

Section 1

DVTEL Latitude 6

Introduction to Networking

Learner guide

version 6.0.1

This page left *almost* Blank intentionally for double sided printing

DVTEL Latitude NVMS 6



1

Objectives

- What Do **YOU** expect from this training?
- Introduction to Edge Devices (PPT #1 part 1)
- Networking Essentials (PPT #1 part 2)
- System Components / Topologies (PPT #2)
- Software Installation
- Admin Centre Setup
- Control Centre Operation
- Assessment (Theory & Practical)



2

Introduction to Edge Devices

(IP Cameras, Encoders & Decoders)



3

Latitude Supported Edge Devices

The Latitude software supports an increasing number of different manufacturers IP Cameras, Encoders & Decoders. The Release Notes detail the devices & level of support.



4

DVTEL are adding to their range of IP cameras & now include IP PTZ dome cameras as well as fixed dome & full body cameras. There are two (2) available streams from DVTEL transmitters, i.e. IP cameras or encoders. The streams are used for live view by clients & recording to archivers. By default the Latitude software is set to use only the one (1) stream (Live).

Edge Device Typical Features

- MPEG4
- MJPEG
- Motion Detection (edge device)
- Dual Video Streams
- Input / Output Pins
- PTZ
- Audio In / Out
- Serial port



5

Dependent on the model of the edge device, some or all of the features are supported. The devices specifications and/or software release notes must be consulted for details.

MJPEG Codec

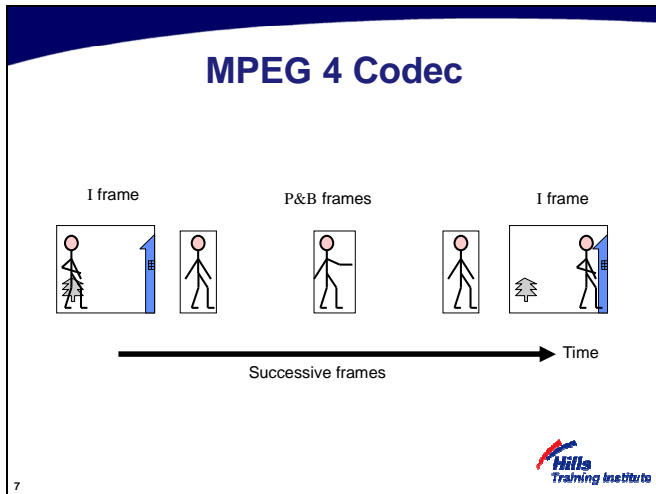


Successive frames → Time

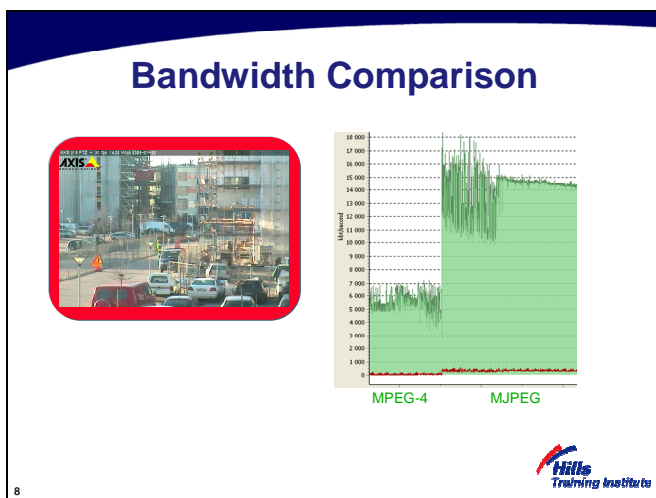


6

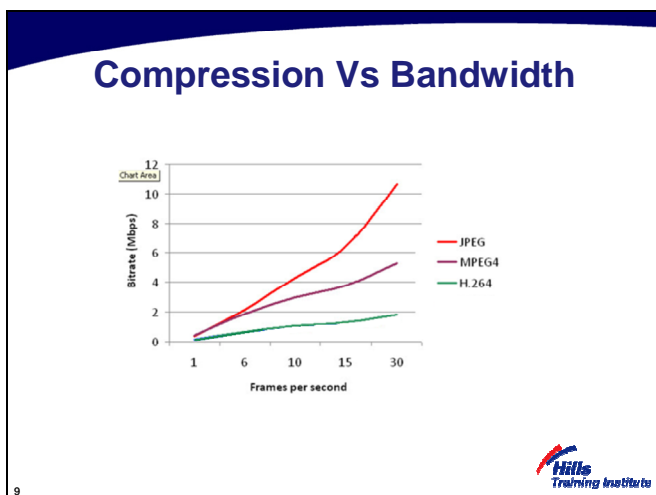
MJPEG uses intra-frame encoding, whereby each frame is individually compressed and contains all the information to create a complete image. This does not take advantage of the similarity between frames.



MPEG4 uses inter-frame encoding or Group of pictures (GOP) concept. The Independent frame contains all the data to create a full image, subsequent P & B frames contain only what's changed info. Thus the overall file size & bandwidth is much less. The Latitude software allows the setting of the interval between the I frames. The I frames do not contain any motion information which is significant for Video Motion Detection at low frame rates.



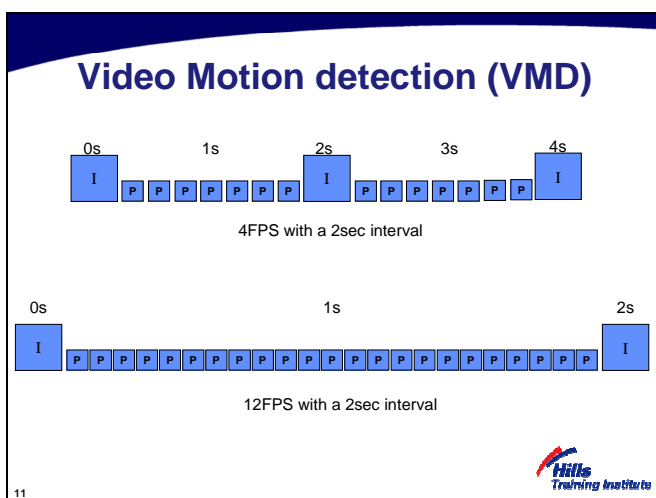
The graph shows the relevant bandwidth of a MJPEG stream compared to a MPEG-4 stream. Why then would MJPEG be preferred in some circumstances? If the transmission was susceptible to frame drop out, then the loss of a frame in MJPEG would provide timelapsed images, but the loss of an I Frame in MPEG4 could mean garbled images for the seconds between I frames. Internet connections & links with low bandwidth availability are susceptible to data loss. Video differs from typical data transmissions, in that the video is time critical. If a packet of data for a Word document is lost in transmission, then it is simply resent using TCP/IP.



This chart relates to the compression available from the Pelco Sarix range of IP Cameras, but is more or less similar as a generality for the CODECs. Note the relative size of the H.264 a.k.a MPEG 4 part 10, which will be the predominant form of compression in the very near future. It is a common convention that when comparing CODECs, MPEG4 part 2 (a.k.a. H.263) is presented as simply MPEG4 & MPEG4 part 10 is presented as H.264.



Note that in this comparison the H.264 image is of a higher quality for the same bit rate. For equivalent quality images, the H.264 signal would be about half the bandwidth of the MPEG4.



If VMD was set for 5 consecutive frames, in the first case it would take >1sec to trigger. In the second case <0.5 sec. DVTEL have recommended the use of a lower key frame rate for VMD. i.e. a high I frame interval. Note that high key frame rates would also have an adverse effect on the HDD recording capacity and bandwidth requirements.



Can you spot the difference? The image on the left is 2CIF, with 4CIF on the right.

Frame Rate

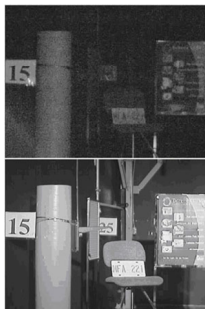
Real Time
Real Motion
Timelapse



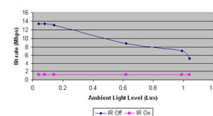
13

The difference between Real Time (25FPS) & Real Motion (12FPS) is almost imperceptible to the human eye. Frame rates below 12FPS are classed as Time Lapse rates.

Illumination



Ambient illumination (0.08 lux)
IR off



Ambient illumination (0.08 lux)
IR on



14

Whilst the ambient lighting in the top picture does give you an image, it's noisy and poor quality. Even though there is no physical motion in the scene, the IP encoder sees the noise as motion, which causes the bandwidth and HDD storage usage to be much higher than the IR illuminated picture on the bottom. A well illuminated scene (White light or IR) will reduce your bandwidth and HDD storage usage compared to a low lit scene. The chart illustrates the bandwidth comparisons between the two images.

Networking Essentials/ Network Products

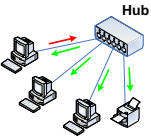


Warriors of the Web




15

Ethernet (Early)



10 Mbps
 20-30% Utilization
 2-3 Mbps

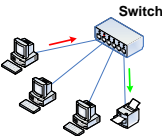
- No Token – Talk when you want
- "Chatty"
- All traffic sent to everyone
- Collisions WILL occur, if so they retransmit



16

Ethernet stations communicate by sending each other data packets, small blocks of data that are individually sent and delivered. Each Ethernet station is given a single 48-bit MAC (Media Access Control) address, which is used both to specify the destination and the source of each data packet. Network interface cards (NICs) hold the MAC address. Conventionally Ethernet nodes are connected in a Star topology using copper twisted pair cables.


Ethernet (Recent)



100 Mbps
 70-80% Utilisation
 70-80 Mbps

Later the HUB was replaced by a SWITCH

- A smaller, more intelligent device
- A Switch can be either a layer 2 or layer 3 device, depending on the functionality required. Layer 3 switches can be much more expensive. (Layer 2 & 3 is discussed later)
- Learns which address is on which port
- Reads data and directs it to destination port versus sending to all ports
- Reduces Collisions
- Increased utilisation up to 70 - 80%




17

Ethernet

Network Evolution

	UTP	Fiber
10 Mbs	1990	1993
100 Mbs	1995	1995
1000 Mbs/1Gbs	1999	1998
10 Gbs	2006	2003
100 Gbs	?	?



18

Ethernet

LANs / WANs / Subnets

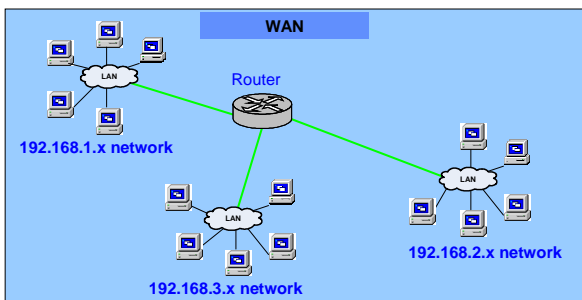
- Moving data within a **LAN** (Local Area Network) is simple as the switch directs traffic to the appropriate port via the MAC address.
- Even with Switches, *saturation* can occur as the network grows.
- A **WAN** (Wide Area Network) is made up of multiple LAN's connected together by *routers*. Each LAN is typically assigned with a unique subnet (Sub network) address. Using smaller subnets can help by separating traffic from other subnets and only allowing traffic to traverse to another subnet when necessary.
- LAN's & WAN's can be seen as the physical aspects of a networks whilst Subnets can be seen as the logical addressing of a network.
- Moving data between Subnets requires some extra hardware
-Let's take a look



19

Ethernet

A routed network



20

By the introduction of a Router into the network, communications between different LANs is possible. We will discuss the determination of LAN later.

Network Addressing

MAC & IP addresses

- **MAC - (Media Access Control)**
Each Ethernet device has a **MAC** address that is "burned in" to the network device at the factory. This address can only be used on the LAN.
The MAC address is made up of six eight-bit hexadecimal numbers.
I.e. 00-A0-D1-A0-6F-EF
- **IP - (Internet Protocol)**
To connect to another network, we need another type of address that identifies both the network and the device (or node). This is where the IP address is used.



21

IP Addresses (IPv4)

- IP Addresses are composed of 4 octets (32 bits total)
- IP Addresses are written in "dotted decimal notation"

I.e. aaa.bbb.ccc.ddd

E.g. 10. 20.30. 15
172. 16. 5. 24
192.168. 1. 10

Note: A new version of IP addressing (IPv6) is being developed and will be introduced into the market place shortly. IPv6 will have 8 sixteen-bit hexadecimal numbers instead of the current 4 eight-bit decimal numbers.
E.g. (EF12:54FF:7D1E:1100:0000:DDCD:16A1:FF11)
The high number of combinations will remove the need for private addresses and port forwarding.



22

IP Addresses (IPv4)

- Each of the four "Octets" is comprised of 8 bits

E.g. 192.168.1.x =

1 st	2 nd	3 rd	4 th
192	168	1	?
11000000	10101000	00000001	00001010

- The decimal weighting of each bit in the octet is represented in the first line of the table below:

	2 ⁷ = 128	2 ⁶ = 64	2 ⁵ = 32	2 ⁴ = 16	2 ³ = 8	2 ² = 4	2 ¹ = 2	2 ⁰ = 1	Dec.						
If all '0'	0	0	0	0	0	0	0	0	0						
If all '1'	1	1	1	1	1	1	1	1	255						
	0	0	0	0	1	0	1	0	?						
	0	+	0	+	0	+	8	+	0	+	2	+	0	=	?

- Question: What is the decimal value of the 4th octet?



23

The binary digit (bit) is the smallest piece of data. The range of an 8 bit data string can be given by 2 to the power of 8 = 256. The first digit in the range is zero & the last is 255.

Subnet Masks

- An IP address is made up of a Network ID and Node ID.
I.e. IP Address = Network ID + Node ID
E.g. street name and house number
- In order to identify which part is the Network ID, you must use a Subnet Mask
- There are three standard subnet masks used.
 - 255.0.0.0 (Class A)
 - 255.255.0.0 (Class B)
 - 255.255.255.0 (Class C)

Note: These are only the standard subnet masks. More complex masks can be used but will not be covered here.




24

Subnet Masks

192.168.1.10 ➡ 11000000.10101000.00000001.00001010
 255.0.0.0 ➡ 11111111.00000000.00000000.00000000
 Class A

Network Address = 192.0.0.0 Broadcast address = 192.255.255.255	Host ID = 168.1.10 Hosts = $2^4 - 2$ = 16,777,216
--	--



The number of bits allowed for the Host ID defines how many hosts are allowed on the subnet.

2 to the power of host bits, minus 2. The minus 2 is to allow for the Network ID and Broadcast address that cannot be assigned to hosts.

E.g. $2^8 - 2 = 254$

Subnet Masks


Subnet Mask Example:

192.168.7.10 = IP Address
 255.255.255.0 = Subnet Mask (Class C)

Produces:

_____ ? = Network ID
 _____ ? = Host ID (Node)

_____ ? = Network Address
 _____ ? = Broadcast Address




The network address & Broadcast address are not used as Node address. A gateway address is conventionally one digit away from either end of the range. Thus it could be 192.168.7.1 or 192.168.7.254

Private and Public IP Addresses

There are a range of IP Addresses that can only be used within your network. These are "Private" IP Addresses. To access these addresses from the Public IP Addresses used on the Internet we need to use **NAT (Network Address Translation)**. This is mentioned later.

Private IP Address Ranges:

- Class A: 10.0.0.0 – 10.255.255.255
- Class B: 172.16.0.0 – 172.31.255.255
- Class C: 192.168.0.0 – 192.168.255.255
- Class D: 224.0.0.0 – 239.255.255.255
(Multicast Addresses)
- Class E: 240.0.0.0 – 255.255.255.255
(Experimental Addresses)



Network Protocols

TCP (Transmission Control Protocol)

TCP is a connection oriented transport protocol in the TCP/IP protocol suite. Whereas the IP protocol deals only with packets (OSI Layer 3), TCP enables two hosts to transfer streams of data at OSI Layer 4. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.

UDP (User Datagram Protocol)

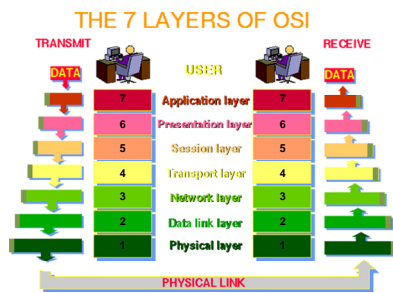
UDP is a connectionless protocol that, like TCP, runs on top of IP networks also at OSI Layer 4. UDP provides very few error recovery services, relying on other layers of the network to perform error detection and recovery. UDP is a fast, lightweight protocol ideal for streaming audio and video traffic over an IP network.



28

Layer 3 (Network Layer)
Layer 4 (Transport Layer)

OSI Reference Model



29

The OSI Model describes how data flows from one computer to another computer in a network.

Typically, when data leaves the transmitting PC at Layer 1, it will travel through Switches and maybe Routers before it gets to the receiving PC. Switches and routers must interrogate the received data to determine how it will be managed. The level of interrogation depends on the intelligence of the device. Basic switches operate at Layer 2, whilst managed switches and Routers typically operate at Layer 3. Commercial grade Layer 3 network devices are typically considerably more expensive.

Bandwidth

The amount of data that can be transmitted in a fixed amount of time.

Bandwidth is usually expressed in **bits** per second (bps), **kilobits** per second (kbps or kb) or **megabits** per second (mbps or mb).

Note: Data storage in hard disks is measured in BYTES not BITS. Typically measured in Megabytes (MB) or Gigabytes (GB) using a "capital B" – don't confuse the two measurements.

[For analog devices, the bandwidth is expressed in cycles per second, or Hertz (Hz)]

Bandwidth is particularly important for I/O devices such as hard disks. For example, a fast disk drive can be hampered by a bus with a low bandwidth. This is the main reason that we are basing our storage systems on high speed communication ports, such as 100Mb, 1000Mb and Fiber (2Gb/Sec (2000Mb/Sec)).

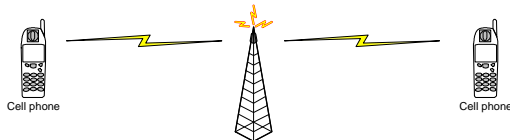


30

Unicast, Broadcast and Multicast

Unicast

Communication that takes place over a network between a single sender and a single receiver. A telephone call is a Unicast transmission.

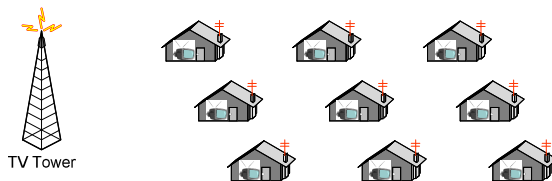


31

Unicast, Broadcast and Multicast

Broadcast

Communication that takes place over a network between a single sender and all receivers on the network. Broadcasts are normally only used by internal network functions (eg the ARP protocol to discover network devices). TV and Radio use broadcasting.



32

Unicast, Broadcast and Multicast

Multicast

For sending large amounts of data to multiple devices. Multicasting is more efficient than normal Unicast transmissions because the server can send out a single message to many recipients simultaneously.

Unlike traditional Internet traffic that requires separate connections for each source-destination pair, Multicasting allows many recipients to share the same source. This means that just one set of packets is transmitted for all the destinations.

A conference telephone call is multicast.

Multicast uses **IGMP** (Internet Group Management Protocol) to manage Multicast streams on a LAN and **PIM** (Protocol Independent Multicast) between LAN's.

Note: All Multicast switches require **IGMP** functionality.



33

Multicasting Querying & Snooping

Querying:

At least one switch on each LAN MUST be setup for **IGMP Querying**. Typically, this should be the core switch (middle of the network). The Querier queries the other multicast switches on the LAN to see what streams (groups) are active and terminates any streams that have not ended correctly.

Snooping:

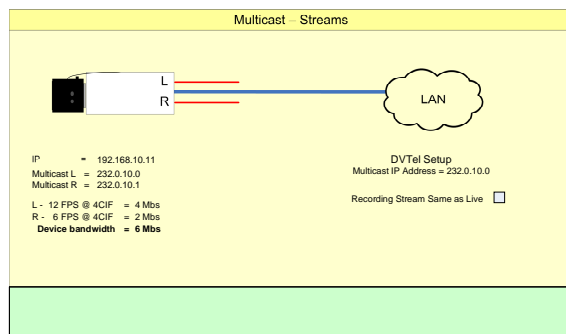
All layer 3 switches on the network **MUST** support **IGMP Snooping**. This allows the switch to snoop its ports for IGMP data.

Note: Check the programming of your switches to ensure you have correct functionality.



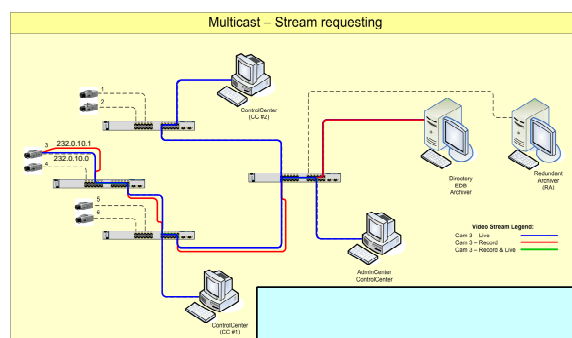
34

Multicasting



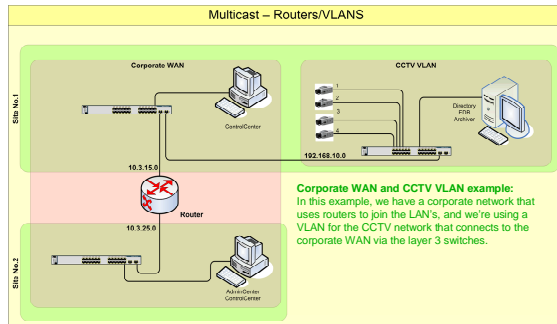
35

Multicasting



36

Multicasting



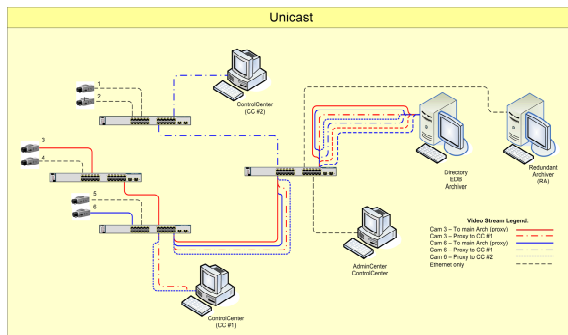
37

Hills
Training Institute

For Multicasting to function across a router or VLAN, PIM (Protocol Independent Multicast) needs to be enabled on all devices linking the networks together.

PIM functionality of a switch/router is typically a licensed feature. \$\$\$

Multicasting

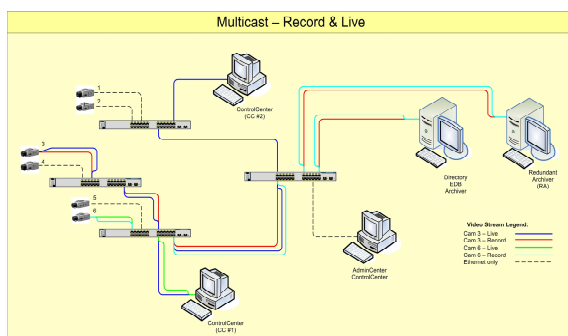


38

Hills
Training Institute

Because the Archiver acts as a video proxy when using a Unicast network instead of a Multicast network, the Archiver works harder to manage the proxying of the video streams.

Multicasting



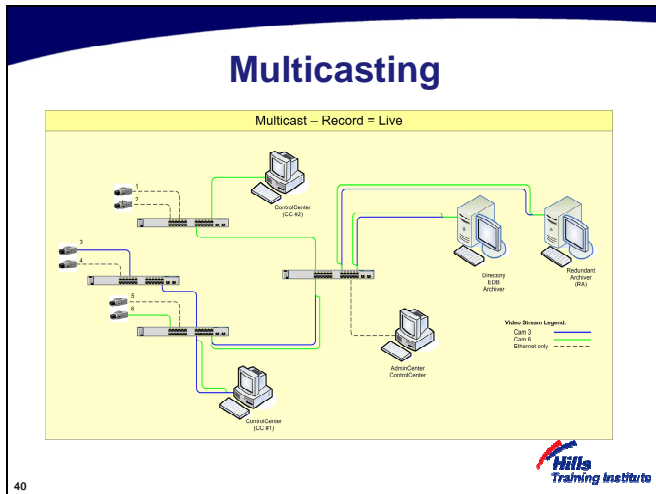
39

Hills
Training Institute

If on a system, video from a single camera is required to be displayed on 2 Monitors & 2 Client stations. Then a single stream is sent from the camera, and the network copies it to each requesting entity.

It is because of multicasting that we can get some economies of bandwidth by selecting appropriate recording & monitoring resolutions & frame rates.

If as in this example the monitoring stream was 2CIF @ 25ips & the recording stream was 4CIF @ 12ips. Then 2 streams are required. One multicast to all the viewing entities at approx 2Mbps & the other virtually unicast to the archiver at approx 2Mbps. To give a total bandwidth requirement of 4Mbps.



If on the other hand, if as in this example the recording stream, lets say hypothetically 25ips @ 2CIF, is the same as the monitoring stream. Then only 1 of the 2 possible streams from the encoder/IP Cam is required. Giving approx 2Mbps bandwidth.

Multicasting

Configuring an AT Switch for IGMP Querying:

```
enable ip
add ip int=vlan1 ip=192.168.0.254 mask=255.255.255.0
enable ip igmp
enable ip igmp int=vlan1
set igmpsnoop fast=multi
create config=dvtel.cfg
set config=dvtel.cfg
```

"show config dynamic" – displays the current switch configuration

41

Hills
Training Institute

Maintain consistency with L3 switch manufacturers, as different manufacturers can utilise multicasting protocols differently. This could cause multicasting issues between different L3 switch manufacturers. As Pacom sells and supports AT products, we can offer a higher level of support in setting up AT devices in a DVTEL system.

DHCP – (Dynamic Host Control Protocol)

- Used to assign IP addresses to network devices automatically
- Device requiring an IP address sends a "global broadcast" searching for a DHCP server
- DHCP Server responds back to the MAC address and assigns it an IP address

42

Hills
Training Institute

DNS – (Domain Name Server)

- Resolves (converts) domain names to IP Addresses



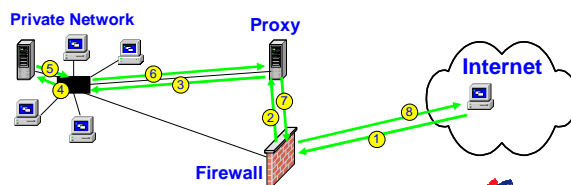
mail.bigpond.com = 144.140.80.10



43

Proxy Server

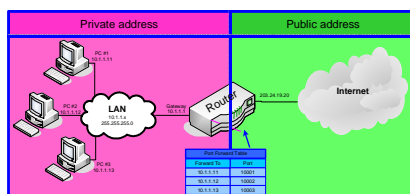
- A "Proxy" is someone or something that does work for you instead of you doing it directly.
(eg proxy voting – voting on your behalf due to absence or illness)
- In many networks, proxies are used to "cache" frequently accessed web sites so that outbound traffic can be reduced.
- In DVTEL networks, a Proxy Server allows internal "Private" data to be securely accessed from the Internet - not directly but via a Proxy.



44

NAT – (Network Address Translation)

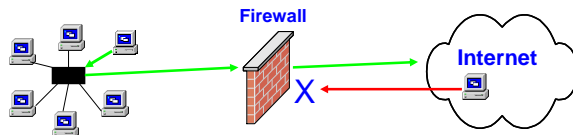
- Allows Private IP Addresses to be accessed from Public IP Addresses for transmission over the Internet
- Provides Some Additional Security (hides internal IP)
- ISP Provides the Public IP
- Any of the three private IP Address ranges can be used internally (10.x.x.x, 172.16.x.x, 192.168.x.x)



45

Firewall

- Protection from Intruders from outside the network.
- Protection from "compromised" machines inside the network that may try to make outbound connections.
- Port level control to safely permit inbound connections to specified addresses and ports



46

DVTel Keyboard

- Look and feel of a traditional CCTV keyboard
 - Rugged construction
 - Large LCD display
- Optimised for Advanced Features of Latitude
 - Control the Latitude system



47

Hardware Grades

- Consumer Grade
 - (cheap, limited functions no IGMP)
- Business Grade
 - (expensive, secure, manageable, more functions)
 - Back Plane Speed is important
 - (overall speed capacity of a switch)

Remember....You get what you pay for



48

Network Diagnostics

The 'PING', 'TRACERT' & 'IPCONFIG' commands are valuable troubleshooting tools – built in to every Windows and UNIX/Linux/Mac OSX system that uses the TCP/IP protocol suite. Network administrators sometime disable the PING and TRACERT commands.

PING

The 'ping' command sends an ECHO REQUEST to a device on the network. If the device is operational, it responds with an ECHO REPLY. Ping is frequently used to see if a device on the network is online.

Usage = PING <IP address> or <URL> or <node name>

TRACERT

The 'tracert' command traces the path through the network from one device to another, returning the time between each segment. Traceroute can be used to diagnose problems on segments of the network between the sender and receiver.

Usage = TRACERT <IP address> or <URL> or <node name>

IPCONFIG

The 'ipconfig' command returns the computers current network settings, including the netmask and gateway settings.

Usage = ipconfig



49

Network Diagnostics

PING Example

```

C:\Documents and Settings\pordjn>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.2.1: bytes=32 time=5ms TTL=64
Reply from 192.168.2.1: bytes=32 time=1ms TTL=64
Reply from 192.168.2.1: bytes=32 time=1ms TTL=64
Reply from 192.168.2.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 5ms, Average = 2ms
C:\Documents and Settings\pordjn>

```



50

Network Diagnostics

TRACERT Example

```

C:\Documents and Settings\pordjn>tracert www.aanet.com.au

Tracing route to www.aanet.com.au [202.61.184.232]
over a maximum of 30 hops:
  0  1 ms  1 ms  1 ms  192.168.2.1
  1  1 ms  1 ms  1 ms  moonwall [192.168.0.1]
  2  11 ms 11 ms 11 ms 203.24.101.23
  3  12 ms 13 ms 13 ms vic-au.aanet.com.au [203.123.72.65]
  4  37 ms 45 ms 43 ms core0.bri.dft.com.au [202.61.186.147]
  5  40 ms 41 ms 41 ms www.aanet.net.au [202.61.184.232]

Trace complete.
C:\Documents and Settings\pordjn>

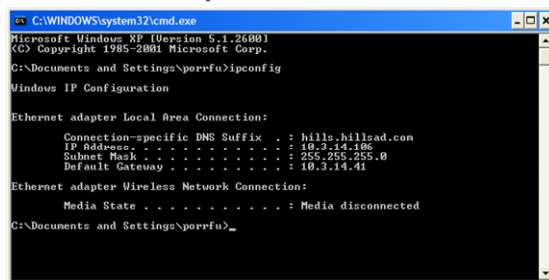
```



51

Network Diagnostics

IPCONFIG Example



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\porrfu>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : hills.hillsad.com
    IP Address. . . . . : 10.3.14.106
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.3.14.41

Ethernet adapter Wireless Network Connection:

    Media State . . . . . : Media disconnected

C:\Documents and Settings\porrfu>
```

