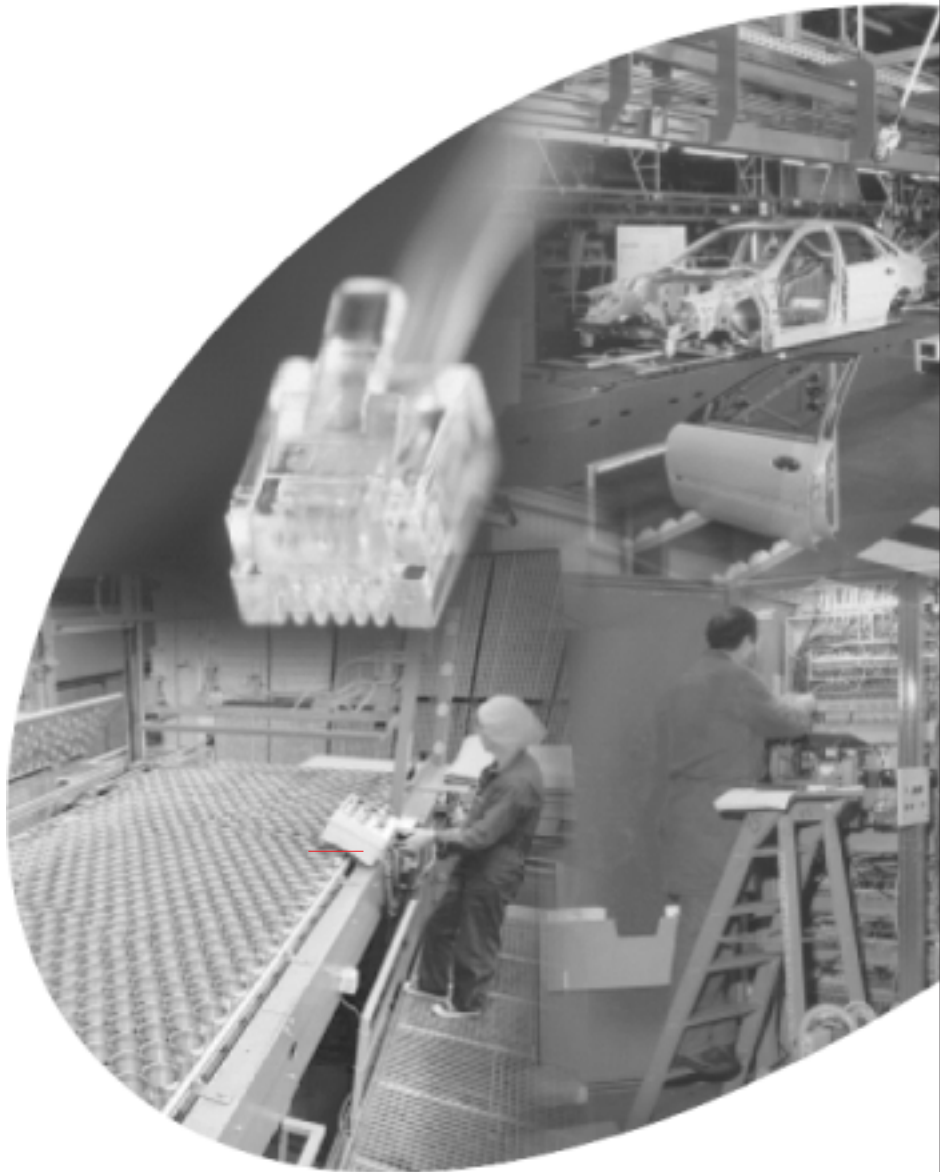


# The Impact of PCs on Industrial Control Networks

Network Services  
*Whitepaper*



July 12, 2002

## The Impact of PC's on Industrial Control Networks

Overview	2
Background	2
Why Broadcasts Can Be Disruptive	3
Choosing an OS for a Factory Floor PC	4
PC Adapter Protocol Configuration	6
Locating Network Resources	8
Broadcast Hazards	11
Technologies to Control Broadcast Traffic	12
Containing Broadcasts	14
Using Multiple Network Adapters in PC's	15
Fault Tolerant Network Adapters	15
Mobile Programming Units	16
Multicast Traffic	16
How to Assess your Existing PC's	17
Conclusion	17

**Schneider Electric**

Telemecanique Automation and Control Services  
One High Street  
North Andover, MA USA  
01845  
Tel. (1) 800-468-5342  
Fax (1) 978-975-9400  
<http://eclipse.modicon.com>

## **Overview**

This paper intends to describe practices used to install PC's on control networks. PC's on control networks have existed for some time using a variety of fieldbus adapter cards, (sometimes coupled with an ethernet adapter in the same PC), to communicate with, monitor and program PLC's. This paper addresses the installation and configuration of PC's used in Ethernet/TCPIP control networks. Proper network configuration on the PC can prevent extraneous traffic that could possibly disrupt operation of high performance, distributed systems that require fast response times.

The publication will educate control engineers on how to:

- Identify network broadcast hazards
- Choose secure PC operating systems
- Reduce the impact of PC's on control networks
- Improve the stability of control networks
- Offer solutions for segmenting networks

## **Background**

PC's serve as programming units, HMI's, SCADA servers, OPC clients and device monitors. Distributing PC's or having portable computers allow programming of devices in proximity to the machinery. In some cases PC's can also function as corporate network clients if such connectivity is available. Schneider Automation recommends that these fixed PC's and visiting PC's, (such as programming units from integrators or contract programmers), use an appropriate configuration for your network to prevent extraneous broadcast traffic from interrupting the operation of your Ethernet control network. Configuration and network resources are covered in detail within the following sections.

Key areas to cover when integrating PC's on control networks are:

- Limiting/Managing Broadcast Traffic
- PC Operating systems suitability
- Proper configuration of each PC protocol stack
- Efficient host name resolution methods
- Network segmentation techniques

Schneider Electric's Network Certification Services team has observed occurrences where an improperly configured computer can generate broadcast burst traffic up to the alarming rate of up to 8 broadcasts per millisecond. As you will discover, every other computer and PLC Ethernet network module on the subnet must process these

broadcasts. This can interrupt communications, and potentially, equipment operation.

## Why Broadcasts Can Be Disruptive

Broadcasts are IP protocol User Datagram Protocol (UDP), messages with a destination IP address that has all ones, or has all ones in the host portion of the address. As opposed to Unicast traffic with its point-to-point, broadcast traffic is sent to, and processed by, every device on the MAC layer, IP subnet. This is also termed the Broadcast Domain.

Examples of network broadcast addresses include 255.255.255.255 and subnet network broadcast addresses like 172.16.1.255 with a 24-bit subnet mask (255.255.255.0). You can determine your subnet broadcast address by substituting all ones in the Host portion of your network address. For examples:

	Network Address	Subnet Mask	Broadcast Address
A	10.10.1.1	255.255.0.0	10.10.255.255
B	192.168.1.1	255.255.255.248	192.168.1.7

In example A, 16 bits of the mask are for the Network ID and 16 bits for the Host ID. In example B, 29 bits of the mask are for the Network ID and 3 bits for the Host ID.

These destination addresses require every device on the same subnet to process the broadcast request to see if they owe a response in return. This causes the network stack on the receiving device to process the destination MAC address, source MAC address, ether-type, length of the message and nature of the UDP request. By processing the Layer 2 MAC, Layer 3 IP and Layer 4 UDP of each broadcast, clock cycles on PLC network modules are diverted for that time from their original mission of processing programmed communication requests and responses.

Broadcast activity is a normal part of Ethernet/TCPIP operation. However, excessive or unnecessary broadcast traffic should be avoided on control networks. Examples of routine and necessary broadcast activity are BootP Client requests, DHCP requests, ARP, and gratuitous ARP. Broadcast traffic such as Bridge Protocol Data Units, (BPDU's), are also generated by some switches to notify each other of topology changes, but are not processed by PLC's because the frame size of 60 bytes is ignored by the PLC network module.

Examples of normal broadcast activity include:

Type	UDP	Purpose	Optimal Frequency
BootP/	68	BootP/DHCP Client Request	1 time to request address

DHCP	67	BootP/DHCP Server Reply	1 time to furnish address
ARP	N/A	Used to resolve IP to MAC address	1 request / 1 reply typical
Gratuitous ARP	N/A	Used by device to announce network availability so others can update cache	1 upon startup

Some multicast protocols such as Bridge Protocol Data Units (BPDU's), use IEEE 802.3 frame formats which may not be processed, (ignored), by the Ethernet II frame format favored by Schneider Automation devices. Networks using the ConneXium self-healing ring monitor device status using multicasts that are distributed on the ring backbone ports and are not distributed to end devices.

Similar to broadcasts, flooded ethernet frames can cause excessive traffic. For example, if an ARP request is sent from a device and the target does not reply with its MAC address, the frame may be flooded to all ports on all interconnected switches on the subnet.

### **Choosing an Operating System for a Factory Floor PC**

One of the first choices when installing PC's on a control network is the Operating System. While the behavior of OS's when connecting to network resources is similar, differences in security features can offer increased benefit. Being able to control whom can logon to and use the PC, and the resources which they have access to, can prevent mis-use.

Key considerations for choosing a PC Operating System for use in control networks are:

- Support for intended applications
- Support for required services and necessary features
- Performance and Stability
- Security

Schneider Automation products and software support the Microsoft Windows operating systems. Among the supported choices, (Windows 95, 98/SE, NT and 2000), Windows NT and 2000 have demonstrated the most robust support in key areas.

A comparison of the platforms identifies feature differences that would be beneficial in an automation environment. While all mentioned operating systems support:

- Local & Remote Hosts files for non-broadcast name resolution
- User profiles
- Support for Name Services

- Support NetBIOS over TCP/IP
- Support for Microsoft Client Domain and Workgroup logons
- Support for multiple network adapters

Windows NT and 2000 additionally support such features as:

- A Secure File system (NTFS)
- Secure local logon with control of user access permissions
- Secure user profile management

Additionally, network services that can run as a process on NT and 2000 Server are:

- WINS                      Windows Internet Name Service
- DNS                        Domain Name Service
- DHCP                      Dynamic Host Configuration Protocol

Most Windows applications are supported on Windows NT and 2000, including those by Schneider Automation. Properly maintained with up-to-date OS Service Releases and patches, NT Workstation and 2000 Professional have shown that a 32 bit multi-threaded, multi-tasking OS with more robust network support, make them an excellent choice for factory floor PC application hosts.

Networking Windows PC's is based upon NetBIOS. NetBIOS is an OSI Layer 5 (Session), protocol which manages the machine names, sessions and data delivery between them. The NetBIOS protocol bases the communications on 16 (byte) character computer names. Computer names and Group names are registered on the network. Using a name service (described further in this document), can avoid the broadcast mechanisms of NetBIOS to locate those resources registered on the network.

When configuring a PC network adapter protocol stack, be advised when working with TCP/IP based control systems that the protocols and services will generate broadcast traffic on your control network, and it may be best to avoid them. Some of these may be pre-installed, or installed by default depending on your version of Microsoft Windows.

NWLink            Internetwork Packet Exchange/Sequenced Packet Exchange) IPX/SPX  
Developed by Novell and based upon Xerox XNS, it uses its own frame format and broadcasts every 60 seconds. IPX/SPX is a 7 layer routable protocol.

DLC                Data Link Control protocol, developed by IBM is used to connect PC's to IBM SNA Mainframe hosts and is also supported by Printer OEM's. Network adapters in laser printers sometimes use DLC for

communication, but can also use TCP/IP.

**NetBEUI** NetBIOS Extended User Interface protocol – Broadcast based peer-to-peer network protocol developed by IBM. NetBEUI uses a sliding window, (adaptive send/and receive message sizes), and is optimized for small LAN's. NetBEUI will not cross routers. NetBEUI will not be supported in Microsoft Windows XP and beyond.

## **PC Network Adapter Protocol Configuration**

Many companies utilize PC's distributed throughout the plant for HMI's and Programming Units. From time to time, they may wish to connect these PC's to network resources such as file servers for downloading PLC applications, software updates, printing reports, etc. The manner in which this is handled can either have little, if any impact on your control network, or it can be quite harmful to production by causing equipment to slow or stop.

Windows PC's originally used NetBEUI to share resources among computers. However, it is a broadcast based protocol and should be avoided. NetBEUI also cannot cross over a router, being broadcast based. Schneider Automation recommends removing NetBEUI from the protocol stack configuration of any PC on a control network. This protocol will install by default on some versions of Windows when the Client for Microsoft Networks is installed, and therefore must be manually removed during configuration.

The IPX/SPX protocol may also install by default on some versions of Windows if a Client for Novell NetWare is installed. This is a legacy Novell protocol that also generates RIP/SAP broadcast traffic. IPX/SPX is also not supported by any Schneider Automation product and should also be removed. Novell now supports TCP/IP natively for accessing NetWare servers should they be installed on your control network.

Configuring your PC's to be able to communicate with each other in a Windows environment requires resolving the Windows NetBIOS computer name with the IP and MAC address. NetBIOS will also publish a list of available resources such as share points and printers. Where NetBIOS once had to broadcast this information to a computer on your network called the Master Browser, there are alternatives available for NetBIOS over TCP/IP.

In the NetBIOS model, there is one computer assigned or "elected" to serve the role as Master Browser for the Workgroup or Domain. Then, for every 10-15 computers added to the network segment, there is a Backup Browser. When a computer joins the network, it broadcasts its NetBIOS computer name (up to 15 characters), to the Master

Browser. The Master Browser maintains a list of all the computers in the workgroup. Should the Master browser become unavailable, the Backup Browser steps in to service the request. Two potential problems with such browsing systems are:

- A Master or Backup Browser on a slow or busy PC will slow down your ability to obtain a list of network browse list (ie. Network Neighborhood)
- If a PC is unable to locate a Master or Backup Browser; (or configured improperly for the network), it will send an election packet. This will force the election for a Master Browser. This can generate substantial amounts of broadcast traffic, as all eligible PC's are required to respond with their capabilities to participate in the election.

NetBIOS over TCP/IP, (NetBT), can function very effectively with proper name resolution method. These methods, discussed in the next section can nearly eliminate any broadcast traffic from interrupting your control network. NetBIOS datagrams use UDP port 138.

As there is one Master browser and an additional Backup browser for every 10-15 computers in a workgroup or domain, it is beneficial to have all computers belong to the same workgroup. Separate work groups will result in more Master browsers and resulting election packets.

## Locating Network Resources

When a PC requests to connect to another device using a name, instead of an IP address, it must have a method of resolving the Host name to the IP address. Name services provide this functionality. The three methods used to accomplish this are:

- **Hosts file**            A file stored locally on each PC or Remotely located  
C:\WINNT\SYSTEM32\DRIVERS\ETC\HOSTS
- **DNS**                    Domain Name Service  
The Internet standard for resolving host names
- **WINS**                  Windows Internet Name Service  
A/k/a NetBIOS Name server used primarily for Windows  
hosts

### Hosts File

A Hosts file is a text file stored locally on Windows computers. Hosts and is a file called with no extension. LMHOSTS.SAM is a similar file with additional options for preloading the file contents into memory upon startup. These files can be edited with the IP and

Host name of a target computer, one mapping entry per line, and a comment field prefaced by a #. Upon boot-up, the Hosts file is cached in memory to speed access when resolving the name of a remote host. A benefit is that if all of your computers have a hosts file containing the IP address and NetBIOS machine names of the targets they need to reach, there will be no broadcasting for resources unless the target fails to respond. The downside is the task of maintaining and distributing updates the hosts file on each computer when a machine entry is added, removed, and IP or NetBIOS name changed. The Hosts file can also be used for connecting to PLC devices by name when applications, (such as Internet Browsers), support it. The hosts file and lmhosts.sam files have sample entries to guide editing. Note that these files can be centrally located with a pointer in the file itself, or can be downloaded through the use of a logon script batch file. This allows updates to be made centrally and distributed automatically by restarting clients.

### Domain Name Service

DNS is the backbone of the World Wide Web, built on a hierarchical method of distributing host and domain databases worldwide. Entries are made into "root" servers which then propagate the updated files to Internet Service Providers (ISP), name servers. Local DNS services are essential if you must reach non-Windows and Internet hosts. Requests are made by PC's (called Resolvers), to DNS servers on TCP port 53. The architecture of the Internet DNS system is beyond the scope of this paper, but suffice to say that you can have a server running DNS to resolve internal hosts, even if there is no connection to the Internet.

The Microsoft DNS service requires NT Server or 2000 Server for installation. Non Windows servers, (such as Linux), run the DNS service as a process or daemon. Pointer records entered into a local DNS server database will return host name queries by clients with the IP address of the requested target. You can install a DNS server completely separate from your corporate network if you like. You then need only enter the pointer records for each host. Note that the protocol stack configuration in each PC must reflect the hostname of the PC, IP Address and Domain name if applicable. The benefit to DNS is that it is universal to all platforms. The downside is that DNS is also static. If there are changes or visitors such as integrators, they will be able to reach network resources, but other PC's may not be able to reach them.

### Windows Internet Name Service

WINS is Microsoft's implementation of Name Services for Windows NetBIOS machines on TCP/IP Networks. The WINS database is distributed and dynamic. Therefore, a client PC configured with the IP address of a WINS server in its TCP/IP settings will register its NetBIOS name, Workgroup and Domain with the WINS server as it starts network services upon boot up. The WINS server, (running on NT or 2000 Server), will

maintain this entry for a configurable length of time, periodically checking for the presence of the client computer. WINS will also perform routine maintenance such as scavenging records of those machine records whose IP addresses or NetBIOS names have changed, as well as machines no longer on the network.

WINS is installed and bound to the network adapter in an NT or 2000 Server as a service. Once installed, a management console application will display the dynamic database of computers, with maintenance and replication utilities. The replication feature allows a primary WINS server to replicate its database to a secondary WINS server for fail-over in the event that the primary WINS server is offline. Windows clients support two WINS servers by default.

WINS is essentially a NetBIOS over TCP/IP Datagram Distribution server, NBDD, defined in RFC's 1001/1002, and uses UDP port 137.

There are four Node Type configurations in WINS:

- B Broadcast node - Uses broadcasts to resolve names
- P Peer node – Uses point-to-point unicast query to NBDD server
- M Mixed node – Uses broadcasts first, then directed queries
- H Hybrid node – Uses directed queries first, then broadcasts

Node type options for NetBIOS over TCP/IP node types are defined in RFC 1001/1002. As the computer names must be unique, there is a name claim process. B nodes, broadcast this claim, while P nodes register the claim directly with the NetBIOS Name Server (NBNS). Correspondingly, when trying to locate another machine name, B nodes will broadcast for its IP address while P nodes query the NBNS. B nodes broadcasting for unregistered or unavailable machines can generate excess broadcast activity.

WINS can also be joined with DNS to have requests for unknown hosts forwarded from WINS to DNS for resolution. This is helpful if you have non-Windows hosts on your network that need to reach resources on Windows PC's. Another advantage of WINS is that it can work through routers. The default B-node type, being broadcast based, will only resolve hosts on a local subnet as broadcasts do not route by default. WINS will work across routers and can be centrally located, servicing several subnets. Either static IP entries or DHCP server assigned NBNS Server IP addresses and node types will allow a directed UDP registration to be sent from the client to the server across a router.

When the WINS client PC requests to reach a resource, such as a server or peer, it will, depending on the node type, query the WINS server with a UDP request for the IP address of the desired target before broadcasting. If using a DHCP server for PC's on

your network, choose a node type of H when configuring the WINS component of DHCP for the least broadcast traffic. All requests for H nodes will be directed to the server.

## **Broadcast Hazards**

The percentage of utilization the network can accommodate will vary according to device speed, duplex and the nature of the data transfer requests, whether Ethernet I/O Scanner or MSTR function block. Unicast ModbusTCP traffic is resilient and guarantees delivery, as it is point-to-point. Every node on the network on the other hand, must address broadcast traffic. Therefore a single frame can generate increased utilization on every populated switch port. Repeated broadcasts with short intervals can increase the traffic load on full duplex devices and increase collisions on half-duplex devices. In some cases, broadcast storms, (which can come from a variety of sources), can generate a very substantial amount of traffic that can slow or stop the operation of devices dependent on Ethernet I/O communications.

The following test results indicate the effect on a simulated cell with 10 Momentum M1e processors running I/O Scanner when increasing amounts of broadcast traffic are injected into the network. These tests were conducted in our lab located in North Andover, Massachusetts.

The first test depicts a server and workstation. Each is configured with no Name Service resource and the following protocols: NetBEUI, TCP/IP, & IPX/SPX. The broadcast sequence and activity describes the workstation locating the server and establishing a connection.

Tests conducted in our Lab have reveal that improperly configured PC's can generate substantial broadcast activity. The following tests outline such behavior:

### Lab Simulation

A PC was configured with TCP/IP only for a different NetBIOS workgroup/domain and IP Subnet with a static IP from that subnet. The PC also referenced an unknown WINS server. This would simulate a visitor plugging their PC onto your control network. Packet capture was done during the client PC machine startup and registration on the network.

### Improperly Configured Client Network Adapter Result

In an attempt to register with the WINS server, the PC emitted bursts of WINS Registration and Query subnet UDP broadcasts. The PC would also issue NetBIOS

datagram broadcasts announcing its workgroup, and that it was the master browser for that domain, after attempts to locate the NetBIOS domain controller for that domain.

The broadcast frequency varies from 3 to 7 messages per second, with a total of 167 subnet broadcasts over a 13-second period. The feature that was most harmful though was that some message bursts produced up to 3 of those broadcasts within 1 millisecond. Ultimately, the PC could not of course browse the network resources without a proper configuration. Unless discarded by switch buffers, these broadcasts could cripple operation of data communications where baseline utilization is greater than 30% of available bandwidth.

Additionally, a foreign PC can issue an “election packet” to force the election of a master browser for this workgroup. This can solicit a response from other PC’s on the network further increasing broadcast activity.

### Name Services Test Result

By comparison, a test with appropriately configured name services, (WINS was chosen for this test), reveals substantially reduced subnet UDP broadcast activity, prompt registration and access to workgroup/domain resources. The name services test produced 26 subnet UDP broadcasts over a 750-millisecond period during the network logon process for the client to log begin directed UDP/TCP communications with a domain controller. The logon process being the moment of greatest broadcast activity for the PC, this can be contained and managed due to its infrequency.

### **Technologies to Control Broadcast Traffic**

Improperly configured PC’s can cause large amounts of broadcast traffic to flood your control network. A broadcast message reaches all nodes on the same OSI Layer 2 (MAC layer) sub-network. Depending on the topology of your network, this can involve hundreds of devices. As the destination MAC address of a broadcast is not node specific, and is usually a query for a resource to reply to the broadcast request, all nodes must inspect beyond the destination MAC header to determine how and if it should respond. The most dangerous broadcasts, causing “broadcast storms”, are those in which an improperly configured, device queries repeatedly for a resource not present on the network. Technologies, which can help contain broadcasts, include:

- VLAN's                      Virtual LAN's separate and segment broadcast domains based upon IEEE 802.1Q
- Routers                      As they function at OSI Layer 3 and do not forward broadcasts

- Layer 3 Switch Perform many common router functions routing VLAN's
- Rate Limiting Found on some switches; this caps the amount of port bandwidth that broadcast or flood traffic may use.

Broadcast storms can also be caused by cabling "loops", when a device has more than one path to reach a target. Hubs or switches interconnected by Inter-Repeater Link cables, (crossover cables), can cause such a storm, if both links are forwarding frames. Exceptions to the concept of multiple interconnections or pathways include the use of Trunking, ConneXium Ethernet Rings and the Spanning Tree Protocol.

- Trunking is a method supported by some Ethernet switches which will bond together, in pairs, up to eight 100 Mbs/Full Duplex links for increased bandwidth between switches, and fail-over should individual links fail.
- The ConneXium Ethernet Ring topology is a physical ring, but a logical bus, opened at the Redundancy Manager switch.
- Spanning Tree Protocol, supported on some Ethernet switches, allows for multiple paths but has only one link set to forward traffic at a time, and the other set to blocking. Multicast Bridge messages convey changes in the topology, such as a failure, which convert the blocking port to forwarding should the original forwarding port be unreachable. This concept is similar to joining multiple ConneXium rings with redundant links, though the recovery time for the ConneXium solution is within 0.5 seconds. The Spanning Tree response can be 30 seconds or more depending on the number of switches involved and the settings of the STP timers.

The chief cause of broadcast traffic by PC's is browsing for network resources such as servers and printers using broadcast based protocols. Connecting to PLC devices causes very little broadcast traffic and typically is little more than an ARP Request by the PC followed by an ARP Reply issued by the target PLC to setup and open a TCP connection between the two devices. Covered in this paper are technologies used to reduce the amount and frequency of broadcast traffic that PC's use to locate servers and other resources.

Networks interconnected only by switches or hubs are typically termed "flat" networks. Breaking up networks using routers or layer 3 switches require the use of name services for locating services across routers as the broadcast based protocols will not route. The number of nodes on a control network is directly related to the communications flow and utilization. Control networks with greater than 30% of utilization should consider placing PC's on a separate subnet or VLAN with routed access to controllers to prevent disruption of the control network communications.

## Containing Broadcasts

Broadcast traffic exists, by default, on OSI Layer 2. Traffic can be contained or managed using Virtual LAN's (VLANS), Layer 3 switches or Routers.

When broadcast traffic is sent onto a network, it propagates to all devices on the same OSI Layer 2 subnet. Broadcast traffic, by default (per RFC 2644), will not cross a Layer 3 device such as a router. Using subnet sizes appropriate to your application can enhance performance by keeping local traffic local, and by preventing broadcast interference on other subnets.

VLAN's can also be used to separate broadcast domains at Layer 2, but must be connected at Layer 3, (through a Router or Layer 3 Switch), to communicate with other devices that are on different VLAN's. VLAN's can also be extended across interconnected switches using features of the IEEE 802.1pQ. This way, automation devices spanning multiple switches can belong to a broadcast domain separate from other devices.

The most often used device to partition broadcast domains is the use of Routers. These devices terminate broadcast domains because broadcasts exist at OSI Layer 2 and routers operate at OSI Layer 3 and above. Figure 1 on page 15 reveals how switches can be connected in different arrangements (ie. Bus, ring, star), but still share a broadcast domain up to the router. This is just one method of separating broadcast domains and subnets by using single Ethernet jacks or "drops" in cell cabinets. This is dependent on the proximity, (100 meters), to an Intermediate Distribution Frame (IDF), to locate the Layer 3 switch.

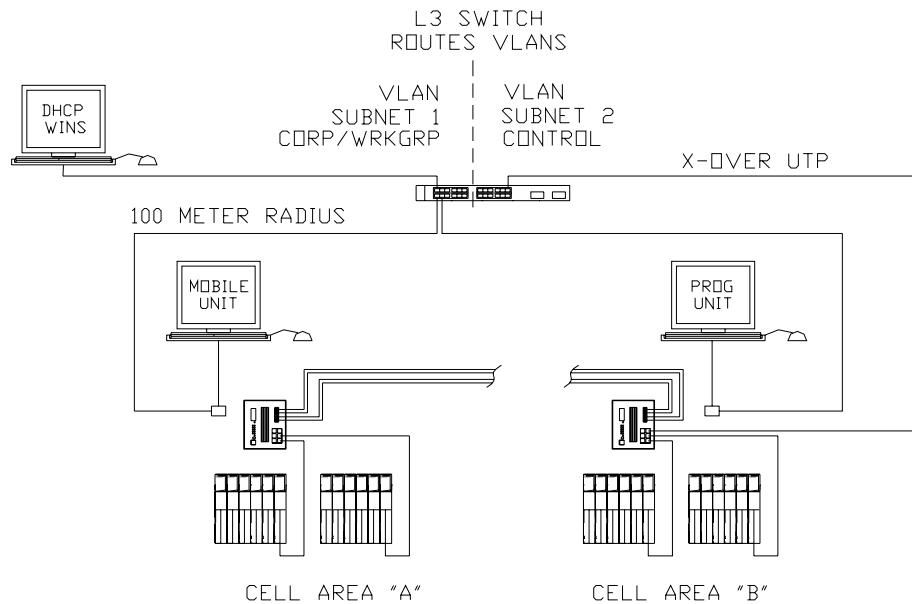


Figure 1

### Using Multiple Network Adapters in PC's (Multi-Homing)

A practical way of separating the PC/Workgroup function, from control networks is to use a second network adapter. Using this arrangement, the services necessary to attach to project servers or even corporate network resources can be individually configured and bound to each adapter. Control side adapters should have a minimum of services while corporate or workgroup side adapters may have other services such as DHCP and WINS bound to them. Note that IP Forwarding should not be enabled on the adapters.

### Fault Tolerant Network Adapters

Though similar to multi-homing using multiple adapters, fault tolerant adapters do not separate networks but share the same network instead. Some adapter manufacturers feature network adapters that support fault tolerance. This is a useful feature for high availability server applications. These adapters can be bound together as a virtual adapter to form a single logical IP address for both adapters. This means that you can install a second network adapter, and using the utility supplied with the adapter, team them together for Link Aggregation (IEEE 802.3ad combines links in pairs to increase bandwidth), and Load Balancing (adapter monitors traffic and shifts I/O accordingly). Note that your switch may have to support IEEE 802.3ad depending on the teaming mode you select. You may also connect each adapter to a separate switch for fault tolerance should the primary switch fail.

## **Mobile Programming Units**

If a network is subnetted into logical networks and you have a mobile programming unit, such as a laptop, you must use an available IP address local to that subnet. The primary benefit is that the programmer is in proximity to the equipment when monitoring or making changes. However, it may not be preferable to run the DHCP services on the control network. While DHCP may be convenient for the programming unit, PLC data communications have static IP address references. An alternative is to have a switch port in each equipment area on a VLAN uplinked and routed at Layer 3. This allows DHCP services appropriate to each subnet and server resource to be available to the programming unit, and connectivity through the gateway to the PLC's in the area. Refer to the figure below. Additional routes, such as to the corporate network, can be filtered to allow connectivity simultaneously to the control network, plant network and corporate network. This is also illustrated in Figure 1. Mobile clients can have DHCP and corporate services available with filtering, broadcast domain separation and Access Control Lists (ACL), for security.

If there are multiple subnets for cells, configure DHCP Relay to forward a DHCP request from a Mobile Programming Unit to the appropriate DHCP Scope. This will apply the proper DHCP Offer with the appropriate subnet IP address and default gateway to the client. The WINS servers can be centrally located and will properly register the NetBIOS machine name. When the machine moves from one subnet to another, the previous registered entry will be marked for deletion or "tombstoned", and replaced with the current entry.

## **Multicast Traffic**

Related to managing broadcast traffic is multicast traffic. With the advent of Publish / Subscribe technology, Multicast traffic will be introduced to control network. Multicast User Datagram Protocol, (UDP), traffic is best managed with switches that can be configured with Group Multicast Registration Protocol, (GMRP). Without GMRP, multicast traffic appears on all ports in a broadcast domain. GMRP, configured at the switch, allows multicast traffic to be directed to only those ports, which are publishers or subscribers.

GMRP is a subset of IEEE 802.1p, which is a MAC layer QoS feature. This allows switch ports to "join" a multicast group and have multicast messages delivered, while ports not subscribed do not receive multicast messages. Using GRMP 802.1p switches for implementing multicast Publish/Subscribe is far more efficient for maintaining your control network bandwidth. GMRP enabled switches will discard multicast frames if the

member set flag is not enabled for that port. Managing multicast groups over routers is accomplished using Internet Group Multicast Protocol, (IGMP). Administrators should use caution when configuring this feature as it may propagate multicast frames to devices that are not subscribed, reducing the available bandwidth on other subnets.

### **How to Assess your Existing PC's**

- Inspect the protocol stack on your factory PC's, printers and servers
- Check stacks for proper addressing, subnet masking and name service options
- Inspect for unneeded client services on the stacks
- Check for unauthorized PC's on your factory network
- Check for unauthorized links to other networks and switches
- Consolidate the number of workgroups and domains on your control network
- Evaluate your current name services methods
- Disconnect unneeded or temporary file shares to other computers
- Monitor your network with a Protocol Analyzer (Sniffer or Ethereal) for broadcasts
  - Note the UDP ports used, source addresses and frequency

### **Conclusion**

PC's can reliably co-exist with automation devices with planning and proper configuration. Among the recommended features to consider when placing PC's on control networks are:

- Proper configuration of a TCP/IP only stack in the PC network adapter
- Proper deployment of name service resources to locate host IP addresses
- Utilizing reasonably sized subnets separated by routers or Layer 3 switches
- Utilizing VLAN technologies with Layer 3 switches
- Installing multiple network adapters when connecting simultaneously to corporate networks

The key to the Transparent Factory is to be able to provide availability for all devices using widely adopted standards based upon Ethernet and TCP/IP. Integrating PC's carefully as part of that strategy should not be overlooked. Well behaved, and properly managed PC's are a vital component to the Transparent Factory concept. Simply plugging in a PC with a "standard build", may introduce problems on your control network particularly as the number of PC's increase. Take steps to plan PC implementation, the services and access required, and evaluate the level of traffic on each subnet before adding PC's.

Inquiries and assistance is available from Schneider Automation. Contact the Network

Certification Services group at 888-266-8705 during business hours (EST) for more information.