power	802.3ab (LLDP Signaling) Support
5010	Yes	Yes	Yes	Yes	Yes	Yes	No
5020	Yes	Yes	Yes	Yes	Yes	Yes	No
5201	Yes	No	Yes	Yes	Yes	Yes	No
5207	Yes	No	Yes	Yes	Yes	Yes	No
5212	Yes	No	Yes	Yes	Yes	Yes	Yes
5215	Yes	No	Yes	Yes	Yes	Yes	No
5215 (Dual Mode)	Yes	No	Yes	Yes	Yes	Yes	Yes
5220	Yes	Yes	Yes	Yes	Yes	Yes	No
5220 (Dual Mode)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
5224	Yes	Yes	Yes	Yes	Yes	Yes	Yes
5304	Yes	No	Yes	Yes	Yes	Yes	Yes
5312	Yes	No	Yes	Yes	Yes	Yes	Yes
5324	Yes	Yes	Yes	Yes	Yes	Yes	Yes
5330	Yes	Yes	Yes	Yes	Yes	Yes	Yes
5340	Yes	Yes	Yes	Yes	Yes	Yes	Yes
5485 IP Pager	No	Yes	No	No	No	No	No
TeleMatrix 3000IP	Yes	No	Yes	Yes	Yes	Yes	Yes
5540 IP Console	Yes	No	No	Yes	Yes	Yes	Yes

Note: The SX-200 ICP CXi controller supports IEEE 802.3af Single Pair (Phantom) power, but not Spare Pair power.

AC Power Adapters

For information on AC power adapters refer to the appropriate Mitel phone data sheet.

Note: The standard 24 VDC power adapter has a 10 ft. (3 m) output power cord. If a longer output power cord is required, you can use Part Number 57004243 (universal AC input and output, 24 VDC, 15 ft. (4.5 m) power cord.

In Line Ethernet AC Power Adapters

A special in-line Ethernet power adapter can provide local power feed to a wide range of Mitel IP phones, refer to Table 9 for details on which models of phones support this powering option. The power adapter plugs into a standard AC power outlet and has two RJ-45 connections, one connecting to the network, and the other connecting to the phone with power feed. Available units are

- 500002070 - 48 VDC Ethernet Power Adapter NA 120 V 50-60 Hz
- 500002080 - 48 VDC Ethernet Power Adapter UK 240 V 50 Hz
- 500002090 - 48 VDC Ethernet Power Adapter Europe 240 V 50 Hz

Note:

1. The 5201, 5207, and 5215 do not accept the AC power adapter, to provide local power to these phones the In-line Ethernet AC Power Adapters must be used.
2. For proper operation, ensure that the Ethernet power adapter and its associated IP phone are co-located

802.3af powering

Power over Ethernet technology allows devices such as IP Phones to receive power as well as data over an existing Ethernet LAN infrastructure. The standard for Power over Ethernet is IEEE 802.3af and Mitel 5xxx series IP Phones conform to this standard.

There are two methods of providing power in the standard:

- “Phantom” power across existing Ethernet wires (RJ-45 pins 1,2,3 and 6). This is the method typically used by 802.3af compliant Ethernet switches. The SX-200-ICP CXi controller uses the phantom (signal pair) method for delivering power.
- “Spare pair” power where power is supplied across RJ-45 pins 4,5,7 and 8. This is the method typically used by mid-span devices that sit between a non- 802.3af Ethernet switch and the end device.

Note: Mitel phones can be powered from equipment that uses phantom powering or spare pair powering.

Devices that provide power provide power by either method are called are called “Power Sourcing Equipment” (PSE) and devices that accept the power are “Powered Devices” (PD).

Mitel IP phones are, therefore, Powered Devices. Some Mitel phones also accept local powering options. For more information, see Table 9.

A Power over Ethernet port produces current limited, low voltage pulses which allow it to probe for a particular impedance at the end of the Ethernet cable. If this “signature” is detected (an IP Phone, for example), then the PSE assumes that power is required. If the “signature” is not detected (e.g. PC NIC), then the PSE does not apply power.

Once the “signature” or impedance has been detected, then the voltage is increased and current draw is monitored. The amount of current drawn allows the PSE to classify the device for Power over Ethernet requirements. Classification is an optional part of the standard and allows the end device (e.g. IP Phone) to “inform” the PSE of its power requirements. It is only performed on initial power up.

- Class 0 is the default. Devices that do not support the optional classification will default to this setting. The default is for 15.4 Watts of power.
- Class 1 informs the PSE that it requires less than 4 Watts.
- Class 2 informs the PSE that it requires 7 Watts.
- Class 3 requests 15.4 Watts (like Class 0) but will always draw at least 7 Watts.

Power required for Mitel IP Phones is fairly constant whether in use or sitting idle. Very loud ringer and handsfree settings can draw more power than normal. Also, additional devices connected to the IP Phone, such as a PKM and a Conference Unit, increase the power required by the IP phone. For details on optional device power requirements refer to “Power requirements for phone options” on page 56.

Table 12, “802.3af Power Class Advertisements,” on page 53 can be used to determine which Class a particular phone advertises.

Third party 802.3af powering

The following vendors offer IEEE 802.3af compliant network equipment that can supply power over ethernet wiring to the phones.

Caution: The information in this section is believed to be accurate but is not warranted by Mitel. Please refer to the respective vendor documentation to verify IEEE 802.3af compliancy.

HP (Hewlett-Packard)

- HP 2650-PWR/2626-PWR
- HP 5300 XL with expandable 10/100 PoE modules

Cisco

- Cisco 3560 series
- Newer versions of Cisco 4500 series

- Newer versions of Cisco 6500 series

Note: Some of the older versions of 4000 and 6000 series are not IEEE 802.3af-compliant (check before using). The older 3524XL-PWR and 3550-PWR are not fully compliant and have been replaced by the newer 3560 series. For switches that are not IEEE 802.3af-compliant, use the Mitel 3300 Power Dongle. (See “Mitel 3300 power dongle (Cisco compliant)” on page 48.)

Others

As the IEEE 802.3af standard becomes more widely adopted, additional vendors are offering IEEE 802.3af compliant products.

Power Dsine

Power Dsine provide a range of in-line power-hubs:

- 6024/6012/6006 (24 port, 12 port, and 6 port, respectively) all provide 802.3af-compliant power
- 8012/8006 (12 port and 6 port, respectively) provides to 802.3af-compliant high power.

The 8000 series of power hubs provides a higher level of power over the Ethernet. The phones do not require this level of power, but work if connected to one of these ports.

A white paper entitled, "Installing an IP Telephony Network using Power Over LAN" published by Power Dsine can be found on the Mitel Online Web site.

Mitel 3300 power dongle (Cisco compliant)

Certain older Cisco network switches are capable of providing power but are not fully IEEE 802.3af compliant. In this instance, a separate 3300 Power Dongle (Cisco-compliant) can be used to get powered operation. The 3300 Power Dongle (Cisco-compliant) may not be required when powering Mitel phones behind a Cisco Catalyst 4500/6500. For this to be the case, you must ensure you are using an 802.3af-compliant version of the 4500/6500 switch. A white paper entitled, "Installing an IP Telephony Network using Power Over LAN" published by PowerDsine can be found on the Mitel Online Web site.

Others

As the IEEE 802.3af standard becomes more widely adopted, additional vendors are offering IEEE 802.3af compliant products.

Planning a PoE installation

When planning a PoE installation the following should be taken into consideration:

Cable power loss

Some power loss will occur over the ethernet cable used to connect the phone to the L2 switch or the mid-span powered hub.

If you are using an IEEE 802.3af compliant L2 switch or mid-span power hub and the power required by the phone set does not exceed 8 W, the power loss in the cable will be approximately 10% of the power required by the phone.

The IEEE 802.3af standard specifies that the PSE must provide a minimum of 15.4 W and that the PD cannot draw more than 12.95 W maximum. The difference between these two figures is intended to allow for cable power losses over 100 m of Category-5 cable when a PSE is powering a PD that draws that maximum allowable power.

In other words this means that under worst case conditions the cable power loss will be 19% of the power required by the phone.

The CXi total power budget of 100 W takes power losses incurred over cables into account, so there is no need for the installer to manually de-rate the 100 W power budget.

The above guidelines are not applicable if you are using a PoE L2 switch that is not IEEE 802.3af compliant.

Power management features in IEEE 802.3af compliant switches

Some innovative vendors of IEEE 802.3af compliant switches, such as Hewlett Packard and Mitel, provide power management features that can help to manage a situation where a group of phones might require more total power than the L2 switch can provide. For example:

- Dynamic Power Distribution: If some phones do not require maximum power the switch will re-distribute the unused power to other phones that may require more power.
- Power Prioritization Per Port: This mechanism allows certain ports or ranges of ports to be deemed “critical”. Power to phones connected to critical ports will be guaranteed, phones connected to ports that are not deemed critical may not receive power if the power capacity of the L2 switch has been exceeded.

For details on specific L2 Switch capability and how to configure port power prioritization refer to the L2 switch documentation.

Note: The SX-200-ICP MX, AX and CX controllers do not provide an integrated IEEE 802.3af PoE. For details on this capability, please refer to the *SX-200 ICP Technical Documentation*.

SX-200 ICP CXi Controller PoE guidelines

The SX-200 ICP CXi Controller supports advanced power management features. For details regarding status screens and how to use the power management features, refer to the *SX-200 ICP Technical Documentation*.

The CXi includes a 16-port managed Layer 2 Ethernet switch. The 16 Ethernet ports comply with the 802.3af Power over Ethernet (PoE) specification, which enables them to deliver power to IP phones and other Ethernet devices over Category 3 or 5 cabling.

The CXi controller’s Layer 2 switch can provide 100 Watts of power to 802.3af-compatible devices according to the following general rules:

- Depending on the phone and option power requirements, up to 16 IP Phones can be supported.
- Up to four PKMs (PKM12 or PKM48) are supported on Dual Mode IP Phones. Only one PKM can be attached to a set. Multiple PKMs on a set require an AC adapter.
- Conference units require an AC adapter.
- Class 1, 2, and 3 devices receive 4, 7, and 13 Watts, respectively. Unclassified (Class 0) devices are budgeted 7.5 Watts by the PoE subsystem, but can receive up to 13 Watts depending on need.
- Port 1 has the highest priority, port 16 the lowest. If the power budget is exceeded, power will be turned off to the ports, starting with port 16 and ending with port 1, until less than 100 Watts is being consumed.
- If the CXi runs out of power budget at port n, then port n will not receive power, and neither will any sets on ports numbered higher than port n.
- A set that is powered with an AC adaptor should have PoE on that port disabled in the CDE, or the set should be attached to one of the highest numbered ports on the CXi. If this guideline is not observed in the event that the AC adaptor loses power, that set may cause a set connected to a higher numbered port to lose power.

Phone power consumption

This section provides tables with information on phone set power requirements, choose the table that is relevant to your particular installation.

Local Power

Table 10 lists the actual power required by the various phone sets. The values in this table can be used to determine:

- what size of UPS would be required to maintain power to the phones in the event of a mains power outage
- if an L2 switch that uses a proprietary PoE (non-802.3af compliant) mechanism has sufficient power capabilities to power the desired combination of phones.

Note: The phone power requirements shown in Table 11 do not include the 3300 Power Dongle power requirements. For example, a 5220 (Dual Mode) phone requires 4.7 watts of power and a 3300 Power Dongle requires 1.4 watts of power. If the 5220 Dual Mode phone is being used in conjunction with a 3300 Power Dongle the power requirement is 4.7 watts + 1.4 watts for a total power requirement of 6.1 watts.

Note: The power values used in Table 11 are based on "maximum worst case" values for the phones. These values might differ from those shown on a phone data sheet since the phone data sheets use "typical worst case" values for phone power consumption.

Table 10: Actual Phone Power Consumption

Device	Power consumption in watts (W)
5201	2.0
5207	3.0
5010	5.0
5020	5.0
5212	4.7
5215	4.7
5215 dual mode	4.7
5220	4.7
5220 dual mode	4.7
5224	4.7
5304	3.45
5312	3.87
5324	3.87
5330	3.9
5340	4.8
5540 IP Console	7.27
TeleMatrix 3000IP	4.7
5310 Conference Unit	5.0
5412 PKM	1.3
5448 PKM	1.7
5485 Paging Unit	5.0
MITEL 3300 power dongle	1.4

Remote Power

As mentioned earlier in this document, there are three communication standards that phones can use to advertise their power requirements to an ethernet switch that supports a PoE mechanism. In all cases both the phone and the powered ethernet switch must comply with the same standard. The three standards are:

- Cisco Discovery Protocol (CDP)
- IEEE 802.3af Power Over Ethernet Standard (PoE)
- IEEE 802.3ab Link layer Discovery Protocol (LLDP).

Note: The CXi only supports the IEEE 802.3af PoE standard.

CDP Power Advertisements

Table 11 can be used to determine which CDP power advertisement a phone will use.

Note: Depending on the particular PoE protocol used, the phone may advertise a power requirement that is different from the actual phone power consumption shown in Table 11. Any differences between advertised values and actual values is intentional to ensure correct interworking with the PoE protocol.

When using PoE to provide power to the phones, consult the data sheet for the mid-span hub or the powered ethernet switch to determine the maximum power supply capabilities of the powered Ethernet switch or the mid-span hub.

Table 11: CDP Power Advertisements

Device	CDP Power Advertisements (see Note)	Power Dongle Included
5201	4.5 W	Yes
5207	4.5 W	Yes
5010	6.3 W	Yes
5020	6.3 W	Yes
5020 + 5310 Conference Unit (Conference unit is powered with AC adapter 24 VDC)	6.3 W	Yes
5020+ PKM(s) (PKMs are powered with AC adapter 24 VDC)	6.3 W	Yes
5212	6.3 W	Yes
5215	6.3 W	Yes
5215 dual mode	6.4 W	Yes
5220	6.3 W	Yes
5220 + 5310 Conference Unit (Conference unit is powered with AC adapter 24 VDC)	6.3 W	Yes
5220+ PKM(s) (PKMs are powered with AC adapter 24 VDC)	6.3 W	Yes
5220 dual mode	6.4 W	Yes
5224	6.3 W	Yes
5304	5.0 W	Yes
5312	6.1 W	Yes
5324	6.1 W	Yes
5324 IP Phone + 5310 Conference Unit	6.1 W	Yes
5324 + PKMs	6.1W	Yes
5330 with backlight	6.1 W	Yes
5540 IP Console	6.1 W	No

Note: These advertised values assume that a 3300 Power Dongle is used with the phones, and the power requirements shown in the table include the power required by both the phone and the 3300 Power Dongle.

IEEE 802.3af Power Over Ethernet Standard (PoE) Advertisements

Table 12 can be used to determine which 802.3af power class advertisement a phone will use.

Table 12: 802.3af Power Class Advertisements

Device	Class Advertised
5201	0
5207	0
5010	0
5020	0
5020 + 5310 Conference Unit (Conference unit is powered with AC adapter 24 VDC)	0
5020+ PKM(s) (PKMs are powered with AC adapter 24 VDC)	0
5212	2
5215	0
5215 dual mode	2
5220	0
5220 + 5310 Conference Unit (Conference unit is powered with AC adapter 24 VDC)	0
5220+ PKM(s) (PKMs are powered with AC adapter 24 VDC)	0
5220 dual mode	2
5220 dual mode + 5412 PKM	3
5220 dual mode + 5448 PKM	3
5220 dual mode + 5412 PKM + 5448 PKM	3
5220 dual mode + 5448 PKM + 5448 PKM	3
5220 dual mode + 5310 Conference Unit + Saucer	3
5220 dual mode + LIM	2
5224	2
5304	2
5312	2
5324	2
5324 IP Phone + 5310 Conference Unit (Conference unit is powered with AC adapter 24 VDC)	3
5324 IP Phone + PKM(s) (PKMs are powered with AC adapter 24 VDC)	3
5324 IP Phone (Dual Mode) + 5412 PKM	3
5324 IP Phone (Dual Mode) + 5448 PKM	3
5324 IP Phone (Dual Mode) + 5412 PKM + 5448 PKM	3
5324 IP Phone (Dual Mode) + 5448 PKM + 5448 PKM	3
5324 IP Phone (Dual Mode) + 5310 Conference Unit + Saucer	3

Table 12: 802.3af Power Class Advertisements

Device	Class Advertised
5330 with back light	2
5330	2
5340	2
5540 IP Console	3
TeleMatrix 3000IP	2

Some Mitel IP Phones do not support the optional classification feature, and the PSE connection defaults to Class 0 (15.4 Watts for the IP Phones, which is more than they require). Some Ethernet switches can run into problems as they cannot supply 15.4 Watts to each port, so the Ethernet switch specifications should be considered prior to deploying phones.

Note: It should be noted that the IEEE 802.3af Classes for advertising power requirements are very granular, for instance Class 1 covers a range of 4 watts. Class ranges are indicated below.

- Class 0 is the default Class. Devices that do not support the optional classification will default to this setting.
- Class 0 requests the PSE to provide 15.4 Watts of power.
- Class 1 requests the PSE to provide from 0 to 4 Watts.
- Class 2 requests the PSE to provide from 4 to 7 Watts.
- Class 3 requests the PSE to provide from 7 to 15.4 Watts (like Class 0), however, the PD willalways draw at least 7 Watts or more.

LLDP Power Advertisements

Table 13 can be used to determine which LLDP power advertisement a phone will use.

Table 13: LLDP Power Advertisements

Device	Power Value Advertised	Power Consumption (Watts)
5201	Not Supported	
5207	Not Supported	
5010	Not Supported	
5020	Not Supported	
5212	47	4.7 W
5215	Not Supported	
5215 dual mode	47	4.7 W
5220	Not Supported	
5220 + 5310 Conference Unit (Conference unit is powered with AC adapter 24 VDC)	Not Supported	

Table 13: LLDP Power Advertisements

Device	Power Value Advertised	Power Consumption (Watts)
5220+ PKM(s) (PKMs are powered with AC adapter 24 VDC)	Not Supported	
5220	47	4.7 W
5220 + 5310 Conference Unit (Conference unit is powered with AC adapter 24 VDC)	Not Supported	
5220+ PKM(s) (PKMs are powered with AC adapter 24 VDC)	Not Supported	
5220 dual mode	47	4.7 W
5220 dual mode + 5412 PKM	64	6.4 W
5220 dual mode + 5448 PKM	64	6.4 W
5220 dual mode + 5412 PKM + 5448 PKM	81	8.1 W
5220 dual mode + 5448 PKM + 5448 PKM	81	8.1 W
5220 dual mode + 5310 Conference Unit + Saucer	47	4.7 W
5220 dual mode + LIM	51	5.1 W
5224	47	4.7 W
5304 IP Phone	37	3.7
5312 IP Phone	47	4.7
5324 IP Phone	47	4.7
5324 IP Phone + 5412 PKM	64	6.4
5324 IP Phone + 5448 PKM	64	6.4
5324 IP Phone + 5412 PKM + 5448 PKM	81	8.1
5324 IP Phone + 5448 PKM + 5448 PKM	81	8.1
5324 IP Phone + Gigabit Ethernet Stand	100	10.0
5324 + Conference Unit module + saucer	97	9.7
5330	59	5.9 W
5340	60	6.0 W
5540 IP Console	73	7.3 W
TeleMatrix 3000IP	47	4.7 W
Gigabit Ethernet Stand (see Note 2)	53 + Phone	5.3 + Phone
Note 1: If a phone does not support LLDP advertisements but does support 802.3af advertisements, then 802.3af will be used. **Note 2**: The Gigabit Ethernet Stand does not send LLDP power advertisements. However, the phone that is used with the stand will detect the presence of the stand and transmit an LLDP power advertisement that includes both the phone power and the stand power.		

Power requirements for phone options

The 5220 and the 5220 Dual Mode IP phones support optional assessories which are powered in different ways depending on the option and the phone:

- 5220 phone options are powered from a 24 VDC power unit only.
- 5220 dual mode phone options are powered from either a 24 VDC power unit or through the Ethernet.

Caution:The 5310 IP Conference Unit can only be powered with an AC adapter that provides a 24 VDC output. To prevent damage to these units do not try to use PoE or the In-Line Ethernet AC Power Adapter to power them.

Table 14: Power Requirements for IP Phone Options

Phone	Conference unit	PKM12	PKM48	PKM48 + PKM48
5220	4.6 W powered from 24 VDC unit	1.5 W powered from 24 VDC unit	2.0 W powered from 24 VDC unit	4.0 W powered from 24 VDC unit
5220 dual mode	5.5 W powered from 24 VDC unit	1.3 W powered from 24 VDC unit or Ethernet	1.7 W powered from 24 VDC unit or Ethernet	3.4 W powered from 24 VDC unit or Ethernet

Note: To determine if your phone is a 5220 IP Phone or 5220 Dual Mode IP Phone, check the label on the back of the set. 5220 Dual Mode sets are marked either “5220 Dual Port” or “5220 Dual Mode”.

Uninterruptible power supply (UPS)

Use uninterruptible power supplies when phones, the associated controller, and the LAN infrastructure need to continue to operate during a power failure. UPSs can range from simple local battery units to larger central installations that include backup generators. Consider the following factors to determine the type of unit to use:

- The power to be drawn by attached units
- The power output of the UPS, and its efficiency with battery capability
- The time the UPS must supply power
- The size of the unit

Worked example

Consider a small installation with a LAN switch and some powered phones. The LAN switch draws 100W and 16 attached phones draw 8W each. The UPS has a 12V battery of 55AH and runs at 70% efficiency. How long can this combination be powered?

- The output power available is 462 VAH (volt-amperes hour) (55 x 12 x 70%).

- The consumption is 228 VA (100 W + 16 x 8 W).
- The time available is 2 hours or 462 VAH / 228 VA.

Note: Volt-Amperes (VA) is equivalent to Watts (W) if the Power Factor Correction (PFC) of the power supply in question has a PFC value of close to 1. Most data switches on the market today will have a PFC value of close to 1.

Emergency service

Emergency service (911) is available from all phone devices according to class of service and restriction settings. The default is to enable this access.

Enhanced 911 (E911) operation is not supported.

A location database is available to keep record of the location of a phone. However, when a phone location is changed, it is necessary to keep the system administrator informed, so that records can be updated to direct emergency services.

Software

The SX-200 ICP supports a number of applications. This includes applications that are embedded in the product (such as voice mail) through to providing DSP resource to allow connections to external devices (for example, a remote central voice mail in another unit). Other interfaces include MiTAI.

Refer to the application's documentation for setup information.

Voice mail

The SX-200 ICP includes an integrated, fully featured voice mail system. Up to 24 ports are available for voice mail calls with support for a maximum of 750 mailboxes and 450 hours of storage time, depending on the hardware configuration of the system.

Table 15: Capacities

Voice mail ports	4 (expandable to 16 on the CX/CXi , 20 on the AX, and 24 on the MX)
Mailboxes	20 (expandable to 748)
Hours of voice storage	4 hours minimum (expandable in CX and MX systems with internal Compact Flash)
Concurrent voice mail or auto attendant sessions	24
Message storage per mailbox	100 maximum messages (programmable)
Message retention	From one day to indefinitely for saved messages; indefinitely for unread messages. (Programmable on a per mailbox basis).
Prompt languages	English, Canadian French, Latin American Spanish with support for bilingual prompting

Performance

System performance index

In order to calculate the performance limits of a system, different weighting values are assigned to various types of calls. Typically an ONS-to-ONS call is considered to have a loading factor of 1.0, and an IP phone-to-IP phone, a loading factor of 3.2. Other call types (ONS to PSTN trunk, IP phone to IP trunk, etc.) are assigned different values based on actual performance tests. Based on the expected calls per hour (CPH) of all of the user ports on the system, a system performance index (PI) can be calculated which indicates the processor loading at those traffic rates. The system PI is used as an indication of how much traffic the SX-200 ICP can handle at any one time.

Check the actual performance with the System Engineering Tool, available through Customer Engineering Services.

In SX-200 ICP systems (AX, CX and MX), the single processor must handle multiple tasks, so the available PI is reduced. This additional load is taken into account automatically in the System Engineering Tool.

In addition to traffic, many other factors affect system PI. For example, a large number of voice mail ports can significantly increase the system PI because streaming data to the hard disk is a CPU-intensive operation. Similarly, call monitors (features, not voice) used for ACD, and several external applications, along with SMDR logging, can add processor load. These are all taken into account automatically in the System Engineering Tool.

Table 16: Factors Affecting Performance Index

System Feature	PI Impact
SMDR reporting (see Note 1)	10%
MiTAI monitoring (see Note 2)	10%
Voice Mail (see Note 3)	30%
Compression (see Note 3)	30%

Note:

1. SMDR reporting will increase the PI of all traffic by this amount.
2. MiTAI monitoring will increase the unit PI of each monitored set by this amount.
3. Maximum voice mail or compression will each use this portion of the system PI limit.

IP Networking and Trunks

The terms “IP networking” and “IP trunks” have become synonymous. However, “IP networking” covers the whole picture, while “IP trunks” refers to the individual call connections.

Note: IP trunking is supported only through the LAN interface on the 200 ICP controller. It is not supported on the WAN interface of the CX/CXi controller.

IP networking node restrictions

An SX-200 ICP is considered a node for IP networking. A node is defined through the numbering plan and must be unique among networked devices. A single controller has the following limitations:

- No more than 200 nodes can be connected to a single node (limited by the available ARS routes).
- No more than 30 (MX/AX) or 16 (CX/CXi) IP trunk calls can be made from one controller at any one time. Clustering

Clustering and networking between units introduces additional burdens to the system that may reduce its capability, depending upon the configuration and use of the system. The configurations usually considered are:

- **Standalone:** An individual unit that is not connected by any form of networking. For example, an SME business.
- **Networked:** A number of locations that are interconnected, but the level of interoffice traffic is not particularly high. For example, a business with multiple corporate offices in different cities.
- **Clustered (with PSTN trunk sharing):** A number of systems that interoperate to create a bigger system. For example, a larger office where there are a number of trunk connections to the PSTN, but where the PSTN can present a call to any of the trunks. Therefore, an incoming call could arrive on any system, and likewise on outgoing call could also go through any system.
- **Clustered (without PSTN trunk sharing):** A business that is connected using a MAN (perhaps dispersed across a city) where each office is connected to the PSTN through local trunks, but where internal traffic can flow freely from office to office. Examples are a campus environment, a large department chain, or a government establishment.

For the SX-200 ICP, both Standalone and Networked (as defined here) are valid and commonly used configurations. Because of the limited number of IP trunks available, the more tightly coupled clustered environment, whether with or without PSTN trunk sharing, is not a practical use of the system.

Call handling, routing, and bandwidth

There are two parts to a call: signaling and voice streaming.

Using TDM, typically over the PSTN, the two parts of the call follow the same path and are closely linked in their routing. In a tandem connection from site A to site C, via tandem site B, voice is handled by the TDM switch at site B. In effect, the tandem TDM switch reroutes the voice part of the call and establishes a second signaling path. It is involved in both voice and signaling connections.

Using IP, voice can stream directly between endpoints (but not always), but signaling still travels via the tandem unit. Thus, in a tandem connection, voice streams directly from A to C, while signaling goes from A to B and then B to C.

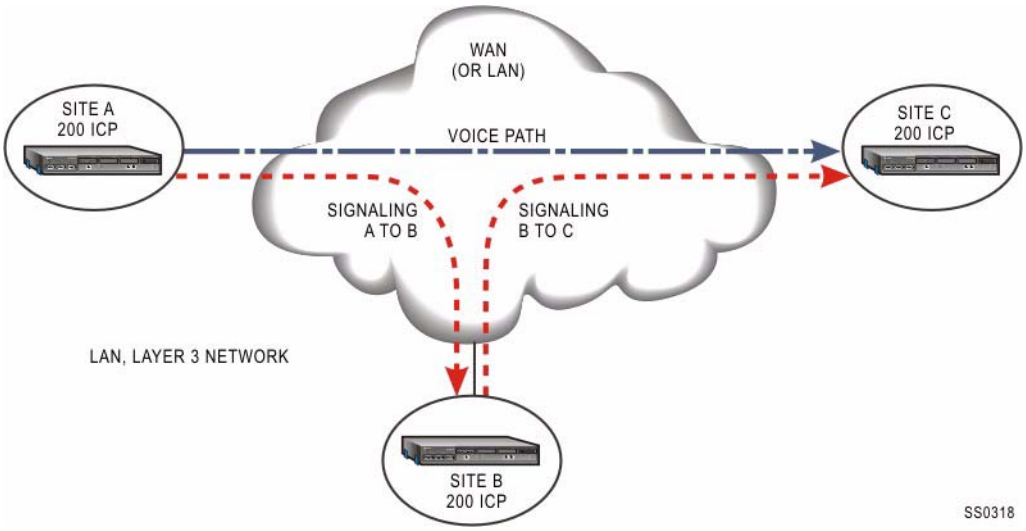


Figure 9: Signaling and voice path example 1

In the tandem case, a virtual IP trunk is used from A to B and another virtual IP trunk is used from B to C. These trunks are counted against the routing limit.

In certain networks, especially external WANs that use VPNs, the most direct path from A to C may actually be through the IP router at site B. However, the SX-200 ICP at this site only handles the signaling and not the voice traffic.

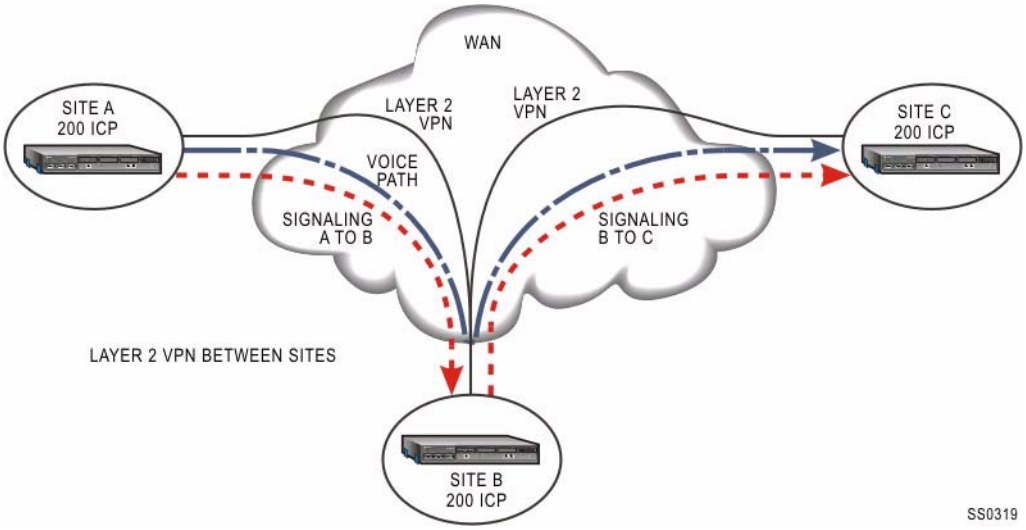


Figure 10: Signaling and voice path example 2

Consider the different routing in different parts of the network when bandwidth calculations are involved.

Number planning and restrictions

Further details can be found within the Clustering documentation.

The length of number plans for clustering should be consistent among all units to prevent confusion in routing. Plan the location of systems and number assignments before installation.

Clustering for larger systems is the recommended configuration.

OPS Manager is recommended to plan and control operation of the different units.

Note: Certain features such as Group and Trunk Hunting are limited to a single controller and do not span the network. Therefore, common groups or departments should be focused onto a single unit.

IP trunk routes and compression

The IP trunk route is a virtual path from one SX-200 ICP to another Mitel PBX (such as, SX-200 ICP or 3300 ICP, for example). One of the parameters assigned to this route is compression. Assuming that the end devices are capable of compression, compression is enabled on the route, and there are sufficient available channels, or sessions, then the end devices stream using compression. Otherwise, the call is blocked, rerouted, or streamed with G.711 (uncompressed).

See “Network Configuration” on page 85 for more details on bandwidth requirements for different LAN and WAN links with and without compression. See also “Compression” on page 75.

Compression and licenses

Some points regarding connections in IP and compression licenses are noted below:

- An IP phone-to-IP phone connection does not use a compression license in the SX-200 ICP when the call is connected by an IP trunk over a WAN.
- An IP phone (node A) to TDM phone (node B) call uses an E2T compression license on node B only when the call is connected by an IP trunk over a WAN.
- A TDM phone (node A) to TDM phone (node B) call uses an E2T compression license on both nodes A and B when the call is connected by an IP trunk over a WAN.
- Conference calls use one compression license for each IP connection in the conference that would normally require a compression license when connected to a TDM device.
- Compression can be used with calls to voice mail, consuming a compression license for calls that would normally use compression when connected to a TDM device.
- Music-on-Hold (MOH) that is passed to a device that normally uses compression consumes a compression license. If MOH is passed to multiple devices, then up to that number of licenses is required.

IP networking and compression licenses

Licenses are needed to obtain both compression sessions and IP networking.

Voice quality is affected by compression and available bandwidth. When to use compression licenses is determined by setting different compression zones and assigning different IP phones to the different zones. The IP networking license determines whether calls can be routed between units over its IP infrastructure, and how many of the sessions are allowed over a particular connection between different controllers. Compression and IP networking work together, but can be used independently.

From a voice quality view, if the number of calls requiring compression exceeds the number of licenses, a call does not fail, but it is not compressed. It will use more bandwidth than expected. Bandwidth calculations are highlighted in the section “Traffic” on page 140. If IP trunks are used, the number of concurrent sessions can also be defined, see the section “IP networking limit working” on page 143.

IP networking and product release compatibility

Product improvement is part of an ongoing and important process which includes the need for new product releases. While every effort is made during the development process to ensure that the new release is compatible with earlier releases, there may be instances where this cannot be fully achieved. This may become apparent due, but not limited to, differences in

expected system operation and feature availability. To minimize such instances, it is recommended that networked units operate with the same release numbers or at least minimal levels between releases. Please contact Mitel Technical Support to determine if such issues are likely when upgrading.

IP networking over Internet

The IP Networking over Internet feature allows ICPs at different sites to be networked via a VPN connection. Being a VPN, this connection is secure, and so will allow the remote units to run with the private address scheme already deployed throughout the business.

The VPN can be used over both a managed network as well as an unmanaged network, such as the Internet. Any data that travels over this VPN is subject to any network impairments that may occur on this external connection. This includes packet loss and jitter. The Internet is an unmanaged network, providing only best effort connection and cannot guarantee Quality of Service.

The data over the VPN is subject to network jitter and packet loss. This will be passed on to the end device. Some of the legacy phones may have difficulty handling high levels of network impairment, and voice quality issues may arise. Newer end devices and the gateways/ICP have the capability to handle this level of impairment.

When using this VPNs over best effort networks, such as the Internet, be sure to only deploy end devices that are capable of handling the potential jitter and packet loss.

Devices that are capable of handling Internet levels of impairment include:

Table 17: IP Networking over Internet - Supported Phones

Phones	IP Networking over Internet
5020	Manual Configuration - Yes
5212	Yes
5215 (Dual Mode)	Yes
5220	Manual Configuration - Yes
5220 (Dual Mode)	Yes
5224	Yes
5304	Yes
5312	Yes
5324	Yes
5485 IP Pager	Yes
YA Softphone	Yes
5330	Yes
5340	Yes
5540	Yes
Navigator	Yes

Table 18: IP Networking over Internet - Supported Gateways

Phones	IP Networking over Internet
Gateway 3300	Yes
Gateway 200	Yes

In order to use a wider range of IP Phones and applications over IP Networking it is recommended that the VPN be passed over a managed network with appropriate Service Level Agreements (SLA). This can be either over the in-built VPN or a separate router and external VPN.

Losses in a PSTN Connection

The following sections highlight the different losses that are encountered in a PSTN connection from one end user to another end user. These are shown for both Analog and digital connections. The effect of adding a PBX into the connection is also shown.

Specifically the losses that might be expected when the PBX is used to make trunk to trunk connections is shown for both Analog and digital connections.

Nominal overall loss value

In normal conversation two people stand apart from each other. As one person talks the sound energy disperses, and the overall sound level at the listener is reduced. The ear is also tuned to particular frequencies, boosting some, reducing others.

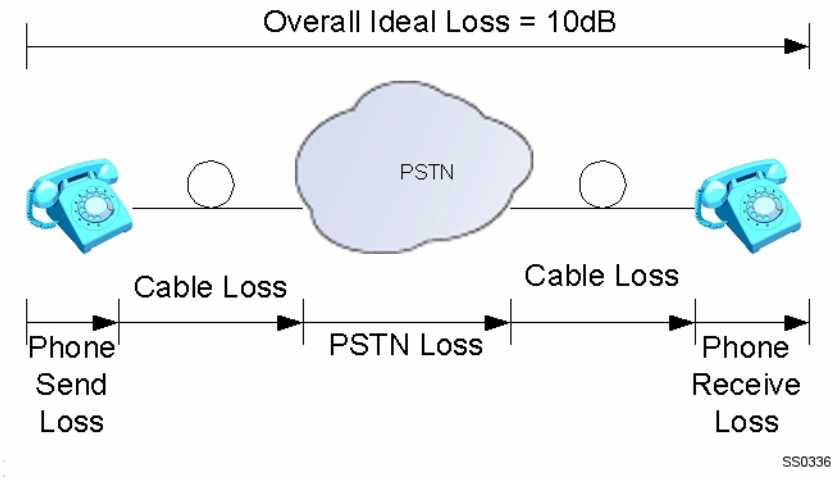
The telephone handset consists of a mouthpiece, or microphone, and earpiece, or loudspeaker. The microphone is held close to the mouth and picks up a lot of energy that hasn't yet dispersed. The earpiece is held tightly to the ear, so overall there is little signal loss through the air.

To make the telephone sound more like a normal conversation, loss is added into the signal path. Over a number of years, the ideal loss has been found to be around 10dB.

This signal loss can come from a number of sources, the primary ones being the end devices, but also the trunk, or line, cable plant and the Central Office/PSTN connection.

Normal subscriber-to-subscriber connection via PSTN

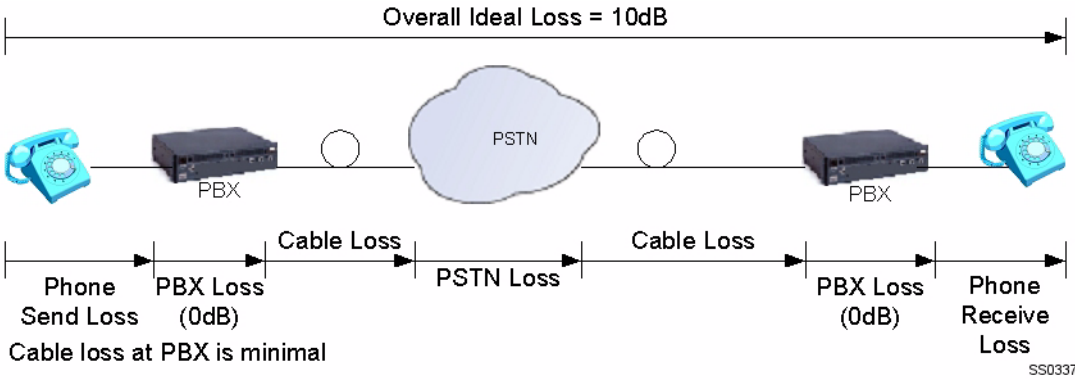
Typically, the connection loss occurs in the phone. Some loss occurs in the central office, or PSTN connection. Additional loss occurs in the cables. Additional losses may be added at the Central Office when cable distance to the subscriber is short.



The PSTN service provider will ensure that most connections will provide around 10dB of loss. Some longer lines, especially rural connections, may introduce additional loss. This results in a slightly quieter than normal connection. Some longer lines may use in line repeaters in order to boost the signals. Some lines may have tuning components added (a.k.a. loaded lines) to adjust the cable losses at different frequencies, often making the line sound 'tinny', or 'toppy'. Today, such lines are generally being phased out, as speech quality is not ideal. Reliable service for MODEM, FAX or DSL connectivity may not be guaranteed, or will show slow operation, e.g. 1200baud but not 28.8kbits/s. Generally these lines are intended for end subscribers rather than for business lines due to the reduced voice quality and limited services that can be provided. Business lines often cost a little more, but are also better maintained and controlled in terms of performance.

PBX-to-PBX connection – analog trunks

A PBX is simply a method of routing or concentrating calls from a number of users, or subscribers, to a limited number of CO connected lines, called trunks. The PBX generally introduces no loss in the connection. (This is not entirely true, as PBX deal with a wide range of devices, but essentially should look like a standard subscriber to the PSTN).



Modern PBX equipment often has the capability to deal with different trunk line lengths and losses. In North America, for example, the loss settings are described in EIA/TIA-912A. This describes operation over short and long trunk lines. These allow cable losses of up to 6dB to be used. Beyond this, the signal level will reduce in much the same way as a standard subscriber, without the PBX.

Typically, loaded lines, and trunk lines showing loss greater than 8dB, from the PSTN, will show voice quality and level reductions. These are not optimal for business operation and should be avoided.

PBX-to-PBX connection – digital trunks

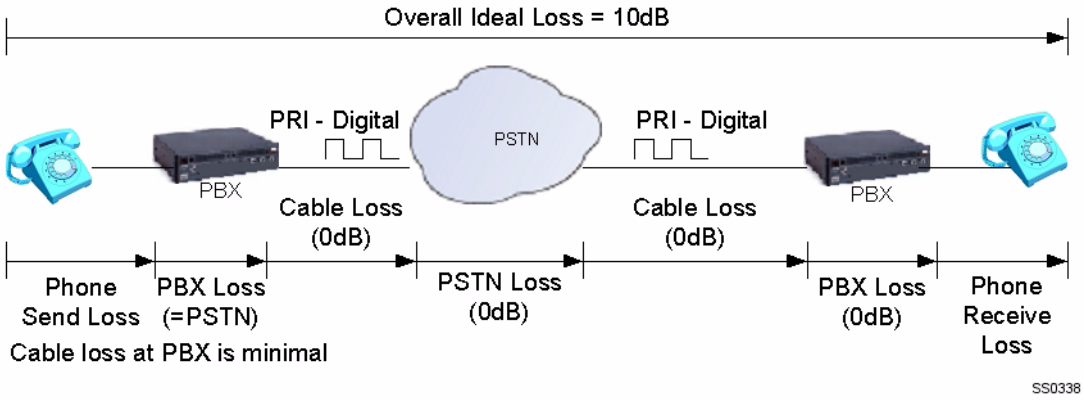
For a number of years the PSTN consisted of Analog and electromechanical switching. Although great in its day, this has largely been replaced with faster and smaller digital switching equipment. World-wide standards through ITU-T (formerly CCITT) have also been agreed so

that different countries can connect at the same speech levels. Digital connections allow both voice and data to co-exist on a common connection. The digital links are also loss-less in terms of voice. The only loss then is at the end connection to the user.

In effect: the PSTN core of the connection is now loss-less, only the edges are subject to loss.

In the case of a normal home subscriber, the loss is introduced at the entry and exit to the PSTN, or Central Office, connection. This is the same as the subscriber to subscriber example, shown above. The subscriber is still subject to the connecting cable loss.

For a business, connected via Analog trunk lines, further loss introduced by the trunk cable, as the Analog trunk still connects to the edge of the PSTN.



Today, modern PBX equipment is capable of connecting to the PSTN core via digital and ISDN connections. These can be PRI link (Primary Rate Interface – 23 or 24 channels depending upon connection protocol for T1 and 30 channels for E1), or in some instances BRI (Basic Rate Interface - 2 channels) These digital connections are loss-less, for voice, to the PSTN core. Because of the direct connection to the PSTN, the PBX is now required to add some of the connection loss that the PSTN previously provided with legacy devices. The losses are only in the end devices, or end points, not in the interconnection. The trunk cable loss, to the PSTN, is no longer an issue for the voice signals. This is almost the ideal connection.

Digital phones (e.g. ISDN) are now superseding Analog phones. The connection losses are fixed directly in the phone, and so the PBX is now simply a digital switching point. Connection to the PBX is over a digitally encoded link, and so that now even local cable loss to the PBX does not affect the voice level. This is the ideal voice connection.

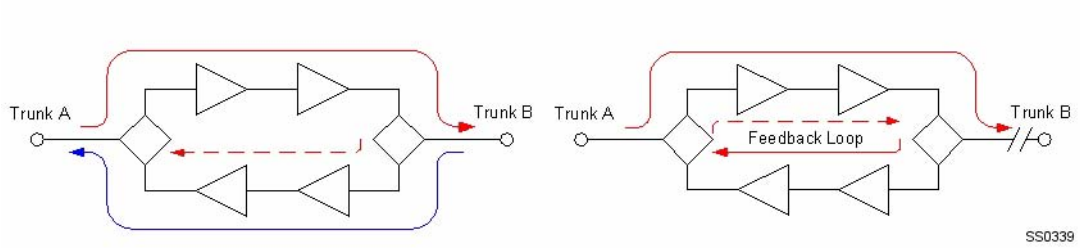
A new type of phone is appearing on the market, the IP Phone. In terms of voice performance this is still a digital phone. It can connect directly to other IP Phones over the LAN/WAN IP infrastructure or to other devices through a gateway (typically IP to TDM). The gateway can be combined within the PBX, or as an external interface. In terms of signal levels, this is no different to the ISDN based phone using BRI/PRI, simply a different digital connection method. This is another advantage of digital connectivity, it is not confined to one mode of transport from one point to another, yet the voice remains intact and at the correct level.

PBX trunk-to-trunk connection – analog trunks

Although many countries disallow trunk to trunk connections, this feature is becoming increasingly prevalent. The main issue, for the PSTN provider, is revenue bypass or loss. In providing a trunk to trunk connection, it has to be remembered that the PBX is located at the edge of the PSTN and not at the core. It is therefore subject to connection and cable losses, both incoming and outgoing. This is the primary reason why a number of administrations, and private companies, operate fixed Analog tie trunks between multiple exchanges of the same business. The tie trunks allow the private network switches to be connected at the core switching levels, without additional PSTN cable loss.

When two trunks are connected together, via an intermediary PBX, this is no different from connecting two normal calls together, each with their own losses. When connected together, the losses combine and the resulting connection can be quieter than expected, being similar to two calls connected in series.

In theory it should be possible to add gain at the PBX connecting the trunk lines together. The PBX is then simply acting as a repeater. The gain that can be placed in a repeater is subject to how well the external line impedance matches that of the amplifiers. During a conversation, the line impedance can be held within defined limits. However, during call set-up or clear-down, the impedance cannot often be guaranteed. During these conditions, such a repeater must remain stable, if it is not to produce loud feedback type signals to other users. For this reason, the gain that can be introduced by an intermediary PBX is limited, and often discouraged. The PBX should normally be considered transparent to the connection.

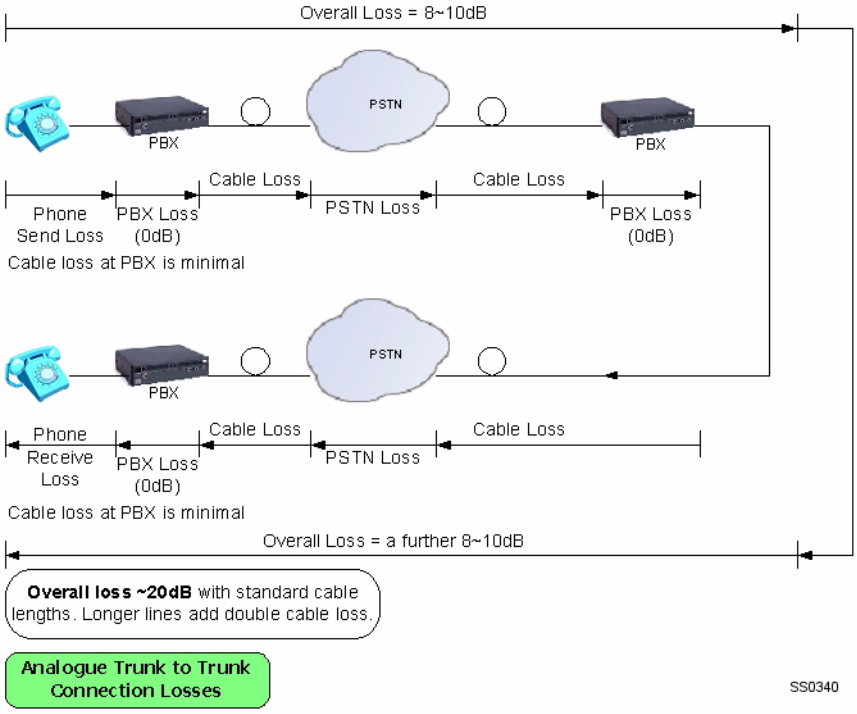


The diagrams above illustrate the connections involved in an Analog trunk to Analog trunk, or repeater connection.

The left-hand diagram illustrates the normal voice flows between the two trunks. Note that both send and receive signals are on the same wire pair at the trunk, but must be split into separate paths in the repeater. Although well designed, this two wire to four wire conversion (one common pair split into a receive pair and transmit pair) is not 100% efficient. Some signal will always leak back. The trick is to make sure that this signal is sufficiently small that it cannot cause feedback around the loop.

In the right-hand diagram the connection to trunk B is disconnected, for example, when a call is being cleared. Now all of the amplified signal from Trunk A cannot leave, and all of this is ‘reflected’ back into the repeater. If enough leaks through the second converter, then the whole circuit will become unstable, producing a howling sound, and be uncomfortable to other users on trunk A.

Assuming zero loss or gain in the PBX, then the diagram below illustrates the connections involved in an Analog trunk to Analog trunk connection. Losses in this case are expected to be in the order of 20dB, or 10dB quieter than a normal connection. This is equivalent to about 3 volume steps on a phone with volume adjust (3dB per step).



Note that every 1dB of cable loss to the intermediary PBX results in an overall reduced signal level of 2dB.

PBX trunk-to-trunk connection – digital trunks

In the digital world, all the required losses are introduced at the end devices, be that in the phone, or in a phone and PBX combination. After that, all devices that connect to the PSTN, via a digital connection, are considered to be part of the core network. Therefore, all digital connections are loss-less to voice traffic. The voice can be passed through a number of telephone switches without loss. This means that a long distance phone call will typically be of equal quality to a local phone call.

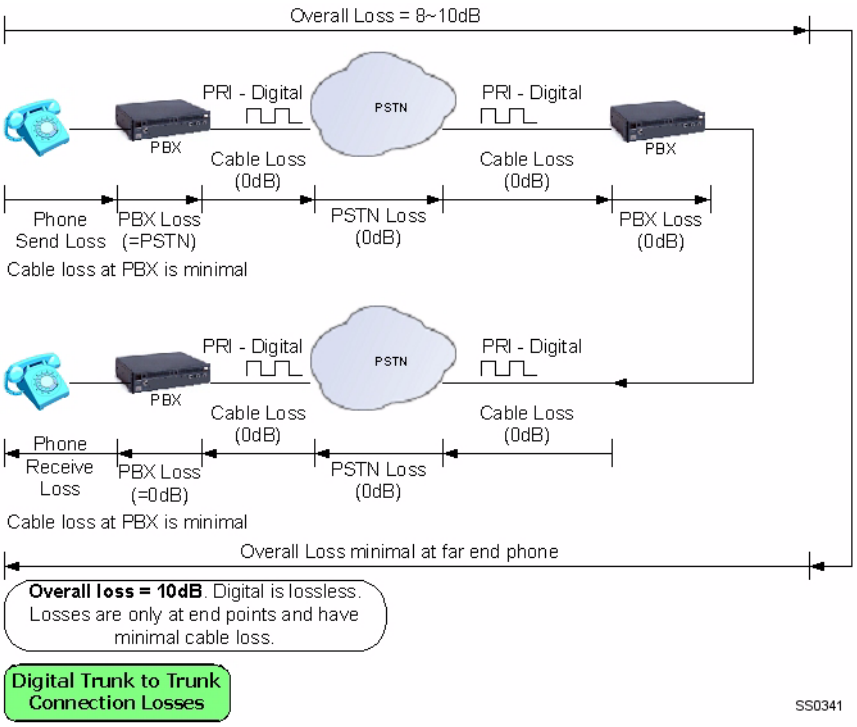
In a trunk to trunk connection situation, since the intermediary PBX is digital, it will not introduce loss, and there are no cable losses between PSTN and the PBX. The two end users will be totally unaware that the call is being switched via a third party.

One note of caution, however. Since digital lines are loss-less it would seem that distance between end points is no longer an issue. This is not entirely true. Over large intra-continental or inter-continental connections a certain amount of delay is introduced. If the far end connection terminates in a two wire to four wire hybrid, or there is acoustic pickup, for example with

hands-free operation, some of the locally sent signal will be sent back. If the delay is short, the user does not notice this. If there is sufficient delay, this returned signal is heard as echo.

Typically, for inter-continental connections, the PSTN will insert echo cancellation to overcome the echo introduced by the long delay.

For shorter intra-continental connections it may not be necessary to insert echo cancellation into the call path. However, if a long distance call is placed to an intermediary PBX, and the outgoing trunk is also a long distance connection, it is possible that the overall end to end delay will be sufficient that any returned signal could be heard as echo. The PSTN will not introduce echo cancellation in this case and the users will hear echo. Certain long distance connections are known to create this effect. Of interest are signals that might be re-routed between cities during congestion or busy periods, or toll free numbers through a central switching agency.



From a voice quality performance view, digital connections are much preferred over Analog connections. Losses between the users are confined to the end devices and not to the vaguaries of the connection path or intervening equipment. From a network planning perspective digital connections provide a common global standard as losses between different network providers, or between different countries, are defined.

Compression

Compression affects a number of call connections. These include

- IP phone to IP phone
- IP phone to TDM and vice versa
- IP phone at a remote site back to TDM or IP
- IP connection across an IP trunk route

Bandwidth requirements

Before determining the bandwidth for particular links, it is important to consider the traffic flow and also where devices are located relative to their controller. The use of compression zones and IP networking also has a bearing on traffic flow in parts of the network.

See “Network Configuration” on page 85 for details on bandwidth requirements for different LAN and WAN links with and without compression.

IP phones and compression

Some IP phones include compression capability and licenses. If required, these devices can stream directly with compressed voice without SX-200 ICP intervention.

Other IP phones, however, do not support compression. Calls to and from these devices are restricted to G.711 only. The following IP phones have this restriction:

- 5001 and 5005
- 5201, 5205, and 5207

SX-200 ICP and compression

A single controller has the following limitations:

- Both the CX/CXi and the MX are capable of providing compression. Additional DSP resources are needed for compression.
- Only two compression zones are possible from a single ICP, local (zone 1) and remote (zone 2).
- E2T compression is used primarily to deal with TDM devices such as ONS phones or PSTN connections.

Internal SX-200 ICP devices and compression

Conference

The conference feature is based on G.711 format, and is considered a TDM device. Compression is needed in the SX-200 ICP to communicate with each IP phone that normally uses compression to a TDM device.

Voice Mail

Internal Voice Mail stores data in G.711 format, but compression can be used to and from this device. An IP phone that uses compression to a TDM device uses compression to the voice mail.

Music On Hold

Music-on-Hold (MOH) can be sent with compression. Each MOH session in IP uses a compression license, according to the compression zone settings.

IP applications and compression

Mitel IP-based applications can support compression.

To get the best voice quality performance from devices such as Speak@Ease™ and IP voice mail, allocate them in a common compression zone with other devices not running compression, for example, default zone 1.

Consider the effect of allocating them to a compression zone where an application is used as a central resource over a WAN link. Bandwidth restrictions may still require compression to be enabled.

IP networking routes and compression

Compression can be enabled in IP networking routes between SX-200 ICP units if the end devices are capable of this operation. For more details see “Compression zones” on page 76.

Compression zones

Compression operation is determined by a number of factors and these include:

- Is there sufficient resource, for example, are there enough DSP channels available?
- Have sufficient licenses been acquired for both IP trunks and compression?
- Can the end device handle compression? Some phones only handle G.711.
- Is compression enabled in the class of service options?
- Are the IP trunks configured with compression?

The ‘placement’ of a phone within one of the compression zones is determined by the COS688 option settings. If a phone has COS688 capability then if the value is set to ‘No’, it is in the LOCAL Zone1; if the value is set to ‘Yes’, then it is in the REMOTE Zone2.

The decision to apply compression, or not, without IP networking, is based on the COS688 option settings and a simple OR algorithm, such as the following:

Option COS688 Setting		Compression
Calling Party	Called Party	
No	No	No
No	Yes	Yes
Yes	No	Yes
Yes	Yes	Yes

Compression is not selected when there is a hard restriction, such as lack of DSP resource, or a phone that is not capable of supporting compression, in keeping with the rules outlined above.

The TDM devices connected to the ICP are always considered to be in the local zone with a COS688 setting of ‘No’. This includes conference and integrated voice mail.

If IP Networking is included in the connection, then that is considered in the same manner. Thus, the Calling Party, the IP trunk and the Called Party need to be set to ‘No’ for compression to be disabled.

Option COS688 Setting			Compression
Calling Party	IP Trunk	Called Party	
No	No	No	No
No	No	Yes	Yes
Yes	No	No	Yes
Yes	No	Yes	Yes
No	Yes	No	Yes
No	Yes	Yes	Yes
Yes	Yes	No	Yes
Yes	Yes	Yes	Yes

Licensing

A number of licenses are needed to operate the SX-200 ICP system:

- **IP device license**
  An IP device license is needed for every IP phone and IP console that is registered with the SX-200 ICP. The SX-200 ICP does not count IP device licenses, but treats them as part of the IP phone license (see next item).
- **IP phone license**
  An IP phone license is a bundled package that includes both an IP device license and an IP user license when associated with an IP phone.
- **ACD agent license**
  An ACD agent license is needed for every active agent logged in to the system. A business that runs shift work patterns may have more agents in the database than those currently logged in.
- **TDM License**
  A TDM license is needed for each TDM device or connection in the system (ONS, OPS, & DNI lines, LS, DID, E&M, T1, PRI trunks – everything except embedded Voice Mail, IP lines, and IP trunks).
- **Digital (Network) Link license**
  A Digital (Network) Link license is needed in order to enable each T1 or PRI link on an MMC module or NSU. A license is not needed for legacy T1 cards, although these still count against the maximum allowed number of links.
- **Compression license**
  A compression license is needed for every call that passes through a SX-200 ICP that requires a compression resource. Calls that typically require a SX-200 compression resource are those that are associated with an IP trunk, where the call traverses TDM to IP, or vice versa, and where there is a remote connection with limited bandwidth. The use of compression is defined through class of service (COS) on the phone and trunk route for each call. Additional DSP hardware allows compression to be added in increments of eight sessions.
- **IP Networking license**
  An IP networking license is a system-wide license that allows access to all IP trunks on the system. An IP networking license is needed for every call that is handled between different controllers.
- **Voice Mail license**
  A Voice Mail license is needed for every simple voice mailbox user that has been configured. Functions include Basic Voice Mail, Basic Auto-Attendant, Voice Mail Language Support, and Multi-level Auto-Attendant.
- **Advanced Voice Mail license**
  An Advanced Voice Mail license is needed for each session of more advanced features that use voice mail services, such as Record-a-Call, Auto Forward to E-mail, and Personal Contacts.

- **Hospitality (Property Management System) license**
  A Hospitality (Property Management System) license is needed to enable access to these services.

Refer to the installation guidelines for more details on configuration of IP networking (IP trunks) and compression zones.

Device licenses

A number of devices require different licenses within the SX-200 ICP in order to operate. These devices are listed in the following table.

Table 19: Devices and Licenses

Device or Feature	License
IP phone and IP console	IP set license
TDM phone	TDM device license.
Wireless phone (SpectraLink)	IP set license
Wireless phone (Symbol)	IP set license
YA client	IP set license
YA softphone	IP set license
ACD Agent	ACD Agent license
Voice Mailbox	Voice Mailbox license (1 per user)
Basic Auto-Attendant	Voice Mailbox license
Multi-Level Auto-Attendant	None
Record-a-Call	Voice Mailbox license
Auto Forward to Email	Email messaging license
NuPoint Messenger (IP ports)	IP set license per port (part of Max Devices)
Analog trunk	TDM device license
IP Networking (IP trunk)	IP trunk license per trunk
Digital trunk (TI, PRI, etc)	Digital Link license per digital trunk span TDM device license per trunk (1 T1 span = 24 TDM licenses)
Compression (TDM/IP)	A Compression license is needed for each TDM to IP or IP to TDM call that requires the use of the DSP compression.
Teleworker Solution	IP set license
6100 Contact Center (see Note)	One IP set license per session/connection to SX-200 ICP
Speech Server (6500)(see Note)	One IP set license per session/connection to SX-200 ICP
Messaging Server (6510) (see Note)	One IP set license per session/connection to SX-200 ICP
Hospitality/PMS	Hospitality option

Note: The licenses described are those applicable to the SX-200 ICP. The 6100, 6500, and 6510 also require application licenses to enable the function.

Licensing limits

License limits are achievable only when the appropriate resources are available. For example, if there is insufficient DSP for voice mail, the operational limit may be reached before the license limit. Be very careful with large numbers of licenses for voice mail and compression. Because DSP resources are allocated at initialization based on option selections and DSP availabilty, not traffic requirements, it is possible to improperly allocate DSP resources and not have enough left for the required number of telecom tone receivers and generators. Limitations to the licenses are shown in the following table.

Table 20: License Limits

License type	MX Limit	CX/CXi Limit	AX Limit
IP set license	248	100	248
TDM devices license	768	768 (maximum 152 supported)	768 (maximum 288 supported)
Compression license	24	16	24
IP networking (IP trunk) license	30	16	30
Voice Mail box license (includes advanced VM licenses)	748	748	748
ACD Agent license • Active Agents Logged In • Agent Ids • Agent Groups	 100 999 (not licensed) 50 (not licensed)	 50 999 (not licensed) 50 (not licensed)	 40 999 (not licensed) 50 (not licensed)
Digital Link license	8	8 (only 1 supported)	8 (only 2 supported)
TDM (Digital) Bays	7	0 (Not supported)	0

Note: All other system licenses (options) are single entry items; i.e. yes/no with no quantity limit.

Licensing example

The following example shows how to determine the number of licenses required. For more accurate traffic calculations, use the System Engineering tool or contact Customer Engineering Services. Please note: the numbers below are approximations.

Consider an installation with two headquarters and one remote office connected to the first headquarters. The following table shows a list of the equipment installed at each of the sites.

Table 21: License Example

Headquarters 1	Remote 1 connected to HQ1	Headquarters 2
200 ICP MX	No controller, linked to HQ1	200 ICP CXi
PSTN access via PRI, 4 links (backup on LS for 6 trunks)	Access via HQ1	PSTN access via HQ1 (backup on LS for 4 trunks)
IP networking to HQ2	Direct connection to HQ1	IP networking to HQ1
Compression enabled to HQ2 Compression disabled to remote	Compression enabled to HQ2 Compression enabled to HQ1	Compression disabled to HQ1 Compression enabled to remote
150 IP phones	20 IP phones	40 IP phones
Includes 20 ACD	No ACD	No ACD
Includes 10 YA	No YA	No YA
16 ONS phones	No ONS	2 ONS phones
24 Voice Mail sessions, 170 Mailbox users	Use Voice Mail at HQ1	10 Voice Mail sessions, 40 Mailbox users
2 Auto Attendant sessions	No Auto Attendant	No Auto Attendant
1 Record-a-Call session	Record-a-Call in HQ1	No Record-a-Call
No TDM networking	No TDM networking	No TDM networking

Taking each of the licenses in turn, the above information results in the following calculations and resulting licenses:

- **IP set license:** IP set licenses apply to IP phones. HQ1 has 150 local IP users, and 20 remote users. Thus 170 licenses are needed. HQ2 has 40 local IP users, so 40 licenses are needed. For the total site, 210 licenses are needed.
- **ACD license:** There are 20 active ACD agents on HQ1, so 20 licenses are needed.
- **Digital Link license:** Only HQ1 has digital links, and these are 4 spans, so 4 licenses are needed.
- **Compression license:** IP phones already include compression licenses, so calls between IP phones do not need additional licenses. Licenses are needed for calls through the 200 ICP. Compression is enabled between HQ1 and HQ2. Compression is disabled between HQ1 and the remote site. So, only trunk calls via HQ1 from HQ2 are needed. There are 40 IP phones, few TDM, so with a trunk traffic rate of 4 CCS (6 CCS x 2/3) then 5 channels are needed (40 x 4 / 36). Since hardware compression comes inblocks of 8, then 8 licenses are purchased for HQ1.

- **IP trunk license:** This includes all calls between HQ1 and HQ2. One license is needed per ICP, for each call between them. For configuration of IP trunk limits on the route, both trunk and internal calls must be considered. From the compression license, 5 channels are needed for trunks. A further one channel is needed for internal calls, making a total of 6 IP trunks (40 X 2/36 X 15% (networking)). Therefore 6 IP trunk licenses will be required on each ICP, for a total of 12 on the installation.
- **Voice Mail license:** At HQ1 there are 170 voice mailboxes. At HQ2 there are 10 voice mailboxes. For the site, a total of 180 licenses are needed.
- **Auto-attendant and Record a Call license:** At HQ1 there are additional services such as two Auto-Attendants and one Record-a-Call. Additional licenses are needed for these features.
- **Hospitality (PMS) license:** There is no connection to a PMS system and so no PMS licenses are needed.

Note: The numbers and calculations are a basic estimation. More accurate results can be obtained by using the System Engineering Tool.

Network Configuration

Use the information in this section to determine the suitability and requirements for a Voice-over-IP (VoIP) installation with the SX-200 ICP when used in a business or Enterprise environment.

The main requirement in assessing and configuring the network is maintaining the voice quality and functionality for the user. This may require that an existing network be changed, or that equipment with certain capabilities be installed.

The main network issues affecting voice quality are

- Delay
- Jitter
- Packet loss

Care has been taken in the design of the IP phones and controllers to reduce echo noticeable with delay through the inclusion of echo cancellation devices. Jitter and a certain degree of packet loss are also taken care of by jitter buffers.

Before implementing a network to handle VoIP, consider the following areas (these are recommendations, and there will always be exceptions):

- **QoS (Quality of Service)** Quality of service is that which is provided to the user, not network equipment settings. However, certain network equipment configurations can greatly assist in ensuring adequate QoS to a user. These include
  - **IEEE 802.1p/Q**: This is also known as VLAN tagging, priority, or COS (different from the PBX/telecom Class of Service). IEEE 802.1p/Q operates at Layer 2 to ensure the highest priority for voice traffic.
  - **DiffServ**: DiffServ is a fixed field in the Layer 3 information that is also used to define different service categories through TOS, priority, and precedence. DiffServ and Type of Service are similar. The older Type-of-Service values are compatible with the newer DiffServ values.
- **Switched networks**: Use switched networks, which then allow full-bandwidth capability to all end points. Networks with hubs include shared bandwidth; no priority mechanisms are available.
- **Network topology**: Networks should be designed in a hierarchical manner where bandwidth between devices is controlled and understood. Simply linking switches in a long chain will work for data, but it introduces jitter and unnecessary bottlenecks between devices.
- **Network pre-Installation and post-installation analysis**: The network should be investigated before installation to determine suitability for VoIP. Once an installation is completed, it should also be tested to ensure that the guideline limits have not been exceeded.
- **Network address translation (NAT) and firewall**: Although there are emerging standards to allow VoIP through firewalls and NAT devices, these are still in early development. To allow voice through a firewall, a number of ports need to be opened, since one controller may use a range of ports that are dynamically assigned. Opening all possible ports negates the usefulness of the firewall. NAT needs to change addresses, but may have difficulty mapping a single controller device to multiple internet addresses, or translating IP addresses that are buried in control messages. Generally, these issues are resolved by using VPNs.

- **Virtual Private Network (VPN)**: VPNs are simply a pipe or tunnel across an ISP network, which allows a remote device to react as though it is still connected to the enterprise network. Be aware that the VPN may be across an unknown network or across the internet. It may be necessary to get certain Service Level Agreements (SLA) to ensure timely delivery of data. Where encryption is used, additional delay may also be added to the data.
- **Teleworker:** The Mitel Teleworker Solution is for remote workers who need to connect to the internet and send traffic through a business firewall and NAT combination.

General guidelines

The main issues that affect system installation and user perceptions are

- Quality of service (voice quality during the call)
- Availability of the service (setting up and clearing voice connections or signaling)

The challenge is to engineer the network to ensure that these quality requirements are met. With TDM, this is possible by providing dedicated connections to the desk. With IP, the network may have to share connections with other devices, such as PCs. The requirements of the PC and an IP phone differ: PCs need to send data as quickly as possible using all available bandwidth, but IP phones must send and receive limited data on a very regular basis with little variation (jitter).

In summary, the challenge is to place connection-oriented devices into a connectionless environment and still maintain the expected operation.

Terminology

Some areas that affect the installation are described below with a brief explanation of their importance.

Delay

As delay increases in a conversation it becomes increasingly difficult to sustain normal two-way communication. Such a conversation rapidly changes from an interactive exchange to an ‘over to you’ radio-style conversation. The delay is noticeable at a 150ms to 200ms delay, and is radio-style by a 400ms delay. The phones and gateway in the controller introduce some necessary delay. These guidelines identify the delays that can be tolerated to ensure that voice quality is maintained.

Echo

Echo generally results from poor termination of a PSTN line or acoustic feedback. When delay is short, echo is usually not heard due to the level of local sidetone. But as delay is introduced, this echo becomes noticeable. To counteract this, the gateway device includes echo cancellation up to 64 ms looking towards the PSTN. The IP phone includes echo-suppression to remove acoustic echo.

Jitter

Jitter is the variation in delay that can occur in networks. The major source of jitter is serialization delay, which occurs when a packet cannot be sent at the ideal time because another packet is already being sent on the same connection. The result is that the packet must wait. For high-speed links, a maximum packet size of about 1500 bytes is sent in microseconds, so jitter is negligible. However, for slower WAN connections, such as a Frame Relay connection, the delay becomes significant.

Extensive use of hubs rather than switches also introduces jitter. Therefore, hub use for larger networks and where connections are shared with data devices is not advised.

Use of multiple WAN connections and load-sharing can also introduce jitter due to different path delays. Ideally, voice should pass down one path or another and may be configurable based on TOS/DiffServ values.

Packet loss

Packet loss within the network can occur for a number of reasons, mainly congestion of a connection, where the buffers can overflow and data is lost. Packets may also be discarded at the gateway or IP phone because the jitter is so variable that the packet arrives too late to be used for voice. Out-of-sequence packets can also occur over WAN connections. These are like packets with excessive jitter and can also result in packet discard. Incorrect duplex settings on LAN connections can also lead to data collisions and packet loss.

Although some packet loss can be handled on an ongoing basis, bursts of packet loss will become noticeable. A network with 0.1% packet loss over time sounds much different than a network with the same loss but occurring in bursts of three or more packets.

Available bandwidth

If a connection is rated at a particular bandwidth, this does not necessarily mean that all of this bandwidth is available. Connections between LAN and WAN network devices include a certain amount of overhead for inter-device traffic, including link terminations devices and general broadcast traffic. A collision in a shared network and guard time between packets also reduces the available time in which data can be sent, because the data is asynchronous to the connection. TDM takes care of this through strategies such as framing and clock synchronization. In summary, the available bandwidth is always less than the connection bandwidth.

Packet priority mechanisms

In a network oriented towards data devices, absolute delay is not as important as accuracy. For voice traffic, however, a certain amount of incorrect or lost information is acceptable, but information delivered in an untimely manner is not. Therefore, it is important to ensure that any voice traffic gets “pushed” to the front of any connection queue. If PC-type data is slightly delayed, this is less important. There are two similar mechanisms at work to determine priority: IEEE 802.1p/Q at Layer 2 and Diffserv (formerly Type of Service) at Layer 3.

WAN connections

The best Quality of Service is obtained when the customer has control of the external WAN connections. This can be achieved by using dedicated leased lines between sites, or by ensuring a guaranteed service-level agreement (SLA) from the external network provider (ISP).

When specifying a SLA it is important that the guaranteed committed information rate (CIR) is specified and includes a guard band. Data sent in excess of the CIR is likely to be discarded during congestion periods in order to maintain guarantees on the SLA. Therefore, it may also be advantageous to split voice traffic from normal data traffic with different SLAs.

For more dedicated links, some additional protocols can be used to improve bandwidth usage. The data in an Ethernet LAN connection includes a data layer for Ethernet and a data layer for IP. In a WAN connection, the Ethernet layer is not needed. However, other layers are needed to transport the IP layer and voice data. As a result, certain WAN protocols can use less bandwidth. These include the more dedicated links such as PPP and compressed PPP.

Transcoding and compression

The terms “transcoding” and “compression” are often used interchangeably. Transcoding is the changing of voice information from one CODEC type to another. However, most CODEC devices rely on G.711 as the base entry level. Therefore, transcoding from G.729 to G.726 is likely done through G.711. Compression is simply reducing the amount of data. For voice traffic, this can be achieved by going from G.711 to G.729, for example.

Any form of voice compression works by removing a certain amount of information deemed non-essential. This may include not sending data during silent periods, as well as sending only the main voice frequency elements rather than the full bandwidth. As a result, some information is lost. Compressed voice is, therefore, never as good as uncompressed voice, but the requirement of intelligibility is maintained. Of the compression CODECs, G.729 has good bandwidth reduction and maintains good voice quality and intelligibility.

In the LAN environment where bandwidth is plentiful, there is probably little reason to compress voice, and so G.711 is normally the CODEC of choice. In a WAN environment, where access bandwidth may be limited, use of the G.729 CODEC can increase the amount of voice traffic that can be carried on a particular link. In some instances, G.711 is still preferable for voice quality, but voice traffic will be limited on the link.

Hub network versus switched network

The best network configuration is one that is entirely switched. Switched networks allow full network bandwidth to be made available to the end user and greatly reduce collisions with a resulting decrease in network usage. This in turn makes more bandwidth available for another application, such as voice. It is strongly advised that VoIP installations use switches within the network architecture.

A hub works by sharing bandwidth among a number of devices. The devices use CSMA/CD to control access, but effectively ‘fight’ each other for access. The devices that fail to get access wait for an available slot. Hubs do not have QoS control. If data needs to be sent in a timely manner, there is a high probability of introducing unnecessary jitter with potential packet loss and degradation in voice quality.

In a switched environment, all ports can pass data to a LAN switch with minimal delay. Data is passed to queues, and priority can be given to types of data, such as those marked by IEEE 802.1p/Q tags. If two devices share a common LAN switch, they can effectively pass data to each other at high speed (as though they were the only devices on the network) while other devices could be doing the same. Using a switch is like having multiple networks. Network efficiency and management are greatly improved.

Since connections in a switched network are typically point to point, there is also the possibility of configuring the connection to be full duplex. This virtually doubles the bandwidth, since data can be sent and received at the same time. In a half-duplex environment, data can be sent or received only sequentially. Equipment configured with auto-negotiation always determines the highest possible data rate and makes it available connection by connection. Simple hubs are generally fixed at 10BaseT half-duplex.

Using a switched network ensures that maximum bandwidth is available to the end devices with minimal delay and best voice quality of service.

LAN architecture

Networks usually consist of different layers. Two main parts are the core network and the access network. Larger networks can include additional layers such as a distribution layer. Ideally, the SX-200 ICP should have a connection higher up in the network, located more towards the core than at an access point. The optimum connection point is in the distribution layer. Phones should connect to the access layer.

Core network

The core network potentially carries data on dedicated links at 1Gbits/s or higher. The switches at this level probably include some Layer 2 and Layer 3 switching and unite a number of subnets, or a small number of units. These units almost certainly have UPS backup and are cross-connected in redundant configurations, so that the failure of one device is unlikely to result in total network failure.

Distribution layer

The distribution layer connects the core network and the users on the access layer. Such a layer is used within a local area, for example, within a single building or in a campus environment. This allows local switching to stay off the core network and provides a level of continued operation if problems occur in the core. Typically, network devices such as servers and printers are connected to the distribution layer. This is where the SX-200 ICP connects in such a large system. Devices in this layer usually use UPS backup.

Access layer

The access layer connects to the distribution layer by single or multiple connections. It provides the slower 10/100 BaseT type of connections to the user. These can be cross-connected within geographic locations. If a device fails here, then only the locally connected devices will fail. These units may or may not have UPS backup. Consider UPS backup when voice devices are connected to the access devices.

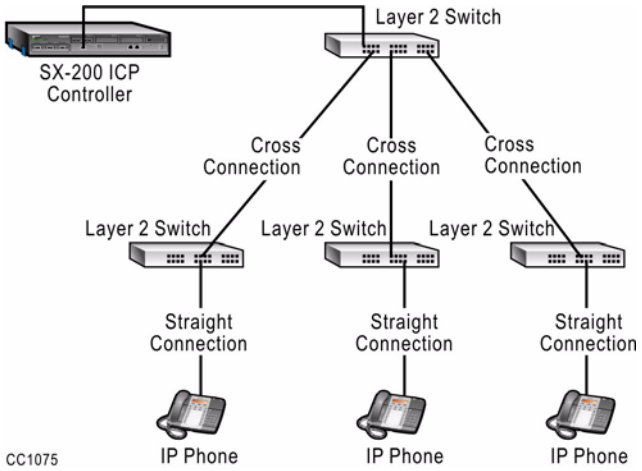


Figure 11: LAN Architecture

In smaller networks, the definitions of the boundaries may become a little blurred. However, even in these smaller networks, plan a tree-type structure between the SX-200 ICP and the phones. Daisy-chaining a number of switches is not recommended since all switches become involved in connections from one end of the chain to the other. Layering will reduce unnecessary traffic.

SX-200 ICP-specific guidelines

The Network Guidelines in the preceding sections cover a number of generic situations that may be applicable depending upon the network to be used. In this section, a number of specific network guidelines are highlighted. For details on AX-specific guidelines, see the *SX-200 ICP CX/CXi and AX Technician's Handbook*.

Location of the SX-200 ICP in a network

Ideally in a hierarchical network design, the SX-200 ICP is located within the distribution layer of the network. See the section "LAN architecture" on page 89 for more details.

The IP phones are in constant communication with the SX-200 ICP. All signaling traffic, as well as traffic to and from the PSTN, goes through the SX-200 ICP. The controller should, therefore, be placed higher up the physical network, at some central switch point (for example, where all the access Layer 2 switches connect, or where there is a router or Layer 3 device to other subnets).

If there are physically separate networks for voice and data traffic, you may still need to link these networks together and to manage the SX-200 ICP from within the data portion of the network. In this case, a router is required.

IP networking support

The use of IP networking suggests that a number of systems are being networked, or that certain remote sites are connected to a common control unit. IP networking can also be across WAN links.

If a WAN connection provides both data and voice traffic on a common path, then priority schemes need to be employed. All IP phones and the SX-200 ICP controller use appropriate Type-of-Service or DiffServ field settings. Priority queuing should be enabled on the end routers, even if priority is not used within a separate voice network. See the section “Configuring network priority” on page 109 for further details.

CXi specific requirements

The CXi product has an integral Layer 2 Ethernet switch providing Power Over Ethernet. This allows the IP phones to be connected directly to the unit. There is also an uplink connection (10/100/100 BaseT) to provide a high-speed connection for up to two expansion units, allowing up to 100 users to be connected.

In addition to the requirements in the overall Network Guidelines section, some further guidelines apply to the CXi unit when used in a LAN environment. Note that in a small installation, the CXi could effectively become the network provider.

- Only connect expansion switches to the 10/100/1G port (non-powered).
- Do not connect expansion switches to the 10/100 LAN ports (powered).
- The SX-200-ICP provides support for the Rapidly Re-converging Spanning Tree Protocol (RSTP) on ethernet ports 1 though 16. For details see the section on RSTP under General Guidelines.
- If RSTP is not enabled on the CXi or expansion switch ethernet ports, exercise caution so that you do not create Layer 2 network loops with the CXi switch and the expansion units.
- This product supports up to two VLANs, including the default VLAN (1).
- Two priority queues are available at the ports. Priority (COS) 0 to 3 in the low priority queue and Priority (COS) 4 to 7 in the high priority queue.
- Untagged data will be tagged with VLAN1 and low priority.
- Where the internal DHCP server is used on the CXi, the VLAN and Priority (COS = 6) will be sent to the phones and these options need not be configured.
- Where an external DHCP server is used, the VLAN option MUST be set to VLAN1 and Priority option set to high, typically 6.
- VLAN priority can be enabled at the uplink port (17) to maintain priority to voice, and is a recommended setting when phones and PCs share the connection path. Priority and VLANs should also be enabled between expansion units for the same reasons, such as voice priority.

IGMP Snooping

The Release 4.0 SX-200 ICP CXi supports IGMP snooping. IGMP (Internet Group Multicast Protocol) is a protocol that allows hosts to subscribe to a multicast group. This allows LAN multicast traffic to be directed only to hosts that have subscribed to the particular multicast group rather than flooding the entire LAN with multicast transmissions.

IGMP snooping allows the CXi to snoop multicast traffic present on the LAN and learn if there are multicast groups in existence. Once the CXi has learnt about all of the multicast groups, it will only send multicast frames to devices that have requested them. When the IGMP Snooping feature is disabled, multicast frames are sent to all devices on the LAN. Disabling IGMP snooping may cause problems with network or device performance.

Rapid Spanning Tree Protocol (RSTP)

As of Release 4.0, the Rapid Reconfiguration of Spanning Tree Protocol (RSTP) is supported on the SX-200 ICP CXi Controller. The SX-200-ICP MX controller does not support RSTP.

For details on RSTP, refer to “Rapid Spanning Tree Protocol (RSTP)” on page 179.

VLANs

The MX controller does not include a VLAN-capable L2 switch. The MX and CXi (when installed in a voice-only network) can be integrated into a network in much the same fashion as servers.

The CXi controller includes an internal L2 switch that is VLAN-capable. As a result, in networks that support both voice and data, the CXi needs to be treated as an integral part of the L2 networking infrastructure.

CXi VLAN behavior

Default VLAN 1

In the default case where the CXi is on the default VLAN (VLAN 1), the CXi accepts, on LAN 1, tagged and untagged frames on VLAN 1. The CXi treats untagged frames as VLAN 1 frames. The CXi prioritizes traffic based on the priority tag and maintains two priority queues. The low priority queue is for untagged frames and tagged VLAN 1 frames with priority 1-3. The high priority queue is for tagged VLAN 1 frames with priority 4-7. Traffic in the high priority queue is processed first.

On egress, all VLAN 1 traffic on ports 1 through 16 is untagged.

On port 17 the user has the option to tag the traffic via the “Tag VLAN 1 on Trunk Port (17)” parameter. Enable this parameter only if a VLAN-capable expansion switch is connected to the port.

The default is "Disabled" (all VLAN tags are removed before being forwarded by the switch).

Voice VLAN

In order for the phones to operate on the Voice VLAN, the CXi L2 Switch must also be on the same Voice VLAN. With the introduction of Voice VLAN support, the CXi will accept untagged VLAN 1 frames and tagged VLAN 1 frames or Voice VLAN frames. Tagged frames arriving on any VLAN other than VLAN 1 or the Voice VLAN will be dropped. Priority queues are maintained as described above, but in this case for Voice VLAN tagged traffic.

On egress, Voice VLAN traffic on ports 1 through 16 remains tagged, VLAN 1 tagging is not preserved.

VLAN Routing

The CXi relies on external routers to perform VLAN routing.

The CXi always maintains Voice VLAN tags on frames leaving port 17 of the CXi.

Figure 12 shows the CXi integrated into a network carrying both voice and data. VLAN 1 is used for non-voice traffic and the Voice VLAN is used for voice traffic. A VLAN-capable managed L2 switch is connected to the CXi Gigabit Ethernet Uplink port for expansion purposes. An external DHCP server is set up to serve VLAN 1 and the CXi internal DHCP server is used to serve the Voice VLAN. Figure 12 shows the usage of VLANs on the various network segments.

Note: The CXi internal DHCP server can be configured to provide DHCP services to both VLAN 1 and the Voice VLAN. If this were the case, an external DHCP server would not be required. However, the external router in the corporate network would need to be configured to support routing from VLAN 1 to the Voice VLAN and DHCP forwarding would need to be enabled on the router.

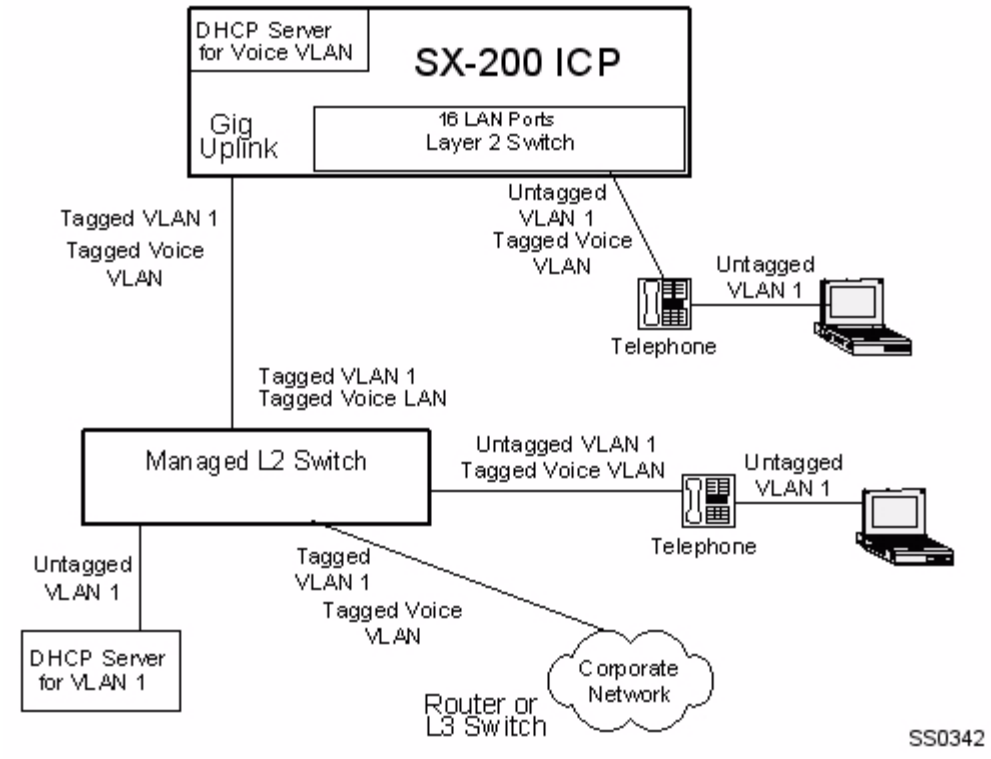


Figure 12: CXi VLAN Behavior

Implementing a voice-only network

In a voice-only network, IP telephony devices are the only devices connected to the controller's network interfaces.

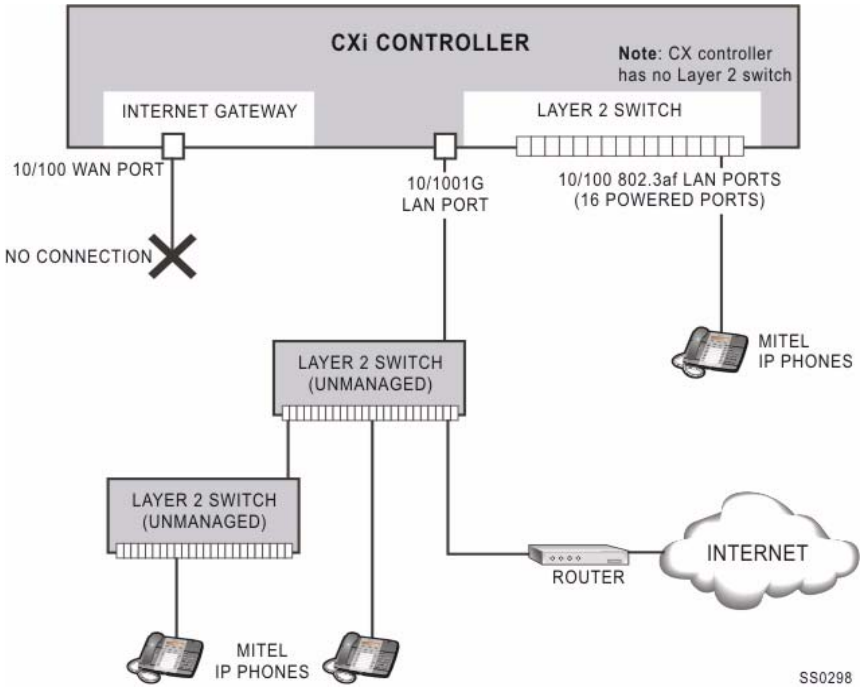


Figure 13: Typical Voice-Only Network

Programming requirements

No changes to the controller's default IP settings are required for a voice-only network; simply plug up to 16 IP phones into the internal Layer 2 switch ports (marked 10/100 802.3af).

Implementing a voice and data network

A voice and data network uses the controller's network interfaces to provide services for IP phone and PCs plus a firewall-protected connection to the Internet.

Figure 14 shows a typical voice-data network. It uses the WAN interface to connect to the Internet. A router plugged into a Layer 2 port on the controller provides an alternate path to the Internet for customers that already have Internet access on their data network. Although not shown, such customers could use their existing DHCP server to service devices connected to the controller. (The server in the controller would be disabled since it's not needed.)

The 10/100/1G LAN port in the illustration is connected to a pair of Layer 2 switches. Multiple switches daisy chained together expand the system to its maximum 100-port capacity. A single 48-port switch can also be used.

PCs are shown connected to the network in two ways: direct to the Layer 2 switch and indirectly through a dual-port IP Phone.

Caution:To ensure optimum network performance, DO NOT connect servers to the 2nd port on IP phones.

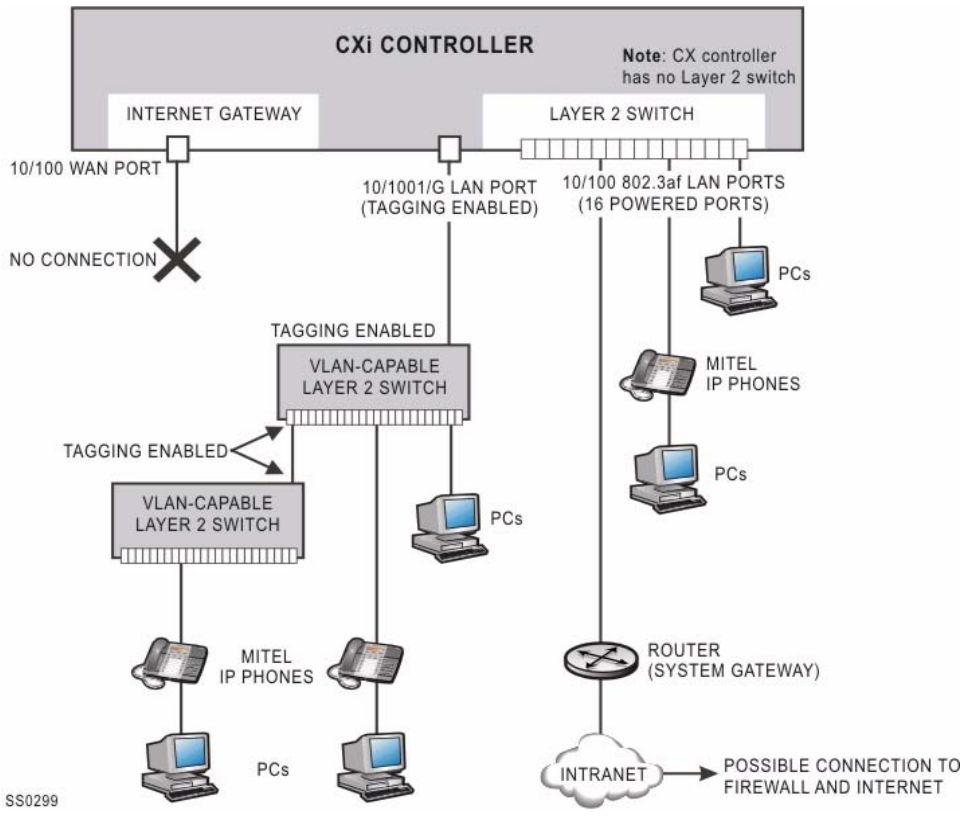


Figure 14: Typical Voice and Data Network

Configuration requirements: controller

- **Internet Gateway (WAN port)** - The address assignment must be specified (PPPoE, DHCP client, or static), and the firewall programmed. For programming instructions, refer to the Technical Documentation.
- **Layer 2 switch** - Updates may be required to prevent IP address conflicts, to allow for traffic between the local and remote subnets, and to ensure quality of service for phone calls with VLAN prioritization. For programming instructions, refer to the Technical Documentation.
- **DHCP Server** - The default address information and options may need changing if installing the controller on a network with multiple subnets. If using an external DHCP server, disable the one in the controller. For programming instructions, refer to the Technical Documentation.

Configuration requirements: other network devices

- **Dual-port IP Phones (5215 / 5220)** - Activation of the 2nd port requires System and Class of Service options.
- **External DHCP Server** - If using an external DHCP server, make sure that it is programmed to provide addresses and options to all devices that require them. Also, make sure to disable the DHCP server in the controller.
- **External Layer 2 Switches** - If a VLAN-capable switch is connected to the 10/100/1G port, program its uplink port to send and receive tagged packets on the default VLAN (1), and make sure that it treats packets with priority 6 as the highest priority. If another VLAN-capable switch is connected to the first, program it with the same settings. On the CXi, enable VLAN tagging on port 17. (This setup allow the VLAN-capable switches to provide the same VLAN prioritization services as the internal Layer 2 switch on the CXi.)
- **Router** - If a router is connected to the local internal network, designate it as the default gateway to ther networks. Program its IP address as the System Gateway IP on the CXi. If an external router is present on the LAN, disable the Router Discovery Protocol on the CXi.

Installing an external Layer 2 switch for line expansion

Voice-only networks

To increaseIP connection capacity, connect a customer-supplied Layer 2 switch to the 10/100/1G LAN port. If required, connect a second switch to the first to expand to 100 lines (the system maximum). For a voice only IP network (i.e. a network with no PCs), system capacity can be expanded to a maximum of 100 users by connecting an expansion Layer 2 switch to the 10/100/1G LAN port of the CX/CXi. Use one 48-port switch or two 24-port switches connected in a daisy chain. As a minimum, the expansion switches should support 10/100 BaseT; preferably they should support 10/100/1000 BaseT. Because some programming may be necessary (such as the port speeds), the expansion switches require a management interface.

Expansion switches for voice-only networks do not require VLAN capability..

Notes:

1. Connect a single expansion Layer 2 switch to the 10/100/1G LAN port only. If using two 24-port switches, connect the second switch to the first in a daisy chain. Do not connect expansion switches to the 10/100 802.3af LAN ports.
2. Mitel telephones require power, which they can receive from an adapter or power brick, or from a powered Ethernet connection. The 10/100 802.3af LAN ports of the CXi provide Power over Ethernet (PoE), as do some expansion switches. The 10/100/1G LAN port does not provide PoE.
3. Category 5 cable is required for the uplink connection between the expansion switches and the CXi, and is recommended for all other Ethernet connections. Category 3 cable can be used to connect single IP Phones directly to the expansion switches or to the Layer 2 switch of the CXi

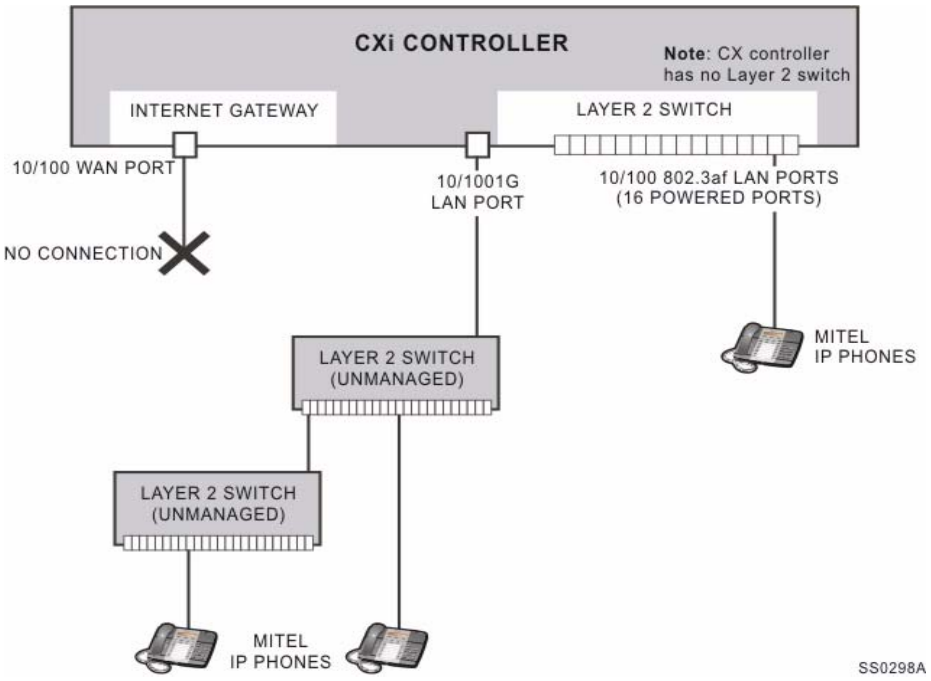


Figure 15: Expanded Voice only System

Voice and data networks

For a voice and data IP network (i.e. a network with IP phones and PCs), system capacity can be expanded to a maximum of 100 phones and 100 PCs by connecting an expansion Layer 2 switch to the 10/100/1G LAN port of the CX/CXi. Use one 48-port switch or two 24-port switches connected in a daisy chain. As a minimum, the expansion switches should support 10/100 BaseT; preferably, they should support 10/100/1000 BaseT.

Note: The expansion switches must be manageable and must adhere to the 802.1p/Q VLAN standard.

Program the uplink port of the expansion switches to send and receive tagged packets on the default VLAN (1), and make sure that the expansion switches treat packets with priority value 6 as highest priority (this is the default setting on most switches). Program the CX/CXi to tag packets on its 10/100/1G LAN port. After you complete this configuration, the expansion

switches will operate like the internal Layer 2 switch on the CXi, prioritizing voice traffic over data traffic.

Guidelines

1. Connect a single expansion Layer 2 switch to the 10/100/1G LAN port only. If using two 24-port switches, connect the second switch to the first in a daisy chain. Do not connect-expansion switches to the 10/100 802.3af LAN ports.
2. VLAN tagging must be enabled on all “trunk” links which connect the expansion switches. For two expansion switches, you need to enable VLAN tags for VLAN 1 on:
   - 10/100/1G LAN port of CXi (port 17)
   - Switch port on first expansion switch which connects to port 17
   - Switch port on first expansion switch which connects to second switch
   - Switch port on first expansion switch which connects to first switch.
3. To maximize the bandwidth capability of the 10/100/1G LAN port, connect it to the highest speed port on the first expansion switch, preferably a 1G port.
4. There are two ways to connect IP devices (PCs) to the voice and data network: directly to a switch or indirectly through a dual-port IP phone.
5. Dual-port phones use the same port speed as the connected PCs. For this reason, PCs with 100 Mbps Ethernet cards are recommended.
6. Mitel telephones require power, which they can receive from an adapter or power brick, or from a powered Ethernet connection. The 10/100 802.3af LAN ports of the CXi provide Power over Ethernet (PoE), as do some expansion switches. The 10/100/1G LAN port does not provide PoE.
7. Category 5 or better cable is recommended for all Ethernet connections in a mixed voice and data environment. However, Category 3 cable can be used to connect single Ethernet devices (IP phones or PCs) to the network.

Maintaining voice quality of service

The following affect voice quality of service over IP connections

- End-to-end delay
- Jitter or delay variation
- Packet loss
  - Due to link congestion resulting in discarded or out of sequence packets
  - Due to lack of or incorrectly configured QoS controls on LAN and WAN connections
  - Due to forced discard of packet caused by excessive jitter

VoIP readiness assessment using Viola

The Viola Networks NetAlly RealTime product solves problems associated with SX-200 ICP (or VoIP) networks. Viola

- Determines if an IP network is currently capable of handling VoIP traffic and at what capacity.
- Documents the tested VoIP call capacity and characteristics of an IP network.
- Determines the cause of voice quality problems encountered within an IP network, locally or remotely.
- Monitors (locally or remotely) the voice quality being delivered by a network, and provide alerts should problems occur.

Typically, networks are designed to handle peak traffic. It is important to determine how well VoIP will perform on a network by measuring simulated VoIP traffic and calculating voice quality based on a Mean Opinion Score (MOS). Some networks only require minor modifications to deliver reliable, high-quality voice service. Others require more significant overhauls.

The NetAlly tool, from Viola Networks, can carry out these assessments of the network and provide reports of potential bottlenecks. Such characterization and testing of the network should be carried out before installation, as well as after installation, to confirm correct operation. Contact Customer Engineering Services to carry out this evaluation. Further details on the test tool can also be found on Mitel OnLine under the products/Integrated Management Applications section.

VoIP readiness testing using Viola flags those parts of the network which require modification. The tables below show the values for the general and advanced parameters to be used in Viola for this test.

Table 22: General Parameters for using Viola

Parameters	G.711	G.729	Comments
MOS Threshold	4.0	3.6	
Loss Threshold (percent)	3.0	3.0	
Throughput Low Threshold (kbits/sec.)	60	7.2	
Jitter Threshold (ms)	10	10	
Delay Threshold (ms)	150	150	Vocoder Delay + Propagation Delay + Jitter Buffer Delay + Transmission Delay
CPU Threshold	80	80	
Quality of Service	40	40	DiffServ(5)

Table 23: Advanced Parameters for using Viola

Parameters	G.711	G.729	Comments
Conversation Duration (sec.)	60	60	
Number of VoIP Calls	Fixed(1)	Fixed(1)	see Call Generation
Number of Measurements	1	1	
Frame Packing (ms)	20	20	
G.711 Payload Type	PCMU 64000 PCMA 64000	-	PCMA 64000 – Europe Only
Base RTP Port	0	0	
Use PLC	No	-	
Silence Suppression	No	No	
Single Receiving Port	Yes	Yes	
Measure CPU	No	No	
Full Duplex Session	Yes	Yes	
Jitter Buffer	Use	Use	Max Depth = 60ms, Initial Playout Delay = 40ms. see Jitter Buffer Description
Packet Latency Tolerance (ms)	3000	3000	

Generating calls

The number of simultaneous full-duplex voice calls generated on the same connection can be generated in one of two modes:

1. Incremental number of calls - Generates a range of calls according to the values provided for the following variables:
   - Maximum: Maximum number of calls to generate on the same connection
   - Minimum: Minimum number of calls to start with on the same connection
   - Step: Number of calls by which to increment the minimum number per period
2. Fixed number of calls - Generates the specified number of calls

Calls need to be generated to estimate the available bandwidth and level of call traffic a particular link can withstand before the voice quality degrades to a point where users can notice. In the preliminary evaluation phase, the incriminated number of calls mode is used to identify the maximum number of calls a test point pair can handle. Then comprehensive evaluation is conducted using the fixed number of calls corroborating the estimates identified during the preliminary evaluation phase by checking call performance over a long period of time.

Jitter buffer description

For payload type G.711 and G.729, use the following values for these two parameters:

- Jitter Buffer Maximum Depth = 60ms
- Initial Playout Delay = 40ms

Network measurement criteria

Assuming that jitter and packet loss are not an issue, the one parameter left that affects the voice and conversation quality is end-to-end delay. From ITU-T recommendations (and practical experience), the end-to-end delay for a voice call should not exceed 150ms. The characteristics of the end devices such as the gateway (Ethernet and TDM bridge in the SX-200 ICP) and the IP phones are known.

In assessing a network, consider the network limits shown in the following table.

Table 24: Network Limits

	Packet loss	Jitter	End-to-end delay	Ping delay
Go!	<1%	<30 ms	<50 ms	<100 ms
Caution	<5%	<60 ms	<80 ms	<160 ms
Stop!	>5%	>60 ms	>80 ms	>160 ms

‘Ping’ delay is the value obtained from using a PC ping utility. The ping utility sends a message from one PC to a second PC. When the second PC receives the message, it sends a message back to the first PC. The first PC determines the propagation delay encountered on the network between the two PCs. Typically in a network, the send and receive paths have equal delays. Estimate jitter estimated by using ping over a short and longer-term period. Estimate packet loss by using ping over a longer period (24 hours or more). Networks that are used for both voice and data can have variations in the amount of network delay. For instance, if computer backup utilities run on a regularly scheduled basis, network delay can increase. Perform longer-period delay measurements over a time period that represents the customer's core operational hours.

Other tools, such as network analyzers, can also be used to determine packet loss. Many analyzers look for VoIP and RTP packets, and can identify when a packet is missing as well as average jitter.

Although ‘Ping’ can be used as a quick check, or as a backup method, it is recommended that networks be fully evaluated before installation. Mitel Customer Engineering Services can perform a full VoIP network pre-installation evaluation.

Determining bandwidth requirements

Things to consider when calculating bandwidth requirements are:

- Level of call traffic (more phone calls means more bandwidth)
- Bandwidth required for speech connections
- Bandwidth required for signaling

In general, the level of call traffic defines the number of Erlangs (busy channels) and hence, the number of “channels”. As a simple rule of thumb, add 10% to the voice bandwidth to ensure adequate signaling bandwidth. In practice, the signaling is needed only to set up a call and clear it down. The signaling messages are also sent via TCP and acknowledged. Some delay is, therefore, tolerated, unlike voice.

For the TFTP server connection, a minimum of 5 Mbits/s should be available to ensure adequate response with 700 phones. The rate can be scaled depending on the number of phones requiring a download, although with a large number of controllers it may be beneficial to include a number of servers. It is advisable to provide a local TFTP server at a remote site, if, for example, the WAN link is limited to 1.5 Mbits/s.

What is wire bandwidth? This is what you pay for (all bits and timing delays put onto the wire).

How is this different from IP (data payload) bandwidth? IP is a number of layers removed from the real connection. It encapsulates the data with routing and address information. It is the basis on which other protocols are then added—such as Frame Relay or Ethernet—to physically move the data around. Each of these protocols adds its own overhead on top of the fixed IP bandwidth. See the section “Configuring network priority” on page 109 for more detail on the frame breakdown for Ethernet. Compare IP bandwidth in the table below with the real wire bandwidth requirements.

What is the signaling bandwidth? The level of signaling is dependent upon call traffic. If there are no phones calls being set up, then signaling is low (less than 1%). However, setting up a call uses both voice and signaling bandwidth. In practice, adding 10% to the voice bandwidth for signaling has been found to be a good ‘rule of thumb’ with sufficient margin.

The following table shows typical wire data rates for different protocols and LAN/WAN interfaces. Note, for example, that a half-duplex link uses twice the bandwidth on the connection than a similar, full-duplex connection for the same voice connections. This is because the half-duplex connection is shared with other devices and the repeater on the link retransmits data received on the receive path for all other devices to hear (it exists on the transmit and receive cable pairs at the same time).

Use full-duplex wherever possible (requires point-to-point connections) in a switched environment, rather than hubs.

As the table shows, the physical wire bandwidth required by an IP phone is usually:

- G.711 (about 100 kbits/s)
- G.729 (about 40 kbits/s)

Table 25: Wire Data Rates

Data Type	LAN Usage at 10 Mbit/s	IP Data Payload	Voice Data Rate (End-to-End)	Voice Streaming at Physical Connection
IP phone (G.711) signaling	burst 0.2%	80 kbits - 800 kbits		
G.711 IP phone 20 ms (LAN - half duplex: hub)	2%	80 kbits/s	64 kbits/s	193.6 kbits/s
G.711 IP phone 20 ms (LAN - full duplex: switched)	1%	80 kbits/s	64 kbits/s	96.8 kbits/s
G.729 IP phone 20 ms (LAN - half duplex: hub)	0.8%	24 kbits/s	8 kbits/s	81.6 kbits/s
G.729 IP phone 20 ms (LAN - full duplex: switched)	0.4%	24 kbits/s	8 kbits/s	38 kbits/s
G.711 IP phone 20 ms (WAN - IP over FR (Layer 2 PVC))	Dependent upon WAN link rate	80 kbits/s	64 kbits/s	94 kbits/s
G.729 IP phone 20 ms (WAN - IP over FR (Layer 2 PVC))	Dependent upon WAN link rate	24 kbits/s	8 kbits/s	40.8 kbits/s
G.711 IP phone 20 ms (WAN - PPP)	Dependent upon WAN link rate	80 kbits/s	64 kbits/s	84 kbits/s
G.729 IP phone 20 ms (WAN - PPP)	Dependent upon WAN link rate	24 kbits/s	8 kbits/s	28 kbits/s
G.711 IP phone 20 ms (WAN - compressed PPP)	Dependent upon WAN link rate	65.2 kbits/s	64 kbits/s	68 kbits/s
G.729 IP phone 20 ms (WAN - compressed PPP)	Dependent upon WAN link rate	9.2 kbits/s	8 kbits/s	12 kbits/s

Selecting a CODEC

The selection of the CODEC to use on a particular connection depends on a number of issues, including:

- Voice quality expected by the user
- Available bandwidth, especially on a WAN link
- The number of devices on a link, and how many are active based on traffic (see the section “Traffic” on page 140).

The voice quality of the CODECs available is usually expressed in terms of a Mean Opinion Score (MOS). The scores range in value from 0 to 5. Anything above 4 is considered toll quality.

The following table shows some typical CODEC MOS scores.

Table 26: CODEC MOS Scores

CODEC type	MOS	LAN bandwidth
G.711	4.4	~100 kbit/s
G.729	4.0	~40 kbit/s

A Mitel IP phone provides both G.711 and G.729a CODEC types.

The G.711 CODEC provides the best voice quality (but at the expense of more bandwidth) and is comparable to TDM-type connections. G.729a provides a good reduction in bandwidth with only minor loss in voice quality. G.711 is used where bandwidth is available, such as in a LAN environment, and G.729a is used in a WAN access environment, where bandwidth is not so readily available. In the SX-200 ICP, the selection of CODEC can be configured through compression zones. Refer to the SX-200 ICP product documentation for more details on the configuration of compression zones.

Place softphones (PC-based), such as YA Pro, on the data VLAN and enable TOS-to-COS conversion (requires L2/L3 switch).

Full duplex and half duplex settings

It is recommended that all LAN connections use Full Duplex settings. This ensures maximum bandwidth and minimum delay. WAN links are typically specified as Full Duplex.

Note: Full Duplex and Half Duplex is often used at the phone to describe the hands-free operation. This has *nothing* to do with the LAN connection. The terms, when used for hands-free operation, refer to whether one party (half a ‘conversation’) can speak or whether it is possible for both parties (full ‘conversation’) to speak at the same time.

Full duplex basics

Even though speech may be half duplex or full duplex to the user, the internal voice codecs are receiving and sending data all the time via the LAN connection.

Each LAN connection includes both a transmit pair of cables as well as a receive pair of cables. In a full duplex *Ethernet* connection, data can be sent and received at the same time.

The transmit and receive pair of connections are *not shared* within the network device (typically a layer 2 switch). Thus, the local phone sends 100kbits/s (G.711) on the transmit pair of cables. It also receives a similar transmission.

As in the case of TDM, both transmit and receive cables are considered a single bundle. Therefore, the device is sending data at 100kbits/s. Of course, without the receive data, it isn’t possible to hold a conversation.

Half duplex basics

With a half duplex *Ethernet* connection, a number of devices can *share* the same data directly. In this case, the network device doesn’t interpret the data, it simply boosts the signal and re-sends it.

To avoid collisions in the shared-data scenario, data that is sent by one device is repeated to all receive pairs of all connected devices. This means that when data is sent, it cannot receive data from another device at the same time; it must wait until the next available time. The phone still continues to send 100kbits/s (G.711) of data, but must wait to receive the returned

100kbits/s. In effect, the phone still sends the same data as a phone connected with a full duplex connection, it simply takes twice as long to send and receive data.

Summary

- A conversation requires equal amounts of data to be transmitted and received.
- The phone always sends and receives the same amount of data via a full- or half-duplex link.
- Full Duplex *Ethernet* connection: Data can be transmitted and received at the same time.
- Half Duplex *Ethernet* connection: Data can only be transmitted or received at separate times, and taking twice as long to complete.
- Half Duplex connections are a less efficient means to transmit voice. Time delay is added and bandwidth is not conserved very well using collision avoidance mechanisms.
- It appears as though a phone connected via a half duplex link takes up more bandwidth, but in reality it takes up more time.

Conclusion: Use full duplex Ethernet connections for maximum performance. Configure any SX-200 ICP network port for auto-negotiation so that the network devices can select the best quality settings.

Determining available bandwidth

The advertised rate for a particular link is the speed at which the data travels; it is not necessarily the available data rate. In practice, a percentage of this bandwidth is lost due to communication between end devices because the data is asynchronous and requires certain guard bands. In a synchronous telecom link these issues are resolved through mechanisms such as framing data into fixed timeslots. The following table contains some simple guidelines for LAN and WAN links.

Table 27: LAN and WAN Link Guidelines

Data connection type	Percentage of bandwidth available	Example
LAN – 10BaseT Half Duplex	40%	10 Mbits/s => 4 Mbits/s available
LAN – 10BaseT Full Duplex	80%	10 Mbits/s => 8 Mbits/s available
LAN – 100BaseT Half Duplex	40%	100 Mbits/s => 40 Mbits/s available
LAN – 100BaseT Full Duplex	80%	100 Mbits/s => 80 Mbits/s available
WAN – 1.5 Mbits/s Frame Relay without QoS mechanism in router	40%	1.5 Mbits/s => 600 kbits/s available
WAN – 1.5 Mbits/s Frame Relay with QoS mechanism in Router	70%	1.5 Mbits/s => 1.05 Mbits/s available

LAN

The following table contains some simple guidelines for LAN connections (assuming that all the available bandwidth is used for voice traffic only).

Table 28: LAN Connection Guidelines

Cable Capacity	Bandwidth	Phone Usage at G.711	Voice Channels G.711	Voice Channels G.729 (x 2.5)
10BaseT Half Duplex	40%	2%	20	50
10BaseT Full Duplex	80%	1%	80	200
100BaseT Half Duplex	40%	0.2%	200	500
100BaseT Full Duplex	80%	0.1%	800	2000

“LAN Connection Guidelines” reflects the maximum usable bandwidth based on the physical connection. Other factors in the network must also be considered including:

- The percentage of data traffic shared with the voice on a common connection.
- The percentage of broadcast traffic. A ‘flatter’ LAN will result in more traffic.
- The percentage of data traffic allowed in the egress queues even under congestion.
- The uplink from a switch may be blocking in terms of possible data input, for example, a 1Gbits/s uplink may not be enough for a 24 port switch running 100Mbits/s on each input link.
- The switch backplane may not handle the data throughput in terms of available bandwidth and packet per second rate.

The “LAN Connection Guidelines” table also shows the maximum capability of a LAN link assuming that the link is used purely for voice traffic. If the link is shared with other devices, such as PCs, then some priority mechanism is required to ensure that the voice gets the available bandwidth when needed. Also, in a busy network with multiple broadcasts, the available bandwidth is reduced by this percentage. For example, in a network with 10% broadcast traffic (at 10 Mbits/s), the 40% available bandwidth is reduced to 30% for a half-duplex link, and the number of voice channels is reduced accordingly.

The ratio from half-duplex to full-duplex is four (not two) because conversations need both a talk path and a listen path. For half-duplex, both paths share the same physical wire; for full duplex, both send and receive can occur simultaneously on different wire pairs.

For half-duplex, the channel availability is 10M x 40% / (2 x 100k) = 20 channels. Only 40% of the bandwidth is available due to collisions and collision avoidance mechanisms. For full-duplex connections, there are no collisions, so usage can double to 80%. Also, there are separate paths for send and receive data, so only half the connection bandwidth is used. Thus 10M x 80% / (1 x100k) = 80 channels.

WAN

A WAN link is generally point to point between routers and, therefore, is always a full-duplex link. The link speed for access WAN connections is also slower, which means the number of available voice channels is reduced.

The following table shows the number of voice channels that a 1.5 Mbits/s link supports.

Table 29: Voice Channels Supported by a 1.5 Mbit/s Link

Cable Capacity	Bandwidth %	Voice Channels G.711	Voice Channels G.729 (x 2.5)
1.5 Mbits/s without QoS mechanism	40%	6	15
1.5 Mbits/s with QoS mechanism	70%	10	26

When a WAN link is shared with other data devices, there are other considerations, including the introduction of waiting delay. The end device sees this as jitter, resulting in potential packet loss, and the user experiences degraded voice quality.

Calculations for the number of voice channels are based purely on exclusive use of the link bandwidth for voice. In reality other factors similar to those of the LAN connection also come into play. This becomes much more acute with much slower WAN links.

The queueing technique and weightings to the COS or TOS value become important. For instance, the use of Expedite Queuing will give better advantage to voice traffic than the simple Weighted Round Robin technique, which allows even a small percentage of lower priority traffic under congestion.

Also, consider that if the CIR (Committed Information Rate) is based exclusively on the voice requirements, additional data above this limit will be marked for “Eligible Discard”. This applies to all packets including voice traffic.

Serialization delay

Serialization delay is due to the fact that data is queued in a particular device, but cannot be sent because another packet is currently being sent. In a fast link, such as in the LAN, the delay is fairly small (a few milliseconds) and is easily resolved with the end-device jitter buffer.

However, in a WAN access connection, the data rate is not as high as within the LAN. In this case, the waiting delay increases as the data rate reduces. If a particularly large packet (for example, 1500 bytes) is being sent, then other devices must wait until it has gone before they can gain access.

The IP phone and gateway devices are capable of handling delay variations up to a limit of 30ms. An ideal limit is 20ms. The following figure shows waiting delay against link speed, as well as against maximum transmission units (MTU). The value for MTU can be programmed in routers so that packets with a payload greater than this number can be reduced in size. The graph shows that when a packet of 1500 bytes is sent, a data-rate of about 700 kbits/s is needed on the WAN link in order to meet the ideal 20 ms limit.

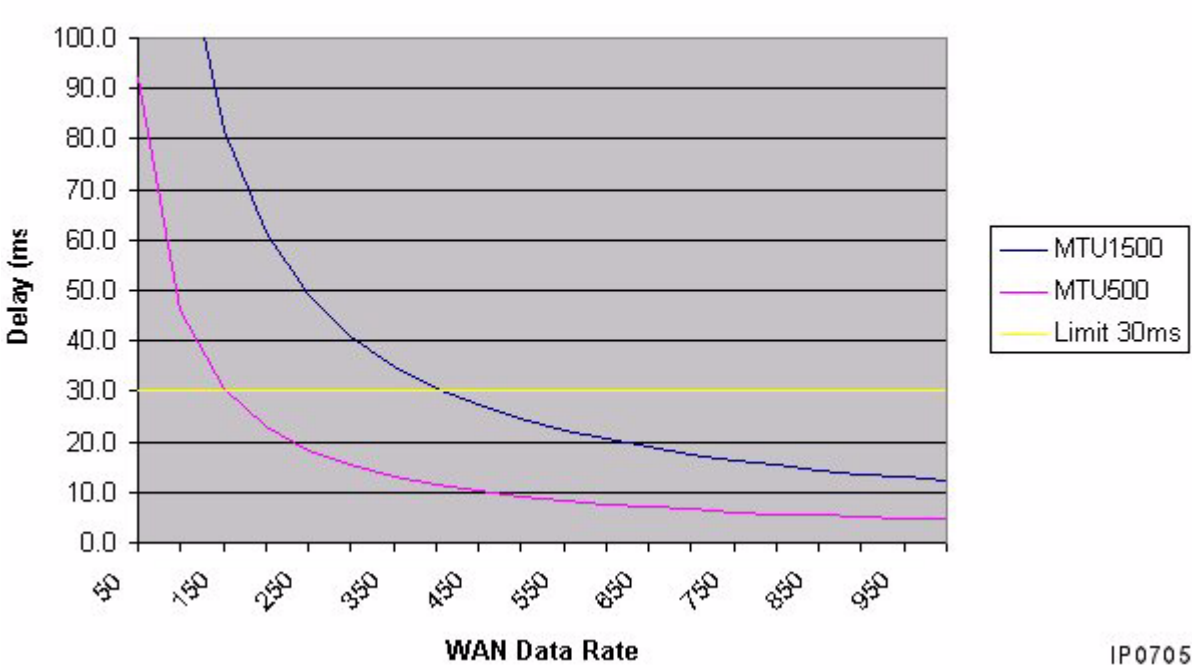


Figure 16: Serialization Delay Frame Relay

By modifying the router MTU value to approximately 500, larger packets are divided up and sent in smaller chunks. The result of this is that there are three times as many opportunities to send the voice data. Thus the data rate link could be reduced to 300 kbits/s.

Note: Some routers do not function with an MTU as low as 500. Internet specifications, for a reduced packet, suggest a lower value for MTU of 576.

Some packets may not allow MTU to cut them down (video can be one of these). The router with the lower MTU might reject these packets, effectively denying access. Also, packets where encryption is used with particular block sizes may also fail to go through a low-MTU connection.

Although the data rates above are minimum recommendations, slower speeds can be used. However, these involve links with strict control of priority queuing and may involve physical restrictions, such as available for PC or phone but not both simultaneously.

For slower links, the recommendation is to reduce the MTU in the routers/gateways to provide more opportunity for voice traffic. A value of 576 has been found to work well.

Configuring network priority

There are two areas where priority mechanisms operate in the network to ensure that voice traffic maintains high priority:

- Layer 2 in the LAN through use of IEEE 802.1p/Q
- Layer 3 in the WAN through use of DiffServ/TOS/Precedence

Caution: If a PC is introduced into the same subnet as the IP phones, whether it is behind a phone or even connected to a Layer 2 device within the subnet, the Quality of Service cannot be guaranteed without the use of VLAN and careful network engineering. VLAN should be used when phones and PC co-exist on the same network infrastructure. TOS or DiffServ should also be used on WAN connections where data and voice share a common connection.

The following figure highlights an Ethernet packet format, and the location of the Layer 2 Priority and Layer 3 Priority fields. This view is of a tagged frame, since it included IEEE 802.1p/Q information.

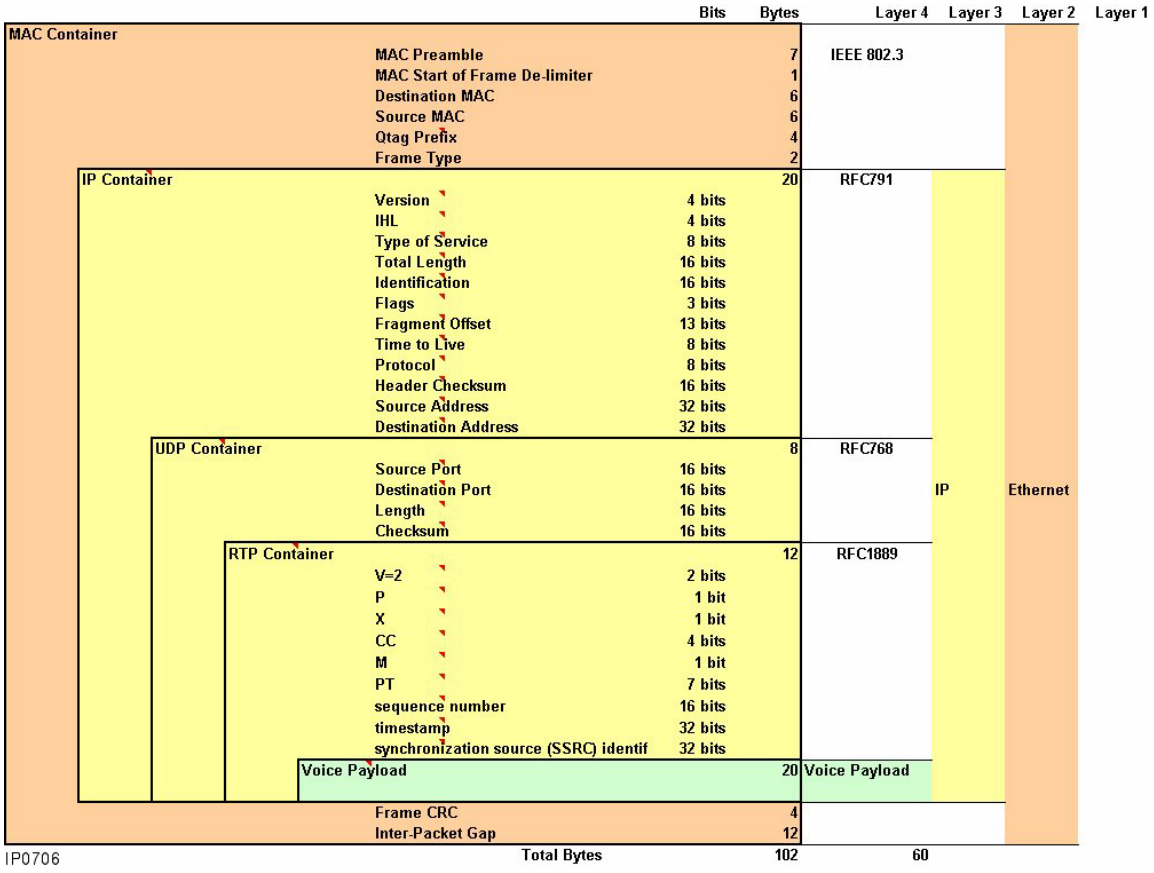


Figure 17: Ethernet Packet Format

LAN Layer 2 priority

The priority mechanism used relies on that described in IEEE 802.1P. This is a subsection of IEEE 802.1Q also known as VLAN tagging.

IEEE 802.1P (Layer 2 priority) uses a field in the IEEE 802.1Q tag to provide eight levels of priority. IEEE 802.1Q is the open VLAN standard that extends the Ethernet header by adding an additional 4 bytes to tagged packets. Because the 802.1P priority is part of the VLAN header,

ports that need to convey multiple VLANs/802.1P priorities must use tagging. This includes ports used between LAN switches and ports connected to dual-port phones.

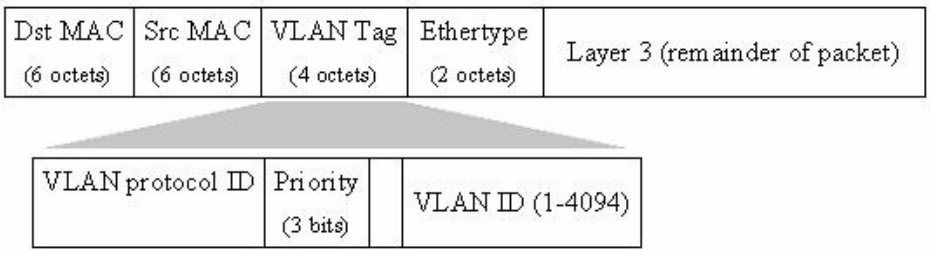


Figure 18: 802.1Q VLAN Tag

With dual-port phones, it is important to configure the LAN switch to use tagging for the voice VLAN and no tagging for the default VLAN, to ensure that voice packets are properly prioritized over data applications from the PC.

One potential issue is the different ways in which these specifications have been interpreted. A number of switches on the market provide VLAN capability, but these may not use all of the sections specified in 802.1Q. The method of configuring the switch ports can also differ.

The main requirements are

- Ports should be configurable to provide VLAN tagging to incoming untagged information and remove this tagging when passing out of the switch. This is used by the controller and associated applications.
- Ports should be configurable to pass all active VLANs with tagging from one switch to another (there is no untagged information present in the connection). This is used between LAN switches and maintains priority information between units.
- Ports should be configurable to accept untagged information, to pass this on to a specified VLAN, as well as to accept tagged information. On egress, the port strips off tagging for data from a specific VLAN, but does not strip data from other VLANs. This is used when connecting the dual-port phones and PCs to the network, so that tagged data goes to the phone and untagged data to the PC.

Some other VLAN guidelines for use with voice are:

- Additional bandwidth is always good.
- Use full-duplex wherever possible.
- Don’t use VLAN 0.
- Set Priority to value 6 for voice.
- Set Priority for untagged VLAN/native VLAN/default_vlan to 0.
- Because Hubs don’t support priority queuing, use managed Layer 2 switches with 802.1p/Q support.
- Don’t use VLAN 1000 and above with Cisco products.

Cisco port examples

The following data is collected from the command line interface (serial connection).

- Dual mode/trunk
  - This mode allows untagged information to be placed onto a specific VLAN as well as passing VLAN tagged data for other VLAN. This configuration is used to connect to a dual-port phone with an attached PC (no VLAN).

    >switchport trunk encapsulation dot1q
    >switchport trunk native vlan 193
    >switchport mode trunk
    >spanning-tree portfast

  - This configuration is for the dual-port phones. The port provides VLAN tagging through the first command line, and the encapsulation type is to IEEE 802.1Q (dot1Q). Cisco also supports a similar scheme of priority with ISL encapsulation, but this is proprietary and does not operate with other vendor equipment.
  - The port is configured so that untagged information is directed to (native) VLAN193.
  - The port is considered a trunk because it handles multiple VLAN connections.
  - The last command indicates that this port is not closed down during spanning tree operations.The network engineer must ensure that there are no network loops behind this connection. This command is used when connecting to a server or to the main controller. This setting may change depending on E911 emergency requirements.
- Access port/non-VLAN-aware device
  - This interface does not accept VLAN-tagged information, but adds tagging information to data between the access port and VLAN712 (the voice VLAN). This is used for the SX-200 ICP controller, or for an application such as Mitel 6500 Speech Server.

    >interface FastEthernet0/19
    >switchport access vlan 712
    >spanning-tree portfast

  - Other commands allow the individual port priority to be specified. In the case of the access port, the encapsulation method is specified elsewhere.
  - While the IEEE specification allows for VLANs from 0 to 4095, not all vendors support this range. As a general rule, VLAN 0 is treated in different ways by different vendors. The recommendation is **not** to use VLAN 0. Cisco also reserves VLAN 1000 and upward for Cisco purposes, so these are also not recommended for use.
- Multi-VLAN port
  - Cisco devices provide this as another port configuration. However, on some of the access switches it is not possible to use multi-VLAN ports and trunk ports on the same unit. Unfortunately, the multi-VLAN port type is needed in order to work with other vendor products. A trunk port can be used, but it also removes tagging from the configured native VLAN, which may not be what is required. An example is a port configured with the native_VLAN to 1. On ingress, tagging is added, but on egress it is removed. Tagging information should be maintained through the network, only being modified at the access points. Removing tagging between switches is not desirable. There are two possible ways out of this situation:

  a. Run ISL between the two units (but then they both need to be Cisco).

or

a. Create a dummy native_VLAN that is not used anywhere else in the network to ensure compatibility with other vendor units and allow products to be mixed. The dummy VLAN does not carry data since there are no end devices configured with this VLAN. This effectively turns the trunk port into a multi-VLAN port for the desired VLAN connections.

HP port examples

The HP switch uses a similar RS232 connection, but the user interface is more menu-driven making the configuration more intuitive. The following figure shows a typical screen display.

```
Actions->   Back     Add     Edit     Delete     Help
Port     DEFAULT_VLAN  voice_vlan    video_vlan    test4
-----  + ------------  ------------  ------------  ------------
  1    | Untagged      Tagged        No            No
  2    | Untagged      Tagged        No            No
  3    | Untagged      Tagged        No            No
  4    | Untagged      Tagged        No            No
  5    | Tagged        Tagged        Tagged        No
  6    | No            No            No            Untagged
  7    | No            Untagged      No            No
  8    | Untagged      No            No            No
  9    | Untagged      No            No            No
  10   | Tagged        Tagged        No            No
  11   | Untagged      No            No            No
  12   | No            Untagged      No            No
                                                   IP0707
```

Figure 19: HP Screen Display Example

The default_vlan is VLAN1. The VLAN numbers are assigned names to help follow which function is assigned to which VLAN. The voice_vlan is VLAN2, the video_vlan is VLAN3, and test4 is VLAN4. The default VLAN is used by the data devices and also by the IP phones when they first start up and look for their correct VLAN configuration. (See the section “Start-up sequence for phones” on page 145.)

The IP devices connected to the port examples above are

- Ports 1 though 4: Dual-port phones with PCs.
- Port 5: Interconnected network switches (only tagged data allowed within network).
- Port 6: Not used with this application. Untagged data on this link goes to VLAN4 only.
- Port 7: SX-200 ICP controller, or similar voice applications such as a Mitel Speech Server (formerly Speak@Ease).
- Ports 8 and 9: PCs.
- Port 10: Router with virtual ports (similar to a connection between switches).
- Port 11: Router port that physically separates VLANs (the data VLAN).
- Port 12: Router port that physically separates VLANs (the voice VLAN).

Note: Using VLAN 0 with HP is not recommended. However, it is possible to extend VLAN numbering up to a maximum of 4095.

More details on configuring different HP network switches can be found in *HP ProCurve Networking IP Telephony Solution Design Guide* and *HP ProCurve Networking IP Telephony Solution Implementation Guide* on Mitel OnLine.

WAN Layer 3 priority

A number of different WAN technologies provide data routing with different priorities and service level agreements (SLA). Most of these deal with the WAN technology, but most rely on information being presented in the Layer 3 Type-of-Service (TOS) field.

The Type-of-Service field has undergone some name and function changes. This field is now also known as Differentiated Services or DiffServ. The DiffServ uses the precedence and some of the TOS bits (TOS instead of Type of Service field) to provide 64 different services. See Figure 17 on page 110 for the location of the Type-of-Service field.

The SX-200 ICP controller and IP phones use the Type-of-Service format for priority and TOS. This complies with RFC791, but also by choice of value, RFC1122 and RFC1349.

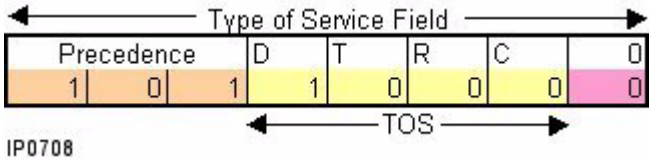


Figure 20: Type-of-Service Field Using Precedence

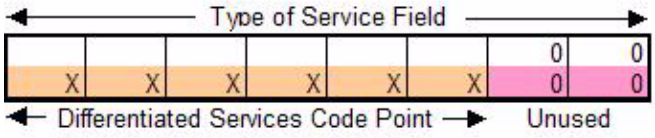


Figure 21: Differentiated Services Code Point in the Type-of-Service Field (newer definition)

The precedence field is similar in operation to the IEEE 802.1P field. In fact, many routers offer the capability of mapping between the two schemes. Once a TOS and precedence is chosen, it never changes. Therefore, the voice application sets the appropriate values before data is sent. Mitel voice applications are fixed with a value of 0xB0, or 176 decimal, for the Type-of-Service field, providing a precedence of five with minimum delay (the D-bit is set). Other vendors may use alternative settings.

For DiffServ routers, the fixed value equates to a value of 0x2C, or 44 decimal.

All that is required is that the router support priority queuing mechanisms, such as Weighted Fair Queuing, Class-Based Weighted Fair Queuing (also known as Low Latency Queue, LLQ) or similar.

With a Layer 3 device, such as a router, the packet-per-second (PPS) throughput is also important. With an IP phone the frame rate is every 20 ms, meaning that the phone sends 50

packets per second and also receives 50 packets per second. Be aware of how vendors specify the PPS rating. For example, with two phones connected to a router, each port sends and receives 50 PPS—that is, 100 PPS per port, requiring that 200 PPS be handled. However, between the phones, only 50 PPS goes one way and 50 PPS in the return direction. Therefore, throughput is 100 PPS. In the following figure, the router has a handling capacity of 15,000 PPS. Throughput is half this number.

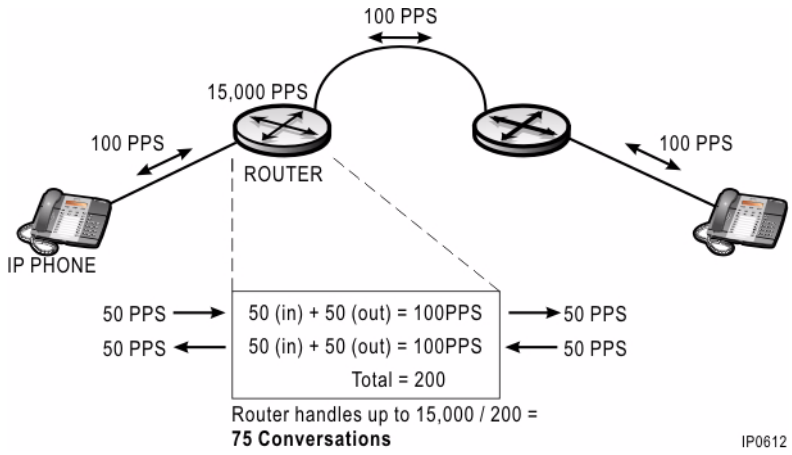


Figure 22: Packet-per-second Throughput Example

Network topology with priority

The following network diagram highlights the use of the dual-port phones and the configuration of a network including VLAN priority and also the use of DiffServ/TOS in the WAN connection.Network topology with priority

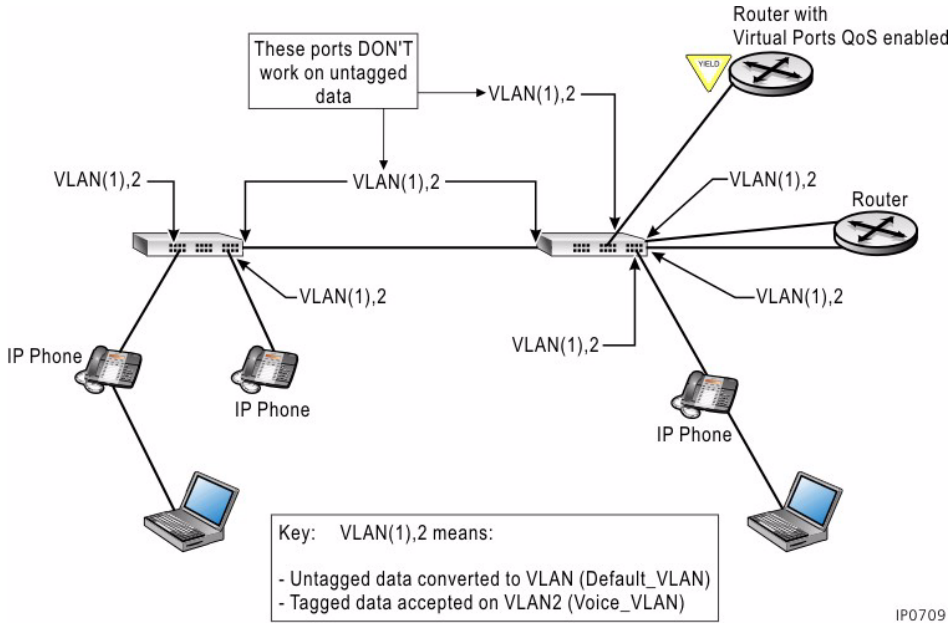


Figure 23: Network topology with priority

In Figure , the network switch ports connected to the dual-port phones must be able to accept both untagged and tagged information. The untagged data is translated to a data VLAN (1). In this case, VLAN1 is also the default or native VLAN. The voice is destined for a voice VLAN (2). In the outgoing direction, these ports must also pass information from the voice VLAN still tagged, but traffic from the data VLAN must be sent untagged for the devices that are not able to handle VLAN information.

The requirement to use VLAN and priority queuing becomes obvious when both data and voice information must share a link between units within the network. It is important that the deterministic voice information gets priority over the non-deterministic data traffic. This is where IEEE 802.1P comes into play (IEEE 802.1P is a subset of IEEE 802.1Q).

Routers or Layer 3 switches involved in segmenting the network also need connections to the different VLANs. Each VLAN is identified by a VLAN number, but also by the unique subnet address. In this way, the routers and Layer 3 switches that are unaware of VLAN can still pass data between the VLANs. A separate physical connection to each VLAN must exist, and the ports on the Layer 2 switch must pass information only to and from one specific VLAN. At the Layer 2 port, the VLAN information is removed on egress and added on ingress according to the port or VLAN configurations.

Some routers are VLAN-aware and are considered to include a virtual Layer 2 switch within the unit, which then directs data according to the VLAN information. These devices are often referred to as including virtual ports. Their advantage is that only one physical connection is required to handle multiple VLANs.

TOS-to-COS (IEEE 802.1P) mapping

In a converged environment with both voice and data traffic on the network, some form of priority mechanism should be used. If a voice device is resident on a data device, it may not be possible to separate the traffic to independent network interfaces. In this case it is likely that both voice and data appear from the same IP address and within the same subnet.

Often the PC does not support VLAN, although it may support priority. Be careful with this setting, since the VLAN tagging is added and the VLAN0 is used. Different vendors treat VLAN0 in different ways. If operation cannot be determined it is better to treat the PC as non-VLAN aware and let the Layer 2 switch tag this with the Default or Native VLAN settings.

For non-VLAN-aware PCs, the only form of priority identification is from within the voice application. The Type-of-Service field is set by this application on the PC. To get the correct VLAN priority, configure the access port in the network to map this Type-of-Service (TOS) information to a VLAN priority (COS). Voice is still on the same subnet (and native/default VLAN) as the data, but where priority schemes exist, the voice is treated ahead of data.

Note: COS is Class Of Service (IEEE 802.1P), not to be confused with the telecom Class of Service value.

On certain combined Layer 2 and Layer 3 switches, the ports may prioritize data based on either COS or TOS/Diffserv data. This may also force a change (unexpectedly) in the COS to TOS mapping information based on internal mapping rules. Usually these can be reconfigured as necessary.

The COS values run from 0 to 7. Typically ‘7’ is the highest value, ‘0’ the lowest. However, newer standards and switches define a COS ‘2’ as ‘best effort’ with ‘0’ and ‘1’ as lower. Also, the default setting on some switches might place COS ‘5’ into the expedite queue, potentially giving this higher priority than ‘6’ and ‘7’. It is advisable to check these settings on the switch to ensure correct and expected operation.

Use of subnets

Creating a flat network appears to speed up transactions due to the high link speed, but Layer-3 switches are hardware-oriented, and perform equally as well as their Layer 2 counterparts.

In the Layer 2 switch environment, data can be addressed directly to a specific port, thereby reducing loading on links not used. However, if the Layer 2 devices cannot identify an address or port location to use, additional protocols are needed to get the information. The additional protocols broadcast data to every port and device, causing the loading on the network to be almost back to that of a shared environment. The Layer 2 devices maintain a list of addresses and port locations in internal memory. If the memory and list is small, the level of broadcasts can also increase, since new information is rapidly aged out of the list.

Therefore, a large flat network can potentially grind to halt, not because of genuine traffic loading, but simply due to the amount of broadcast traffic that is required. Using subnets helps by segmenting broadcast domains. The Layer 2 devices subsequently need to hold less information, and so broadcast less often.

Smaller subnets are therefore preferable to reduce the level of broadcast traffic within a particular network domain.

Including Layer 3 devices improves speed within communities of interest and the overall network, and reduces the burden on the system to all broadcast traffic. It is also a requirement for VLANs to operate correctly and provide the voice priority that is required when using dual-port phones.

Enhanced Network Functionality: VMPS, CDP, and Location Change Indication

Caution:SX-200 ICP Release 2.0 enhanced Mitel IP Phones to be compatible with Cisco Discovery Protocol (CDP), so phones can detect voice VLAN information. Configuration of the access ports to the IP phones could potentially be different from settings prior to Release 2.0.

Note that the following descriptions apply to an installation where the network is shared with both voice and data, and where the network is separate from the SX-200 ICP. Such an installation would be expected with the MX controller. These settings would also apply to a smaller installation where the CX/CXi is not the primary network switch. Where the CX/CXi is the primary network switch, it is unlikely that VMPS and hence, CDP, will be encountered, and so these advance settings may not be necessary.

Enhancements in Mitel IP Phones in Release 2.0 and higher include:

- Support of dual-port IP phone operation in the presence of Cisco VLAN Membership Policy Server (VMPS) security and dynamic VLAN configuration. Single-port IP phone operation is possible with VMPS prior to Release 2.0 (described in following sections).
- Voice VLAN configuration via CDP.

As a side effect of some of these settings, the **portfast** setting will operate as expected, because on trunk ports 'portfast' is ignored. Another added benefit is the reduction in the number of VLANs present at the port and, hence, a reduction in broadcast traffic to the end devices (IP phones).

Note: You can still use the older port settings for new installations or following an upgrade, but it is strongly recommended that you use the new port settings if the system is connected to Cisco access equipment.

These enhancements and access network port configurations are described in the sections below. The following table highlights the features and their availability at different product releases:

Table 30: Enhanced Network Functionality

Product Release	Phone Operation Mode	Voice VLAN Configuration with CDP	Operation with VMPS
Pre Release 2.0	Single Port	Not available	Yes (altered DHCP setting)
	Dual Port	Not available	No
Release 2.0 and higher	Single Port	Yes	Yes
	Dual Port	Yes	Yes

The individual functions of VLAN and VMPS are described in the sections below. Single port IP phone operation, with VMPS, prior to Release 2.0, requires some changes to the network port and DHCP settings that are different from previous guidelines, which used the double DHCP fetch mechanism.

The network port configuration examples shown in the following sections are based on the Cisco3550 Layer 2/3 switch. Network configuration principles are also described, as the actual commands may differ between network switches, vendors, and software version installed.

Executive summary

CDP and VMPS

- If CDPv2 is not running in the network, then functionality is the same as it was prior to 2.0.
- If CDPv2 is running and the auxiliary VLAN is Null, then functionality is the same as it was prior to 2.0.
- For a new installation, where CDP is enabled, the Auxiliary VLAN should be used.

- CDP can run independent of VMPS.
- To use dual port phone functionality when using VMPS then CDPv2 with the auxiliary VLAN set must be used.

Network QoS settings in a Cisco environment

A number of higher-end Cisco switches have the capability to monitor both Layer 2 and Layer 3 QoS settings at ingress. They can also modify either of these settings based on the other setting, as well as changing values, if necessary. Good understanding of these settings is needed if correct operation is to result throughout the network. To simplify the installation and use some pre-packaged commands, such as **auto-qos**, a COS value of 5 is recommended throughout the network. Other values, such as 6, can still be used, but will require additional tuning of the configuration at different ports.

In order to make the QoS settings work, the following points need to be considered:

- QoS must be enabled for the entire switch.
- The default COS and DSCP settings of the switch may not be those needed for voice.
- Settings that are needed include:
  - Change mapping COS 5 to DSCP of 46 (Expedited Forwarding (EF) setting).
  - Ensure that COS 5 is mapped to the EF queue.
  - Enable the EF queue.
  - Trust incoming ports based on COS value for end points, phones, SX-200 ICP and voice servers.
  - (PC phones may require DSCP remapping as well as DSCP to COS conversion).
  - Enable CDP.
- **Auto-qos trust** will change a number of these settings.
- Some additional tuning may be needed to the settings to get full operation.

SX-200 ICP network port settings

Where the SX-200 ICP is connected to a separate network, it is basically a voice server. The network port should be set accordingly, and is required to provide the following functions:

- Adding 802.1 Q-Tagging and priority (COS) to incoming data (ingress)
- Remove 802.1 Q-Tagging and priority (COS) to outgoing data (egress)
- Provide access to a single fixed VLAN
- The network Layer 2 port should be configured to **portfast** or without Spanning Tree Protocol

A typical port configuration example, for the SX-200 ICP, is shown:

```
Switch# configure terminal
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport mode access
```

```
Switch(config-if)#  switchport access vlan 2
Switch(config-if)# mls qos trust cos
Switch(config-if)# mls qos cos 5
Switch(config-if)# wrr-queue cos-map 4 5
Switch(config-if)# priority-queue out
Switch(config-if)# spanning-tree portfast
Switch(config-if)#  end
Switch#
```

Applications and other voice servers

There are a number of other applications that reside on dedicated voice servers. An example might be Speak@Ease or voice mail. Within call control, these devices register as phones. However, the network connections of these devices are not capable of supporting VLANs directly, or having multiple devices on the same LAN connection.

Thus, the network configuration for an application server should be configured as an access port with the Native VLAN set to apply tagging (802.1Q) to the voice VLAN. Where there is only a single connection to the server, STP should be turned off or configured to '**portfast**', if practical.

Mitel IP Phone

With the SX-200 ICP Release 2.0 and higher, a number of enhancements have been included within Mitel IP Phones. The network functions and required network port settings are described in the sections below. It should be noted that the example configuration commands might differ where multiple functions are required at a particular port.

The migration of the network port settings, in line with the upgrade of system software revisions, is covered in "Migration of network port settings from prior to post Release 2.0" on page 129.

Mitel IP Phone enhancements from Release 2.0

Prior to Release 2.0, the Mitel IP Phones would obtain VLAN information dynamically using a double DHCP fetch mechanism. With Release 2.0 and higher, this information can also be obtained via CDP when using CDPv2 compliant devices, such as Cisco Layer 2 switches. In the port configuration example shown below, the voice VLAN is on VLAN2 and the default/data VLAN is on VLAN100. The phone starts on VLAN100 (untagged), obtains information from DHCP and switches to VLAN2 (tagged), where it obtains a local IP address again from DHCP.

Prior to Release 2.0, only limited operation with VMPS was possible, requiring different network configurations and DHCP information (details are given in a later section). Generally, this meant that phones and PCs could not share the same network port, when VMPS is active. With Release 2.0 and higher, it is now possible for CDP to allow both phones and PCs to share the same network port with VMPS.

Be aware that some of the Layer 2/Layer 3 switches have the ability to map COS to TOS and vice versa as well as overwriting values. Care should be exercised in using QoS settings to ensure that the correct values continue throughout the network. This may also require adjustment of the mappings. Some Layer 2 access switches are unaware of Layer 3 QoS settings, and so some commands will be unavailable.

The original double DHCP fetch mechanism still works and remains the same, unless the customer requires a change.

An example of a Mitel IP Phone port configuration follows:

```
Switch# configure terminal
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport trunk native vlan 100
Switch(config-if)# mls qos trust cos
Switch(config-if)# mls qos cos 0
Switch(config-if)# wrr-queue cos-map 4 5
Switch(config-if)# priority-queue out
Switch(config-if)# switchport trunk allowed vlan remove 3
Switch(config-if)# spanning-tree portfast
Switch(config-if)# end
Switch#
```

This set of commands carries out the following, in order of sequence:

- The port is configured as a trunk, capable of handling all VLAN on the switch or in the network.
- The trunk protocol to use is 802.1Q framing (Ethernet frame type 8100).
- Trunk ports can direct untagged information to a particular VLAN; in this case, to VLAN 100.
- The port will trust the priority information presented in any VLAN tagged frames and leave any DSCP settings unmodified (may not be available on Layer 2 only switches).
- The default priority for COS is 0, which will be assigned to untagged traffic.
- The Expedite Forwarding queue (Q4) is enabled with a COS value of 5.
- This is an optional command and removes VLAN3 from the allowed list of the trunk connections to the port. This reduces traffic (multiple broadcasts, etc.) from this port by removing all unnecessary VLANs.
- This allows Spanning Tree Messages through, but will not disconnect the port during the learning phases of this protocol. Only possible with an end device with a single network connection.

VLAN/CDP network port configurations (Release 2.0+)

Prior to Release 2.0, Mitel IP Phones discovered VLAN information dynamically through DHCP. This operation is still present, but with Release 2.0 and higher, the Mitel IP Phones now have the capability of using CDP to discover VLAN information.

If not manually programmed, the Mitel IP Phones will continue to use DHCP to locate VLAN and Priority information if any of the following conditions are true:

- CDPv2 is not present on the switch
- CDP is disabled
- The Auxiliary_VLAN, or Voice VLAN, information is clear, or NULL. (A VLAN ID of '0' is not a NULL value.)

Caution: When the phones are used in Dual Port mode, if VMPS is used, then CDP must also be used.

There are certain network configurations and settings that will allow a single IP phone to be used with VMPS, without CDP, although this is not expected to be the normal mode of operation. This is described under the VMPS section.

In SX-200 ICP Release 2.0 and higher, Mitel IP Phone messages are compatible with CDP, so the phones are able to determine additional VLAN information required to direct them to a voice VLAN. There are now three potential methods to include information into the IP phones; these being, in priority order:

1. Manual Entry at boot time.
2. CDP.
3. DHCP.

The ability to provide partial information at each stage now allows these three modes to be used together to ease installation. For example, the IP phone's IP address may be supplied manually, but the RTC address could be picked up via DHCP. Also, CDP does not provide priority (COS) information, so the VLAN could be picked up from CDP, but the priority (COS) provided by DHCP.

Note: Default Priority with CDP: Where CDP provides the VLAN information, Layer 2 priority (802.1P), or COS, information is not provided and so the IP phone will default to a priority value, or COS, of 5. In this case, the phones will be compatible with Layer 2 settings that might also be employed by Cisco IP Phones. This will ease some installations allowing certain textbook examples to be used. For a **Cisco environment**, many installations are using a **COS value of 5**, although with other vendor equipment, a value of 6 is still preferred. DHCP can be used to override this default COS value, allowing CDP to provide the VLAN information. This is an important network QoS change introduced at Release 2.0.

Table 31: VLAN Priority Information

VLAN Information	Priority Information (location)	Priority (802.1 P)/COS Value
Manual Entry	Manual, DHCP	0-6
CDP	Default	5
CDP	DHCP	0-6
DHCP	DHCP	0-6

In order to obtain VLAN information via CDP, some network port settings need to change. The ideal settings are

- Set the network port as **Access** (this can be static, or set to dynamic for use with VMPS).
- Enter the Voice VLAN, or the Auxiliary_VLAN, setting.
- Enter the data, or default, VLAN into the Native_VLAN setting (note that this value can change if VMPS is active).
- In DHCP, there is no requirement to enter VLAN or Priority into the default/data VLAN (during upgrade to 2.0, this setting may still be needed).
- Set the Priority field to ‘6’ in the voice VLAN scope of DHCP

The commands required to change the network port settings are:

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 100
Switch(config-if)# mls qos trust cos
Switch(config-if)# mls qos cos 0
Switch(config-if)# wrr-queue cos-map 4 5
Switch(config-if)# priority-queue out
Switch(config-if)# switchport voice vlan 2
Switch(config-if)# spanning-tree portfast
Switch(config-if)# end
Switch#
```

The above set of commands carries out the following, in order of sequence:

1. The port is configured as a static access port.
2. Untagged data is sent to VLAN 100.

3. The port will trust the priority information presented in any VLAN tagged frames and pass through any Diffserv settings unmodified.
4. The default priority for COS is 0, which will be assigned to untagged traffic.
5. The Expedite Forwarding queue (Q4) is enabled with a COS value of 5.
6. The Voice VLAN, or Auxiliary_VLAN, is set for VLAN2.
7. Spanning Tree Messages are allowed through but will not disconnect the port during the learning phases of this protocol.

On some network switches the Voice VLAN is identified through the Auxiliary_VLAN command of '**set port auxiliaryvlan 0/1 2**'. This sets port 0/1 to VLANID 2 for voice traffic.

VLAN Membership Policy Server (VMPS)

VLAN Membership Policy Server (VMPS) provides two main features when installed and operational. These are

- Security Checking
- Automatic assignment of VLAN for untagged traffic.

Since a network port can have only a single untagged to tagged VLAN mapping, VMPS is typically used to identify a single attached device to the appropriate VLAN. Multiple devices with different VLAN requirements will cause the switch port to shuttle between settings, with resulting poor operation. A phone and PC would normally be such a combination. IP phone messaging compatibility with CDP overcomes this limitation. Thus, an IP phone that is compatible with the Auxiliary_VLAN setting in CDP can be used with another attached device, such as a PC. An IP phone that cannot determine the Auxiliary_VLAN setting will be treated as a single end device, and require an entry in the VMPS database.

When the VMPS (Server) is enabled, a MAC address to VLAN mapping database is downloaded from a TFTP server and VMPS begins to accept client (access switch) requests. When a valid request from a client is received, the VMPS searches through the database for a MAC address to VLAN mapping. The VMPS will then instruct the client how to configure the port for access and also which VLAN to enable.

Access can be restricted to certain ports, as well as denied for certain MAC addresses (such as a known attacker). In either of these cases, the ports can also be configured to simply deny access, or can be physically shut down. Re-enabling a shutdown port, **no shutdown,** requires configuration access to the network switch of the affected port, for example, via the serial interface or Telnet.

A '**fallback**' VLAN can also be defined for devices that are unknown, but that may be granted limited access, for example, to a guest VLAN. Access to the remainder of the network will then be controlled through the VLAN router.

Table 32: VLAN Membership Policy Server (VMPS)

Recognized Device	Allowed Access	Fallback VLAN Defined	Secure Settings	Action
Yes	Yes	N/A	N/A	Send dynamic VLAN
Unknown	Unknown	Yes	N/A	Fallback VLAN (guest)
		No	vmps mode open	Access denied
		No	vmps mode secure	Port shutdown
Yes	No	N/A	vmps mode open	Access denied
		N/A	vmps mode secure	Port shutdown

Some other rules that apply to configuration of VMPS include:

- **A dynamic port can belong to only one VLAN** (that is, one device per port, or common group of devices per port. Note: The number of attached devices differs per switch product.)
- The VMPS must be configured *before* the access ports are enabled as dynamic.
- When a port is configured as dynamic, spanning-tree Portfast is enabled automatically for that port. Automatic enabling of spanning tree Portfast prevents applications on the host from timing out and entering loops caused by incorrect configurations. You *can* disable spanning-tree PortFast mode on a dynamic port, but it is not recommended.
- If a port is reconfigured from a static port to a dynamic port on the same VLAN, the port connects immediately to that VLAN. However, VMPS checks the legality of the specific host on the dynamic port after a certain period, and may disconnect if not valid.
- Static secure ports cannot become dynamic ports. Security on the static, secure port must be turned off before it can become dynamic.
- Trunk ports cannot become dynamic ports. Trunks must be turned into access ports before being changed from static to dynamic in order to work with VMPS.
- A port that enters the ‘shutdown’ state blocks *all* access. This includes a connected IP phone, if the attaching PC is not accepted.
- The VTP management domain of the VMPS client and the VMPS server must be the same.
- When a link is active and validated it may remain open for some time. This can be changed through the ‘**vmps reconfirm**’ interval command. This defaults to 60 minutes, but may need to be reduced for tighter security. A network port setting, confirmed for a PC behind an IP phone, will remain in effect for this interval, even if the PC is disconnected. To clear the port settings, the IP phone must reset the link status, by being reset or temporarily disconnected, for example.

VMPS and network switch software revisions

Only certain network switches can be used as VMPS servers. Typically, these are the higher end ‘core’ switches such as the 4000 and 6000 series. A number of other network switches can be a VMPS client. VMPS Server software is also available for Windows and Linux server platforms.

A number of network switches will support VMPS and also Auxiliary_VLAN (or voice VLAN) for the IP phone. However, it has been found with some ‘access’ switches that these two functions may not be available at the same time, so *either* but *not both* functions can be provided. Examples of these network switches include the 2900XL and 3524/48XL devices.

Two different operating system families are present in the Cisco network switches, hence the apparent multiple entries in the revision list: This is current information but may change with future Cisco releases.

Table 33: VMPS Server and Client Support

Network Switch	VMPS Server Support	VMPS Client Support
Catalyst 4000 Family (CatOS)	Yes (7.2 (x) and later)	Yes (all software releases)
Catalyst 4000/4500 (IOS)	Not currently supported	Yes (12.1(13) EW and later)
Catalyst 2900XL/3500XL	Not supported	Yes (11.2(8) SA4 and later, Enterprise Software Edition
Catalyst 2950/2955/3550	Not supported	Yes (all software releases)
Catalyst 2948G-L3 Catalyst 4908G-L3	Not supported	Not supported
Catalyst 5000/5500 Family	Yes (2.3.x and later)	Yes (2.3.x and later)
Catalyst 6000/6500 Family (CatOS)	Yes (6.2(2) and later)	Yes (all software releases)
Catalyst 6000/6500 Family (IOS)	Not currently supported	Not currently supported

Use of VMPS with ICP prior to Release 2.0

Message compatibility with CDP support was introduced in the Mitel IP Phones in the Release 2.0 time frame. This compatibility allows the IP phones to operate in dual port mode with an attached PC, using VMPS. However, prior to this release, it is possible to use VMPS, but this requires careful consideration in terms of port settings and entries into the DHCP server.

Note: CDP can also be turned off at a port. The IP phones cannot operate as dual port devices with VMPS in this situation. Therefore, CDP must be enabled to use VMPS and an attached PC.

Since VMPS adjusts the Native_VLAN setting dynamically, it can only do this for ***one*** VLAN, typically associated with ***one*** connected device. Prior to Release 2.0, all Mitel IP Phones are unaware of CDP Auxiliary_VLAN settings. Thus, Mitel IP Phones prior to this release cannot operate as a dual port device, such as with a PC.

To use VMPS with a Mitel IP Phone prior to Release 2.0 requires the following network settings:

- Only one physical device (IP phone) can be connected to a network port configured to use VMPS.
- The DHCP server should not identify the VLAN or Priority (effectively making the phones run untagged) in the voice VLAN scope.
- Default VLAN and priority is not needed in DHCP, as the network port will be configured via VMPS.
- The Layer 2 switch port should be configured with the **dynamic VLAN** setting.
- The Layer 2 switch port should be set up as an **access port.**
- The Layer 2 switch port should be set to add **priority** at **value 6** (backward compatible with other Mitel IP Phones). Other values may also be chosen.
- The MAC address of the IP phones should be identified in the VMPS server and the voice VLAN to use. (The range of ports within this VLAN can also be configured, providing restricted access and movement for the phones.)
- Once authorized, the VMPS will configure the value of the Native_VLAN setting to that of the voice VLAN. The network switch port will add the tagging and priority rather than the IP phone. A DHCP-request will not return VLAN information, and the phone will only do a single IP address fetch.

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan dynamic
Switch(config-if)# mls qos trust cos
Switch(config-if)# mls qos cos 5
Switch(config-if)# wrr-queue cos-map 4 5
Switch(config-if)# priority-queue out
Switch(config-if)# spanning-tree portfast
Switch(config-if)# end
Switch#
```

Note: Once a port is configured for dynamic VLAN that it automatically has spanning-tree configured as '**portfast**'.

Use of VMPS with SX-200 ICP Release 2.0 and upwards

With the SX-200 ICP Release 2.0 and higher, Mitel IP Phone messaging is compatible with CDP, so the phones can determine additional VLAN information required to direct them to a voice VLAN through use of the Auxiliary_VLAN method. This means that the Native_VLAN setting is available for use via VMPS. In effect, the two settings run in parallel.

Since there are now two methods, or paths, to gain access through the network port, both an IP phone and a PC can be attached to the same network port. The PC will use the Native_VLAN configuration through VMPS, and the IP phone will use the Auxiliary_VLAN configuration. The auxiliary VLAN is also known as the voice VLAN on certain network switches. This method also reduces the level of broadcast traffic that might also be present on a port configured as a trunk.

VMPS allows the following settings and actions to be carried out at a Layer 2 switch port:

- It can dynamically adjust the Native_VLAN setting of the port.
- It can allow or deny access to a device based on MAC address.
- It can allow access to unrecognized devices, but to a restricted VLAN, such as guest, and apply router restrictions between VLANs.
- It can shut a port down, requiring manual intervention to bring the port back.
- It can specifically deny access to certain recognized devices. Most unknown devices might go to a guest VLAN, but certain rogue devices will be specifically blocked. In this mode, the port may be set to simply deny access, or to shut the port down.

Shutting down a port is a good way to restrict access, but it will also affect the operation of the phone, or any other device, attached to this port.

Caution: This could be considered a form of denial of service. Simply plugging in a rogue PC to a number of network ports could disable access to legitimate users. Be careful to select the appropriate settings.

With Release 2.0 and higher, the Mitel IP Phone will obtain the VLAN information via CDP, if available. In this case, the phone will not need to use the double fetch method via DHCP. In this case, the first DHCP request will be on the voice VLAN with tagged frames.

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan dynamic
Switch(config-if)# switchport voice vlan 2
Switch(config-if)# mls qos trust cos
Switch(config-if)# mls qos cos 5
Switch(config-if)# wrr-queue cos-map 4 5
Switch(config-if)# priority-queue out
Switch(config-if)# spanning-tree portfast
Switch(config-if)# end
Switch#
```

Migration of network port settings from prior to post Release 2.0

With Release 2.0 and higher of the SX-200 ICP, Mitel IP Phone messages are compatible with CDP, so the phones are able to detect VLAN information. A system being upgraded to this software release from a prior version will have different functionality, and potentially different network settings. This may require some network changes. However, if new functions such as VMPS are not being implemented, the changes are minimal.

If VLAN information is not available via CDP, then the Mitel IP Phones will use DHCP to obtain this information. This VLAN information may be made unavailable, in CDP, if it is not programmed via 'voice VLAN' or Auxiliary_VLAN settings. CDP can also be turned off with the '**no cdp run**' command. This setting is *not recommended* for IP phones because other information such as power provisioning is also passed via CDP. Power provisioning is covered in CDPv1 and may also be available on network switches other than Cisco. If CDP is disabled then ensure that power can be provisioned through another method, such as 802.3af.

If the voice VLAN, or Auxiliary_VLAN, is programmed on the network switch then it *must* be programmed with the voice VLAN. The IP phone will take this information, if available.

If the voice VLAN is not programmed and the port is configured with the settings prior to Release 2.0, then the **trunk** setting will allow all tagged frames to pass, except those specifically excluded. In this case, the Mitel IP Phones will not get information via CDP and will continue to use DHCP as before.

If the voice VLAN, or Auxiliary_VLAN, is programmed, then the IP phones will pick up this information and immediately tag the outgoing information for the voice VLAN. Since the trunks allow all tagged frames to pass, then the IP phone will obtain access to the correct VLAN. In this situation, it is not necessary to program the VLAN and Priority information into the default/data scope for DHCP. However, it might still be necessary to program the priority information in the voice VLAN scope to override the default setting obtained through use of CDP.

Thus the Mitel IP Phones will continue to work with the previous network settings. However, with the inclusion of CDP it is possible to change the ports to **access** rather than **trunk**. This provides additional benefit in reducing the level of broadcast information on this connection. When **pvst** (per VLAN Spanning Tree) is enabled, as needed for location move identification, setting the port for **access** also reduces the level of information sent on this port.

Table 34: Network Port, DHCP and VLAN Settings on Release 2.0

Release	Port Settings	VLAN via CDP	IP Phone VLAN	Native_VLAN use	DHCP default scope	DHCP voice scope
Prior 2.0	Trunk	No	Obtained via DHCP default scope	PC and IP Phone	VLAN (required), Priority (required)	VLAN (optional), Priority (optional)
Post 2.0	Trunk	No	Obtained via DHCP default scope	PC and IP Phone	VLAN (required), Priority (required)	VLAN (optional), Priority (optional)
						Page 1 of 2

Table 34: Network Port, DHCP and VLAN Settings on Release 2.0 (continued)

Release	Port Settings	VLAN via CDP	IP Phone VLAN	Native_VLAN use	DHCP default scope	DHCP voice scope
Post 2.0	Trunk	Yes - Voice	Obtained via CDP	PC only	VLAN (optional), Priority (optional)	Priority (optional)
Post 2.0	Access - Static	Yes - Voice	Obtained via CDP	PC only	VLAN (optional), Priority (optional)	Priority (optional)
Post 2.0	Access - Dynamic	Yes - Voice	Obtained via CDP	PC only (configured via VMPS)	Dynamic via VMPS. Entries for IP phone not possible.	Priority (optional)
						Page 2 of 2

Following an upgrade of the system software:

- the initial boot load in Mitel IP Phones will not recognize CDP and will attempt to obtain VLAN information via DHCP.

  In this case, the port needs to continue to operate as a trunk *or* the Auxiliary_VLAN must be programmed. The phone will then obtain information from the DHCP default/data scope and register with the SX-200 ICP on the voice VLAN. At this point the phone will upgrade and reboot. Following reboot, the Mitel IP Phone will then be able to recognize CDP and use this information.

- it is prudent to check the priority settings in DHCP.

  If DHCP is still used, then DHCP settings likely do not need to be adjusted. However, where CDP is used, then the DHCP priority option may no longer be needed. Typically, the Access Layer 2 network switches only have two priority queues and COS 5 and 6 go into the same queue. However, the DSCP value on the uplink from these L2 switches may still be 44. The core switch, therefore, needs to change DSCP 44 to 46, or use the COS 5 value to map the DSCP to 46.

NetBIOS and PC settings

The NetBIOS protocol can rapidly fill a network with broadcasts and background traffic, reducing available bandwidth to other applications, including voice.

NetBIOS types include:

- B-node: Uses broadcasts to resolve names.
- P-node: Uses point-to-point communications with a NetBIOS server (such as a WINS server) to resolve names.
- M-node: Uses broadcasts first (B-node), then directed name queries (P-node) if broadcasts are not successful.
- H-node: Uses name queries first (P-node), then broadcasts (B-node) if the name server is unavailable or if the name is not registered in the WINS database.

Use H-node to reduce the level of broadcast traffic in a network.

Determine the settings at the command prompt using the command ipconfig /all.

For further details, go to:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winxppro/reskit/prjj_ipa_zrjq.asp

Fax and modem connections over IP

Under normal circumstances, do not consider Fax over IP without appropriate interfaces to provide signal redundancy and error correction. The two most prominent protocols allow a standard T.30 fax to be connected over IP using either T.37 or T.38 protocols. These are generally point-to-point connections and provide a means of toll bypass. Fax within a pure IP environment makes little financial sense, considering that e-mail is far less sensitive to timing and clock issues, and generally uses an error-correcting IP protocol to ensure delivery.

The T.37 protocol is store and forward, and is equivalent to sending a fax through an e-mail service. This method of transport is now being superceded by T.38, which is more real-time.

The SX-200 ICP does not currently support internal T.37 or T.38 gateways. External gateways can be connected to ONS and LS ports for TDM switching to the PSTN.

However, the controllers can handle IP trunk forwarding between controller units (also called G.711 cut-through). In effect, the fax data modulated signals are passed as voice across the IP network. For this reason, compression cannot be used on these signals. Fax machines are also sensitive to time delays and error rates. Typically, fax machines are designed to run over TDM links. A lost IP packet can contain a significant quantity of data.

Within the PSTN, echo cancellers will be disabled if tone detectors within the PSTN detect a FAX calling tone (2100 Hz).

The controllers, however, do not support this functionality. As a result, if an analog FAX machine is connected directly to an ONS or LS port on the controller so that the data can be transported to another controller via IP trunk forwarding, the controller will not disable the internal echo canceller. The presence of an echo canceller will impede the ability of the FAX machine to establish a full duplex connection and the FAX machine may need to resort to establishing the connection in half duplex mode.

FAX and modem performance guidelines

Due to the many variables involved in sending fax data over IP trunks, there is no guarantee for reliable transport. However, practical experience has shown that with some careful network considerations such a link can be made to work. These considerations include

- The IP trunk link must use G.711 only.
- The error rate on the link must be below 0.1%.
- The link delay must be below 200 ms.
- Jitter must be less than 30 ms (ideally less than 20 ms).

WARNING: Modem signals require a special connection setup to be sent over an IP network. There are a number of proposed standards for modem over IP, but these have yet to be ratified. It is, therefore, not recommended to send modem signals over an IP network at the present time.

Wireless phone performance on the SX-200 ICP

SpectraLink wireless phones

Mitel has partnered with SpectraLink to provide wireless IP phone connectivity to Mitel's SX-200-ICP.

The SpectraLink e340 h340 and i640 Wireless Telephones, which are IEEE 802.11b (WI-FI) compliant, support Mitel's MiNet signaling protocol.

The SpectraLink e340, h340 and i640 phones do not use a unique device type. These phones register with the IPC as Mitel 5220 IP phones.

Equipment involved

Integrating a SpectraLink wireless network into a Mitel VoIP network requires the following building blocks:

- SpectraLink wireless phones, e340, h340 and i640 devices
- A Wireless Access Point (AP). This is the gateway between the wireless LAN and the regular LAN.
- A SpectraLink Voice Priority Server (SVP). The SVP server ensures that voice packets receive priority over data packets on the wireless LAN.
- A DHCP server for the SpectraLink phones (which can be the ICP)
- A TFTP server for the SpectraLink phones (which, by default, will be the ICP)
- A TFTP server for the SVP server (which, by default, will be the ICP).

Wireless LAN considerations

An IEEE 802.11b wireless LAN, like a regular LAN can provide connectivity to both voice and data users. Voice and data devices have different requirements for QoS and, as a result, place different demands on the LAN infrastructure.This is true of both wired and wireless LANs.

For wired LANs, these different requirements for voice and data are well understood and are covered elsewhere in this document and must be taken into consideration when designing a wired or wireless LAN.

However, due to the nature of wireless LANs, there are additional issues which are unique to wireless LANs that must be taken into consideration when designing a wireless LAN. These issues are best addressed by consulting the appropriate wireless phone documentation.

Detailed information regarding SpectraLink equipment, network engineering guidelines and numerous discussion papers can be found on the SpectraLink world wide web site, the URL is http://www.spectralink.com/service/manuals.html.

Additional information can be found on the Mitel On Line Web Site, under "Solutions" and then under "Wireless".

Coverage and capacity

The APs provide the radio frequency (RF) link to the wireless phone sets, each AP will have a limitation on the number of wireless phone sets and wireless PCs that the AP can support due to site-specific issues such as RF coverage areas, bandwidth limitations and user expectations.

When designed correctly, the wireless LAN will ensure:

- QoS for wireless phone users
- Fair LAN access for wireless PC users
- Reliability and functionality that meet the customer's needs.

The SpectraLink system does not support roaming across subnets. This means that a SpectraLink phone will not maintain a call in progress when the user roams into a different subnet. Once a user has entered a new subnet, that user will need to re-initialize the SpectraLink phone before call can be made.

Connectivity to the wired LAN

To ensure adequate bandwidth and eliminate collisions, connections from SpectraLink equipment into the wired LAN should be made with Ethernet switches rather than Ethernet hubs. Auto-negotiation should be enabled on the Ethernet switch ports so that the Ethernet switch can take advantage of the highest speed interfaces available on SpectraLink/DECT equipment. Category-5 cable should be used to make the connection between the Ethernet switch and SpectraLink/DECT equipment.

Other considerations

Depending on the particular installation, the following topics may need to be considered:

- E-911 is not supported on wireless phones, users should not place 911 calls from these phones or the database entry should be entered manually to point to the default building entrance point.
- Transmission of data and voice over an RF link presents potential security issues that system administrators and users should be aware of. For example, it is recommended that encryption be enabled.

- Electro-Magnetic Interference generated by wireless phones and PCs might need to be considered in sensitive environments such as health care facilities, research laboratories and some industrial sites since this interference could affect the operation of critical equipment in the facility.
- Likewise, Electro-Magnetic Susceptibility needs to be considered since reception on the wireless phones may be affected by other RF devices, such as microwave ovens and certain portable phones. A site survey is strongly recommended.

IP ports

The table below shows the IP port numbers used with the SX-200 ICP. It is not a definitive list, but is sufficient to identify voice connectivity. New features and applications may result in additions to this list.

Although the list can be used to open up access across a firewall, where a firewall and NAT are used (for example, at the internet), there might be issues with simply opening up ports from a functional and security viewpoint. For more details, see the sections “Firewalls and NAT” on page 164 and “Teleworker” on page 165.

Table 35: TCP/UDP IP Port Numbers used by SX-200 ICP

IP port number	Transport	Function
53	UDP	DNS
67	UDP	DHCP Server
68	UDP	DHCP Client
69	UDP	TFTP
80	TCP	HTTP
443	TCP	HTTPS (SSL)
1066	TCP	X-NET and IP-Networking
1067	TCP	Secure IP Networking (SSL)
2000	TCP	CDE Telnet
3999	TCP	PDA, SAC (5330 Comms)
5000 to 5414	UDP	Voice (Gateway) Pre-release 3.0
6800	TCP	MiNet Server
6801	TCP	Secure MiNet Server (SSL)
6802	TCP	Secure MiNet Server (AES)
6830	TCP	VM CMPS Server
6900	TCP	MiNet Client
7011	TCP	Data Services Server
7012	TCP	My Administrator (CDE GUI)
		Page 1 of 2

Table 35: TCP/UDP IP Port Numbers used by SX-200 ICP (continued)

IP port number	Transport	Function
8000	TCP	MiTAI
8001	TCP	MiTAI (SSL)
9000	UDP	Phone Voice Channel 1
9002	UDP	Phone Voice Channel 2
15373	TCP	ACD Real Time Events
20001	UDP	TFTP
49500 to 49549	TCP	Data Services Connection (Default)
50000 to 50127	UDP	Voice (Gateway) Release 3.0
61320 to 61328	TCP	User Defined (Hotel PMS/Call Log)
		Page 2 of 2

Note: Ports 5000 to 5414 and 6801 are no longer user but are listed for informational purposes only.

Mitel IP Phone

Through the different releases of the SX-200 ICP, a number of different enhancements have been included within the Mitel IP Phones. The different functions and required network port settings are described in the sections below. It should be noted that the example configuration commands may differ where multiple functions are required at a particular port.

The migration of the network port settings, in line with the upgrade of system software revisions, is covered in “Migration of network port settings from prior to post Release 2.0” on page 129.

The Mitel IP phones are compatible with CDP and are able to utilize this information for VLAN and location change discovery (Release 3.0 and later). In order to ensure that these work as expected, it is recommended that ports connected to Mitel IP phones and using CDP have the **cdp timer** and **cdp holdtime** values left at their default values of 60 and 180 seconds respectively. If enabled, **cdp advertise-v2** should be left in the default state.

Mitel IP Phone enhancements from Release 3.0

Prior to release 3.0, the Mitel IP Phones ignored STP messages. Since the IP phone is an end device, there was no requirement for STP to be enabled, so it was configured as **no spanning-tree** or as **portfast**. With release 3.0, the Mitel IP Phones are capable of listening to STP BPDUs (Bridge Protocol Data Unit). This information can be used to identify when a phone has changed location. However, in order to get location change indication, Spanning Tree information must be made available. With Release 3.0, Mitel IP phones can read information from either Spanning Tree or Cisco Discovery Protocol, to identify when a phone has changed location. The selection of the relevant information is made in the Location Change and E911 application associated with the controller.

Prior to release 3.0, the Mitel IP Phones would obtain VLAN information dynamically using a double DHCP fetch mechanism. With release 3.0, this information can also be obtained via CDP when using CDPv2 compliant devices, such as Cisco Layer2 switches. In the port configuration example shown below, the voice VLAN is on VLAN2 and the default/data VLAN is on VLAN100. The phone starts on VLAN100 (untagged), obtains information from DHCP and switches to VLAN2 (tagged), where it obtains a local IP address again from DHCP.

Prior to release 3.0, only limited operation with VMPS was possible, requiring different network configurations and DHCP information (details are given in a later section). Generally, this meant that phones and PCs could not share the same network port. With release 3.0, it is now possible for CDP to allow both phones and PC to share the same network port.

Be aware that some of the Layer2/Layer3 switches have the ability to map COS to TOS and vice versa as well as overwriting values. Care should be exercised in using QoS settings to ensure that the correct values continue throughout the network. This may also require adjustment of the mappings. Some Layer2 access switches are unaware of Layer3 QoS settings, and so some commands will be unavailable.

The original double DHCP fetch mechanism still works and remains the same, unless the customer requires a change.

An example of a Mitel IP Phone port configuration follows:

```
Switch# configure terminal
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport trunk native vlan 100
Switch(config-if)# mls qos trust cos
Switch(config-if)# mls qos cos 0
Switch(config-if)# wrr-queue cos-map 4 5
Switch(config-if)# priority-queue out
Switch(config-if)# switchport trunk allowed vlan remove 3
Switch(config-if)# spanning-tree portfast
Switch(config-if)# end
Switch#
```

This set of commands carries out the following, in order of sequence:

- The port is configured as a trunk, capable of handling all VLAN on the switch or in the network.
- The trunk protocol to use is 802.1Q framing (Ethernet frame type 8100).

- Trunk ports can direct untagged information to a particular VLAN; in this case, to VLAN 100.
- The port will trust the priority information presented in any VLAN tagged frames and leave any DSCP settings unmodified (may not be available on Layer2 only switches).
- The default priority for COS is 0, which will be assigned to untagged traffic.
- The Expedite Forwarding queue (Q4) is enabled with a COS value of 5.
- This is an optional command and removes VLAN3 from the allowed list of the trunk connections to the port. This reduces traffic (multiple broadcasts, etc.) from this port by removing all unnecessary VLANs.
- This allows Spanning Tree Messages through, but will not disconnect the port during the learning phases of this protocol. Only possible with an end device with a single network connection.

Location change indication

The location change detection is achieved by enabling Spanning Tree Protocol at the network port that the IP phone is connected to. The port can still remain in **portfast** since the phone only has one network connection. One of the three Spanning Tree Protocols should be enabled at the network port and throughout the network. A description of these settings is covered in “SX-200 ICP network port settings” on page 119.

With Release 3.0 and later it is possible for Mitel IP phones to read information from either Spanning Tree or Cisco Discovery Protocol to identify when a phone has changed location. The selection of the relevant information is made in the Location Change and E911 application associated with the controller.

VLAN/CDP network port configurations (Release 3.0+)

With Release 3.0, IP phone location change detection can be accomplished via one of the Spanning Tree Protocols (STP or RSTP) and via the Cisco Discovery Protocol. Furthermore Release 3.0 provides for automatic updating of the CESID data base. For details refer to the section in this document on E911 Network Support and Location Change Indication

Prior to release 3.0, the Mitel IP Phones discovered VLAN information dynamically through DHCP. This operation is still present, but with Release 3.0 the Mitel IP Phone messages are compatible with CDP, so the phones are now able to discover VLAN information via this method also.

If not manually programmed, the Mitel IP Phones will continue to use DHCP to locate VLAN and Priority information if any of the following conditions are true:

- CDPv2 is not present on the switch
- CDP is disabled
- The Auxiliary_VLAN, or Voice VLAN, information is clear, or NULL. (A VLAN ID of ‘0’ is not a NULL value.)

Caution: When the phones are used in Dual Port mode, if VMPS is used, then CDP must also be used.

There are certain network configurations and settings that will allow a single IP-phone to be used with VMPS, without CDP, although this is not expected to be the normal mode of operation. This is described under the VMPS section.

In Release 3.0, the Mitel IP Phone messages are compatible with CDP, so the phones are able to determine the additional VLAN information required to direct them to a voice VLAN. With Release 3.0, VLAN information can also be obtained through LLDP. There are now four potential methods to include information into the IP-phones; these being, in priority order:

1. Manual Entry at boot time
2. LLDP
3. CDP
4. DHCP.

The ability to provide partial information at each stage now allows these modes to be used together to ease installation. For example, the IP phone's IP address may be supplied manually, but the RTC address could be picked up via DHCP. Also, CDP does not provide priority (COS) information, so the VLAN could be picked up from CDP, but the priority (COS) provided by DHCP.

Note: Default Priority with CDP: Where CDP provides the VLAN information, Layer 2 priority (802.1p), or COS, information is not provided. If the VLAN information is provided via CDP then the IP phone will provide a default priority value, or COS, of 5 unless provided by other means, e.g. manual or via DHCP. In this case, the phones will be compatible with Layer 2 settings that might also be employed by Cisco IP Phones. This will ease some installations allowing certain textbook examples to be used. For a Cisco environment many installations are using a COS value of 5, although with other vendor equipment, a value of 6 is still preferred. DHCP can be used to override this default COS value, allowing CDP to provide the VLAN information. This is an important network QoS change introduced at release 3.0.

Table 36: VLAN Priority Information

VLAN Information	Priority Information (location)	Priority (802.1 p)/COS Value
Manual Entry	Manual, DHCP	0-6
LLDP	Manual, LLDP, DHCP	0-6
CDP	Default	5
CDP	DHCP	0-6
DHCP	DHCP	0-6

In order to obtain VLAN information via CDP, some network port settings need to change. The ideal settings are

- Set the network port as **Access** (this can be static, or set to dynamic for use with VMPS).
- Enter the Voice VLAN, or the Auxiliary_VLAN, setting.
- Enter the data, or default, VLAN into the Native_VLAN setting (note that this value can change if VMPS is active).
- In DHCP, there is no requirement to enter VLAN or Priority into the default/data VLAN (during upgrade to 3.0 this setting may still needed).
- If the VLAN information is obtained via CDP and the default priority value of 5 is not to be used, remember to program this value elsewhere, e.g. the Priority field in the voice VLAN scope of DHCP

The commands required to change the network port settings are:

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 100
Switch(config-if)# mls qos trust cos
Switch(config-if)# mls qos cos 0
Switch(config-if)# wrr-queue cos-map 4 5
Switch(config-if)# priority-queue out
Switch(config-if)# switchport voice vlan 2
Switch(config-if)# spanning-tree portfast
Switch(config-if)# end
Switch#
```

The above set of commands carries out the following, in order of sequence:

1. The port is configured as a static access port.
2. Untagged data is sent to VLAN 100.
3. The port will trust the priority information presented in any VLAN tagged frames and pass through any Diffserv settings unmodified.
4. The default priority for COS is 0, which will be assigned to untagged traffic.
5. The Expedite Forwarding queue (Q4) is enabled with a COS value of 5.
6. The Voice VLAN, or Auxiliary_VLAN, is set for VLAN2.
7. Spanning Tree Messages are allowed through but will not disconnect the port during the learning phases of this protocol.

On some network switches the Voice VLAN is identified through the Auxiliary_VLAN command of '**set port auxiliaryvlan 0/1 2**'. This sets port 0/1 to VLANID 2 for voice traffic.

Maintaining availability of connections

This topic refers to the signaling quality of service. It is a measure of how long a user needs to wait before a service becomes available, or whether the user becomes blocked from using a function. Examples of this are delay in receiving dial tone, or blocking that can occur if there are insufficient PSTN trunks.

System capabilities

As the system grows and traffic increases, it has to deal with more tasks, resulting in slower feature interaction. ICP systems are engineered to ensure that with different combinations of devices, services are still maintained within normal working parameters. The exact details are not captured here, but are specific to particular releases, since changes in software or hardware have a bearing on the results.

Traffic

The largest effect on performance and availability is the level of traffic that the units need to handle. A number of areas are affected by traffic:

- Trunks to PSTN
- E2T (Gateway) channels
- DSP channels
- LAN blocking between devices
- WAN blocking between end points.

The traffic guidelines used to calculate system performance are:

- Standard busy office traffic equals 6 CCS (about 6 calls per hour).
- ACD traffic equals 27 CCS (about 27 calls per hour).
- 36 CCS = 1 erlang = 3600 call seconds during the busy hour.
- Traffic is split roughly 65% to and from trunks, with the remainder internal or intercom traffic.
- Traffic blocking is calculated using ErlangB formula.
- Traffic blocking probability for internal/intercom traffic is P.001 (1 in 1000 calls blocked).
- Traffic blocking probability for trunk traffic is P.01 (1 in 100 calls blocked).

You can calculate the amount of TDM traffic that needs to be presented in terms of CCS and match this to a number of trunk channels. With IP, fixed channels do not exist, so this calculation is more complicated.

To calculate the amount of traffic that can be handled over a LAN or WAN link, apply the bandwidth calculations in the section “Determining available bandwidth” on page 106. Use these to work out the number of voice channels and assign a particular CCS rating.

WAN traffic working example

In this example, assume the following configuration:

- 50 IP phones at the corporate centre.
- 10 IP phones over a T1 link at a remote site.
- Trunk traffic is 65% of all traffic.
- Traffic between remotely located IP phones stays local to the remote site (it does not traverse the WAN link).

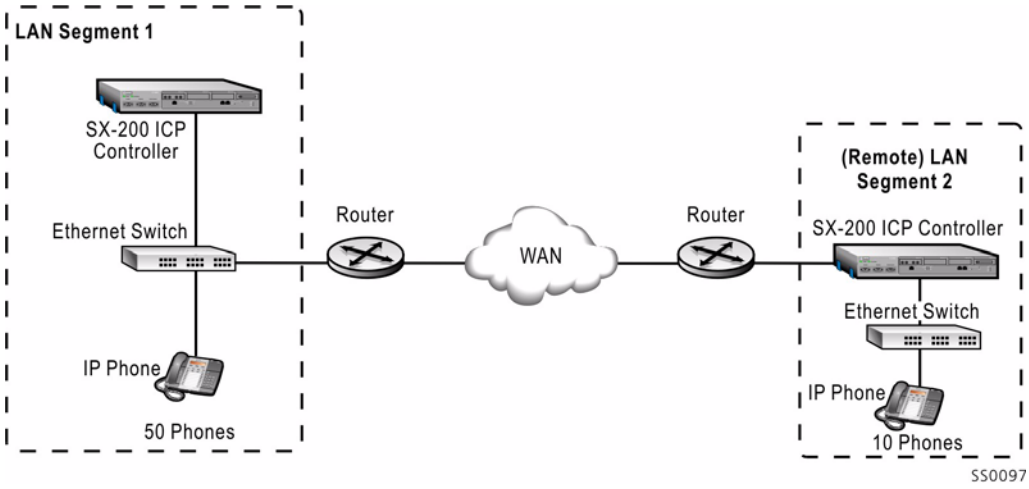


Figure 24: WAN Traffic Example

Table 37: CCS Calculation Example

Calculation	Formula	Result
Remote phones		10
Total CCS at the remote site	Remote phones x 6 CCS	60 CCS
Percentage of trunk traffic	Total CCS x 65%	39 CCS
Percentage of intercom traffic	Total CCS x (100 – trunk traffic)%	21 CCS
Local intercom traffic	Intercom traffic x Ratio of local phones / total phones (21x10/60)	3.5 CCS
Total traffic over the WAN	Total traffic – local traffic	56.5 CCS

Therefore

- The total traffic handled is 60 CCS.
- 3.5 CCS is local traffic.
- WAN traffic is 56.5 CCS = 60–3.5.

A previous calculation showed that a T1 WAN link could handle six G.711 voice channels without QoS enabled. From ErlangB tables with P.001 blocking, such a link can handle 41.1 CCS. Therefore, there is a mismatch between presented traffic and carrying capacity.

Solutions that come from this example can then be covered by:

- Compression (G.729) to the remote phones can be used to increase the voice channel capability. However, it also reduces voice quality, which may not be acceptable.
- The WAN link bandwidth can be increased.
- The blocking ratio can be changed to P.01, and such a link would handle 68.8 CCS.
- The number of remote phones or the overall number of phones can be reduced.
- Ensure that QoS/Priority mechanisms are in place and active.

These are all potential solutions and each has to be investigated to understand the nature of the installation. Doing this calculation before equipment is bought and installed ensures that such issues are highlighted.

Assume that the routers have the capability of prioritizing traffic and the customer does not want to use compression for trunk or internal calls. Thus, all calls will use the G.711 coding scheme. The standard trunk blocking, P.01, is acceptable. The WAN link is over Frame Relay and is a routed VPN (Layer 3).

- ErlangB compensation will be used to estimate the maximum expected number of ‘channels' required to handle the expected peak rate. (An under-provisioned link could result in voice quality degradation.)
- 56.5 CCS results in 6 ‘channels' for voice at P.01 (using standard Erlang Tables).
- 6 ‘channels' at 83 kbits/s requires 499 kbits/s.
- Signaling adds an overhead of 10% taking the total to 550 kbits/s.
- The **CIR for Frame Relay** would be 550 kbits/s or **576 kbits/s**, if rounded to the nearest 64 kbits/s. Rounding down to 512 kbits/s leaves minimum bandwidth during the busy period and may result in slower signaling, and degraded voice, as packets will be marked for discard at the router if the CIR is exceeded.
- Ideally, the link should not be more than 70% utilized so the **bit rate** should be 784 kbits/s, or **832 kbits/s** when rounded to the nearest 64 kbits/s. Since fractional T1/E1 is often based on larger boundaries, it is likely this would be rounded to 1.024Mbits/s.
- The calculations are all based on the expected busy hour call traffic, and CIR is specified to ensure adequate bandwidth is guaranteed during this period should the Frame Relay network also be busy (people tend to make phone calls and answer e-mails at the same time). Other (smaller) values of CIR could be specified, and may well work, but during busy periods the response to features may be slow and voice quality may be affected.

IP networking and use of compression

IP networking allows the construction of larger systems, and the combining of systems in different geographic locations into a single system.

If LAN/WAN connections exist between nodes, this medium can be used to pass traffic. A limit on the number of conversations for this connection is programmed at installation. If the limit is exceeded, an alternative path is tried through ARS, either through a different node connected by IP trunks, or through the PSTN TDM network.

The value of the IP trunk restriction is set for a particular connection. This setting relies very much on traffic and also the bandwidth available.

Since the bandwidth is derived from the number of conversations, it is important to understand which CODEC is used across the link (G.729, G.711, or a combination of both).

Note: In Release 2.0, Music On Hold and message to and from Voice Mail can be handled with G.729, if available.

Also, the level of networking between nodes and whether it includes PSTN trunk traffic or only internal intercom traffic needs to be understood.

As a general guideline, consider that a single node might have a high networking traffic ratio of 15%. For a particular node with a number of devices, the amount of traffic to and from this node remains constant. What differs is the level of traffic destined for another particular node. For example, 15% of traffic might be destined for the second node in a two-node system, but 7.5% is destined for each of the other two nodes in a three-node system. Obviously, in the second scenario, less bandwidth is needed to and from a particular node, but the total per node remains about the same.

Compression operation is determined by a number of factors:

- Are there sufficient resources (for example, are there enough DSP channels available)?
- Have sufficient compression licenses been acquired?
- Can the end device handle compression? Some phones can handle only G.711.
- See the application information to determine whether compression is handled.
- Is compression enabled in the Class-Of-Service options?
- Are the IP trunks (IP networking routes) configured with compression?

IP networking limit working

Consider the following example:

- Two equal-sized systems.
- 250 IP devices/phones.
- Calls from TDM, or to TDM devices including trunks, use G.711 CODEC.
- Calls between IP devices use the G.729 CODEC.
- Traffic is typically 35% (100-65) internal, the remainder to and from PSTN trunks.
- Calls internally are typically 50% outgoing and 50% incoming.
- Traffic is rated at 6 CCS per device.
- Traffic between nodes is 15%.

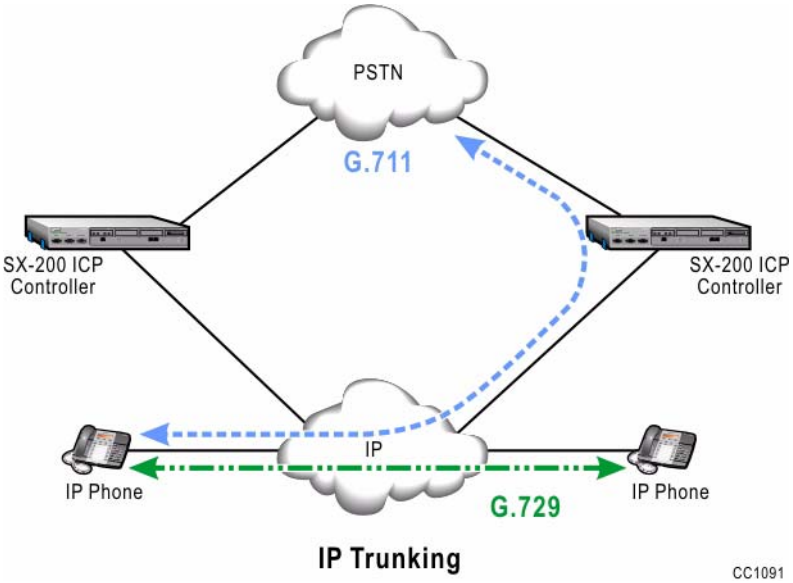


Figure 25: IP Trunk Limit Example

The following table shows the calculations.

Table 38: IP Networking Limit Calculations

Calculation	Formula	Result
Traffic from IP sets	Number of sets (250) x 6 CCS	1500 CCS
Percentage networked	Total traffic x 15%	225 CCS
Percentage traffic intercom	Networked traffic x 35%	79 CCS
Percentage traffic trunk to PSTN	Networked traffic – intercom traffic	146 CCS
Total Number of IP trunk channels needed	ErlangB on total IP trunk traffic (225 CCS)	13 channels (P.01)
Number of channels needed for PSTN trunks (G.711)	ErlangB on PSTN trunk traffic (146 CCS)	10 channels (see note) (P.01)
Number of channels needed for intercom/internal traffic (G.729)	ErlangB on Intercom traffic (79 CCS)	7 channels (see note) (P.01)
Bandwidth needed (use worst case)	Number of G.711 channels (10) x 100k + [Total number of channels (13) – PSTN trunk channels(10)] x 40k	1120 kbits/s
WAN bandwidth required	Assume with QoS so / 70%	1600 kbits/s
Number of channels (IP trunk) for IP networking	Total number of channels	13 Channels

Note:

- Seven channels are needed for internal traffic and ten are needed for external traffic, but together the total is only 13. The reason is that a number of channels have shared use: in this case, it is 4 (10+7-13). The higher G.711 rate is used to ensure adequate bandwidth at all times.
- This data rate is close to a T1 rate. Options are to increase the available link rate by upgrading to an E1 link or to multiple T1 links, or to accept a lower quantity of IP trunk calls (a slight reduction in inter-node traffic).
- The bandwidth calculations should also include signaling and link utilization factors.
- With IP networking, it is possible to restrict the number of conversations on a connection, so although calculations suggest 13 channels, the link settings could be set to only 10 channels to reduce bandwidth usage. ARS will then come into play when this number is exceeded, resulting in the call being routed elsewhere, such as TDM, if possible, or presentation of re-order/busy tone to the user.
- The bandwidth calculation is based on TDM calls not being compressed, which would be the case if compression licensees have not been obtained. If compression licenses are available, then typically IP networking to TDM connections would use compression and less bandwidth. However, the number of ‘channels’ remains the same either way.

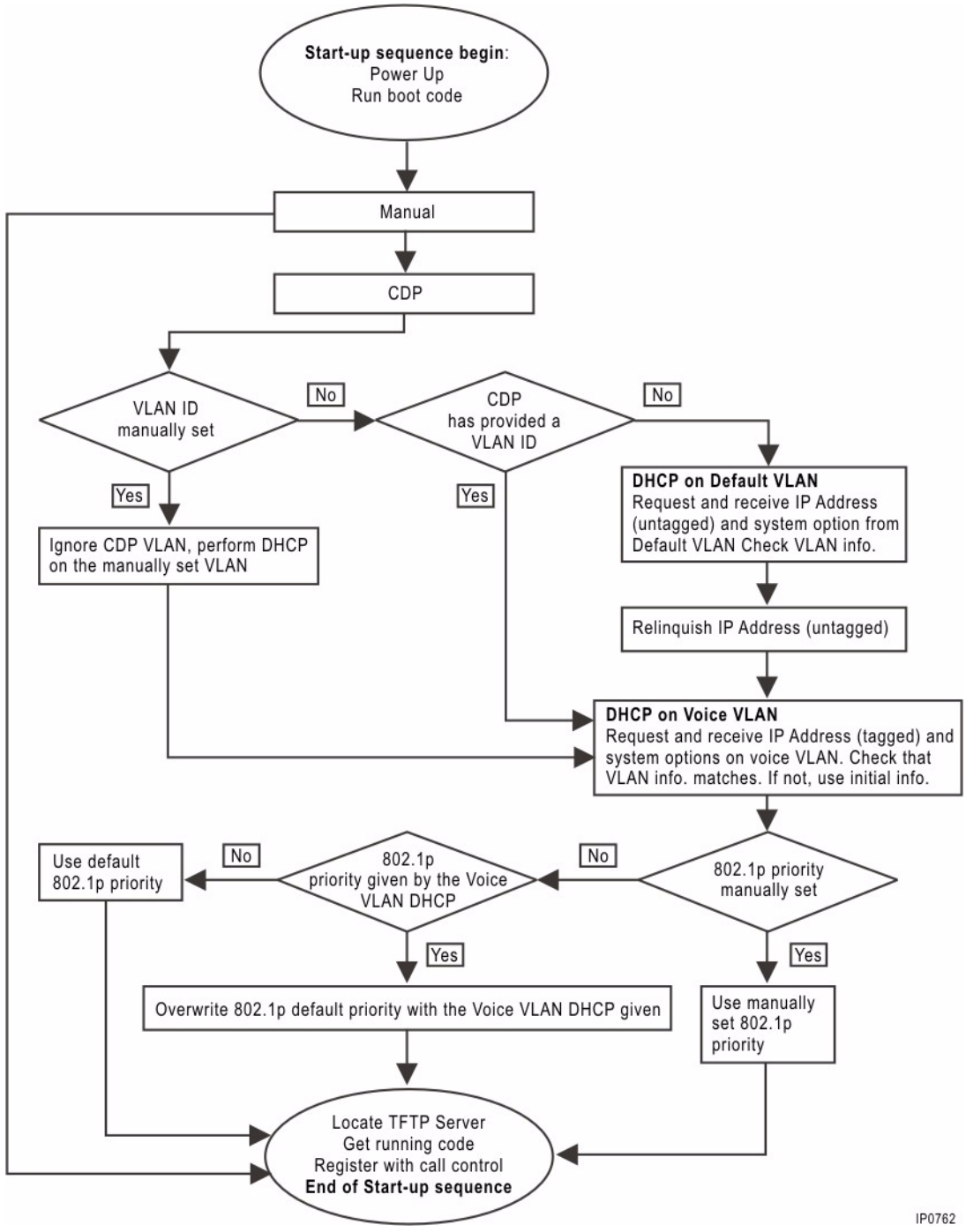
Getting started

The previous sections have dealt with network conditions and call traffic. However, before any of this can occur, the system first needs to be installed and the end devices need some code to get them running.

Start-up sequence for phones

Prior to Release 2.0, the phones used DHCP or manual input to determine VLAN settings. With Release 2.0, phone messaging is also compatible with CDP, so the phones are able to discover VLAN information, if present. There are now three potential ways to include information in the phones; these being, in priority order:

1. Manual Entry at boot time
2. CDP
3. DHCP



Since the phone could double the retrieval of information depending on the way information is entered, it is important that the DHCP servers for the voice and data VLANs each have the same VLAN and priority information.

Also, the ability to provide partial information at each stage allows these three methods to be used together to ease installation. Prior to Release 2.0 all information had to be entered either

through DHCP or manually, but not a combination. For example, the VLAN can be manually entered and the IP Address determined through DHCP.

This sequence works with either multiple DHCP servers, one on each VLAN, or the router/Layer 3 switch connecting the VLANs has DHCP forwarding capability (also known as DHCP Relay, or IP Helper on certain vendor equipment).

Using the internal SX-200 ICP TFTP server is recommended. An external TFTP server can be used, but it is then important to ensure that the downloads maintain version control with upgrades that get applied to the ICP. In a multiple-ICP installation with multiple versions, this can become network management overhead.

One of the options that the IP phone obtains is the RTC (Real Time Controller and call control) address of a SX-200 ICP. Since the address in this DHCP option is not dynamic, this address must be pre-assigned statically within the ICP before it is connected to the network.

The sequence above assumes that the phones get information from a DHCP server. The information can also be manually entered into a phone as it starts to boot up, to make sure the information is fixed and requires little DHCP intervention. This method is particularly useful if a phone is used on a remote WAN link and the router cannot forward DHCP requests, or if a local DHCP server does not exist. It is also useful on VPNs, for the same reasons.

Startup sequence for the controller

The controller startup sequence involves bringing up the RTC where call control resides. This also includes the local DHCP and TFTP servers.

In order to correctly program some of the options within DHCP, such as the RTC and TFTP server, it is necessary to pre-assign an IP address to the SX-200 ICP. This address is used by the IP networking handler and is entered into the database of other remote ICP units.

The DHCP server in the SX-200 ICP controller should be used for local devices on the voice VLAN. This can be disabled, but then an external DHCP server is required to service devices on the voice VLAN.

DHCP options

Since the DHCP server options can differ from release to release, consult the associated documentation for the product.

In Release 4.0, DHCP Options 128 - 133 are replaced by a series of "tags" that form an ASCII data string in Option 125 (default for Mitel-specific options) and Option 43 (for Mitel- and non-Mitel-specific options.)

The following table shows the options currently used.

Table 39: DHCP Server Options

DHCP option	Information	Tags
003 – router address	IP address (for example, 192.167.22.251)	
Prior to Release 4.0		
128 – (specific) TFTP server	IP address (for example, 192.167.22.10)	
129 – (specific) RTC	IP address (for example, 192.167.22.10)	
130 – (specific) IP identifier	“MITEL IP PHONE”	
131 – debug	IP address (for example, 192.167.22.100)	
132 – (specific) VLAN ID (32 bit)	0x2	
133 – (specific) Priority (32 bit)	0x6	
Release 4.0 and higher		
125 - Vendor Specific	ASCII string of “tags”	**id**:ipphone.mitel.com TFTP Server = **sw_tftp** SX-200 IP Addr = **call_srv** IP Phone Analyzer = **ipa_srv** VLAN ID = **vlan** VLAN Priority = **l2p** Diffserv Codepoint = **dscp** HTTP Proxy Server = **app_proxy*** *not used on the SX-200 ICP

Option 131 is the IP address of a PC that is running the IP Analyzer software. Use this software to check normal operation and to obtain device and call statistics.

The VLAN (132) and Priority (133) Options are present (or not), depending upon whether VLAN is used within the network. If not present, the IP phone does go through the second sequence of determining an IP Address at startup and continues to operate in an untagged mode.

Note that in the CXi platform when VLAN settings are enabled, that this is only on VLAN1. Thus, option 132 should be defined to 0x1. Option 133 can still be used to define priority, and 0x6 is still recommended.

DHCP lease time

To allow users to move off the local subnet, or to let new users join a subnet, a method is needed to give up an IP address and to obtain a new address. If a phone is disconnected, it obviously cannot talk to the DHCP server, so another method is needed to free up unused addresses. DHCP lease time clears out unused IP addresses and makes them available for new requests.

The timer can be set from a few minutes to months. The default is set to **8 hours**, which keeps the amount of checking to see if an IP address is still in use to a reasonable level while providing adequate recovery time to free up any unused addresses.

The exact lease time to use depends upon the system requirements. If there are plenty of spare addresses, then the lease can be extended. Some users will specify up to a week to allow a system to maintain the same IP addresses over a long weekend when power is removed. If addresses are less available, and phones are more mobile, shorter times are preferred.

Note: It is possible to run out of IP addresses with permanent leases. The recommendation is to minimize use of these addresses. For example, a laptop user who roams from office to office plugs in the laptop, receives a permanent address, and then disconnects the device. The IP address is never released by the user, and the address is never handed out to another user because the lease never expires. Eventually the server can run out of addresses.

Cables and connections

Although often hidden, the cable plant provides the connection between the end user and the data service (the IP phone and SX-200 ICP). Because data is sent at high speed, there are requirements that need to be met in order to get the best performance.

Once sent, voice packets cannot be recovered, and so it is important to ensure that the cable plant is capable of handling the data without loss, or at worst a factor of 10 better than the guidelines for ‘green’ operation as shown in the section “Network measurement criteria” on page 102. This needs to be verified before installation. A lossy network might not show itself with PCs attached because PCs resend information if it is lost. The effect for the PC user is simply a slow file transfer. The effect on the IP phone user is interrupted conversation.

In order to ensure a good network installation, at a minimum, use the guidelines in the following sections.

Cable types

Use a minimum standard of a CAT 5 cable between devices. For added performance, use CAT 5e or better between patch panels and between switch devices. Total cable lengths should not exceed the Ethernet requirements as highlighted in specification ANSI/EIA/TIA-568-B 2001 section 4.

Document ANSI/EIA/TIA-568-B 2001 also highlights good wiring practices, such as

- Grounding requirements
- Cable runs and mixing of cable types
- Cable bend radii

Cables are available in a number of data types. Those recommended for this application are

- CAT 5
- CAT 5e
- CAT 6.

Connectors should also conform to the same requirements. An end-to-end connection is only as good as its weakest link. If the cable used is CAT 6, but the connectors are CAT 5, then performance will not exceed CAT 5. If CAT 3 connectors are used, the cable run is not guaranteed to work at CAT 5 rate.

Consider other possible uses for the cables and future expansion requirements. It is easier at initial installation to specify a slightly higher-grade cable than to retrofit later. Structured wiring schemes are always preferred as they can be connected in star and ring configurations with little change within the building.

Ethernet cable distances

Cable runs for Ethernet are specified up to 100m when the correct cable type is used. This includes the internal building wiring as well as patch leads at either end. The limitation on this distance is quite strict and operation is not guaranteed beyond a total length of 100m. More details can be found in ANSI/EIA/TIA-568-B 2001 section 4.

Internal building, or horizontal cable runs, should not exceed 90m, to allow for an additional 5m of cable at both ends for connection to the end devices from the wall jack. Additional connections in the cable run add attenuation. Use the guidelines in the following table for installation.

Table 40: Recommended Distances for Cable Runs

Cable Run	Maximum Recommended Distance
Horizontal or intra-building run	Less than 90 m
Wall jack to end equipment (IP phone)	Less than 3 m
Layer 2 switch to MDF (direct connection)	Less than 3 m
Layer 2 switch to power hub	Less than 2 m
Power hub to MDF	Less than 2 m

These recommended distances are shown in the following figure.

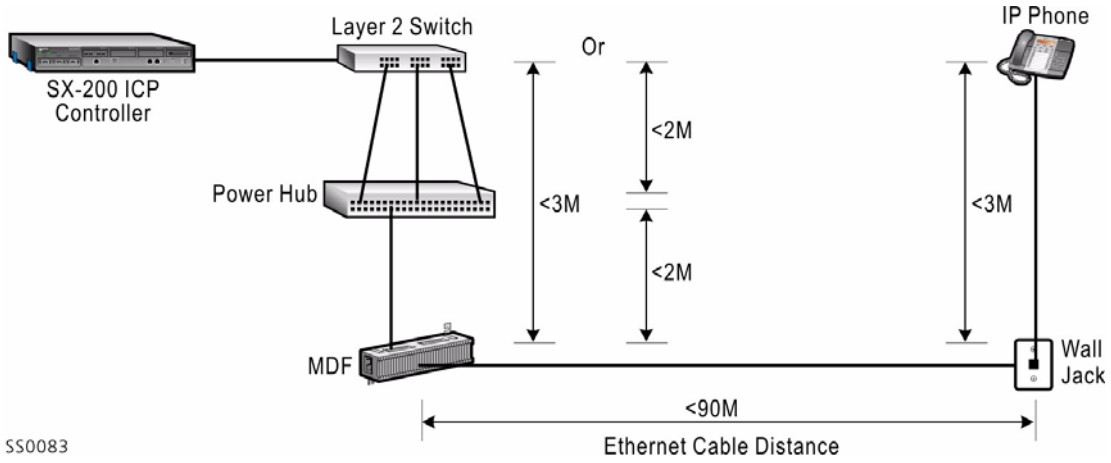


Figure 26: Recommended Distances for Cable Runs

Straight and crossover cables

Two types of cable connection are used to connect between network equipment devices and also from the network equipment to the end equipment:

- Straight connection, used to connect end users to the network (for example, an IP phone to a switch)
- Crossover connection, used to connect between network equipment (for example, between switches)

The connections between devices contain pairs of wires to transmit data and to receive data. The transmit and receive pairs must swap over to make a connection work, otherwise, transmit connects to transmit, and no data passes. The switch ports in the network normally provide this crossover. This means that the connection between end device and switch can use a straight connection.

However, when switches within a network connect to each other there are two crossovers, thus nullifying the effect. A crossover cable is needed for these connections. Alternatively, some switches provide an additional port with the crossover removed, allowing a straight cable to be used. Both physical ports on such a connection cannot be used simultaneously, otherwise, data corruption occurs. In the following figure, the port labeled 5X would be used to connect to an end device OR the port labelled 5 would be used to connect to an X port of another switch.

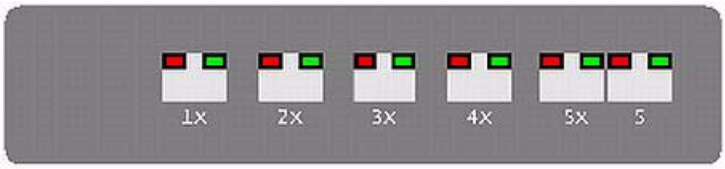


Figure 27: Straight and Crossover Port Example

Some switches provide auto crossover detection, so that straight connections can be used for all connection leads.

Identification of connection cables

Since a network includes a mix of straight and crossover cables, they need to be identified for easier maintenance view. Identify each type with an additional marker, or label on the cable, or use a color code to quickly identify cables (for example, white for connections to users, red for crossover and inter-switch connections).

Test the cables to identify which cable is which type. Another simpler method is to look at the color of the wires inside the RJ-45 plug. If the color order is the same in both plugs, then the cable is a straight connection. If they are different, then it is a crossover cable. Be careful, since other telecom functions, such as PRI, also use RJ-45 connections. In the following figure, for the straight cable, the orange and green pairs are in the same position. For the crossover cable, the orange and green pairs swap positions between the connectors.

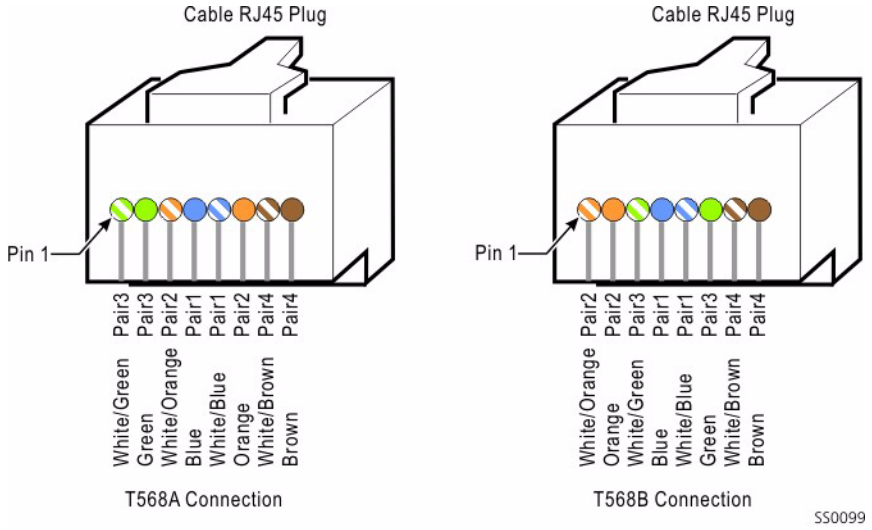


Figure 28: Using Wire Color Order to Identify Connection Cables

The cables shown are those expected in new installations, namely, a T568A connection to a T568A for a ‘straight cable’, and a T568B connection to a T568A for a ‘crossover cable’. It is also possible to get ‘straight cables’ that have a T568B connection to a T568B, but these are more likely in older installations.

International standards recommend that new installations conform to the T568A wiring format. However, a number of current installations may have wiring to T568B. As long as a common format is used throughout the installation, and there are no unexpected swaps, then electrically the color is less important (for example, all wall jacks to T568A or T568B, but not a mix).

Analog local loop characteristics

The analog local loop is basically a pair of twisted cables that connects the end-user to the local exchange, or CO. The cable carries both AC voice signals and DC power feed to the end device, typically a telephone. Flow of DC current informs the CO that the end device is active, whether this device uses the current or not. The longer the cable and the thinner the cable, the more resistance there is to both the AC and DC signals. If there is too much resistance, then not enough DC will flow to power the end device, or to inform the CO that the device is active. Also, with distance the AC signal will become attenuated and it may become difficult to hold a conversation.

Because of the cable resistance and capacitance, or coupling between the two wires and with other wires, the cables also attenuate higher frequency signal more than lower frequency signals. This effect is also dependent on the cable thickness and length. Thinner and longer cables are most affected. With particularly long cables, even the voice signals are affected at higher frequencies. To overcome some of these losses the cables may have some small in-line transformers added. This then becomes a ‘loaded line’. Such a line will restore some of the voice frequencies, but at the expense of higher out-of-band voice frequencies. For voice signals this is not a worry. However the change to the voice channel may be enough to impair data services and MODEMs from operating at full capacity.

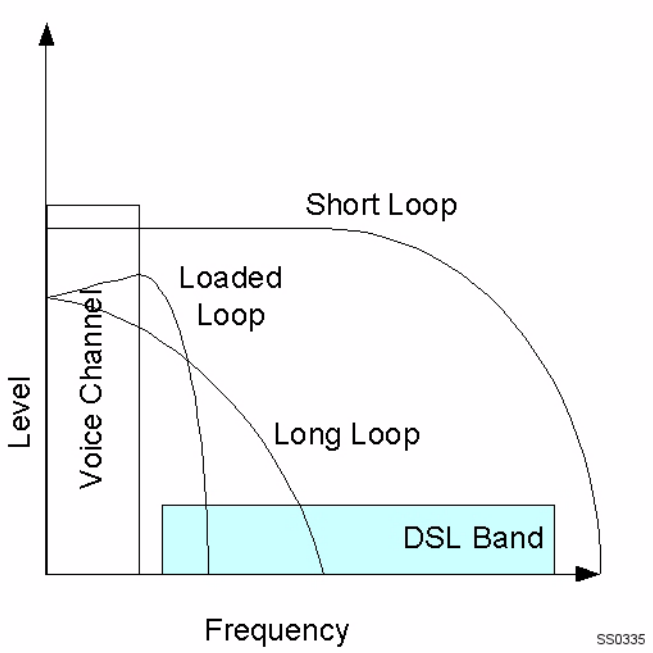


Figure 29: Analog Loop Characteristics

For DSL, or ISDN over DSL, connections, the DSL MODEM makes use of the much larger out-of-band frequencies that the cable can carry. However, with longer cables, such a MODEM cannot work reliably as the effective data rate gradually reduces. With a loaded line, the higher frequencies are cut so much that a DSL MODEM will generally not work, or operate at a much reduced capacity.

To cater for different line lengths and conditions a number of parameters need to be considered. In North America these are now covered by three different loop designs known as:

- Carrier Serving Area (CSA)
- Revised Resistance Design (RRD), and
- Modified Long Route Design

Different countries may use variations on these settings. However, those that are capable of running 56kbits/s modems and ISDN typically will use the CSA working rules, with line attenuation up to about 5dB.Lines with higher operating voltages, such as 75V, may be used to continue to supply the necessary line current to the far end device. Usually, such lines will also be ‘loaded loops’ and may fall into the RRD or even MLRD working zones.

Most new lines will fall under the CSA working rules, especially where DSL services are to be provided.

Some characteristics of the different lines are shown below:

Table 41: Line Characteristics

Design Parameter	Carrier Serving Area (CSA)	Revised Resistance Design (RRD)	Modified Long-Route Design (MLRD)
Loop Resistance	Not applicable Limited by overall loss	0-18kft (0-6km): max. 300 ohms (including phone) 18-24kft (6-7km): max. 1500ohms (inc. phone)	1500 ohms to 2800ohms (inc. phone)
CO additional gain	0dB	0dB	1500-2000 ohms: +3dB 2000-2800 ohms: +6dB
Maximum Loss	5dB	18kft: 8dB (some administrations 8.5dB)	8-10dB
Loop Current	Constant Current or ~57mA into a 430ohm resistance (no loop)	18kft: ~27mA (into 430ohm load) 24kft: ~25mA (into 430ohm load)	2800ohm: ~15mA (into a 430ohm load) Note: less than 20mA may not be enough power for some phone sets.
Cable Gauge	26AWG: 9kft (3km) 24, 22, 19AWG: 12kft (4km)	26, 24, 22AWG 26AWG limited to 15kft (5km)	24, 22AWG
Loading Coils Fitted	No	H88 units over 18kft (6km)	H88 units
Typical Line usage	Business and home subscriber with Internet, HDSL, ADSL. IDSL connections, and special services, e.g. CLASS/CLIP	Business and home phone connection (to 18kft). Limited IDSL services up to 18kft (6km)	Rural phone connection to home subscriber. No digital services.
New business installation	Recommended	Not Recommended	Not Recommended

Due to field engineering difficulties most new installations are now based on the CSA plan. Longer distance connections are catered for with remote digital repeaters or channel banks. Some longer distance cables do still exist however, but would not generally be used for business connections due to the increased line attenuation and limits to other services such as FAX and MODEM.

Most business PBX will cater for the CSA and limited RRD (up to 18kft/6km) situations. Longer RRD connections may have additional attenuation.

Table 42: Line Attenuation

Line Loss	0 to 3dB	3dB to 6dB	6dB to 8dB	Beyond 8dB
Short Line setting	Good	Quieter	Soft	Too Quiet
Long Line setting	Loud	Good	Quieter	Soft is too Quiet

The Analog circuits provided with the MITEL PBX will cater for lines from 0dB to 6dB of loss. Longer lines with up to 8dB of loss can still be used, but longer distance calls will sound quieter than internal calls. Lines with further attenuation will always sound quieter than internal calls.

Determining the line type should be as simple as asking the installer, or phone service provider. However, this may not always be true. The supplier may know the connection at either end, but not necessarily the plant in between. It can be common for a supplier to provide different cable types to the same installation. Quite often, an existing installation may have a long line connection back to the local exchange, or CO. When the installation is upgraded, additional shorter lines may be provided from a local channel bank, or MUX. Thus the installation may have a combination of lines.

Most new installations are now based on the CSA standard.

As an aid to determine which line is fitted, it is possible to measure line feed current. This is not a definitive test as both CSA lines and RRD lines share similar current characteristics. The test requires a measurement of the open circuit voltage, and the current with a shorted loop and with a resistive loop, at the customer demarcation point. The resistive load is to simulate a telephone and requires a 430ohm resistor rated at 2W or higher. It will get hot on short lines.

- Measure the open voltage.
- Measure the current through the resistor
- Measure the current without the resistor (see Note, below)

Note: Use this measurement as a backup to the other two. On a short line, current of 120mA, or more, may be present. Also, a long duration short circuit may also indicate a line fault, which may also raise alarms with the service provider to investigate the line fault condition, e.g. downed cables, etc.

Some simple results come from this:

- The voltage should be a nominal 48Vdc (see Note, below)
- The current through the resistor should be >20mA
- If the current readings, through the resistor and without the resistor, are the same then the line uses constant current feed and is based on CSA.

Note: Some administrations use higher voltages of 60Vdc and even 75Vdc. In this case the table below and results above may not be applicable. The only universal constant, is that the current should be greater than 20mA, and there should be around 9-12Vdc across the line when the phone is off-hook (or a simulated phone load is used).

With Resistor (non-constant current)	Without Resistor (non-constant current)
<20mA (MLRD – loaded line) >20mA (RRD – loaded line) >22ma is good, less than 18kft (RRD) >30ma is good (CSA or RRD)	<25mA (MLRD – loaded line) >25mA (RRD – loaded line) >28mA is good, less than 18kft (RRD) >39mA is good (CSA or RRD)

Installation guidelines

Before installing a PBX into a customer site it is important to do some preliminary investigation to find out how the customer will use the system and also what lines are available. As described above, there are a number of connections and local loops that can give reduced voice quality.

Some specific areas to investigate are:

- If trunk to trunk connections are common, consider installing a PRI/BRI digital trunk rather than Analog trunks (BRI/PRI are considered loss-less to voice)
- If conference calls with multiple external parties are common, consider installing PRI/BRI digital trunks rather than Analog trunks
- Digital lines, such as PRI/BRI, are preferred connections to the CO
- Are the Analog trunk levels well controlled, these can be measured using test signals from the CO such as ‘digital milliwatt’ and a level meter at the customer premises. (Backup is to measure current flow through 430ohm resistor. Beware that 40mA and 25mA are standard constant current feeds even on short lines, but that a long line may also give 25mA)
- If the line loss is more than 6dB then the voice levels both in and out will that of a home subscriber and less than ideal for a business installation
- If the line has loading coils fitted, it will not be suitable for DSL connections, nor is it likely to offer other services such as CLASS/CLIP. It will also potentially have lower voice signal levels.
- Are all the incoming trunks from the same vendor/supplier? There may be differences in operation.
- Do the Analog trunks come from a common group, for instance a supplier could provide one long line (previous connection) and new lines from a local channel bank. The line lengths are different and the impedance settings will be different. Measure them all.
- Get a description of the line type, length and impedance; for example
    - Business line (nominally complex)
    - Tie line to another PBX (nominally 600ohms)
    - From a local repeater or amplifier (nominally 600ohms)
    - Bundled packages such as Centrex lines and CLASS (nominally Centrex)
    - From an older aDSL supplier (nominally DSL). [Newer DSL installations look more like Complex or Centrex, i.e. the original line type]
    - Loaded lines – These lines have specific ideal impedance, but in practice this varies with line type and distance. Custom installation may be necessary
- Poorly matched Analog lines will result in increased echo and returned signal. In built echo cancellers will work, but may struggle if the impedance is a particularly bad match, with some echo being heard at the start of a call, and potentially during a call should a line condition change occur.
- Too quiet a signal can result in the incoming user signal sounding broken when the internal user speaks. Appropriate line levels and line matching should be selected.

Powering phones

The newer range of Mitel IP phones can be powered only from the LAN. Consider power to the phones and whether it needs to be maintained during a power failure. The network switches and the SX-200 ICP also need power backup if the phones need to continue to work. Power to the phones can be provided by an external supply such as a power adapter, or by an additional power unit (“power-hub” as shown in the section “Ethernet cable distances” on page 150) that is placed in series with the connections between the access switches and the phones. Some Layer 2 switches incorporate power feed, although these tend to be larger devices, rather than direct retail devices. Power feed should conform to IEEE 802.3af. Cisco products providing power, not to IEEE 802.3af, can be used with the MITEL power dongle (Cisco compliant) to obtain power.

For more information on power requirements and available devices that support power over ethernet, refer to the section “Power” on page 43.

IP phone LAN speed restrictions

The IP phones are configured to auto-negotiate the LAN speed settings. Ensure that the Layer 2 switch setting is also configured to auto-negotiate to reduce the possibility of a duplex mismatch and potential loss of data, and voice.

Although IP phones auto-negotiate the network connection speed to 100Mbits/s full duplex, note the following limitations:

- Both ports on the phone are limited to the lowest negotiated setting.
- The 5001, 5005, 5201, 5205, and 5207 phones are configured for auto-negotiation, but are limited to 10Base-T (10Mbits/s) full and half duplex.

Future migration

In designing the network, consider the business migration path as this may influence the type of network devices that are initially bought and installed. How many additional users and data devices may be needed? How should the network be segregated?

Network configuration summary

In brief, these guidelines are exactly that: guidelines. Because LANs are so diverse and equipment changes so quickly, review the following recommendations to provide the best operating conditions:

- Use networks with VLANs (IEEE 802.1p/Q) with dual-port phones.
- The network should be fully switched.
- Where data devices (PC and voice devices) share the infrastructure, use managed Layer 2 switches capable of supporting VLAN operation.
- The ports must allow for the interface speed to be configured either manually or automatically. Automatic configuration is the simplest and preferred operating mode.

- TOS to COS conversion can provide additional priority marking when PCs are used as voice devices.
- Routers or Layer 3 switches must be available to connect between VLANs.
- For Access connections to an end device where a network loop cannot exist, Portfast settings may be used to minimize network disconnections.
- The controller should be located behind a network Layer 2 switch.
- Ensure that the PPS rate of the routers and switches is adequate for the amount of voice traffic expected.
- Wherever possible, provide the most bandwidth. Use full-duplex instead of half-duplex.
- The SX-200 ICP and IP phone Ethernet ports are hard-coded to auto-negotiate. Ensure that the network Layer 2 ports are also configured to auto-negotiate.
- If the network consists of multivendor units, ensure that they all inter-operate correctly.
- Use MTU on routers, especially for slower-speed links (anything less than T1 rates).
- Ensure that end-to-end delay, jitter, and packet loss are within acceptable bounds.
- Ensure that there is sufficient bandwidth on a WAN link for the amount of expected traffic. Do not overload.
- Provide a realistic blocking number for IP trunk restriction (consider bandwidth).
- Do not share the voice VLAN with data devices. Although this is not possible for the CXi, ensure that there are multiple priority queues with voice in the highest queue.
- Place softphones (PC-based), such as YA Pro, on the data VLAN and enable TOS-to-COS conversion (requires L2/L3 switch).
- Do not put servers or printers behind a dual-port phone; provide them with a dedicated port.
- Ensure routers support DHCP forwarding, or provide multiple DHCP servers and copy phone-specific information between DHCP servers to ensure phones start up correctly.
- Ensure routers support ICMP Redirect to reduce bandwidth requirements when the default gateway device is not the correct one to direct traffic to.
- To get the maximum data rate from a phone, connect a 100BaseT NIC on the PC to the phone and ensure that it is configured for auto-negotiation. The phone defaults to the slowest speed for both ports.
- Ensure CAT 5 or better cabling is installed to get best performance. CAT 6 may be required for patch cables, if a number of patch panels are used in a wiring run.
- Consider the subnet size and the NetBIOS configuration used. A subnet of 254/24 devices works well.
- The controller uses some internal IP addresses in the range 192.168.10.0/28 to 192.168.13.0/28. Communication to the SX-200 ICP using an IP address in these ranges will fail to get a response.

Note: None of these reserved addresses can be used by devices that need to communicate with the SX-200 ICP (for example, MITEL Phones, E2T, OPS Manager). These reserved IP address ranges can be used elsewhere in an IP network (such as a network not connected to the SX-200 ICP). The ICP should not be programmed with IP addresses in the range 169.254.0.0/16 as these addresses are reserved for future use.

- Use of the internal TFTP server of the SX-200 ICP is recommended. This ensures that device downloads maintain correct revision level with the appropriate controller following any upgrades.

Pre-commissioning Checklist

This section helps system administrators, network designers, and installation personnel verify that the major areas of concern have been addressed before the system is put into service.

When providing a solution to a customer there are a number of stages that need to be considered. These typically include

- Pre-testing and analysis of customer installation
- Planning and design proposal for installation
- Installation and commissioning
- Maintenance and future upgrades

Installing a telephony system requires some forward planning with the customer to determine the type of phones and features required, and their location. Integration with a data network adds a number of other areas to consider. For example, it is necessary to consider if the installation adds on to existing equipment or whether it is a new installation.

The Mitel MiService Client Services Team (part of Customer Engineering Services) can provide assistance in answering some of these questions. Some key areas of assistance include

- IP readiness review
- System configuration analysis
- Determining if and when to upgrade the network
- Managing the transition to IP Telephony
- Commercial aspects of a transition
- Identifying other areas of opportunity for business improvement

The lists in the following sections are not exhaustive, but are intended as a guideline of questions and areas to consider, especially with respect to installation on a data network. Remember that it is easier and more cost-effective to consider the requirements up front, rather than afterwards.

General considerations

- Obtain a network diagram of the proposed networking infrastructure.
- Does a legacy PBX need to be supported?
- How many sites, buildings, floors, wiring closets, and nodes are there?
- Is the design adequately sized for TDM, IP, call features, and resources?
- How much growth is anticipated? Should the solution accommodate the expected growth now or simply address the current requirements and grow as needed? Consider the network devices and cabling as well as telecom requirements.
- Consider spares and response time in the event of a failure. Is network redundancy required?

- Obtain information on site power distribution and physical layout.
- Obtain a telephony network diagram and understand the following:
  - Physical and logical distributions of phones
  - Emergency Support (for example, 911, 999, 112)
  - PSTN trunk connections, gateway requirements, compression, IP networking
  - Location of applications such as Voice Mail, Auto Attendant, and so on
  - Other TDM services such as fax and modem. Modems do not work across IP trunks because of required echo cancellation techniques. Fax works under limited settings, although a T.38 gateway is recommended.
- Where a resilient network configuration is in use, be aware that the smaller CX/CXi and MX ICP platforms cannot have multiple LAN connections.
- The controller reserves some IP addresses for internal use. Communication to the controller using an IP address in these ranges will fail to get a response. These include the following:
  - 192.168.10.0 to 192.168.10.15
  - 192.168.11.0 to 192.168.11.15
  - 192.168.12.0 to 192.168.12.15
  - 192.168.13.0 to 192.168.13.15

Note: None of these reserved addresses can be used by devices that need to communicate with the SX-200 ICP (for example, MITEL Phones, E2T). These reserved IP address ranges can be used elsewhere in an IP network (for example, a network not connected to the SX-200 ICP).

Network pre-installation considerations

- Is this a new installation or an addition to an existing installation?
- How many users are on the system and how are they distributed?
- Is the system adequately sized for TDM, IP, features, and resources (for example, DSP)?
- Is this a multiple unit system? Is clustering needed?
- Are IP networking, licenses, and compression required?
- Are there remote workers (teleworkers)?
- Are there remote controller units (for example, in a branch office)?
- How much bandwidth is required for the backbone, server, and end nodes?
- What available features does the budget allow for? Redundant power supplies and UPSs? Redundant uplinks?
- What type of WAN links and PSTN trunks will be used to connect remote sites?
- Does the existing cable plant need to be upgraded?
- The network should never bottleneck. Deploy non-blocking, high-performance, high-capacity switches. Understand the capacity of switches feeding on to the core as well as to the access layers.

- Consider points of failure and design to minimize, such as redundant network, spanning tree, and so on.
- How is power distributed? Is power backup needed?
- Have the network guidelines in the section “Network Configuration” on page 85 also been considered?

Network design process overview

Include the following steps when designing an IP telephony network solution:

- Perform an assessment of the current network.
- Determine additional bandwidth and performance required.
- Design a network topology including the IP telephony equipment.
- Design a consistent end-to-end QoS policy.
- Consider ongoing engineering requirements: networks and requirements evolve even after an installation is complete.

Layer 2 and LAN connections

Quality-of-service settings

Within the Enterprise that VLAN (IEEE 802.1p/Q) is supported and can be configured. Consider the following:

- Phone connections can handle both tagged and untagged traffic.
- The port supports multiple egress queues.
- The port supports Spanning Tree for Emergency location.
- The port supports power, if provided through the LAN.
- Can the port’s connection to the SX-200 ICP provide VLAN and priority tagging?

Traffic and bandwidth

- Identify areas of high traffic, for example, ACD agents where additional bandwidth may be needed, or where an ICP rather than a router is required.
- Consider the network guidelines and traffic as highlighted in the section “Network Configuration” on page 85.
- Consider the IP address range and size. Larger means less Layer 3 switching, but more broadcasts, negating the effect of the Layer 2 switching fabric.

DHCP

- Consider the location of the DHCP servers and the number of scopes to be handled.

Note: Each SX-200 ICP system comes with its own DHCP server.

- Consider the lease time for the DHCP server. A starting value of **8 hours** is recommended. This can be reduced for a more mobile environment, or increased in a more stable environment.

TFTP

- More TFTP servers improve startup time when there are a large number of phones starting at once. Note that each SX-200 ICP system comes with its own TFTP server, but additional external servers can also be used. Consider upgrades and how to control this across external TFTP servers.

Layer 3 and WAN connections

Quality-of-service settings

- Ensure that routers have the ability to adjust MTU and support TOS/DiffServ settings.
- For devices that bridge VLANs, ensure that the COS (Layer 2 priority) can be defined or that TOS/Diffserv to COS conversion is supported.
- Ensure that the routers can provide ICMP-Redirect, especially where multiple paths may exist.

Traffic and bandwidth

- Identify areas of high traffic.
- Consider the network guidelines and traffic as highlighted in the section “Network Configuration” on page 85.
- When using a WAN link, ensure adequate Service Level Agreement on the connection.
- What type of connection is used between remote sites (for example, dedicated line, Frame Relay, MPLS VPNs)?
- Ensure adequate bandwidth for particular WAN protocol and number of channels. Consider signaling and end-device overhead. What is the CIR?

DHCP

- Where DHCP is used, but a local DHCP server is not available, ensure that the router is capable of forwarding DHCP requests (also known as 'IP-helper' on certain products).
- Ensure that there are no DHCP forwarding loops created.

Firewalls and NAT

Firewalls are intended to restrict unauthorized access to a network. Given the number of IP phones that may be active at the same time, it is necessary to open up a number of ports on

a firewall in order to facilitate access. In such scenarios, the firewall is much less effective against network intrusion.

Network Address Translation is good for reducing the number of addresses seen to the internet from a particular business. However, such devices need to understand the underlying protocol to work effectively. If a Mitel IP phone is used on the internet through NAT, there is a high possibility that the voice streaming will not work. Users of Mitel IP phones, on the Internet, should use the Teleworker solution.

Caution: Some firewalls and security checking applications monitor the LAN for data anomalies in the traffic. Voice traffic sometimes appears as an anomaly. Therefore, additional programming or exception-conditions applied by this application to accept voice traffic as genuine is necessary.

Teleworker

- This feature allows a Mitel IP phone to be used over the Internet.
- It contains the necessary security and encryption to be used in parallel with a firewall and Network Address Translation within a business.
- It contains the necessary translation of messages to the phones on the internet to ensure that voice and signaling work as though within the business.
- Delays are longer on phones within the LAN, because the uncertain nature of the internet requires that additional buffering be included to reduce packet loss issues.
- Voice streaming occurs only between the Teleworker phones and the MITEL Teleworker Solution Server. This means that two Teleworker phones that need to connect to each other still require a MITEL Teleworker Solution Server. This is because of security. Ensure adequate bandwidth for call paths where Teleworkers are within a common location.

Appendix A. CAT 3 Wiring

CAT 3 Wiring Practices

Category 3 (CAT 3) refers to a type of UTP copper cabling that meets specific transmission characteristics (see CAT3/EIA/TIA-568 wiring standards). CAT 3 also refers to the installation practices observed when routing these cables as well as the interconnection and end point termination methods used. The following sections detail further practical issues to be used in conjunction with the specification.

Although CAT 3 cabling is not recommended for new installations, there may be instances where CAT 3 is encountered in an existing installation. CAT 3 installations can fall into different categories with unique pitfalls:

- CAT 3 cabling plant was installed for supporting traditional telephony equipment. This type of installation will potentially contain a number of CAT 3 violations that did not interfere with traditional telephony applications but will present problems for data transmission and VoIP.
- CAT 3 cabling plant was originally installed for supporting traditional telephony equipment. At a later date spare cable runs were inspected and qualified to support 10M Ethernet. Part of this cabling plant will be CAT 3 compliant and part will not be CAT 3 compliant. An installation in this category needs to be carefully re-qualified to CAT 3 standards.
- CAT 3 cabling plant was installed to support a LAN technology other than 10M Ethernet, such as Apple Talk, Token Passing Ring, or a proprietary networking technology. An installation in this category needs to be carefully qualified to CAT 3 standards.

It is becoming increasingly difficult to find CAT 3 cables and connectors. The cost of CAT 5 components has been reduced so much that it is not cost-effective to install new CAT 3 networks. For new installations, only CAT 5 or better should be considered.

Many network devices now are capable of operating at both 10BaseT and 100BaseT. Devices will typically select the higher rate. Using CAT 3 introduces extra difficulties with these newer devices because the connection speed needs to be restricted to 10BaseT because of the cable capabilities. Often, the ability to provide this restriction can only be provided through manual selection, negating the benefits of using Auto-speed configuration. The cable capacity cannot be accurately determined so the end devices must be configured to inhibit them from selecting the higher data rates. If there is a mismatch between auto negotiation and manual settings, the link will default to the lowest setting of 10BaseT half duplex.

Common guidelines and restrictions for CAT 3 installations

- IEEE 802.3 hubs/repeaters should not be used in a network that is going to carry VoIP traffic due to the limited number of conversations and high level of jitter and packet loss than can be introduced with other devices. Use only Layer2 switches at the access points.
- Connections between L2 switches must be at 100BaseT or better (using CAT 5 wiring or better), including connections to the ICP controllers.

- The network infrastructure and capabilities should be considered in a network that still employs CAT 3 cable. It may not be capable of handling the Packet Per Second rate needed for a number of voice devices, as well as the bandwidth throughput. If a connection exists to data devices, such as PCs, the use of VLANs and priority mechanism is recommended.
- It is highly recommended not to connect PCs to the phones, and to connect these on a separate LAN infrastructure. The second port on the IP-Phones can be disabled in the SX200ICP through option 131 and COS setting 280.
- Telecom cable is **not** CAT3, but CAT 3/CAT 5 can be used as telecom cable. Make sure it really is CAT 3, or better, by consulting the manufacturer of the cable, *before* installing the equipment.
- Note that cables used as telecom wiring may also have different wiring pairs in the termination jacks as well as termination resistors, e.g. if ISDN has been used. These need to be corrected, or removed. Ensure that any bell capacitors and master/slave jacks have been removed. The cable route should be point to point without spurs or stubs. A cable tester that uses Time Domain Reflectometry should be used to verify the integrity of cabling runs. Visual inspection and ohmmeter tests may be insufficient. Be careful about pair splitting which may not be apparent on telecom cable (this is where the two pairs result in a Tx/Rx & Tx/Rx combination, rather than Tx+/Tx- and Rx+/Rx- pairs). Ensure that any bend radii have not been exceeded. In effect – be suspicious of an older wiring plant – Test!
- Pay close attention to wiring practices at the distribution frame and at the desktop and ensure that these practices comply with CAT3/EIA/TIA-568 wiring standards, these standards are much more stringent than the wiring practices used for traditional voice wiring. For example, in traditional voice cabling when an installer punched down cabling pairs on a termination block (BIX/Krone block) it was very common to unwrap the twisted pairs from an individual cable for ease of installation or to use untwisted cables to implement a cross connect. While this practice was acceptable in a voice network it will introduce problems into a data network.
- Typically Ethernet cables are an in-house building wiring, and normally should not leave the building. Telecom cables have special protection applied to cables external to the building. It may be required that in order to extend Ethernet externally to the building that a routers and special cable protection be applied at either end of the link.
- The EIA/TIA-568 standard provides numerous structured wiring recommendations regarding the routing of cables. The CAT 3 cabling plant should comply with these recommendations so that the chances of encountering network impairments due to cross talk and electrical noise is minimised.
- It is unlikely that CAT 3 cables will carry the full complement of pairs normally found with CAT 5. Unless phantom power feed is provided, the end devices will require separate power feed to operate. This may include local power units or the inclusion of a power feed hub in series with the cable runs. Consider which devices need UPS support in the event of power failure. The CXi hardware provides phantom power feed.
- Only the SX200ICP CXi platform provides ports capable of powering IP-Phones directly and having CAT 3 connections. All other platforms, including the SX200ICP MX platform, are intended for connection to a separate LAN infrastructure and a CAT 5 cable is required in this case. CAT 3 may exist elsewhere in the network.
- The Gigabit Ethernet stand must not be used with CAT 3 cables.

- The Wireless LAN (WLAN) stand should not be used with CAT 3 cables.It is recommended that the WLAN stand be connected to the wired network via CAT-5 running at 100 Mbps full duplex.

Summary of CAT 3-specific network configurations

There are a number of different installation combinations and devices that can run with CAT 3 cables. However there are also many exceptions and variations that might not make this work. The underlying principles in making the installation work are:

- The devices connected via CAT 3 must be restricted to 10BaseT operation only
- Standard 10/100/1000 Auto-negotiation will not guarantee to be restrict to 10BaseT with CAT 3 cable and should therefore be avoided; use manual programming at either, or both, ends of the link.
- Power over Ethernet may not be guaranteed. Phantom power feed will allow the CAT 3 data pairs to be used.
- If auto-negotiate fails, because one end device is programmed manually, the default is to used 10BaseT half duplex. Therefore manually setting ports to 10BaseT half duplex will result in a correctly configured connection.
- Where multiple devices are connected to a common network port, use of CAT 5 is recommended, with the higher available speeds.

To simplify installation, the following installation rules can be applied:

- Where CAT 3 wiring is used, the network device ports should be manually configured for 10BaseT half duplex. This will allow devices to be moved and maintain their settings as well as fixing the speed based on the cable run.
- Phones with a single connection can use CAT 3. An exceptions isYour Assistant Softphone.
- The Your Assistant Softphone should be connected to the network with CAT 5 only. Your Assistant is essentially a PC.
- Phones that connect to the network with an attached PC should use CAT 5, as should the connection to the PC.
- Individual PCs can use CAT 3.
- Servers generally require high-speed connections and should use CAT 5 only.
- Connections from the ICP WAN port should be via CAT 5 cable.
- All other connections between the ICP controller to ASU units, to NSU units, should use CAT 5. Note that there is a distance limit of 30m on these connections.
- Connections from T1/E1 (PRI) or BRI circuits can use CAT 5 cable (and RJ45 connector), but these are considered as telecom connections, and different cable pairs may be used.
- Connections between network switches and infrastructure should use CAT 5.

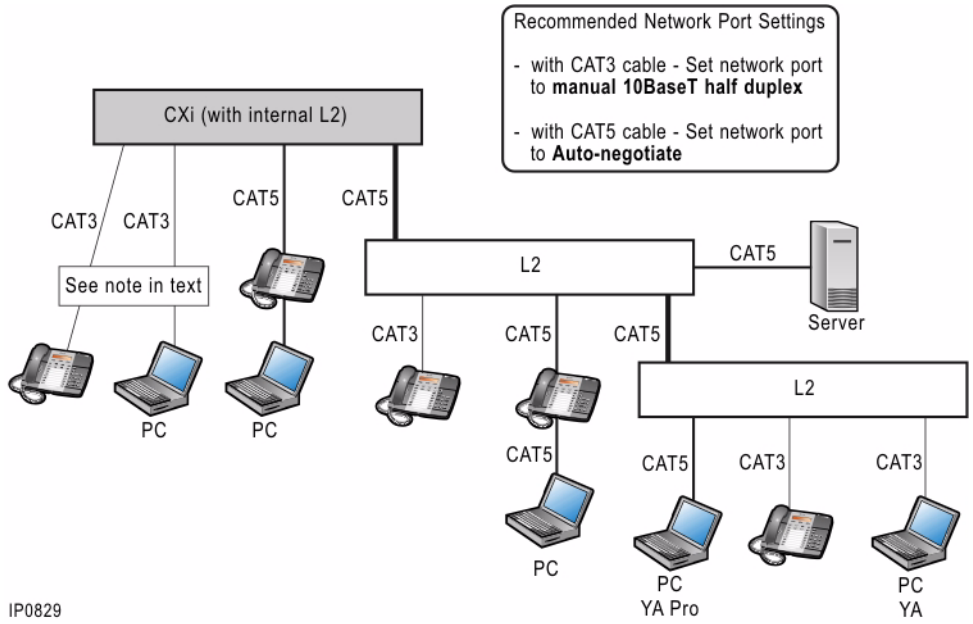


Figure 30: CXi Minimum Cable Standard

Note: In Release 3.0 and higher all port settings can be configured independently of port and function. Prior to release 3.0, settings for speed, duplex and flow control all had to be manually configured, or all set to 'Auto'.

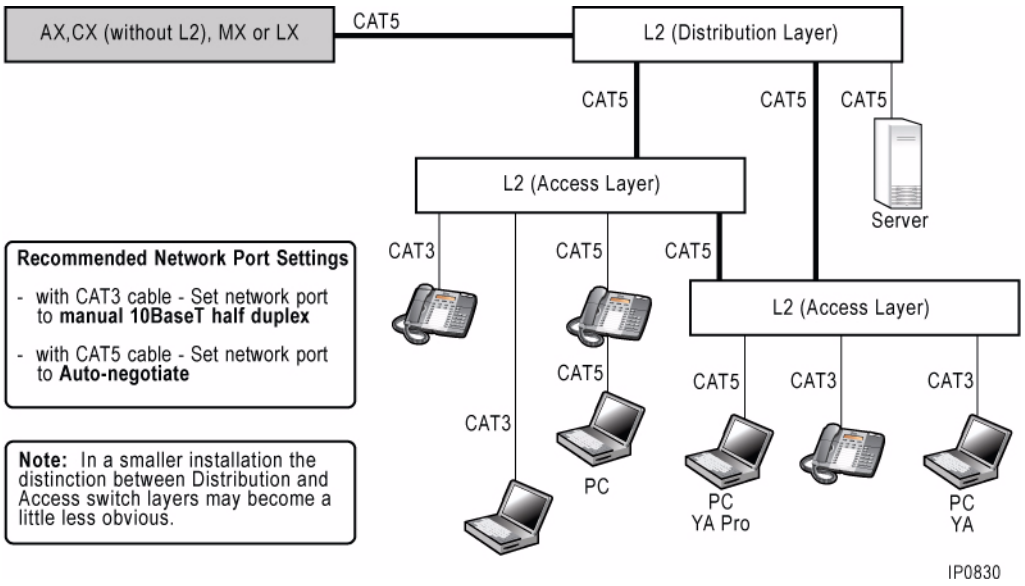


Figure 31: CX and MX Minimum Cable Standard

Appendix B. VoIP Security

Security Support with Mitel VoIP

Since 3300 Release 6.0 and SX200ICP Release 3.0, a number of devices in the Mitel IP product range now include additional security measures. These include:

- Encryption of voice and signalling payload data
- Network Access Authentication (802.1x)

Encryption is used to ‘hide’ the information that is carried in the payload from unauthorised users and applications. Network access authentication is a method to restrict connections to the network, or guide the device to particular parts of the network.

Data Encryption

Encryption is used to ‘hide’ the information content of both the signalling information and the voice streaming. The network connection, or path, remains the same whether the data, in the payload, is secured or not. Both secure and non-secure devices use the same network paths to establish voice connections.

Although quite complex in detail, data encryption involves two main aspects. These are:

- Key exchange
- Data Encryption, and decryption

Encryption is the method used to scramble the actual data, using the available key information, such that it cannot be easily read and decoded by a third party. Only the end points have the necessary key information to encode and decode the data correctly. The method used to pass this key information between end points is known as the key exchange.

There are a number of standard methods to encrypt data. These are very secure in their coding, and have been field tested over a number of years with critical information such as financial and personal data. From a user view, all that is important is to know that the data is secured. The method to use to encrypt the data is negotiated by the end points. If one, or both, of the endpoints do not support encryption, the connection may still be established, but will be unsecured. In this way a voice call can still be established to equipment that doesn’t support encryption methods.

Bandwidth considerations (voice and signalling encryption)

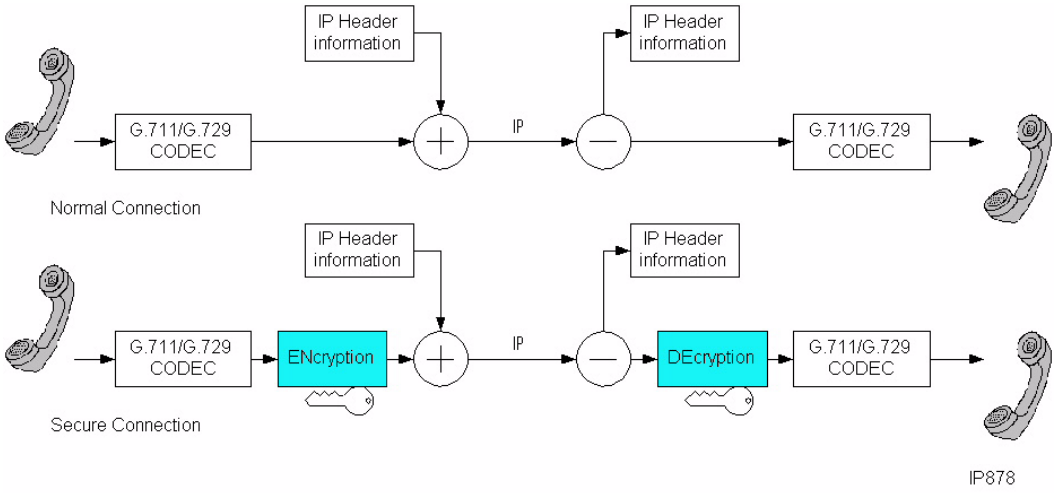
The secure connection uses data encryption to modify the contents of the payload, so that someone collecting data packets will be unable to read the real contents. It doesn’t modify the contents of the IP header, since this is still needed to pass data over the existing Layer3 routers and Layer 2 network switches. If the headers were also encrypted, then every router in the path would need to know how to decipher the information.

The data in the payload is intended for a particular application. It is the application that knows how to decode the information. For the Voice over IP application, this payload contains the signalling information or voice streaming.

When the data is encrypted, it is simply replaced with a scrambled version. This is a 1 for 1 transformation, so there are no additional bytes. As a result, the bandwidth is the same for encrypted or non-encrypted information.

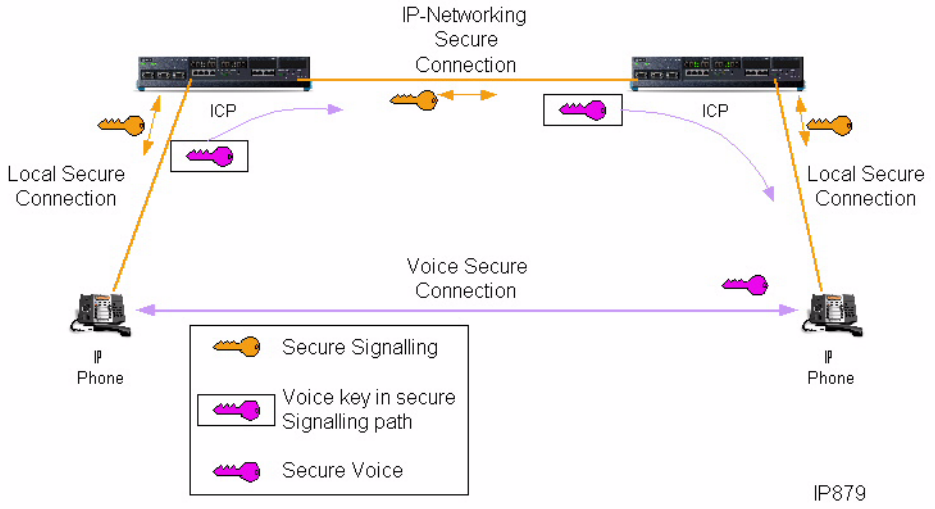
For the signalling information, there are some additional messages related to setting up the secure connections. However, these are minimal when compared to the remainder of the signalling bandwidth, which is already quite low. For voice information the bandwidth remains the same for both encrypted and unencrypted payloads.

As an analogy, the encryption can be considered as simply another voice CODEC or an additional process in the voice-streaming path. For voice streaming, G.711 and G.729 CODECs are often used. The encryption merely makes these secure, so the result is a secure-G.711 and a secure-G.729 CODEC. The bit rate remains the same, as does the network bandwidth requirements.



Signalling and media paths

The signalling path is generally between the controller and the IP Phone, or end-device. This path is established as a secure connection. Signalling information is interpreted within the controller. Where a message needs to be sent to another controller, such as with IP-Networking, or to another end device, an independent secure connection is used. Thus a call between two phones on two controllers will require the establishment of three secure signalling channels, that is a secure connection at each controller and one between the controllers.



The signalling paths with security do not take different network routes compared to those without security. The only difference is that the contents of the payload are encrypted, or ‘hidden’. The only additions, for security, are some messages to establish the point to point secure connections and the negotiation of the secure voice connection. Thus the signalling is secured; MiNet becomes Secure-MiNet and MiTai becomes Secure-MiTai.

Once the signalling paths are established and a voice connection can be made, the two end devices will negotiate the keys and method of voice encryption. Once agreed, the voice now streams directly between the two devices. This is the same as the unencrypted case, only the voice data is now ‘hidden’.

Voice streaming security (SRTP)

Secure RTP is basically the standard RTP payload, but with some form of encryption applied to it. This provides added confidentiality, message authentication and replay protection over the standard RTP protocol. A call will be encrypted, and uses the most secure method, if both ends support encryption. Calls initiated on a controller, an IP Phone, or an end device that does not support encryption (pre-release 6.0) are still supported, but will not be encrypted.

Signalling security

Two main methods are used to secure a signalling channel. These are:

- SSL
- Secure MiNet

Secure MiNET uses a predefined algorithm to encode the signalling messages. Negotiation of the encryption method to use is not needed and this provides a simpler and faster method to establish secure connections.

In addition to Secure MiNET, a standard encryption method that uses SSL is also available on certain end devices. SSL is used to negotiate which encryption method to use at the end points. This standard will allow interaction with third party applications.

The IP Phones will determine which secure method to use, starting with SSL, then secure MiNet, then unsecured. The ICP uses multiple IP ports to differentiate these protocols (6800, 6801, 6802) as defined in the IP port information. If the relevant port is blocked, for instance with a firewall, or a router, the negotiation may fail and may result in no connection being established.

IP-Networking communication between ICP controllers and gateways only use SSL, or no encryption.

Encryption support

A number of end devices support secure signalling and secure voice media streaming. The following table lists the devices and security support:

Table 43: Security Support by Device

Device	Secure Signalling (SSL)	Secure Signalling (Secure MiNET)	Voice Encryption
Controller/Gateway			
SX-200 ICP CX/MX/AX	No	Yes	Yes
Phone			
5001	No	Yes	Yes
5005	No	Yes	Yes
5010	No	Yes	Yes
5020	No	Yes	Yes
5201	No	Yes	Yes
5205	No	Yes	Yes
5207	No	Yes	Yes
5212	Yes	Yes	Yes
5215	No	Yes	Yes
5215 (Dual Mode)	Yes	Yes	Yes
5220	No	Yes	Yes
5220 (Dual Mode)	Yes	Yes	Yes
5224	Yes	Yes	Yes
5230	No	Yes	Yes
5140	No	Yes	Yes
5240	No	Yes	Yes
5485 IP Pager	No	Yes	Yes
			Page 1 of 2

Table 43: Security Support by Device (continued)

Device	Secure Signalling (SSL)	Secure Signalling (Secure MiNET)	Voice Encryption
5304	Yes	Yes	Yes
5312	Yes	Yes	Yes
5324	Yes	Yes	Yes
5330	Yes	Yes	Yes
5340	Yes	Yes	Yes
5540	Yes	Yes	Yes
Navigator	Yes	Yes	Yes
YA Client	No (See Note)	No (See Note)	N/A
YA Softphone	No (See Note)	No (See Note)	No
YA Server	No (See Note)	No (See Note)	N/A
SpectraLink wireless	No	No	No
DECT wireless	No	No	No
Teleworker Server Int	Yes	Yes	Yes
Teleworker Server Ext	Yes	Yes	Yes
Speak@Ease (6500)	No	No	No
NuPoint (6510)	No	No	No
			Page 2 of 2

Note: The MiTai connection from the MiTai client, or server, to the ICP is secure with SSL only. Other connections are not secured.

Voice streaming to external gateway PSTN connection

In this case the voice path is established between the IP-Phone and the IP/TDM Gateway. This might be the local ICP, or another unit dedicated to this function and connected via IP-Networking. There is no difference in the connection path between secure and non-secure call establishment. Connections will be established as secure, where possible.

Voice streaming to TDM connections

Where an ICP has a number of TDM connected devices, calls to these devices will be via local IP/TDM gateway. Encryption applies to the packet part of the connection, and so the IP path to the gateway will be secure, where possible. The connection on the TDM side will remain, as it always has, with a dedicated connection to the end device.

Voice streaming to internal voice mail, Record-a-Call and conference

Where there are internal features to the ICP, these are considered TDM device. Encryption applies to the packet part of the connection, and so the IP path to the gateway will be secure,

where possible. The connection on the TDM devices will remain as it always has with a dedicated connection to the requested service.

A conference call with a number of users requires multiple connections to the IP-gateway. Connections between the IP end device and this gateway will be encrypted, where possible. Connections to the Conference Bridge are established over the internal TDM infrastructure. PSTN connections, or TDM devices, connected into this bridge will not use encryption, but will maintain their normal dedicated connections.

Voice streaming to applications

A number of applications and end devices support encryption. However, there are some that do not support encryption measures. As a result of this, connections to these devices will be established without encryption.

Application support for encryption is identified in the table above.

Note that end devices that connect to the external port of the Teleworker solution are secure. However, when similar end devices are used within the LAN environment, these may not be fully secured. This applies to are the YA Softphone and YA Client. Further details can be found in the Teleworker Engineering Guidelines. The Teleworker Server (6010) also terminates both internal and external secure connections. This allows for differences in encryption methods, or external secure connection and unsecured internal connection.

The SpectraLink wireless phones may use a level of security on the air access interface (radio link), such as WEP or WAP2. However, this only covers the wireless connection and not necessarily the remaining connection across the remaining network infrastructure.

Secured access with 802.1x

A number of networks now support a level of access restriction to the network ports. A device that connects to one of these ports needs to be authenticated as valid before connections can be established. There are a number of protocols that can do this:

- Cisco VMPS
- 802.1x

The Cisco VMPS is described elsewhere within the Engineering Guidelines.

IEEE 802.1x is similar in operation to VMPS, but uses a RADIUS Server for authentication. Devices that authenticate through 802.1x will require an identification and password to gain access. There are a number of protocols that are used to establish the initial connection. Mitel end devices (‘supplicants’) support the EAP-MD5 protocol.

If the administrator configures the L2 for port access control, the connected IP Phone will prompt the user for a user account and a password if one has not already been entered beforehand, or information saved in the phone is invalid. Based on the response, the port may be opened

for access, the VLAN settings may change, the port could be opened to a guest VLAN, or it could be shut down.

When a PC is connected to a port, it will be interrogated in the same manner as the phones, and user input will be required. The same results will likely occur.

Typically 802.1x will only allow a single device to be authenticated and connected to a port. This restricts how devices can be connected into the network infrastructure. Where a network port only supports a single connected device, then for full authentication only a phone or a PC should be connected to this port. If it is required to connect both a phone and a PC, in this situation, then only the phone should provide authentication. If authentication is provided only by the PC and it isn't present, the phone may not work.

Not all network access devices place single device restrictions on connected devices. It is known that HP switches will allow multiple devices to be connected and authenticated to a single port. With Cisco switches, where the IP-Phone uses the Auxiliary_VLAN setting, both an IP Phone and a connected PC can operate off the same port.

A PC connected behind a phone may need to authenticate access. Failure to do this correctly may result in the network port being shut down. This may result in the IP Phone also being disconnected. Ideally the PC should be programmed with the necessary information for 802.1x authentication through the 'PC Network Properties'. If not, then it is possible that the PC could fail the authentication timeout, at the port, or at subsequent authorisation requests. It may also be necessary to connect the PC to the phone after the phone has authenticated connection.

An 802.1x port may be configured to request authentication only at startup of the network port and may include regular authentication retries.

Because authentication is based on a network port becoming active, it is possible, with some network switches, that an unathorised device can be connected behind an IP-Phone, once the IP Phone has itself gained access to the port. It is therefore recommended to enable the reauthentication response to regularly check access to the port and identify such connections. The default time is often of the order of 3600 seconds.

The following list highlights those MITEL IP Phones that support 802.1x:

Table 44: 802.1x Support by Device

Device	802.1x Support
5001	No
5005	No
5010	No
5020	No
5201	No
5205	No
5207	No
Page 1 of 2	

Table 44: 802.1x Support by Device (continued)

Device	802.1x Support
5212	Yes
5215	No
5215 (Dual Mode)	Yes
5220	No
5220 (Dual Mode)	Yes
5224	Yes
5230	No
5140	No
5240	No
5485 IP Pager	No
5304	Yes
5312	Yes
5324	Yes
5330	Yes
5340	Yes
5540	Yes
Navigator	Yes
YA Softphone (PC)	If on PC
YA Client	If on PC
SpectraLink wireless	No
DECT wireless	No
	Page 2 of 2

Appendix C. Rapid Spanning Tree Protocol

Rapid Spanning Tree Protocol (RSTP)

As of Release 3.0, the Rapid Reconfiguration of Spanning Tree Protocol (RSTP) is supported on the SX-200-ICP CXi Controller.

About STP/RSTP

In an Ethernet network that is not using STP/RSTP, multiple active paths between devices are not allowed since multiple paths will cause network loops. See the following Figure.

Network loops are unacceptable because a broadcast or multicast packet sent from Station “A” to Station “B” will be forwarded by Switch “B” to Station “B” and also back to Switch “A”, when Switch “A” receives the packet it will then forward the packet back to Switch “B” and the cycle will repeat for infinity causing a broadcast storm.

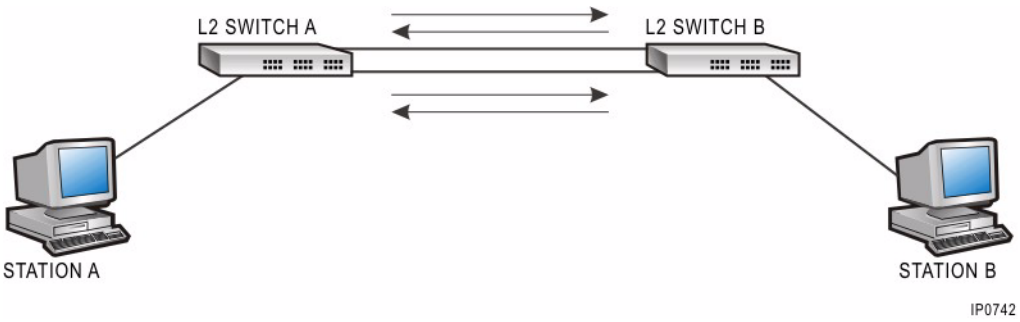


Figure 32: Network Loop

Note that some older L2 switches may only support an older version of the protocol called Spanning Tree Protocol (STP).

The Rapid Reconfiguration of Spanning Tree Protocol (RSTP) is also a Layer 2 Link Level protocol specified by the IEEE (802.1w) that runs on bridges and switches.

STP and RSTP serve the same purpose. The difference between the two protocols has to do with how quickly the algorithms can converge on a network. RSTP "reconverges" networks faster than STP.

The guidelines in this section are applicable to both STP and RSTP, any differences between the two protocols will be highlighted.STP allows for physical path redundancy by placing redundant network paths into a standby mode by blocking traffic on redundant port.

Should a currently active network path fail due to a Bridge/Switch failure or a network cabling failure, STP will enable the network path that was previously held in a standby mode and network connectivity will be restored. The following Figure depicts how STP breaks a potential network loop by blocking traffic on one of the ports on Switch “B”.

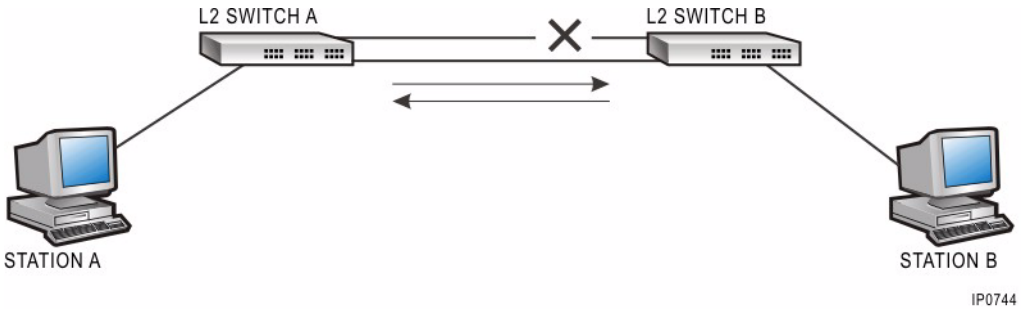


Figure 33: Network Loop Broken by STP

STP, network topology, and terminology

- **Bridged LAN versus Switched LAN**

  Bridges and switches are Layer 2 devices that are used to forward packets between different network segments.

  Switches offer better data throughput and higher port density than bridges. As a result, Switches have displaced bridges as the preferred internetworking solution.

  A bridged LAN is composed of two or more LANs that are interconnected with bridges. In a bridged LAN that is running STP, the logical centre of the network is called the root bridge.

  A switched LAN is composed of two or more LANs that are interconnected with switches. In a switched LAN that is running STP, the logical centre of the network is called the root switch.

  This document uses the terms bridge and switch interchangeably.

- **Port States**

  STP places a port into one of the states listed below. The state of each port dictates how the port handles received packets and whether or not it will forward packets. A special packet called a Bridge Protocol Data Unit (BPDU) is passed between bridges and switches to communicate information about the bridge/switch to other bridges/switches in the network. STP relies on the information carried in these BPDUs to learn about the network topology.

  - **Blocking—**A port in the blocking state does not perform frame forwarding, As a result, a port in this state prevents packet duplication by blocking transmission on a duplicate link. The blocking state is used to prevent network loops. Received frames will be discarded and frames will not be transmitted out of this port. BPDUs received will be processed but BPDUs are not transmitted on a port in the blocking state.
  - **Listening/Learning**—A port in the listening/learning state is preparing to participate in frame forwarding. Frame forwarding is temporarily disabled to prevent network loops. Received frames will be discarded and frames will not be transmitted out of this port. BPDUs received will be processed and BPDUs will be transmitted on a port in the listening state.
  - **Forwarding—**A port in this state is participating in frame forwarding. Received frames can be forwarded and forwarded frames can be submitted for transmission. BPDUs received will be processed and BPDUs will be transmitted on a port in the forwarding state.

- **Disabled**—A port in this state does not participate in frame forwarding, nor does it participate in the Spanning Tree Protocol. Received frames will be discarded and frames will not be transmitted out of this port. BPDUs received will not be processed and BPDUs will not be transmitted on a port in the disabled state.

- **Root Switch**

  Within a STP enabled LAN one Switch is elected to be the Root Switch. The Root Switch becomes the logical centre of the network. All ports on the Root Switch become Designated Ports. All decisions made by STP, such as which ports to block and which ports to put in forwarding mode are made with respect to the Root Switch.

- **Root Port**

  All Switches (except the Root Switch) in the network must select one of their ports to become the Root Port. The Root Port is a port that leads back to the Root Switch and has the lowest path cost. Path cost for all ports in the network are determined by STP, the value of a particular path cost is based on the interface speed and how far away from the Root Switch this port is.

- **Designated Port**

  Any Switch ports in the network that are responsible for connecting a LAN segment will become Designated Ports. Designated Ports are responsible for forwarding packets on behalf of that particular LAN segment.

- **Bridge Protocol Data Unit (BPDUs)**

  STP defines a specialized packet called a Bridge Protocol Data Unit (BPDU). All Switches in the network transmit BPDUs to their neighboring Switches.

  A BPDU contains parameters specific to the Switch that generated the BPDU, such as Bridge Priority, Path Cost, Port Priority and various STP timer values.

  In Release 3.0 and higher of the SX-200-ICP, these parameters are set to default values and are not user configurable. (See “SX-200 ICP CXi Release 3.0 and higher RSTP default parameters” on page 185.)

  STP uses the information contained in the BPDUs to create a mental picture of the network, elect a Root Switch, select Root Ports and select Designated Ports. When this process has completed the ports that are not Root Ports or Designated Ports will be placed into a Blocked state. STP then will start the final stage of convergence whereby the Root and Designated Ports are prepared to enter the Forwarding state.

  Figure 34, ”Converged STP Network,” p. 182, depicts an STP network that has converged or stabilized. Using this Figure as a reference it can be seen that

  - L2 Switch 1 has been elected the Root Switch and all of it's ports have become Designated Ports
  - L2 Switch 2 has selected it's port connecting to LAN B to be its Root Port (since this port has the lowest Path Cost to the Root Switch) and its port connecting to LAN C to be its designated port.
  - L2 Switch 3 has selected its port connecting to LAN B to be its Root Port (since this port has the lowest Path Cost to the Root Switch) and its port connecting to LAN C is put into a Blocking state to prevent a network loop from being formed.
  - L2 Switch 4 has selected its port connecting to LAN C to be its Root Port (since this port has the lowest Path Cost to the Root Switch) and its port connecting to LAN D to

be its designated port.

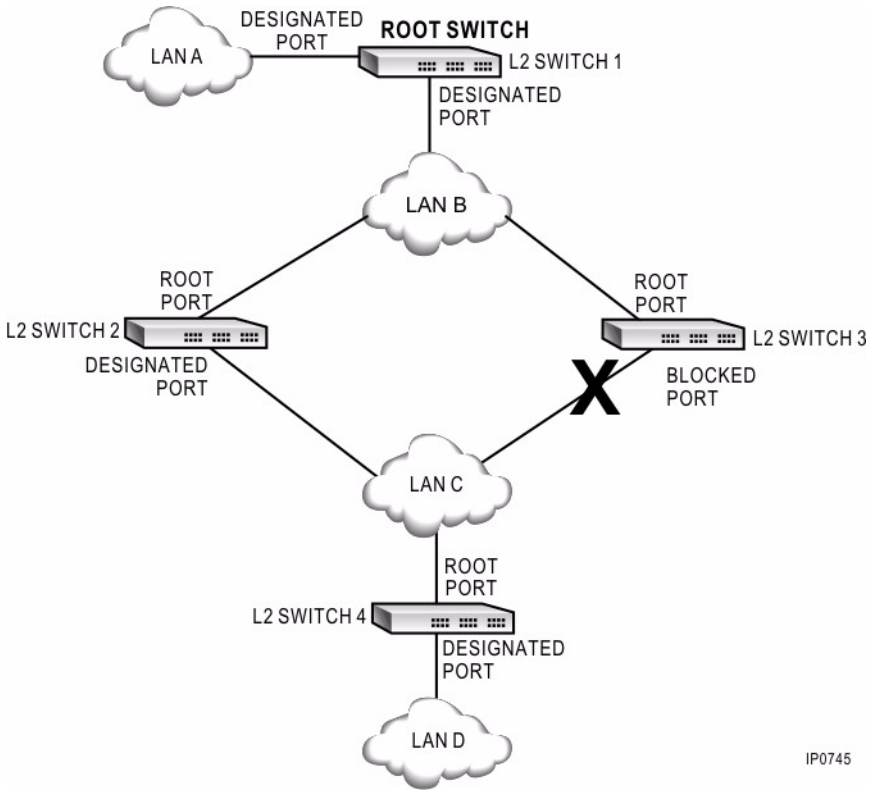


Figure 34: Converged STP Network

Note: A Designated port is the side of the switch that is opposite to the Root port, the designated port can provide connectivity to a LAN or a single network element.

STP network design guidelines

This section is intended as a design guide for the System Administrator or Installer.

Caution: Enabling STP in a live network will cause service disruptions to the end users while the network is converging. To avoid impacting users, enabling of STP should be conducted outside of core hours or during a scheduled maintenance period.

- ❒ Create an accurate diagram of the network. This diagram should include interface speed information.
- ❒ The System Administrator should establish which switch will be the Root Switch (the Root Switch should be a powerful switch).
  - The SX-200 ICP should not be used as the Root Switch. To safeguard against this occurring the SX-200 ICP is factory programmed with the highest possible value for Bridge Priority.
  - The Root Switch should be located in a position that will minimize the average

distance between the Root Switch and all other network elements. Typically the Root Switch should be in the core network. Note that STP has a 7 hop limit, see “Topology restrictions” on page 185.

- If possible, high usage servers and routers should be directly connected to the Root Switch.

❒ Once you have decided which Switch should be the Root Switch, reduce the value of the Bridge Priority on this Switch to the lowest possible value. Since a lower value equates to a higher priority this ensures that STP recognizes this switch as the Root Switch.

❒ Understand where the redundant links are located and where blocking might occur. If the Root Switch is optimally located and optimally connected in the network, tuning of individual port costs to control which ports get blocked should not be necessary.

- Be aware that under some circumstances due to poor location of the Root Switch, poor interconnection of Switches to the Root Switch or non standard values for port costs, STP might utilize a non-optimum link and block the optimum link. For example, given a choice between a 10 Mbp/s link and a 100 Mbp/s, STP should choose the 100 Mbp/s link for making the active connection and the 10 Mbp/s link should be put into a blocked state (see “Efficient usage of inter-switch connections” on page 183).
- Try to keep the number of blocked ports in the network to a minimum. A blocked port is all that prevents a network loop, by minimizing the number of blocked ports in the network there is less risk of network problems due to a blocked port being erroneously moved into the forwarding state.

❒ It is recommended that you use the factory default STP parameters for your L2 switches. Only the following parameters might require changing:

- Bridge Priority, used to select the Root Switch.
- Port Cost, used to select link redundancy or control traffic load balancing and bandwidth optimization.

Efficient usage of inter-switch connections

As mentioned in the previous section the System Administrator should not allow STP to blindly choose which network paths will be active, instead the System Administrator should have a good idea of what connections will provide optimum bandwidth usage so that he can guide STP through appropriate network design to provide optimum connectivity.

This section provides an example of one scenario where STP does exactly what it is supposed to do, however, if the System Administrator had configured the network differently a more efficient usage of available connections would have been selected by STP.

In the following diagram there is a 1G Ethernet connection available that could have been used to connect L2 Switch A to L2 Switch B, however it was not used.

When STP converged the network the following decisions were made:

- L2 Switch A was elected as the Root Switch and placed both Port 1 and Port 2 into a Forwarding state.
- L2 Switch B placed both Port 1 and Port 2 into a Forwarding state.

- SX-200 ICP B placed Port 1 into a Blocked state to prevent a network loop and placed Port 2 into a Forwarding state to provide connectivity to L2 Switch B.
- SX-200 ICP A placed both of it's Ports into a Forwarding state to provide connectivity to L2 Switch A and L2 Switch B.

STP did what it was supposed to do, it removed any network loops and provided connectivity to all devices. But it should be noted that all of the traffic intended to move between L2 Switch A and L2 Switch B now has to flow through SX-200 ICP A. This is not a problem to the ICP but all of this traffic is forced into flowing over a 100M Full Duplex link when the 1G Full Duplex link available on the L2 Switches could have been utilized.

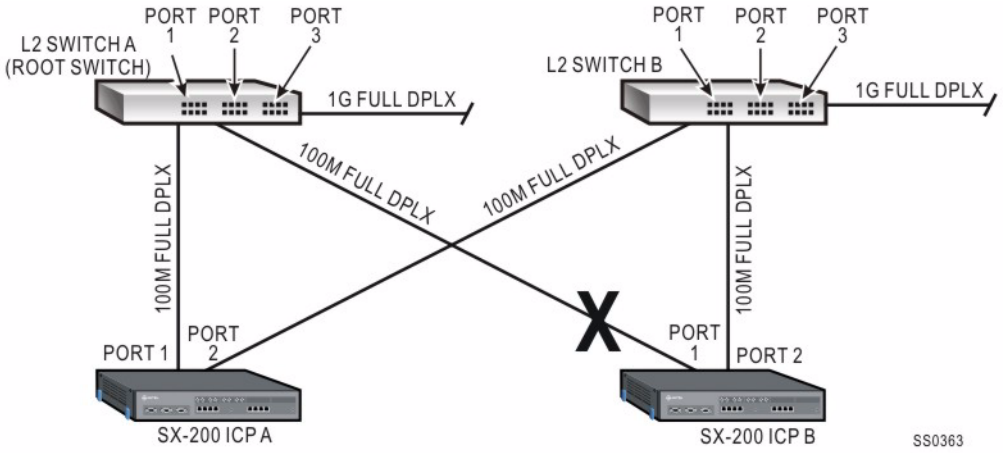


Figure 35: Inefficient Use of Connections

The following diagram depicts how STP would have converged the network had the 1G Full Duplex link been available.

When STP converged the network the following decisions would have been made:

- L2 Switch A was elected as the Root Switch and placed all of it's Ports into a Forwarding state.
- L2 Switch B placed all of it's Ports into a Forwarding state.
- SX-200 ICP B placed Port 1 into a Blocked state to prevent a network loop and placed Port 2 into a Forwarding state to provide connectivity to L2 Switch B.
- SX-200 ICP A placed Port 2 into a Blocked state to prevent a network loop and placed Port 1 into a Forwarding state to provide connectivity to L2 Switch A.

Now all traffic intended to move between L2 Switch A and L2 Switch B is transported over the 1G Full Duplex link.

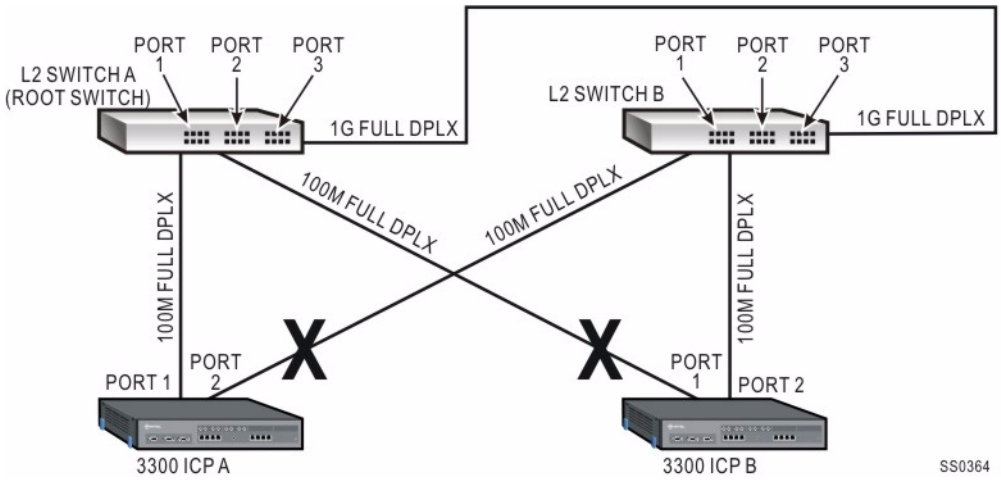


Figure 36: Efficient Use of Connections

Topology restrictions

STP/RSTP is by default set to to a 7-hop limit, which is a result of the default STP/RSTP aging parameters. Basically, this means that frames should not pass through more than 7 bridges as this limits the size or diameter of the bridged STP/RSTP network to a maximum of 7 hops.

SX-200 ICP CXi Release 3.0 and higher RSTP default parameters

In Release 3.0 and higher, the System Administrator has the ability to enable or disable RSTP. The CXi ships with RSTP disabled and the bridge priority set to 61440.

These parameters can be changed via CDE; for details, see the Technical Documentation.

The System Administrator cannot alter any of the other RSTP parameters. The SX-200-ICP RSTP algorithm is based on the IEEE 802.1w standard. Below are the RSTP parameters and their default values.

Note that bridge priority is set to a high value which in turn means a low priority. This value was chosen to minimize the possibility of the SX-200-ICP CXi becoming the Root Switch. It is the Root Switch parameters that control overall network RSTP operation.

Bridge parameters

- STP ENABLE-false (Factory Default this setting is programmable)
- BRIDGE PRIORITY-61440 (Factory Default this setting is programmable)
- BRIDGE MAX AGE-20 seconds
- BRIDGE HELLO TIME-2 seconds
- BRIDGE FWD DELAY-15 seconds

Port parameters (Ports 1 to 16)

- PORT ENABLE-true
- PORT FAST-false
- PATH COST-10Mb/s = 2,000,000
- PATH COST-100Mb/s = 200,000
- PATH COST-1Gb/s = 20,000
- PORT PRIORITY-128

STP/RSTP performance and convergence

When a topology change takes place in a well designed network running STP, the network does not reconverge for approximately 50 seconds; a network running RSTP takes about 3 seconds to reconverge.

When a topology change takes place in a well designed network running STP the network will not reconverge for about 50 seconds. The protocol uses this guard time interval to ensure that all ports that should be blocked do get put into the blocking state before any ports get put into the forwarding state. This ensures that loops do not get created during a topology change.

Convergence time can be optimized with the correct usage of Port Fast, Uplink Fast and Back Bone Fast when configuring the L2 switching infrastructure. For details refer to the L2 Switch vendor's documentation.

Convergence time can also be optimized when the number of Bridge or Switch hops is kept to a minimum.

Altering L2 Switch STP/RSTP timer values is not a recommended method of obtaining optimal convergence times unless the System Administrator has a thorough understanding of STP/RSTP and understands the risks involved.

Using non-default values for STP/RSTP timer values will decrease the guard time interval referred to above which in turn erodes any reconvergence safety margin in the network and increases the possibility of loops being formed while STP/RSTP is reconverging.

Minimizing bridge/switch hops

Achieving optimal STP/RSTP convergence times involves minimizing the number of Bridge or Switch hops in the network.

The root L2 switch should be one of the Core Network L2/L3 switches. If additional access network L2 switches are required for connecting phones, the switches should be added at the same level as the existing access layer switches so that additional switch hops are not added, e.g. the phones are directly connected to the access layer network.

Physical connection, Layer 2 switch to ICP

If Spanning Tree is not running on the L2 switch, there should be only one physical connection between the distribution network L2 switch and the ICP. The connection should be made with a Category-5 or better UTP cable.

If Spanning Tree is running on the L2 switch and you are using a controller with RSTP enabled, here can be multiple physical connections between the distribution network L2 switch(es) and the ICP. The connections should be made with a Category-5 or better UTP cable.

Note: The System Administrator should enable STP on the ICP before completing the physical connections to the L2 switch(es).

If STP/RSTP is running on the L2 Switch and you are using a controller with STP/RSTP disabled, use only one physical connection between the distribution network L2 switch and the ICP. This will ensure that loops are not created. Make the connection with Category-5 or better UTP cable.

If the System Administrator chooses to have multiple connections between the ICP and the L2 switch, the following requirements must be met:

- STP must be running on the L2 switch.
- The L2 port used to connect to the ICP must not be set to PortFast, this is to ensure that this port fully participates in the STP algorithm.
- The System Administrator must ensure that no one alters the above settings on the L2 switch at a future date.

Port settings for connecting L2 switches to ICPs

The L2 switch port that is used to connect to the ICP should be configured with the following

settings:

- If Spanning Tree is not running on the L2 Switch, the L2 Switch port should be configured to allow for speed and duplex Auto-Negotiation. The port should be capable of running 100Mbits/s FULL DUPLEX.
- If STP/RSTP is running on the L2 Switch but STP/RSTP is disabled on the ICP, then the ICP is not participating in STP/RSTP.

  In this scenario, if there is only one physical connection between the ICP and the L2 switch, the ICP should be treated as an end point, and

  - the L2 Switch port should be configured for PortFast operation (ensures that this port skips the first stages of the STP Algorithm and directly transitions to Forwarding mode).
  - the L2 Switch port should be configured to allow for speed and duplex Auto-Negotiation. The port should be capable of running 100Mbits/s FULL DUPLEX.

  In this scenario, if there are multiple physical connections between the ICP and the L2 switch the ICP should not be treated as an end point, and the L2 Switch port should not be

configured for PortFast operation (ensures that this port participates in the STP/RSTP algorithm).

  - the L2 Switch port should be configured to allow for speed and duplex Auto-Negotiation. The port should be capable of running 100Mbits/s FULL DUPLEX.

- If STP/RSTP is running on the L2 switch and STP is enabled on the ICP, then the ICP is participating in STP/RSTP. There can be two or more physical connections between the ICP and the L2 switch(es), and as a result, the ICP must be treated as an STP/RSTP participant, and
  - the L2 Switch port should NOT be configured for PortFast operation (PortFast should be disabled to ensure that this port fully participates in the STP/RSTP algorithm).
  - the L2 Switch port should be configured to allow for speed and duplex Auto-Negotiation. The port should be capable of running 100Mbits/s FULL DUPLEX

Enabling STP/RSTP

The SX-200 ICPs are shipped from the factory with STP/RSTP disabled. The SX-200 ICP's integral L2 switch will start running during the SX-200 ICP initialization/boot phase.

The following precautions should be observed to prevent temporary network loops from forming and to minimize network disruptions:

- If multiple cables are connected between the SX-200 ICP and the L2 switch(es) during the initialization/boot phase a network loop will be created by the SX-200 ICP, this loop will impact the network in a detrimental way unless STP has been previously enabled on the L2 switch(es).
- The safest way to proceed is to configure the L2 switch(es), enable STP/RSTP on the SX-200 ICP and then connect the cables.

Caution: Enabling STP/RSTP in a live network will cause service disruptions to the end users while the network is converging. To avoid impacting users, enabling of STP/RSTP should be conducted outside of core hours.

Networks running different versions of STP

There are many of versions of Spanning Tree Algorithm (STA) protocols in existence, a number of these are proprietary and there are three main open standard protocols as listed below. This document does not discuss proprietary STAs, the three open standard STAs are described below.

IEEE Standard 802.1D, also known as Spanning Tree Protocol (STP), provides convergence times of about 50 seconds.

IEEE Standard 802.1w also known as Rapid Reconfiguration of Spanning Tree Protocol (RSTP) provides convergence times in the order of 1 to 3 seconds.

IEEE Standard 802.1s also know as Multiple Spanning Trees Protocol (MSTP) provides support for multiple VLANS and provides convergence times similar to RSTP.

Using the SX-200-ICP CXi in networks running other versions of STP

The SX-200-ICP CXi supports the IEEE Standard 802.1w Rapid Reconfiguration of Spanning Tree Protocol.

RSTP is compatible with MSTP which means that the SX-200 ICP CXi can be deployed in a data network that is running MSTP. RSTP/MSTP convergence times of 1 to 3 seconds will apply to the network segments running RSTP/MSTP.

RSTP is backwards compatible with STP which means that the SX-200 ICP CXi can be deployed in a data network that is running STP.

RSTP convergence times of 1 to 3 seconds will apply to the network segments running RSTP and STP convergence times of 50 seconds will apply to network segments running STP.

When deploying the CXi in a network running STP, the System Administrator should pay particular attention to how Port Cost is programmed on the L2 infrastructure. Port Cost is used to select link redundancy or control traffic load balancing and bandwidth optimization. When installing the CXi ICP into a RSTP or MSTP based network, the System Administrator might need to adjust certain parameters in the L2 infrastructure and/or comply with specific L2 topology recommendations. These details are outside of the scope of this document since they are typically vendor specific and can also be specific to a certain model of L2 switch.

The System Administrator should refer to the L2 switch Vendor's documentation for planning the integration of the SX-200 ICP into a RSTP or MSTP environment.

STP and VLANS

The 802.1d and 802.1w MAC Bridges Spanning Tree Protocol does not sense VLANs. Therefore, it does not directly affect the portion of the network utilized by the SX-200 ICP and the IP phones. If this protocol is being used throughout the network, the System Administrator needs to be aware that STP and RSTP are insensitive to VLANs.

The following diagram shows two 802.1Q compliant L2 Switches. VLAN 1 is connected via the 802.1Q trunk and the regular link. VLAN 2 is only connected via the 802.1Q trunk. VLAN 1 presents a problem in that it forms a network loop. When STP is enabled on L2 Switch A and L2 Switch B STP will break the loop formed by VLAN 1 by blocking one of the ports on one of the L2 Switches. If STP chooses to block one of the ports used for implementing the 802.1Q trunk there will be two outcomes:

- The network loop will be broken, as it should be.
- Connectivity for VLAN 2 may be broken, this is not desirable.

To find the preferred solution to this problem the System Administrator should consult the L2 vendor's documentation.

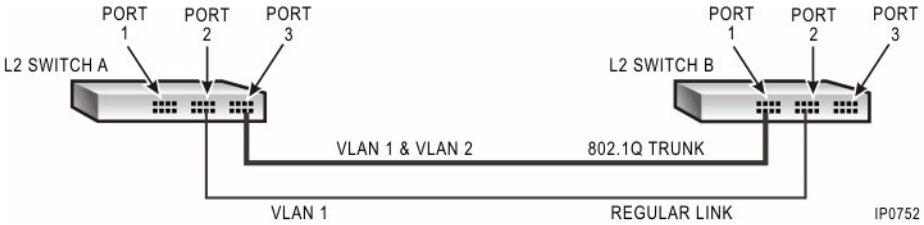


Figure 37: Asymmetrical VLANs

Known issues

Failure to forward BPDU packets

Failure to Forward BPDU Packets Causes Network Loops. Some third party switches do not forward Bridge Protocol Data Unit (BPDU) packets when STP/RSTP is disabled on the switch. This will prevent switches that are running STP/RSTP from detecting network loops since STP/RSTP relies on BPDUs to determine if a network loop exists. This situation can cause broadcast storms and connectivity issues. To correct this situation

- Replace the offending switch with a switch that is fully STP/RSTP compliant.
- Enable STP/RSTP on the offending switch.

A unidirectional link that remains in an enabled state will fail to forward BPDUs in one direction. This situation can be caused by defective cabling or defective interface hardware. For example if a link between switch A and switch B is provided by a fibre cable and the A to B transmit fibre is defective but the transmission path from B to A is functional the following will take place:

- BPDUs transmitted by A will not be received by B.
- If B is supposed to be in the Blocking state it can only remain in the Blocking state if it is receiving BPDUs from a switch with a higher priority.
- Since B is not receiving BPDUs from a switch with a higher priority, B will start to forward traffic to A and this will create a network loop that STP is unable to detect.

To try and prevent this situation from occurring:

- Some L2 switch vendors provide proprietary schemes for detecting unidirectional links. If this feature is available the System Administrator should enable the feature.

Ethernet duplex mismatch causes network loops

Ethernet duplex mismatch is one of the leading culprits for STP/RSTP failures and problems. The problem is created when one device has been hard coded into full duplex mode and the other device is set for auto-negotiation. This results in the device that is set for auto-negotiation moving into the half duplex mode because the hard coded device is unable to auto-negotiate.

If a switch sends BPDUs out of a port that is set to half duplex to a switch port that is configured for full duplex operation the duplex mismatch can cause a network loop to occur.

The reason is that the full duplex switch will transmit packets even if the half duplex switch is transmitting. If there is enough traffic originating from the full duplex switch the half duplex switch will be unable to successfully transmit packets due to collisions and the collision/backoff algorithm, this includes BPDU packets.

Eventually the full duplex switch will conclude that it has stopped receiving BPDUs from the half duplex switch and conclude that this link or switch is faulty, the full duplex switch will then unblock it's previously blocked port and a loop is created.

To correct this situation:

- Ensure there are no duplex mismatches between switch ports.
- If the switch vendor has provided a mechanism for detecting duplex mismatches it should be enabled.

Appendix D. VoIP and VLANs

VoIP Installation and VLAN Configurations

Although this document states VLAN configurations, it can also be used to consider whether VLAN is needed, or not, for a particular installation.

There are, currently, six configurations that have been identified. These are not expected to cover all possible configurations, there will always be exceptions, but as a guideline for the more general installations. The number of configuration variations has arisen because of the introduction of the CXi product, which includes a VoIP capable Layer2 switch. In effect the CXi is now an integral part of the network, whereas the MX and AX are considered more as an end point or server within the network.

The main installations that are likely to be encountered are:

- A standalone CXi, voice-only devices, including expansion Layer 2 switch.
- Segregation of data and voice networks, with a router connecting the two. (In effect this is a physical solution, rather than the logical solution through use of VLAN.)
- Standalone CXi unit with dedicated ports for voice and data devices, no expansion switch.
- CXi with expansion Layer 2 switch, voice and data using dedicated ports on both CXi and expansion switch
- Data devices using second port of voice devices, i.e. both devices share a common connection
- CXi is more a server and connects to a larger network infrastructure. The voice and data devices are connected elsewhere within the network. (This is also the connection scenario for the MX.)

When to use VLAN?

VLANs are used to provide a level of logical separation between voice devices and other devices in the network. The main requirement is to ensure that there is adequate priority setting at the various network egress points, and that priority queues are enabled at these points. Layer 2 priority setting can only be provided in conjunction with VLAN settings.

The simple question to ask is probably “will the voice information need to share a common connection with other data?” If it does, then priority schemes are needed at that point, which implies VLANs are needed, at that point. Larger networks will also tend to use VLANs to provide a level of isolation and security between different services. However, the main requirement with voice, is to get access to the priority settings and information.

Network configurations

The following is a brief description of the different network configurations and whether VLANs are needed.

Standalone CXi, voice only

This is a self-contained configuration, with only the CXi unit involved in the network. There are only voice devices connected to the CXi.

There is only a single device at each egress point of the Layer 2 switch, and so there are no contention issues with data. There are also no data devices, so assigning priority to voice is meaningless, since all voice devices will have equal priority. The network switch internal bandwidth is in excess of the port capabilities, and much higher than the voice devices need to handle. There is unlikely to be any throughput issues.

Connection to an expansion Layer 2 switch is also not an issue. Again the connection bandwidth (Gig Ethernet) is in excess of that needed for the number of voice devices. Again VLAN and priority settings will not provide benefit on this link.

In effect, for this configuration, there is **no requirement for VLAN settings**.

Physical segregation of voice and data networks

One method to maintain priority between voice and data networks is to operate these as two independent networks. Although this may seem a little counter intuitive, it can be useful in providing demarcation between the different services where different personnel look after different parts of the network. The two networks are then joined at a higher level through a router. The two ‘networks’ would still need to be considered as a single system and IP addresses assigned as appropriate.

From the voice side of the network this is very similar to the standalone case. The main difference is a single connection to a router. This should be taken from the highest hierarchical point in both voice and data networks.

Connection of the router allows various PC devices to gain access to services of the ICP controller (CXi), if needed. For basic data operation, use of VLANs is unlikely to be needed, since the bandwidth available at the CXi will be higher than the router connection.

The one exception to VLAN usage might be on the data side of the network where YA softphones are in use. These devices are PC based, but are in effect voice devices. For the YA softphone, it is possible to queue data within the network, based on the value of the DSCP/Type of service field. It may be necessary to implement VLAN within the data section of the network in this case. The standard PC services will then take a VLAN and low priority value. The voice applications will need to map the Type of service field to a VLAN priority, to ensure correct priority queuing. All data from the PC will be in the same VLAN, just voice will have a higher priority marking. The router will remove the VLAN information.

So, in general:

- VLAN is not needed in the voice portion of the network
- VLAN is not needed in the data portion of the network, except when YA softphones are in use.

Standalone CXi without expansion switch, dedicated voice and data ports

In this configuration, the CXi controller becomes the network, albeit limited to 16 ports. There are no egress queuing issues since each device, either voice or data, has its own dedicated port. In this situation, the internal switching bandwidth of the internal Layer 2 switch exceeds that from the external ports. There is no need for priority mechanisms, hence no requirement for VLANs.

With this reduced configuration, there is **no requirement for VLAN settings**.

Expanded CXi, dedicated voice and data ports

This is similar in configuration to the standalone CXi with dedicated voice and data ports. The biggest difference is the connection between the CXi controller and the expansion Layer 2 switch. This link will be shared between voice and data devices. In practice, if the data requirements are low, then there should be sufficient bandwidth to run without priority queuing. However, data demands can vary, and there is a potential for congestion. In this case the voice traffic should be tagged with the higher priority.

The link between the CXi and expansion Layer 2 switch should have **VLAN enabled**.

The individual end devices can have VLAN and priority assigned at the ingress point of the network switches, and may use a common VLAN (and subnet). The priority will obviously be different. However, this is a physical implementation and requires ports to be reconfigured every time a device is moved. A general setting can be applied, with the data devices going to the default VLAN and the voice devices being assigned to the voice VLAN, such as through DHCP, or manual settings.

In this case the individual access ports should have **VLAN enabled**.

Common network connection for both voice and data devices

Where voice and data devices share a common connection to the network, there is a mix of data possible on the connection. On ingress to the network port, the phone will prioritise data. However, on egress, at the far end connection, this will not occur. Priority marking is needed to allow the egress priority to be carried through the network.

For this configuration **VLAN should be enabled at access and network device interconnections**.

Connection to corporate network

In this case the end devices are likely physically connected to network devices that are remote from the controller, e.g. different floors, separate building, etc. The connections through the network will carry a wide range of information, both data and voice. The controller is likely to be connected to the network at a point normally associated with other server devices. In this case it will be a voice server, be it a group controller, a voice gateway, or combination thereof.

Connections for the end devices, such as the phones, require **VLAN to be enabled**, at the access points.

For the controllers, or servers, **VLAN and priority is also needed**. However, this can be configured in different places. The VLAN, and priority, information can be added at the network access point. In this case all information will carry the voice VLAN, but will also carry equal priority for all services. It is also possible to differentiate services and overwrite the VLAN priority by mapping the type of service (Layer 3) priority field into the VLAN priority field. This is sometimes described as ‘TOS to COS’ or ‘DSCP to COS’ conversion.

Alternatively, the VLAN can be added at the server/controller and the network access point configured to accept VLAN information.

Glossary of Terms

AAP– Air Access Point. 802.11 wireless radio base station which may handle multiple devices and be networked.

ACD – Automatic Call Distribution. A package of advanced call processing features, relating to groups of agents who handle calls and agent supervisors.

Alarms. On the SX-200 ICP system, fault conditions are divided into three levels of urgency: minor, major, and critical.

- Minor alarms indicate problems affecting a portion of the system, such as failure of a line or trunk circuit.
- Major alarms indicate problems causing a system-wide degradation of service.
- Critical alarms indicate serious problems that cause automatic activation of system fail transfer.

AMB – Analog Main Board. The primary, integral, analog interface card for the CX/CXi and MX platforms contains a mixture of LS and ONS circuits, MOH, and door contacts.

Analog/Digital (A/D). Implies the transformation of analog signals (such as normal telephone speech signals) into their equivalent digital data signals. An A/D converter is the device generally used to perform this transformation. A D/A converter is a device that converts digital signals into their analog form (if required).

Analog Transmission. The transmission of a continuously varying signal. For example, in the transmission of speech the magnitude of the signal at any instant in the transmission path is proportional to the magnitude of the original input. This type of transmission is distinct from digital transmission in which the original input is encoded (for example, CODEC) and the resulting line signal is in digital form.

Answering Point. A device to which an incoming call is directed. It usually consists of an industry-standard telephone or an attendant console. Under certain conditions, an answering point may be a hunt group, a trunk, an ACD path or a device such as a night bell, an answering machine or a recorder/announcer machine.

AOB – Analog Option Board. The secondary integral analog interface card for the CX/CXi and MX platforms containing a mixture of LS and ONS circuits.

Application Processor. In a hospital, governmental agency, or a university environment, a processor can contain one or more application programs to meet a customer's particular needs. An application processor is usually set up to be accessed directly by an input/output device, however, in an SX-200 ICP system, the processor can be accessed by multiple input/output devices connected to the system.

ARP – Address Resolution Protocol. A Transmission Control Protocol/Internet Protocol (TCP/IP) suite that "maps" IP addresses to MAC addresses.

ASCII – American Standard Code for Information Interchange. A code developed by the American Standards Association for both synchronous and asynchronous data transmission between DTEs. Characters consist of an 8-bit binary code and incorporated parity bits.

ASU – Analog Services Unit. This unit provides a combination of analog ONS interfaces for phones and/or LS trunks.

Asynchronous Mode. In asynchronous data transmission, the time between bytes (characters) is indeterminate and depends upon external factors. The transmitted data has its own start and stop elements, and thus controls the receiving device. See also Synchronous Mode.

Attendant. The person assigned to handle calls at the attendant console.

Authorized Access Codes. The SX-200 ICP System can only be accessed for programming, maintenance or administration purposes by first entering an authorized access code (user name and password).

Autobaud Detection. Upon receipt of one or more characters, some data communication equipment can determine the baud rate of the transmitting source and then set its receive circuits to accommodate this baud rate. In the SX-200 ICP System, this feature applies to datasets and to the maintenance/CDE port which automatically adjusts their baud rate to match that of the terminal during initial setup.

Automatic Route Selection. Automatic route selection software automatically selects the optimum trunk route when a user makes a call. This selection is based on many factors, including cost, user priority, the day, and time of day.

B Channel. The 64-Kbit channel of a DNIC device which can carry digitized voice or ASCII characters at a maximum rate of 19.2 Kb/s.

Bay – Interface cabinet. On the SX-200 ICP and related products, a backplane and cabinet used to hold different interface cards, such as ONS, DNIC, and LS trunks.

BCC – Bay Control Card. Provides control for all peripheral interface cards.

Blocking. The condition existing in a switching system when the immediate establishment of a call is impossible due to insufficient switching connections being available in the system at that time.

BRI – Basic Rate Interface. The digital ISDN connection to a PSTN or local digital phone. Consisting of two digital channels for voice and data, this is the smallest quantity of digital channels that can be delivered. Variants include the U interface in North America and S0 in Europe.

Busy Hour. The hour when a system carries the most traffic (the busiest hour of the busiest day of a normal week).

Call Control. Software to create connections and paths between end user devices.

Call Processing. See Call Control.

CAT5 – Category 5 Cable. A UTP cable type used in a LAN which is capable of 100 Mbits/s transmission.

CCS – Centium Call Seconds. A measure of call traffic. For example, one call lasting 100 seconds is referred to as 1CCS.

CDE – Customer Data Entry. A command line interface used to configure the ICP.

CDP – Cisco Discovery Protocol. A Cisco proprietary protocol for determining certain operating modes of connected equipment, for example, power requirements and provisioning.

CEID – Cluster Element ID. A means of identifying different system units to maintain a consistent numbering plan.

CIM – Copper Interface Module. A TDM interface module used to connect the ICP to various peripherals via CAT-5 UTP.

CIR – Committed Information Rate. A means of identifying how much information in a connection MUST be carried. For example, CIR = 64 kbits/s for voice.

CLASS – Custom Local Area Signaling Services. Variations on the definition primarily include caller display, such as caller name and number.

Class of Restriction (COR). Controls station and trunk access to trunk circuits. It performs functions similar to toll control and is programmable on a station (or trunk) basis.

CLIP – Calling Line Identification Presentation. Displays calling party information.

CO – Central Office. Local Branch Exchange (for the PSTN) providing connection between PSTN and local lines, or loops, to the subscriber.

CODEC – COder and DECcoder. Coder and decoder are commonly used as a single function. A means to convert analog speech into digital PCM and vice versa.

CODEC/Filter. The chip used in the SX-200 ICP System consisting of a CODEC, filter and other elements. It forms part of the peripheral card, with the CODEC portion performing the necessary A/D and D/A functions, and the filter portion providing low–pass filtering for the line transmission.

Controller. Control element of ICP (see also RTC).

COS – Class of Service. This refers to the priority value in the Layer 2 part of an IP packet when IEEE 802.1p is used.

CPH – Call Per Hour. For example, 6CPH means 6 calls per hour.

CSMA/CD – Carrier Sense Multiple Access Collision Detect. The mechanism used on shared Ethernet connections to ensure that devices are not sending simultaneously, and if they are, to initiate a back-off and retry algorithm.

CTI – Computer Telephone Integration. A means of combining computer functions to control operation telephony equipment.

D Channel. The 16 kbit/s control channel of a DNIC device.

Data Communication Equipment. A modem or a local maintenance port, for example, can be used as a communications line or data device to data terminal equipment (DTE) interface over an RS-232 line.

Data Terminal Equipment. Terminal equipment, usually consisting of a keyboard and video screen or printer, which is used to communicate with a variety of other equipment (such as another DTE or a computer).

DCE – Data Communication Equipment. See Data Communication Equipment.

DECT – Digital Enhanced Cordless Telephony. Originally, a European standard for digital cordless phones, now a worldwide standard. Hence, the name change to Enhanced. Standard DECT phones are not available in North America.

DHCP – Dynamic Host Controller Protocol. A means of passing out IP addresses in a controlled manner from a central point/server.

DID – Direct Inward Dialing.

DiffServ – Differentiated Services. A protocol for specifying and controlling network traffic by class, so that certain types of traffic get precedence. For example, voice traffic, which requires a relatively uninterrupted flow of data, might get precedence over other kinds of traffic. This uses the Type of Service field at Layer 3 in an IP packet and is the most advanced method for managing traffic in terms of what is called Class of Service (CoS).

Digital/Analog. A term used in connection with the conversion of digital signals to equivalent analog signals. The original signals are usually in analog form and are converted from analog to digital signals for transmission (see also Analog/Digital).

DN – Directory Number. A telephone or extension number.

DNIC – Digital Network Interface Circuit. A chip used as the basis for several sets which handle both voice and data.

DNS – Domain Name Server. A means of translating between typed names and actual IP addresses, for example, microsoft.com = 207.46.134.222

DOD – Direct Outward Dialing.

DPNSS – Digital Private Network Signaling System. A British common channel signaling protocol for requesting or providing services from/to another PBX.

DSCP – DiffServ Code Point. See also Diffserv.

DSP – Digital Signal Processor. This is a programmable device that can manipulate signals, such as audio, to generate and detect a range of signals, for example, DTMF signaling.

DSU – Digital Service Unit. A peripheral which provides digital ports for the ICP.

DTE – Data Terminal Equipment. See Data Terminal Equipment.

DTMF – Dual Tone Multi-Frequency. In-voice-band tones used by telephones to signal a particular dialled digit. Also known as touch tone.

E – Erlang. A measure of usage of a resource, for example, 0.75e = 75%. 1 e=36 CCS.

E and M. A type of tie trunk. Also the signaling method used for this and for other types of trunks. The term is derived from the use of the E and M leads forming part of the trunk equipment, and taken, to denote the receive and transmit leads used to pass supervisory conditions over the trunk, respectively.

E1. Primary Rate running at 2.048 Mbits/s providing 30 channels of voice of Pulse Code Modulation (PCM).

E2T – Ethernet to TDM gateway. The conversion of voice streaming between TDM and IP.

E911 – Enhanced 911 (Emergency Services). Also, 999 (UK) and 112 (International).

ESM – Enhanced System Manager. A means to program a system from the maintenance shell.

FAX – Facsimile. A means of transmitting printed text or picture information with acoustic tones.

FIM – Fiber Interface Module. A multi-mode fiber optic TDM interface module used to connect the ICP to various peripherals.

FTP – File Transfer Protocol. An electronic method to transfer file information.

Full Duplex. A method of operation which allows simultaneous transmission from both ends of a communications link.

G.711. PCM Voice Streaming. ITU standard for conversion of voice-streaming to digital Pulse Code Modulation (PCM) (64 kbits/s).

G.729. Voice Streaming CODEC. Reduced bit rate from G.711 (8 kbit/s).

Gateway. A path between different media streaming technologies, in this case, between TDM and IP.

Group Controller. This is where the call control of the ICP is in control of a number of units, where the functions are more dedicated, for example, to a separate gateway.

GRP – Gateway Routing Protocol. A generic term which refers to routing protocols.

HSRP – Hot Standby Routing Protocol. A Cisco proprietary protocol used to increase availability of default gateways used by end hosts.

ICMP – Internet Control Message Protocol. Messages to help identify when devices are present and create warnings when they fail.

ICP – Integrated Communications Platform. Includes gateway function, call control, plus a number of other features, such as voice mail. Variants include the **CX/CXi** (Compact) and **MX** (Medium) platforms.

IP – Internet Protocol. An encapsulation protocol that allows data to be passed from one end user to another. Typically, this was over the Internet, but the same protocol is now used within businesses.

IP Address – Internet Protocol address. A 32-bit address assigned to hosts using TCP/IP. An IP address belongs to one of five classes (A, B, C, D, or E) and is written as 4 octets separated by periods (dotted decimal format). Each address consists of a network number, an optional subnetwork number, and a host number. Together, the network and subnetwork numbers are used for routing, while the host number is used to address an individual host within the network or subnetwork.

IrDA – Infrared Data Association. An industry-sponsored organization established in 1993 to create international standards for the hardware and software used in infrared communication links. Infrared Radiation (IR) is the same technology used to control a TV set with a remote control.

IRDP – ICMP Router Discovery Protocol. An extension to the ICMP protocol that provides a method for hosts to discover routers and for routers to advertise their existence to hosts.

ISDN – Integrated Services Digital Network. An integrated, digital, PSTN network carrying both voice and data and providing direct digital connectivity to the user via BRI or PRI connections.

ISL – InterSwitch Link. Cisco proprietary protocol for passing data between Layer 2 switches while maintaining priority and VLAN information.

L2 – Layer 2. The second layer of encapsulation of data to be transferred. Typically, with TCP/IP, this includes the MAC layer.

L3 – Layer 3. The third layer of encapsulation of data to be transferred. Typically, with TCP/IP, this includes the IP address.

LAN – Local Area Network. This is a network within a local area, typically within a radius of 100m. The transmission protocol is typically Ethernet II.

LCCR – Least Cost Call Routing. See Least Cost Routing.

LCR – Least Cost Routing. See Least Cost Routing.

Leased IP. An IP address that has been assigned through DHCP and is valid only for the duration of the agreed lease time.

Least Cost Routing. One of the functions of automatic route selection which refers to the economical aspects of the ARS facility. In least cost routing, the trunk circuits are programmed with regard to the effects of the costs of the possible alternative trunk routings. In practice, the customer may require the economical aspects to be subordinate to the overall traffic efficiency requirements of the System. For example, less costly trunk routes may be available, but offer too low a traffic grade of service for the customer's needs. Actual requirements may be subject to traffic analysis of the customer's needs.

LED – Light Emitting Diode. Those flashing red and green lights on the box!

LS – Loop Start. This is a particular analog trunk protocol for signaling incoming and outgoing calls.

MAC – Media Access Controller. This is the hardware interface through which data (media) travels. Typically, this will be assigned a world-wide unique address.

MAC – Move, Add, Change. Action of changing a phone location and number. (Made much easier with IP!)

Main Distribution Frame. The main distribution frame (MDF) forms the interconnection point between the in-house PBX, for example, the SX-200 ICP System, and the internal and external cabling to the PBX. The MDF provides a convenient and flexible means of interfacing the cabling to the system.Also known as the cross-connect field.

MAN – Metropolitan Area Network. This is a larger network that may connect a number of LANs within a business, as well as a number of businesses. Typically, this would cover a city area, and use fiber optics to get maximum bandwidth.

MDF. See Main Distribution Frame.

MFRD – Mitel Feature Resources Dimensions. A definition of the number of features that can be used on a particular unit.

MiNet – Mitel Network Protocol. An ISDN-based protocol used to signal between phones and controllers, for example, key and display information.

MiTAI – Mitel Telephony Application Interface. The Mitel implementation of TAPI used to connect to external applications, for example, to ACD controllers.

MMC – Mitel Mezzanine Card. MITEL standard of interconnection and form factor for different functional modules found in systems, for example, DSP and T1/E1.

MODEM – MOdulator-DEModulator. Device that converts digital and analog signals. At the source, a modem converts digital signals to a form suitable for transmission over analog communication facilities. At the destination, the analog signals are returned to their digital form. Modems allow data to be transmitted over voice-grade telephone lines.

MOH – Music on Hold.

MPU. Main processing unit. In the SX-200 ICP, this refers to the CPU in the controller.

MSDN – MITEL Superswitch Digital Network. MITEL-specific DPNSS.

MTBF – Mean Time Between Failures. The statistical time between expected component failures.

MTU – Maximum Transmission Unit. An MTU is the largest size packet or frame, specified in octets (eight-bit bytes), that can be sent in a packet- or frame-based network, such as the Internet.

NAT – Network Address Translation. A means of translating internal IP addresses to a defined limited range of internet IP addresses. The benefit is the ability to use a limited range of internet addresses and map these to a much larger internal range.

NetBIOS – Network Basic Input Output System. An API that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS.

NFAS – No Frame Alignment Signal. Also AIS (Alarm Indication Signal/All 1s) for E1.

NIC – Network Interface Card. Physical connection to the network. In a PC, this is often a plug-in card.

NSU – Network Services Unit. An interface which connects the PSTN Primary Rate trunks to the ICP.

ONS – ON premises Set. A two-wire analog telephony interface, within an office environment, which is not passed outside.

OPS – Off Premises Set. A two-wire analog telephony interface, typically installed external to a building, such as an external shed, or guard house.

OSPF – Open Shortest Path First. A link-state routing protocol used for routing IP traffic over the most cost-efficient route.

PABX – Private Automatic Branch Exchange. This is a specific form of PBX, where operation and call routing is controlled by the user and handled automatically.

PBX – Private Branch Exchange. This is a privately owned telephone system, usually within a business, that allows phone connections within the business as well as out to the PSTN. Other features are also included, such as call transfer, conference and voice mail.

PC – Personal Computer.

PCB – Printed Circuit Board.

PCM – Pulse Code Modulation. The digital representation of analog signals.

PDA – Personal Digital Assistant. A handheld personal organizer that can interface to a PC or a Mitel PDA Phone.

PDF – Portable Document Format. A documentation standard.

PER – PERipheral cabinet. Used on the SX-2000 and related products. This is a backplane and cabinet to hold different interface cards, such as ONS, DNIC, LS trunks, etc.

Peripheral Interface Card. A card which provides the interface facilities between the external peripheral equipment, such as stations, trunks and attendant consoles. A prime function is to convert the external analog inputs to the internal digital PCM signals (and conversely convert digital PCM to analog output).

Permanent IP. An IP address that has been leased (from DHCP) on a permanent basis.

PFC – Power Factor Correction.

PI – Performance Index. A unit-less value used to determine calls that a system can handle based on traffic patterns and connected devices. An ONS-to-ONS call is typically 1PI.

Ping – ICMP Echo. On a PC, use of this command sends a test message and waits for a reply to determine if a network device is reachable.

PKM – **Programmable Key Module.**

PMBX – Private Manual Branch Exchange. More for historic interest, this is an older form of PBX, where operation and call routing is handled manually through an operator. Today, most PBX equipment is handled automatically.

PoE – Power over Ethernet. A general term now standardized under IEEE802.3af.

POTS – 'Plain Old Telephone Service'. Basic dial phone and voice connection service, largely superseded by ISDN. A POTS phone is typically an analog device, without active electronics and most likely with a rotary dial.

Power Fail Transfer (PFT). See System Fail Transfer.

PRI – Primary Rate Interface. This is a connection to the PSTN where a number of trunk channels are multiplexed onto a common connection. Both T1 and E1 variants are available.

PSTN – Public Switched Telephone Network. The telephone network, such as Bell, AT&T, or BT, that provides local and long distance connections.

PTT – Poste, Telefonie, Telegrafie. PSTN services. Often countries combine postal services and telephony under a common service provider, for example, the government.

Q.Sig – ISDN signaling. In accordance with the G.931/2/3 range of ITU specifications.

R2 – In-band inter-Register signaling standard 2. Used to signal between different COs to provide call setup and cleardown. Often used where ISDN is not fully available, or the network is analog-based.

RAC – Record a Call. Integral feature to allow calls to be recorded to voice mail.

RDN – Remote Directory Number. The Remote DN Table is used to identify alternate ICPs when checking for device availability, and to determine whether a device is located on the Primary or Secondary ICP.

RFC – Request For Comments. A document that is created, maintained and distributed by the Internet Engineering Task Force. An RFC is the vehicle used to discuss and develop a networking related protocol. RFCs usually get approved and issued as standards.

RFP – Radio Fixed Part. A DECT cordless radio base station which may handle multiple devices and be networked.

RGP – Router Gateway Protocol. A means whereby routers on a common subnet can communicate and identify each other. Useful when ICMP Re-direct is needed to identify an alternative path.

RIP – Routing Information Protocol. A networking protocol that maintains a database of network hosts and routers and exchanges information about the topology of the network.

RS-232C. A North American data interchange standard, issued by the Electronics Industries Association (EIA). The equivalent European standard is the V.24 specification.

RTC – Real Time Controller. This is the control block within an ICP. This includes Call Control as well as internal controls for the unit.

RTP – Real Time Protocol. Protocol used to identify sequence of voice packets with timing information before being sent to a user via UDP.

SMDR – Simple Message Detailed Recording. Call logging information.

SME – Small to Medium Enterprise. A small- to medium-sized business.

SNMP – Simple Network Management Protocol. Standard for configuration and passing information between data devices to allow network management.

Static IP. An IP address that has been manually assigned and fixed. Typically, static addresses are exceptions within DHCP.

Station Message Detail Recording (SMDR). Records and prints the details of incoming and outgoing trunk calls in the SX-200 ICP system. Details include the numbers of all parties involved in the call, the time and duration of each call, account codes and other pertinent information.

STP – Spanning Tree Protocol. A means whereby the network can determine multiple paths between two points and disconnect them to leave a single path, removing broadcast issues.

Stratum – Clock accuracy standard. Specifies clock accuracy in particular ranges. Lower values are higher accuracy and found in the ISDN network. Typically, PBX equipment is either Stratum 3 or 4.

Subnet – Short for "subnetwork". An identifiably separate part of an organization's network. Typically, a subnet may represent all the machines at one geographic location, in one building, or on the same local area network (LAN).

Synchronous Mode. This term is associated with data which is transmitted in a continuous stream at a fixed rate, with the receiving terminal synchronized to the transmitting terminal by means of elements transmitted on a regular basis. See also Asynchronous Mode.

System Configuration. The hardware and software initially installed for the system. Any subsequent additions, deletions and any other changes which occur result in the creation of a new system configuration. The list of hardware and software items which comprise the current system configuration can be obtained on command from the maintenance terminal.

System Fail Transfer (SFT). A feature which allows selected stations of the system (or portions of the system, according to the type of outage), to be transferred to certain trunks. Such transfer action is automatic in the event of a failure of the main power supply.

T1. Primary Rate. Provides 23 or 24 channels of trunks per connection.

T.37. Internet Protocol for FAX (Store and Forward). A means of taking a TDM FAX, converting it to data, passing it via IP and reconverting it back to TDM.

T.38. Internet Protocol for FAX (Real Time). Similar to T.37 in function, but carried out in 'real' time, for example, with minimum delay.

TAPI – Telephony Applications Programming Interface. TAPI is a standard programming interface that lets you and your computer communicate over telephones or video phones to people or phone-connected resources.

TAR – Tape Archive and Retrieval. A file transfer utility.

TCP – Transmission Control Protocol. The methods of transmitting data between two end-points using IP acknowledgement.

TDM – Time Division Multiplex. A means of combining a number of digitally encoded data or voice channels onto a common digital stream, such as T1.

Telco. An abbreviation of tel(ephone) co(mpany).

TFTP – Trivial File Transfer Protocol. A simplified version of FTP used to transfer data with minimal overhead.

TOS – Type of Service. A field within the Layer 3 (IP) encapsulation layer used to identify service parameters, such as, delay and priority of handling.

TUG – Teleworker User Gateway. An internal name for the Teleworker interface.

UDP – User Datagram Protocol. A Layer 4 protocol used to stream voice. It is considered connectionless, with minimal handshaking and overhead.

Unicast. A process of transmitting messages from one source to one destination, as opposed to a broadcast or multicast.

UPS – Uninterruptible Power Supply. A unit capable of providing output power for a period of time when the local mains supply fails. Usually relies on storage devices such as batteries.

UTP – Unshielded Twisted Pair. Cable that reduces emissions and maintains an impedance match through the twists per meter in the cable without resorting to shielding.

VLAN – Virtual LAN. A means of providing virtual LANs on a network using common physical components. Such VLANs are logically unconnected, except through some Layer 3 device.

VM – Voice Mail.

VMPS – VLAN Membership Policy Server. A Cisco proprietary facility that configures certain Cisco switches for security blocking, at the network access point, and automatically programs the port to the appropriate VLAN for the connecting device.

VoIP – Voice over IP. What this is all about! Sending voice over the data networks using the TCP/IP protocol.

VRRP – Virtual Router Redundancy Protocol. Standards-based protocol used to maintain availability of default gateways and routers to end users.

WAN – Wide Area Network. A network connection to a network that could be global, for example, via Frame Relay.

WAV – WAVe file. An audio file format, created by Microsoft, that has become a standard PC audio file format for everything from system and game sounds to CD-quality audio. A Wave file is identified by the .wav file name extension.

X-Net – Switched DPNSS signaling. Uses switched voice channels to pass information between networked controllers, typically over TDM. Requires ISDN connectivity.

YA – Your Assistant. A PC-based office management application. YA Pro, the enhanced version of YA, includes a PC-based phone.

Index

P

Q

S

Global Headquarters	U.S.	EMEA	CALA	Asia Pacific
Tel: +1(613) 592-2122	Tel: +1(480) 961-9000	Tel: +44(0)1291-430000	Tel: +1(613) 592-2122	Tel: +852 2508 9780
Fax: +1(613) 592-4784	Fax: +1(480) 961-1370	Fax: +44(0)1291-430400	Fax: +1(613) 592-7825	Fax: +852 2508 9232

For more information on our worldwide office locations, visit our website at www.mitel.com/offices

www.mitel.com