s

Internetworking for Automation

Schneider Electric North America
Network Certification Services

November 25, 2003

b

Schneider Electric, North America
One High Street
North Andover, MA USA
01845
Tel. (1) 800-468-5342
Fax (1) 978-975-9046
http://eclipse.schneiderautomation.com

S

Executive Summery

This is the first in a series of papers covering internetworking technologies to educate the Automation user. As Ethernet proliferates for SCADA and control applications, connectivity between networks and locations will become increasingly important. These papers are designed to give the Automation professional an understanding of internetworking core concepts, methods, and the technology choices available.

The topic of internetworking covers a broad range of choices and permutations. Because of the breadth of the subject, the full report has been divided into 9 sections:

Section I	Summary of Internetworking	Overview of all sections
Section II	WAN Physical and Data Link Circuits	Details of ISP and Telecom Carrier Choices
Section III	Routers	Function, features and subnetting
Section IV	Routing Protocols	Types, features and behavior of routing protocols
Section V	Wireless Systems	Details of how wireless systems work
Section VI	Security	Details of firewalls, intrusion detection, and encryption
Section VII	Testing and Troubleshooting	Troubleshooting of WAN connection Issues
Section VIII	Glossary	Glossary of WAN terms

With the advent of Transparent Factory, Schneider Electric’s road map for Automation open connectivity, more customers are using ModbusTCP with Wide Area Networking (WAN) technologies to securely connect to automation equipment across the factory floor or across the world for maintenance, monitoring and SCADA data collection. Extending your reach across the enterprise can reap great rewards for real time information on factory equipment status, output, order scheduling and systems management.

While some users deploy Ethernet enabled devices on a single OSI layer 2 subnet, many users are connecting devices to back office ERP and MES systems for real-time information that can update order management systems. This can involve connecting across multiple Ethernet routers and a firewall through the factory core network, or extend across the globe through many routers and two or more firewalls. During transit, ModbusTCP packets may undergo many transformations from one packet switching network to the next, and could then subject to permissions, port filtering and encryption/decryption for secure access at the destination. We will explore these packet transitions, latencies, security threats, detection methods and protective techniques.

We will also explore the choices in selecting the WAN technology appropriate to the remote site. Availability of services and service providers can vary from one site to another, depending on geographical network access availability, provider services and local ISP offerings. Making the sensible selections from the available choices can provide increased performance and reliability while reducing capital equipment costs and monthly service provider fees.

Connecting to corporate headquarters business systems over the Internet involves crossing several routers and may have the packet transitioning from one frame format to another. Packets that are part of the same overall message request may also take different paths to reach the same destination. This is the function of the Internet. While packets may be routed from the site to the ISP over a dedicated circuit, they will likely be disassembled, reassembled, error checked and re-clocked several times as they cross from one carrier to another towards the final destination.

ModbusTCP works well as it conforms to the OSI layered architecture, is connection oriented for reliable communications, and is an open standard on TCP port 502. For internetworking Schneider Electric web enabled devices, the following ports must be made available for remote access through a perimeter router and firewall by authorized users:

- TCP Port 502 Open ModbusTCP well know port for querying PLC registers
- TCP Port 80 Used for HTTP Web page communications on embedded PLC servers
- TCP Port 21 Used for FTP communications downloading Java applets from PLC servers

The type of security management to access these devices depends on their location within the network (internally located versus being located on the DMZ), and the specific role of the device. If using programming software or SCADA for data collection, port 502 would be the only port necessary to be accessed. If you are accessing default or custom web pages, access to TCP ports 80 and 21 would additionally be required.

When connecting to a device across the Internet, the preferred method is through a Virtual Private Network (VPN). This authenticates the requestor and prevents unauthorized parties from accessing the device. The VPN will connect either from a remote user to a router or firewall, or connect from one router/firewall to another router/firewall.

Organizations are turning to VPN's as a means of wide area networking. Whereas a company wanting to connect a location in Boston for example, to a location in Detroit would have to have a private leased line or circuit, the company can now connect each site in Boston and Detroit to each local ISP. Then, using VPN technology create a secure, encrypted 'tunnel' between the two sites over the Internet. The effect of this leads to dramatically lower costs.

There are several methods of session management, encryption and authentication devices covered in Section VI "Security". In essence though, the function and intent is the same. A VPN authenticates a remote host and creates a secure, encrypted tunnel between the two points. Even if an intruder were to somehow capture data, it would be unusable because of the high level of encryption and the lack the 'key' to decrypt the data.

VPN technology uses a selectable level of encryption for the tunnel. The greater the encryption level, the greater the security but at the cost of performance. Encryption and decryption can reduce performance to a fraction of the maximum unencrypted performance. When considering a connection for WAN or ISP purposes try to anticipate the level of encryption desired, and number of remote VPN connections, to provide satisfactory performance. Increasing the encryption level typically requires increasing the bandwidth of the WAN circuit for the same net throughput. Additional information on VPN's can be found in Section VI 'Security'.

If you have questions regarding these technologies, or would like assistance with your networking project, contact Schneider Electric Network Certification Services at 800-468-5342, or visit us on the web at http://eclipse.modicon.com

S

Section I Summary of Internetworking

Internet Routing Summary

As you can imagine, the Internet is a mesh of many distributed networks. As packets move throughout the Internet, they transition from one physical and data link format on one system to the format of another. Routers are the core devices that perform this transition from one network system and/or type to another, and also determine the best path to reach the final packet destination. Routers may also perform supplemental duties such as security, authentication, intrusion detection and filtering. In essence though, all routers perform packet forwarding and maintain a table of paths to reach a destination called a ‘Routing Table’.

Communicating the topology of the network and any changes to member routers is performed by a routing protocol. When a router boots up, it will broadcast its presence to any neighboring routers. After initial sequencing, the router will exchange routing tables with other routers. The other routers in turn will note the change in the network and propagate that change to yet other routers. Though there are significant differences between the mechanics of the routing protocols, the premise remains the same: to efficiently forward packets along the best path, and to respond to any changes in the network. A router can also run multiple protocols (multi-protocol routing), with each protocol connecting different network collections or types. This report however, will focus specifically on IP routing.

To understand how packets traverse routers from one network to the next, consider how the Internet itself is structured. Internet Service Providers (ISP) logically provide the delivery of Internet service.

ISP’s in turn are divided into strata as follows:

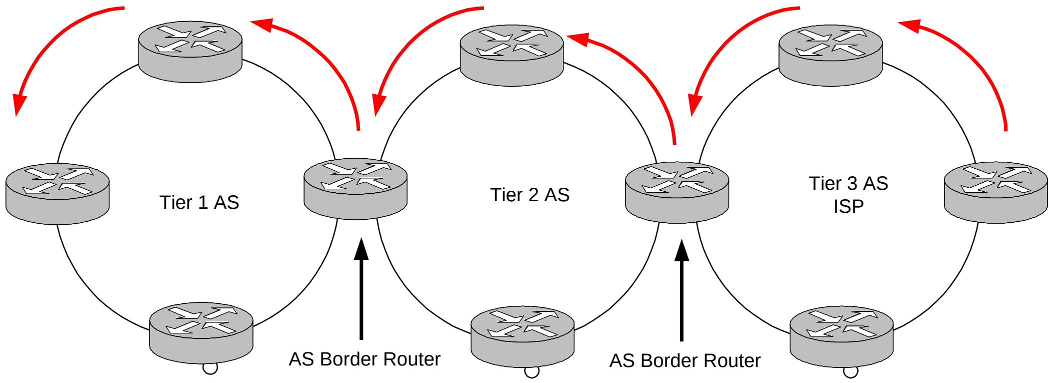
• Tier 1	Network Service Providers	Interconnect with each other
• Tier 2	Regional Service Providers	Interconnect with one or more Tier 1 providers
• Tier 3	Local Service Providers	Interconnect with Tier 2 providers

Tier 1 providers are the primary backbone of the Internet, interconnecting countries and continents. Tier 2 providers, as indicated, are more regional in focus and can service large areas of the US or smaller countries. Tier 3 providers provide service locally to end-users. However, an end user, corporate or individual, can also connect directly to a Tier 1 or Tier 2 provider.

Each ISP, as well as private organizations, maintain a network of routers called an Autonomous System (AS). A 16 bit autonomous system identifier included in the routing updates identify routers in that organization to each other. Member routers send periodic ‘Hello’ packets as a keep-alive mechanism for their status, propagates routing table updates and respond to changes within the autonomous system or from external systems. This way routers can identify and authenticate to each other without paying attention to routing information used by other autonomous systems. Of the two types of routing protocols, internal and external, an interior routing protocol manages updates within an autonomous system, and an exterior routing protocol manages updates between autonomous systems.

S

For example, when your ModbusTCP packet is bound for a destination over the Internet, it is forwarded from your perimeter router to your ISP that may be a tier 3 provider. Your ISP may then forward that packet to a connection point for a tier 2 provider, an so on. As you can see, the Internet is made up of many networks, working together to hand off the packet from one autonomous system to another. A router that interconnects autonomous systems is a ‘Border Router’ as shown in the following figure which illustrates a packet traveling from a source on the right towards a destination on the left. Note that after going through the tier 1 ISP, the process may be reversed as it moves from tier 1 back to tier 2 and so on, depending on the destination. Returning packets reverse the process though they may take a different physical path if a change in the network has converged.



One of the obvious considerations for Automation is latency. Internetworking over the Internet would not be a good choice for control where response time is critical, but would be an excellent choice for monitoring and SCADA. Section VIII ‘ Testing and Troubleshooting WAN Connections’, lists some tools that you can use to gauge the latency for a destination from a source host. Note however, that performance over the Internet can vary as routers become congested or routing paths converge changes.

Routing protocols receive information about network changes either periodically at regular intervals, or immediately after a change has occurred depending on the protocol and its configuration. The time for the network to respond to those changes is called convergence time. Some protocols (covered in detail in Section IV ‘Routing Protocols’) converge slowly after a scheduled update, and others very quickly and efficiently by responding immediately to a change and propagating that change information. When choosing and configuring a routing protocol, factor in the required convergence time in to prevent routing loops and avoid timing out responses. Protocols that converge slowly, or only on a scheduled updates are also more prone to routing loops by advertising bad routes that are no longer reachable.

s

For small internetworks RIP 2 may be an acceptable protocol if simplicity is a higher priority than redundancy. For larger internetworks requiring fast convergence, a better choice may be Enhanced Interior Gateway Routing Protocol (EIGRP) or Open Shortest Path First (OSPF).

Both protocols along with others are detailed in Section IV ‘Routing Protocols’.

When connecting to your ISP, if you only have a single router and connection, it will be the next hop/default route and may not require a routing protocol at all. All traffic bound for and from the Internet will use this gateway. However, if you have more than one interior router, or exterior routers interconnecting remote sites, a routing protocol is essential.

Packet Forwarding

When a device has a packet that is bound for a remote network, the TCP/IP stack looks at the source and destination IP address. It performs a Boolean AND with source address and subnet mask, then the destination address and subnet mask. Then it compares the two results. If the result is the same, the destination is on the local subnet, thus the stack issues an ARP request broadcast to find the MAC address of the intended recipient. If the results of the Boolean AND are different, the destination is on a remote network thus the stack forwards the packet to the default gateway.

To summarize what a router does with a received packet bound for a remote network, consider that it performs the following operations:

- Strips off the 48 bit Source MAC
- Strips off the 48 bit Destination MAC
- Strips off the 32 bit FCS.
- Looks at the Type Of Service (TOS) field in the IP header to see if it should be forwarded on a priority path
- Looks at the destination IP address of the packet
- Consults the routing table for a path to that network
- If there is no corresponding entry for the destination network, it uses the default path 0.0.0.0
- Decrements the Time To Live (TTL) value by 1
- Re-computes the CRC in the IP header
- May optionally encrypt the packet
- Formats the packet for the next hop depending on the physical and data link interface type
- Forwards the packet to the next router or ‘hop’

If the router is connecting Ethernet to Ethernet, it will also:

- Consult its ARP cache for the MAC address of the next hop and write that as the destination MAC
- Write its egress (outbound) MAC address in the source MAC field

S

WAN Interfaces

Depending on the type of egress interface, the packet may be formatted in an entirely different way than Ethernet. As you know, Ethernet operates at OSI Layers 1 and 2, while IP operates at Layer 3 and TCP at Layer 4. Like Ethernet, most WAN interfaces operate at Layers 1 and 2.

The physical layer interface is the connection required to insert the packet onto the wire or media, and the data link layer is the protocol used for transmission.

Some examples of physical layer WAN circuits are

- T-1, T-3, E-1
- DS0, DS3
- ISDN BRI
- ISDN PRI
- xDSL
  Analog POTS
- SONET

Some examples of data link layer formatting protocols are

- ATM
- Frame Relay
- PPP
- HDLC

When choosing Internet service, a selection from each is required. The criteria guiding this choice will be:

• Performance	How much bandwidth is required?
• Availability	What offers are available at the site from Telecom Carriers and ISP's?
• Cost	What is the recurring monthly cost of the service?

Detailed information on the operation of these circuits can be found in Section II, 'WAN Physical and Data Link Circuits'.

Choices can range from simple V.90 dial up modem link over an analog phone line, to 622 Mbs ATM over OC-12 SONET fiber. Not surprisingly, the difference in pricing is as big as the difference in performance.

Depending on the circuit choice, the packet may be fragmented as it passes from Ethernet onto the WAN. Some circuit types like Frame Relay use variable packet lengths (like Ethernet), and others like ATM use fixed packet lengths of 53 bytes called cells. Variable packet lengths tend to have a bit more latency because the router or packet switch has to read in the entire packet and error check it before forwarding (store-and-forward). Cell based packet

S

switches have higher performance and better quality of service because all cells are the same size. Note that some WAN implementations can use Permanent Virtual Circuits (SVC) or Switched Virtual Circuits (SVC). The choice of circuit type can have an effect on cost and performance. Factors to consider in SVC's is call setup that introduce additional latency but can have a lower overall cost. Details on circuit type are covered in Section II 'WAN Physical and Data Link Interfaces'.

As the packet travels from one autonomous system to another, it may encounter different physical and data link protocols. Therefore, it may be formatted, transmitted and reformatted over many hops. Each hop introduces a bit of additional latency. Other factors that can affect performance is if packets are forwarded along separate paths. A change in topology at a remote provider can cause re-convergence that would be transparent to the user, but affect the route to the destination. This is not inherently a problem for ModbusTCP because if packets arrive out of order, the TCP segment sequencing will reassemble them correctly at the destination host. ModbusTCP is 'connection oriented' and a reliable transport mechanism.

To summarize, the choices available to you will depend on the services available at the site to be internetworked. Some choices have distance limitations from a telecom carrier Central Office (CO), or Point-Of-Presence (POP). Contacting telecom carrier providers and ISP's in the area to be served is a good way of narrowing down the available offers. Note that the choices at each end of the WAN may be different as IP layer 3 and above operates independently of the lower layer WAN switching protocol.

From there, consider how many devices or users will be accessing the WAN router, both internally and externally. Some choices like ADSL will have different upstream and downstream speeds. Estimating the amount of steady state and burst traffic is essential for satisfactory performance. Once you have your choices narrowed down, it is largely a matter of cost, both in terms or monthly charges, and capital costs.

Both Telecom Carriers and ISP's can also assist with equipment leasing, installation and monitoring. For critical circuits consider a Service Level Agreement (SLA), with your providers. Such an agreement can help recover costs due to an unscheduled outage, or inferior performance.

Choosing a Router

Routers range from Small Office Home Office (SOHO) routers, to high-end Internet backbone routers. For the most part, aside from cost, the chief differences are performance, scalability, features and redundancy. While the SOHO router can handle a modest routing table with a handful of entries, backbone routers handle 100,000 entry Global routing tables that can be 30 MB or more. Details on understanding routers and comparing router features can be found in Section III 'Routers'.

The performance of the router can be judged by the packet-forwarding rate in packets-per-second (pps), memory and CPU processing power. Note that when referencing router performance specifications, that speed ratings in pps are typically done using 64 byte packets. Clearly you want a router that has a higher packet forwarding rate that the circuit you order. You should also consider the CPU processing power to accommodate all of the interfaces you expect to add, now and in the future, along with your choice of routing protocol. Protocols like OSPF are much more CPU intensive than RIP for example. Routing paths are mathematically calculated using algorithms that take into account the route metrics (cost, delay, reliability, number of hops etc) and paths of each potential route. Other factors that consume CPU time are processes like Access Control Lists (ACL), Firewall feature sets, Intrusion Detection processes and terminating external VPN connections. Plan ahead to consider all of the physical interfaces, logical sub-interfaces, processes and features the router will be expected to handle when selecting a platform.

Extending your Network with Wireless

Though wireless Ethernet is somewhat outside the internetworking realm in the strict sense of IP routing, it is commonly considered for extending networks. Wireless is gaining in popularity as standards evolve for some applications however, companies considering wireless for the factory floor would have to evaluate the sources of RFI, which could cause connections to drop. The effective range of conventional 802.11 derivatives varies from a few hundred feet to thousands of feet, but with machinery, RF interference, rotating machinery, metallic structures, and line-of-sight obstacles, the connection quality could be diminished substantially. Refer to Section V 'Wireless Systems' to see what makes the best choice for your application.

When considering wireless, regardless of the standard chosen, it is wise to perform a site survey to determine the expected signal strength and to discover any sources of obstruction or interference.

Wireless networks are typically bridged between nodes. Routing can take place after the packet has been received by the bridge, but is not a requirement. Wireless works in two modes:

- Point-to-Point — Two wireless bridges or repeaters communicating directly (Ad Hoc Mode)
- Point-to-Multipoint — Multiple remote wireless bridges communicating with a common 'Access Point' (Infrastructure Mode)

When wireless devices boot up, they will either associate with their peer, or look for an access point to associate with. Wireless devices operate at OSI layers 1 (PHY) and 2 (MAC) substituting the role played by the media, and a portion of the role played by the Ethernet Hub or Switch port. Similar to Ethernet, a collision-based system is used for traffic management, but with a collision avoidance mechanism. Similar to CSMA/CD (Carrier Sense Multiple Access/Collision Detection), the wireless CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) method uses a backoff timer to defer sending a packet. However, while CSMA/CD starts the backoff timer immediately after a collision, and then sends hoping that the media is idle, collision avoidance mechanism starts the backoff timer after it has detected idle on the media. In either case, it is a contention-based system that can reduce your effective throughput depending on the number of devices completing for bandwidth and the utilization level of those devices. Note however that while CSMA/CA devices can detect when the wire is busy, in a Point-to-Multipoint environment, other remote units do not know when the others expect to transmit. Thus not knowing what remote peers are doing, only knowing if the access point is available, can have an impact on throughput. Additional detail on Wireless frame formatting can be found in Section V 'Wireless Systems'.

Wireless systems use 'Spread Spectrum' technology to distribute the signal over the range of the available frequency. This allows the signal to be more resilient to interference. The signaling methods used by wireless are:

S

FHSS Frequency Hopping Spread Spectrum. FHSS hops from one narrow band to another within a wide band at different frequencies to prevent contention with other devices by choosing one of 50-75 channels depending on which frequency is used. FHSS also adds a header to the payload for signaling and formatting before transmitting on unlicensed frequencies. FHSS will jump from one channel to another to prevent contention with other devices that may be on the same channel. The receiver ‘hops’ frequencies in synchronization with the transmitter to receive the data. The FCC dictates that a device cannot remain on a single channel longer than 0.4 seconds at 900 MHz and 30 seconds at 2.4 GHz.

DSSS Direct Sequence Spread Spectrum. DSSS uses one of 14 channels. Each channel is 22 MHz wide and is considered the more reliable of the choices. DSSS spreads the signal over the band and takes each bit of data and encodes is with a random binary value. The sequence of bits added are chips (called the ‘chipping’ code). When the signal arrives at the receiver, the receiver reverses the process to decode the original data bit. DSSS is therefore difficult to eavesdrop, resilient to interference by spreading the transmission over a wider band, and allows multiple access.

Microwave Operating in the 18-19 GHz range, this requires an FCC license to operate. Also requires line-of-sight to bridge networks with distance depending on the equipment used.

Actual throughput is dependant on factors such as distance (speed is inversely proportional to range), and encryption. To prevent an intruder from capturing and decoding your data out of the air, Wireless Equivalency Protocol (WEP) keys are employed to encrypt your transmission. However, encrypting, transmitting and decrypting those 40 or 104 bit WEP keys will increase your security as they decrease your throughput. (Note that 40 bi4 WEP keys add an Initialization vector to actually create a 64 bit key, and 104 bit WEP uses likewise create a 128 bit key)

External high-gain antennae can extend your range, however placement is key. Part of the wireless deployment should include a site survey to evaluate locations for antennae. Avoid placing antennae where the signal can be reflected by building and landscaping for line-of-site access to remotes.

Lastly, consider that the overall connection is contention based, usually connecting to Ethernet at 10 Mbs half duplex after crossing the wireless bridge. Since performance degrades as the number of remotes are added, and the bandwidth is a function of range and obstacles, plan fewer, not more remotes per Access Point for best performance.

Note that FHSS and DSSS are not interoperable. When you configure remotes to operate with an Access Point (AP), all remotes must operate using the same method when connecting to single AP.

Standards used for wireless Ethernet are:

- IEEE 802.11 Up to 2 Mbs speed at 2.4 GHz using DSSS or FHSS
- IEEE 802.11a Up to 54 Mbs speed at 5.0 GHz using OFDM – 12 channels
- IEEE 802.11b Up to 11 Mbs at 2.4 GHz using DSSS known as Wi-Fi.
- IEEE 802.11g Up to 54 Mbs at 2.4 GHz

S

The most widely used standard is IEEE 802.11b, however the increased bandwidth and interoperability with 802.11b, 802.11g is gaining acceptance quickly.

Ranges vary with obstacles and environment of course, but with external, roof top antennae, the range can be extended substantially. Range is largely a result of the transmission, antenna placement, antenna type and orientation. Note that low power laptop PCMCIA wireless adapters may have limited range due to battery requirements, heat dissipation and sub-optimal antenna orientation. Though the range is variable for each installation, as a rough guide, you can expect the range for all of the IEEE 802.11 technologies to be up to 200-300 feet indoors and 600-1000 ft outdoors with line-of-sight.

Ethernet Radio based systems can extend the bridge distance for 10 miles or more, with the trade-off being throughput. Instead of 2-54 Mbs throughput at short range, radio modems operating in the unlicensed 900 MHz and 2.4 GHz spectrum can provide throughput of 19,200-512 Kbs. 802.11 devices, while popular, compete with more proprietary devices that also used the unlicensed 900 MHz band spectrum but have ranges beyond 25 miles with external high-gain antennae.

Good security practices when using wireless include:

- Do not broadcast the SSID (Service Set ID) for other intruders to learn
- Use WEP keys for encryption
- Use MAC Filtering (a predefined list of MAC addresses allowed to access the AP)
- Use a RADIUS server to authenticate the user, not just the machine

For additional details on radio, 900 MHz, 2.4 GHz and 5 GHz, and encryption see Section V ‘Wireless Systems’.

Internetworking Security Threats

With the growth of the Internet, complexity of applications and communications, and evolving ingenuity, there continue to be a number of threats which can disrupt not only communications between networks, but communications within a network if it is compromised internally. Often, fast propagating large-scale attacks make the news, though there are smaller attacks on a daily basis that do not. Though there are many types of attacks, there are products, methods and practices that can defend against them.

Details on how to avoid or mitigate the threats below can be found in Section VI ‘Security’.

Often there are 3 parties involved in an attack:

- Attacker — Instigator of the attack
- Victim — One or more hosts which may be used unknowingly to help mount an Attack. Can be a non-secure router or computer that the attacker uses.
- Target — The intended object of the attack

S

A sample of the types of attacks that can occur include:

IP/MAC Spoofing   When a machine with perhaps a locally administered MAC address, can forge the IP or MAC address of another machine. This makes an attack appear to come from another machine than the attacking source.

DOS   Denial of Service. This attack on a host causes enough resources to be consumed, such that the device either crashes, or is rendered unreachable and cannot accept new connections. Often it comes from one or more hosts, or comes from a host that appears to have spoofed another IP address.

DDOS   Distributed DOS attack, where multiple victim machines attack a single machine

Packet Replay   Essentially is the collection of a packet trace and the replaying of the trace to an intended target. It can also involve collecting a single, harmful packet that can be altered and replayed to a victim machine continuously.

Man In the Middle   When a hacker collects a packet that is part of a TCP transmission, then modifies the packet to redirect the traffic to him, and re-inserts the packet back onto the network to your destination. Typically done with unencrypted packets.

Frag Attack   When an IP packet is fragmented because it is larger than the MTU, a flag is set in the IP header indicating that the segment is a fragment. The packets continue until the EOF (End of Fragment) flag is set. In a frag attack, packets are continually sent excepting the EOF flag. This causes the receive buffer on the target machine to fill beyond capacity.

Smurf Attack   An ICMP packet has the source address of the target forged and sent to a broadcast address the network. This causes receiving machines to respond back, to the victim. All of the machines responding back then can produce serious network congestion.

SYN Flood   A type of attack where TCP connections are initiated for the initial step required to establish a socket connection (SYN, SYN ACK, ACK), but does not complete the connection. Instead the attacker attempts to open additional connections with each consuming a socket and memory. This continues until all sockets are in use and the host becomes unreachable.

Land Attack   A forged packet with the victim’s source and destination IP address and TCP port the same is sent to the victim. This causes the victim to try to connect to itself, and can lead to a crash.

S

ICMP Flood
Can be installed as a script on unsecured hosts. The hosts can trigger the script to execute all victims to ping a single target. Not as harmful as other types of attacks, but ICMP can also be used to probe systems.

Tribe Flood
A distributed attack where the attacker exploits a ‘Master’ machine to instruct daemons (processes on slave machines), to execute any of a number of flood attacks. The Master can communicate instructions to attack via ICMP to the daemons.

Trojan
Viruses or worms can typically infiltrate a network attached to another victim application. The most common entry point is through email with the Trojan disguised as an attachment.

Worm
Whereas a virus is designed to replicate itself by attaching to another victim program, a worm is scaled down such that it re-distributes itself across networks.

Virus
A piece of code designed to replicate itself for malicious intent, usually by exploiting an installed victim application.

Ping of Death
The attacker sends an IP packet with a bogus fragment to the target. The fragment starts before the end of the packet, but is extended beyond the allowable packet length (65,535 bytes). This can cause unprotected machines to crash. Though the name is drawn from the ICMP command PING, it is actually and IP packet.

Port Scan
Involves probing a target machine to see which TCP or UDP ports on the machine are ‘listening’ and available.

Ping Sweep
Similar to a port scan, a range of IP addresses is ‘pinged’ to see which may be available for further probing should they reply.

Mitigation and Intrusion Detection

With so many types of attacks out there, there are ways to prevent your organization from becoming a victim. To protect your network, initiate a plan that first of all, minimizes your exposure, detects when an attacker is either probing for information, or is launching an attack and mitigates the impact of such an attack.

Methods of mitigating such attacks include installing a Firewall and Intrusion Detection System (IDS). A firewall will perform a ‘Stateful’ inspection of each incoming packet by examining it all 7 OSI layers. For increased performance, many firewalls perform this between layers 2 and 3. The packet characteristics (source, destination, TCP/UDP port, flags, etc) will be compared against a rules database. If the packet clears the rules database it is forwarded, if not, it is discarded. Firewalls can also log activity in and out of the firewall. The log files can be voluminous if logging activity is detailed, but can also be a very useful tool in detecting suspicious activity.

S

Intrusion detection systems monitor traffic in and out of a router or firewall looking for traffic types or patterns consistent with an attack. The IDS can then alert the administrator, or in some cases, modify the ruleset of the firewall to discard all packets from a host will ill intent.

Encryption is an important method of preventing attacks. When using secure servers and file systems, or encryption techniques like IPSec or SSH, the attacker first has the considerable obstacle of decoding the packet to begin collecting information.

A sample of good security practices include:

- Physical security of network devices, servers, wiring closets, etc.
- Use of RADIUS servers for port based and network based authentication
- Use of ACL's
- Monitoring of Syslog and Firewall logs
- Maintain up-to-date patches and fixes
- Use of Secure Shell (SSH) for CLI administration of network devices
- Drafting of a Network Access Policy
- Periodically Scan for unknown wireless AP's
- Shut down unused interfaces
- Terminate unused services
- Store configuration files on a secure server with detailed annotations. This can help pinpoint vulnerabilities and expedite recovery in the event of an attack.
- Document your network thoroughly and keep it up to date
- Do not forward SNMP through the router and use an SNMP ACL. Remember to change the community strings from the default value an disallow write access unless necessary
- Disable TCP and UDP small services (echo, discard, chargen)
- Disable HTTP access to the router
- Disable unused interfaces
- Disable IP directed broadcast (Smurf Attacks)
- Disable Mask replies
- Disable any ad-hoc routing by Proxy ARP
- Logout CLI access after a time of inactivity
- Log ACL messages to the Syslog server for the full range TCP and UDP 1 – 65535 with timestamp
- Block or drop any inbound packet with a bogus, non routable address (10, 127. 172, 169, 192.168)
- Block packets with the same incoming and outgoing addresses (Land attack)
- For up-to-date advisories on current Internet threats, visit the Carnegie Mellon CERT Coordination Center at http://www.cert.org

Demilitarized Zone

For certain applications that require remote or public access, a Demilitarized Zone (DMZ), allows the devices or servers to be placed outside of the internal or ‘Trusted’ network. The Internet is considered an ‘Untrusted’ entity but access by public or untrusted hosts may be best left placed on the outside to further protect you internal hosts.

The DMZ serves as a buffer zone that allows public access without exposing the interior network. Typically, packet filtering is done from the untrusted network to the DMZ, with another layer of packet inspection from the DMZ to the internal, trusted network. Servers placed in the DMZ include web servers, FTP servers and SMTP gateways. Details on how establish and use a DMZ can be found in Section VI ‘Security’.

Conclusion

While there are some risks in internetworking, it can be agreed that the benefit can far outweigh the risk. Using good security practices and carefully monitoring your network can greatly reduce the risk of compromise. Collecting information from a web enabled automation device, across the Internet, can provide very valuable real-time data to an organization. Sample configurations and illustrated examples in Section VII ‘Example Configurations’, can help you to identify which technology choices may be most appropriate for your organization.

This series intends to bring a greater understanding to the technologies involved so that the Automation user can make an informed decision and plan intelligently.

For additional information, or assistance with your network project, please call Schneider Electric Network Services at 800-468-5342, or visit us on the web at http://eclipse.modicon.com

Copyrights and Trademarks

Transparent Ready	is a registered trademark of Schneider Electric
Transparent Factory	is a registered trademark of Schneider Electric
ModbusTCP	is a registered trademark of Schneider Electric
CERT	is a registered trademark the Software Engineering Institute at Carnegie Mellon University